TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Foreign Affairs Committee
Subcommittee on Europe

Europe in the Crosshairs: China's Hybrid Warfare Against U.S. Interests

CRAIG SINGLETON

Senior Director and Senior Fellow, China Program
Foundation for Defense of Democracies

Washington, DC
December 16, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Section I. Introduction and Executive Summary

Chairman Self, Ranking Member Keating, and distinguished members of this subcommittee, thank you for the opportunity to testify on China's hybrid warfare activities in Europe.

At its core, China's strategy centers around a campaign to influence European decisions before a crisis, so that when a crisis comes Beijing faces a more divided, distracted, and dependent continent. To achieve this objective, Beijing invests in peacetime penetration and pre-crisis coercion, aiming to transform seemingly commercial or cultural tools into pressure points.

Overall, Beijing treats Europe not as a secondary theater but as a central arena in its long-term competition with the United States. Europe remains a critical source of specialized technologies and manufacturing equipment, capital, and diplomatic legitimacy for Beijing's global ambitions. If Beijing can blunt or break transatlantic resolve, it improves its chances of prevailing in future fights over Taiwan, global standards, or sanctions, because any U.S.-led response will be slower, narrower, and easier for China to circumvent.

China wages this competition in Europe primarily through hybrid means. Chinese leaders see no bright line between war and peace, or between domestic security and foreign policy. Cyber intrusions, data collection, Confucius Institutes (CIs), problematic university partnerships, supply-chain consolidation, and quiet economic threats all sit inside China's concept of comprehensive national security. The aim is to shape Europe's information space, economic structure, and strategic imagination long before open confrontation.

Europe's response has improved but remains uneven. Several European governments have taken important steps on 5G, enhanced investment screening, and developing anti-coercion instruments. Yet significant vulnerabilities persist in ports, telecom networks, green transition supply chains, and unregulated research ecosystems. In key sectors, Europe still depends on Chinese technology, capital, and raw industrial inputs in ways that Beijing can weaponize in a future crisis.

To understand today's hybrid threats, I find it helpful to think about Beijing's approach in three phases. The first phase is penetration: gaining access to European digital networks, political debates, and knowledge institutions. The second phase is pre-positioning, in which Beijing converts presence into structural leverage by quietly creating chokepoints where commerce today can become coercion tomorrow. The third phase is pressure, where once these dependencies exist, Beijing can threaten to restrict market access, slow exports, withhold critical components, or unleash cyber and information pressure to punish European governments for stepping out of line.

Importantly, China's hybrid campaign in Europe is not a mirror image of Russia's aggression. Moscow relies on overt military aggression and crude disinformation. Beijing prefers more patient penetration, subtler influence, and pressure often camouflaged in soft-power packaging. However, the two strategies often complement one another. Russian kinetic and information attacks drain European unity, while Chinese economic and technological leverage makes it

harder for some governments to absorb the costs of a long struggle. Together they seek to corrode confidence, fracture alliances, and normalize a narrative of Western decline.

For the United States, the stakes are straightforward. A Europe that is more dependent on China, more vulnerable to coercion, and more skeptical of U.S. intentions will be a weaker partner in any contest with Beijing. Conversely, a Europe that is more resilient, more diversified, and more aware of China's hybrid playbook will be a powerful force multiplier for U.S. strategy. Put simply, transatlantic strength is not just about troops and tanks; it is about who controls the ports, platforms, pipelines, and public narratives that shape crisis choices.

In my testimony today, I will address three questions. First, how do Chinese leaders conceptualize hybrid warfare in Europe, and what does that reveal about their long-term objectives? Second, what are the main domains in which Beijing is building leverage in Europe, from cyber and information spaces to critical infrastructure, supply chains, and research institutions? Third, how effectively are Europe and the United States responding, and what more can Congress do to reduce vulnerabilities and raise the costs of Chinese coercion?

I will conclude my testimony with concrete recommendations for the committee's consideration. They focus on strengthening U.S. tools at home, supporting Europe in de-risking critical dependencies, building a transatlantic hybrid defense architecture that treats Chinese activities with the same seriousness as Russian ones, and raising the costs for Beijing's continued support to Russia's war and coercive activities in Europe.

Section II. How Beijing Thinks About Hybrid Warfare in Europe

Chinese leaders do not use the phrase "hybrid warfare" the way Western analysts do. They frame these activities under Xi Jinping's comprehensive national security concept, which treats security as borderless and continuous and requiring of every element of China's composite national strength.[1] In this worldview, there is no distinction between war and peace, or between domestic control and foreign influence. Activities that Europeans might view as normal diplomacy, commerce, or cultural outreach sit inside a larger contest over whose standards, supply chains, and stories will define the future. In this framework, Europe is not a distant theater. It is a key arena where Beijing can weaken American power indirectly by reshaping European choices on China, Russia, technology, and global rules.

Under this doctrine, the real work of conflict happens long before any crisis boils over. Chinese actors seek early access to European networks, data, debates, and decision-makers. They do not need to flip a single switch in a crisis for this strategy to matter. The accumulation of seemingly small advantages over time — an overlooked research partnership here, a port investment there, a Confucius Institute contract on a key campus — creates a landscape in which Beijing enjoys more leverage and Europe faces more latent risk.

[1] Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before the House Committee on Homeland Security*, March 5, 2025. (https://www.fdd.org/analysis/2025/03/05/countering-threats-posed-by-the-chinese-communist-party-to-u-s-national-security)

Beijing's political warfare tradition reinforces this mindset. Chinese strategists emphasize winning what they call the "three warfares" of public opinion, psychological pressure, and legal positioning long before any armed conflict.[2] In practice, that means shaping how European elites and publics perceive China's rise, how they define escalation, and how they evaluate U.S. policy. If Beijing can normalize the idea that China is an essential economic partner, a responsible stakeholder, and a distant security actor with little direct bearing on Europe's safety, it narrows the range of responses European governments will consider in a crisis.

Europe holds a special place in China's thinking for three reasons.

First, Europe is a decisive source of specialized semiconductor manufacturing technology, capital, and standards setting. European firms and regulators help determine global rules in fields ranging from privacy and competition to so-called green technologies and industrial policy. If Beijing can influence those rules or bind European companies into Chinese-led ecosystems, it gains enduring structural advantages.

Second, Europe is the core of the U.S. alliance network beyond Asia. When Washington coordinates sanctions, export controls, or military posture, European alignment often determines whether those measures bite or merely signal. A Europe that doubts U.S. reliability, fears economic retaliation from China, or views Taiwan and technology controls as primarily American preoccupations is less likely to join serious measures against Beijing.

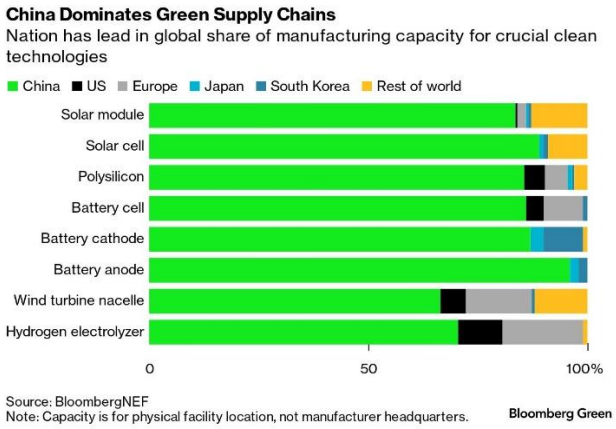
Third, Europe is a primary target for narratives that depict the West as divided, declining, and drained of resources. Russian information operations lean heavily on these themes.[3] Chinese outlets and officials increasingly echo, refine, and legitimize similar messages, but with a more polished economic and diplomatic veneer. Together, they aim to persuade European publics that the cost of confronting authoritarian powers is too high and U.S. leadership is too erratic.

Beijing's hybrid warfare logic in Europe follows a consistent sequence. The first task is penetration. Chinese state and party organs push for access to European data, infrastructure, and influence channels. They do so through cyber intrusions, talent programs, joint ventures, political friendships, and cultural platforms.[4] Confucius Institutes and related entities seek not only to teach language but to embed curated depictions of China on European campuses. Research partnerships with Chinese institutions of concern provide a path into sensitive labs and high-

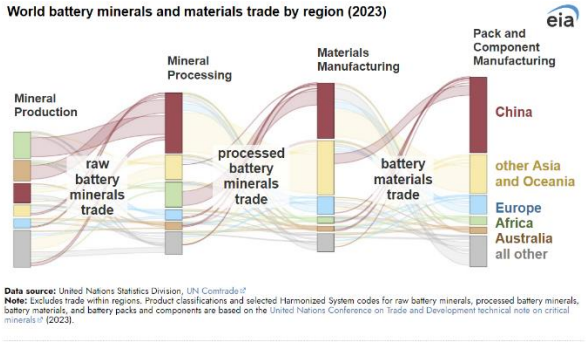
[2] Thomas Joscelyn, "Warfare Is More Than Just Bullets," *The Dispatch*, November 12, 2021. (https://www.fdd.org/analysis/2021/11/12/warfare-is-more-than-just-bullets); Samantha Ravich and Mark Montgomery, "China's Accelerating CEEW Campaign," *Foundation for Defense of Democracies*, October 28, 2022. (https://www.fdd.org/analysis/2022/10/28/chinas-accelerating-ceew-campaign)
[3] Ivana Stradner and John Hardie, "Cognitive Combat: Russia," *Foundation for Defense of Democracies*, June 28, 2024. (https://www.fdd.org/analysis/monographs/2024/06/28/cognitive-combat)
[4] Emily de La Bruyère and Nathan Picarsic, "Made in Germany, Co-opted by China," *Foundation for Defense of Democracies*, October 14, 2020. (https://www.fdd.org/analysis/2020/10/14/made-in-germany-co-opted-by-china); Jack Burnham and Duncan Larazow, "Chinese Electric Buses Trigger Cybersecurity Alarm Across Europe," *Foundation for Defense of Democracies*, November 25, 2025. (https://www.fdd.org/analysis/2025/11/25/chinese-electric-buses-trigger-cybersecurity-alarm-across-europe); Mark Montgomery and Annie Fixler, "NATO's Critical 1.5 Percent," *The Cipher Brief*, June 23, 2025. (https://www.thecipherbrief.com/nato-s-critical-1-5-percent)

value datasets.[5] State-linked media and social media operations amplify content that flatters China, questions U.S. intentions, or magnifies divisions within and between European societies.[6]

The second task is pre-positioning. Once access exists, the priority shifts to turning it into structural leverage. Investments in ports, shipping terminals, and logistics hubs give Chinese firms visibility into European trade flows and, in some cases, influence over key chokepoints. Stakes in telecom networks, cloud providers, and data centers position Chinese equipment and software at the heart of Europe's digital life. Dominant market shares in solar panels, batteries, and other green technologies make Europe's energy transition more dependent on Chinese supply chains. Here, hybrid warfare does not rely on spectacular acts of sabotage. It rests on the quiet conversion of commercial presence into strategic dependence.



Source: Bloomberg[7]



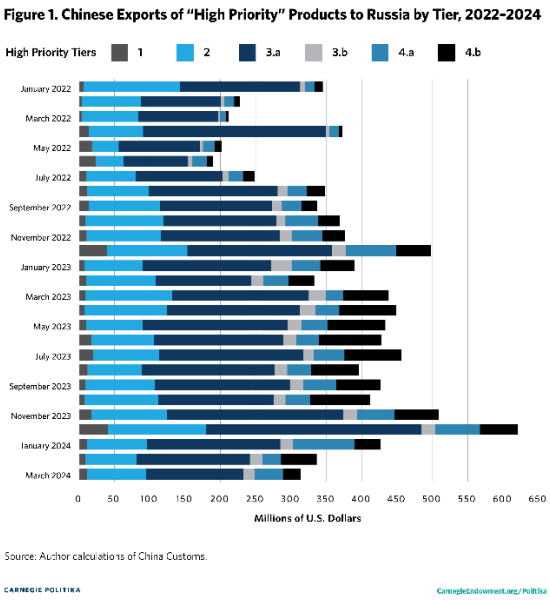
Source: U.S. Energy Information Agency[8]

The third task is pressure. Beijing does not always need to exercise this pressure to benefit from it. The perceived threat that China might restrict exports, cancel contracts, or quietly discourage investments is enough to shape behavior in European capitals. When pressure does become overt, it often arrives in hybrid form: targeted trade restrictions combined with veiled diplomatic warnings, negative media campaigns, and threats to redirect tourists, students, or capital. In parallel, cyber operations can signal that critical infrastructure is vulnerable, while information campaigns cast blame for any economic pain on the United States or on European leaders who, in China's eyes, provoked the situation.

China's support to Russia's war against Ukraine fits squarely within this hybrid logic. Beijing has not committed troops or openly violated its own rhetoric about opposing proxy wars. Instead, it has positioned itself as a diplomatic bystander while supplying dual-use goods, components,

[5] Emily de La Bruyère and Nathan Picarsic, "Made in Germany, Co-opted by China," *Foundation for Defense of Democracies*, October 14, 2020. (https://www.fdd.org/analysis/2020/10/14/made-in-germany-co-opted-by-china)
[6] Viviane Teitelbaum, "Protecting Allied Societies from Disinformation Emanating From the People's Republic of China," *NATO Parliamentary Assembly*, October 11, 2025. (https://www.nato-pa.int/document/2025-chinese-disinformation-report-teitelbaum-011-cdsrcs)
[7] "Xi Heads to Europe Dangling Economic Carrots as Tensions Rise," *Bloomberg*, May 3, 2024. (https://www.bloomberg.com/news/newsletters/2024-05-03/xi-jinping-goes-to-europe-dangling-economic-carrots-next-china)
[8] "China dominates global trade of battery minerals," U.S. Energy Information Agency, May 21, 2025. (https://www.eia.gov/todayinenergy/detail.php?id=65305)

machine tools, and other items that help sustain Russia's war machine.[9] This approach allows China to prolong a conflict that drains European budgets, depletes Western stockpiles, and tests political cohesion, all while claiming neutrality. It is indirect but deliberate pressure on Europe's strategic endurance.



Source: Carnegie Endowment for International Peace[10]

Understanding this conceptual frame matters because it shapes what Beijing considers success, which is not simply preventing additional U.S. troops in Europe or avoiding new sanctions. It is a Europe that self-censors on sensitive issues, hesitates to support U.S. measures, fears the economic cost of pushback, and treats Chinese pressure as an unavoidable fact of life. That is the strategic horizon against which we should judge individual Chinese actions in cyber space, in the information domain, and across Europe's critical industries.

Section III. Risks to Europe's Networks, Politics, and Information Space

Beijing's hybrid campaign primary takes shape in Europe's networks, politics, and information spaces. In practical terms, that means burrowing into European cyber infrastructure, building political and institutional footholds, and shaping how European publics understand NATO, the United States, and China itself. These activities are not separate tracks; they are mutually reinforcing lines of effort that set the stage for later leverage and coercion.

A. Cyber campaigns and pre-positioning in European networks

[9] Jack Burnham and John Hardie, "China-Russia Defense Cooperation Showcases Rising Axis of Aggressors," *Foundation for Defense of Democracies*, June 10, 2025. (https://www.fdd.org/analysis/policy_briefs/2025/06/10/china-russia-defense-cooperation-showcases-rising-axis-of-aggressors)

[10] Nathaniel Sher, "Behind the Scenes: China's Increasing Role in Russia's Defense Industry," *Carnegie Politika*, May 6, 2024. (https://carnegieendowment.org/russia-eurasia/politika/2024/05/behind-the-scenes-chinas-increasing-role-in-russias-defense-industry)

Chinese cyber operations against Europe focus primarily on espionage and pre-positioning, rather than the disruptive sabotage more often associated with Russian actors. The aim is to map European systems, harvest sensitive information, and quietly position Chinese services inside networks that matter to NATO and EU decision-making.

Recent cases are instructive. In May 2025, the Czech Republic publicly accused China of conducting a "malicious cyber campaign" against its Foreign Ministry. Prague attributed the intrusions to APT31, a group linked to China's Ministry of State Security, and described the attacks as sustained efforts since 2022 against a ministry network used for diplomatic communications.[11] NATO and the European Union issued statements of solidarity and warned that such activity undermines European security.

Czech President Petr Pavel subsequently warned that China now poses a cyber threat to Europe on par with Russia, noting that Chinese operations have become more professional and that responsibilities have shifted toward state security organs.[12] He drew a distinction between Russia's focus on sabotage and China's emphasis on intelligence collection and long-term positioning, but stressed that the strategic effect on European security is comparable.

These and other incidents are part of a broader pattern. U.S. and UK authorities have charged Chinese state-backed hackers for sweeping espionage campaigns that also touched European officials, companies, and critical infrastructure.[13] Chinese operators target foreign ministries, parliaments, political parties, defense contractors, and telecom networks. They seek access to policy deliberations, alliance consultations, and technical data on energy, transport, and industrial systems.

For NATO and U.S. interests, this matters in three ways. First, sustained access to European ministries and infrastructures gives Beijing insight into allied planning and red lines, including on Russia policy and Indo-Pacific issues. Second, embedded footholds in ports, energy grids, or telecom networks creates options for calibrated disruption in a crisis, even if China has not yet exercised them.[14] Third, Chinese and Russian cyber actors increasingly study each other's methods and, in some cases, complement one another's efforts. Europe faces a blended environment in which Russian actors may focus on kinetic-adjacent disruption while Chinese actors quietly harvest the intelligence and access needed for long-term strategic leverage.

B. Political influence tools: parties, partnerships, and platforms

Alongside cyber penetration and pre-positioning, Beijing invests heavily in political and institutional influence. The Chinese Communist Party's (CCP) United Front system targets political parties, business elites, diaspora communities, and opinion-shapers across Europe. Its

[11] Karel Janicek, "Czech Republic accuses China of 'malicious cyber campaign' against its foreign ministry," *The Associated Press*, May 28, 2025. (https://apnews.com/article/czech-republic-china-cyber-attacks-nato-163e7e752624b9e243a31d533f7fcaa2)
[12] Raphael Minder, "Chinese cyber threat to Europe on par with Russia's, warns Czech president," *Financial Times* (UK), June 19, 2025. (https://www.ft.com/content/63720831-8805-497d-8145-1713e450a55a)
[13] Department of Justice, Press Release, "Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians," March 25, 2024. (https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived)
[14] Mark Montgomery and Annie Fixler, "NATO's Critical 1.5 Percent," *The Cipher Brief*, June 23, 2025. (https://www.thecipherbrief.com/nato-s-critical-1-5-percent)

task is to cultivate voices that will argue for accommodating Beijing, resisting strategic decoupling, and keeping China policy at arm's length from broader NATO debates.[15]

United Front and party-to-party work in Europe includes parliamentary friendship groups, sub-national "sister city" and province-to-province ties, and engagement with local business associations.[16] These channels provide Beijing with levers to reward friendly actors and sideline critics. In some cases, Chinese interlocutors have used access and economic promises to encourage European politicians to oppose sanctions, downplay human rights concerns, or advocate ostensibly more balanced positions on NATO and U.S. policy.

Within this broader ecosystem, Confucius Institutes (CIs) and rebranded cultural centers serve a specific function: shaping norms and narratives on campus. Europe today reportedly hosts well over one hundred CIs, with significant concentrations in the United Kingdom, Germany and France, even as some countries such as Sweden, Poland, and the Czech Republic have begun to close or reassess them.[17] These centers promote language and culture, but they also project a carefully managed image of China. Topics Beijing deems sensitive, such as the Tiananmen Square massacre, often receive limited treatment or are kept outside CI programming altogether.

In other democracies, investigations have documented CI officials objecting to Dalai Lama visits, ordering references to Taiwanese sponsors stripped from conference materials, and contributing to self-censorship on issues like Tibet, Taiwan, and Tiananmen — concerns that led bodies such as the American Association of University Professors (AAUP) and Human Rights Watch to warn that CIs can undermine academic freedom.[18]

For Beijing, these facets are features, not bugs. CIs are norm-shaping nodes. They influence which materials students see, which guest speakers are welcome, and which conversations feel too controversial. Over time, this soft pressure can produce a campus climate where criticism of the CCP is seen as impolite, politicized, or risky for institutional partnerships. It is a low-cost way to dull scrutiny of China's behavior, including its support for Russia's war machine, its human rights record, and its coercive tactics toward European states.

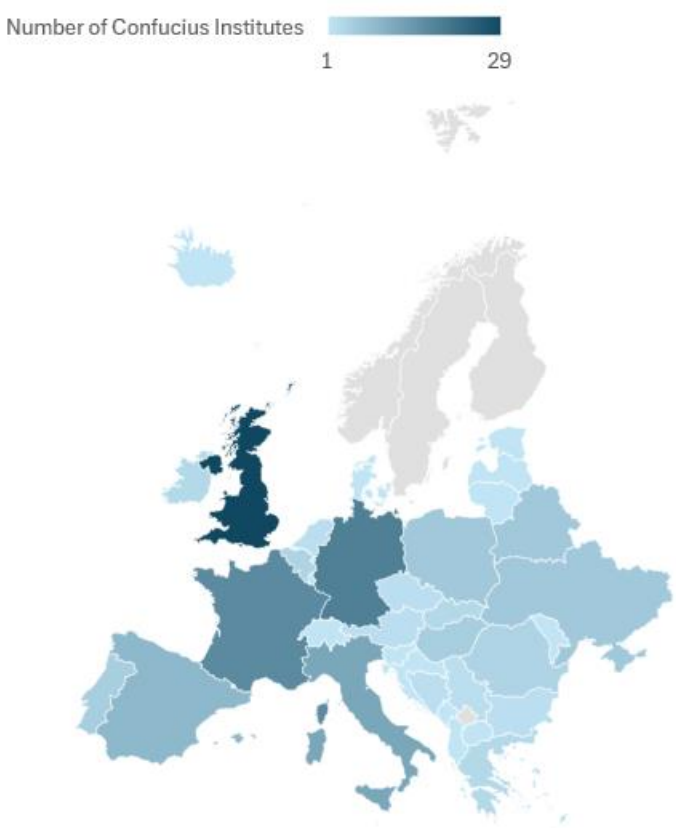
---

[15] Toshi Yoshihara and Jack Bianchi, "Uncovering China's Influence in Europe: How Friendship Groups Coopt European Elites," *Center for Strategic and Budgetary Assessments*, July 1, 2020. (https://csbaonline.org/uploads/documents/CSBA8225_%28Uncovering_Chinas_Influence_Report%29_FINAL.pdf)

[16] Ryan Fedasiuk, "How China's united front system works overseas," *The Strategist*, April 13, 2022. (https://www.aspistrategist.org.au/how-chinas-united-front-system-works-overseas)

[17] "Expansion of the Confucius Institute in Serbia despite controversies in Europe and the USA," *The GeoPost*, November 15, 2024. (https://thegeopost.com/en/news/expansion-of-the-confucius-institute-in-serbia-despite-controversies-in-europe-and-the-usa); Dominika Urhová, "The Demise of Confucius Institutes: Retreating or Rebranding?" *China Observers*, September 5, 2024. (https://chinaobservers.eu/the-demise-of-confucius-institutes-retreating-or-rebranding)

[18] Rachelle Peterson, "Outsourced to China: Confucius Institutes and Soft Power in American Higher Education," *The National Association of Scholars*, April 2017. (https://files.eric.ed.gov/fulltext/ED580866.pdf); "Report: The Deletion of Pages from EACS Conference materials in Braga," *European Association for China Studies*, July 30, 2014. (https://chinesestudies.eu/2014/report-the-deletion-of-pages-from-eacs-conference-materials-in-braga-july-2014); Elizabeth Redden, "Censorship at China Studies Meeting," *Inside Higher Education*, August 5, 2014. (https://www.insidehighered.com/news/2014/08/06/accounts-confucius-institute-ordered-censorship-chinese-studies-conference); "On Partnerships with Foreign Governments: The Case of Confucius Institutes," *American Association of University Professors*, June 2014. (https://www.aaup.org/reports-publications/aaup-policies-reports/policy-statements/partnerships-foreign-governments-case); "Resisting Chinese Government Efforts to Undermine Academic Freedom Abroad: A Code of Conduct for Colleges, Universities, and Academic Institutions Worldwide," *Human Rights Watch*, March 21, 2019. (https://www.hrw.org/sites/default/files/supporting_resources/190321_china_academic_freedom_coc_0.pdf)



Source: Dig Mandarin; NATO Strategic Communications Center of Excellence[19]

Research partnerships provide a parallel track. Under Horizon Europe and other frameworks, Chinese and European institutions have built extensive cooperation in advanced materials, artificial intelligence (AI), quantum, biotech, and other dual-use fields. Many of these projects are legitimate and beneficial. Yet some involve Chinese universities and labs that sit at the core of Beijing's military-civil fusion system. In response, the European Commission has begun moving toward excluding Chinese institutions from large parts of Horizon Europe, particularly in clusters covering health, civil security, and digital, industry, and space, and is considering outright bans on entities under China's Ministry of Industry and Information Technology.[20]

From a hybrid-warfare perspective, these political, educational, and research tools serve a common purpose. They embed Chinese influence inside the institutions that generate Europe's ideas, technologies, and policies. They cultivate elites who see China as a necessary partner and view firm alignment with U.S. China policy as needlessly risky. They also give Beijing early

[19] "Confucius Institutes Around the World – 2024," Dig Mandarin, October 12, 2024. (https://www.digmandarin.com/confucius-institutes-around-the-world.html); "Confucius Institutes," NATO Strategic Communications Center of Excellence, June 16, 2019. (https://stratcomcoe.org/publications/hybrid-threats-confucius-institutes/88). Note: the map reflects 2024 data and may have changed.
[20] Markus Weisskopf, "Horizon Europe: The areas from which China is to be excluded," *Table Briefings*, November 13, 2025, (https://table.media/research/news-en/horizon-europe-the-areas-from-which-china-is-to-be-excluded); David Matthews, "EU plans to ban Chinese universities from half of Horizon Europe," *Science Business*, November 11, 2025. (https://sciencebusiness.net/news/r-d-funding/horizon-europe/eu-plans-ban-chinese-universities-half-horizon-europe); Gabriele Manca, "The EU realpolitik turn in research cooperation with China," *Central European Institute of Asian Studies*, November 26, 2025. (https://ceias.eu/the-eu-realpolitik-turn-in-research-cooperation-with-china)

warning and informal veto points over moves that might tighten export controls, restrict investment, or elevate China alongside Russia in NATO threat assessments.

C. Disinformation and narrative shaping: targeting NATO cohesion and transatlantic trust

The third pillar of China's hybrid strategy in Europe is information manipulation and narrative warfare. Here, Beijing's efforts often intersect with, and sometimes amplify, Russian disinformation. Both regimes target NATO and EU cohesion, attempt to erode public trust in democratic institutions, and seek to redefine the terms of debate around Ukraine, Gaza, sanctions, and the U.S. role in Europe.

Recent analyses by European institutions and independent researchers have documented growing Sino-Russian convergence in foreign information manipulation. Russian campaigns tend to lead with aggressive narratives and falsified content, while Chinese outlets, diplomats, and proxies echo and legitimize compatible themes, often in more measured language. The shared goal is to portray the West as divided and hypocritical, and to blame NATO and the United States for instability.[21]

Source: Voice of America[22]

On Ukraine, Chinese messaging in Europe frequently emphasizes calls for peace and dialogue while casting sanctions and military support as escalatory and economically self-defeating.[23] Chinese state-linked media and content-sharing agreements have, in other regions, helped disseminate Russian narratives that frame the war as a proxy conflict provoked by NATO

[21] Tamás Matura, "Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies," *Center for European Policy Analysis*, June 30, 2025. (https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference); "3rd EEAS Report on Foreign Information Manipulation and Interference Threats," *European Union External Action Service*, March 19, 2025. (https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf)

[22] Liam Scott, "China, Russia Target Audiences Online With Deep Fakes, Replica Front Pages," *Voice of America*, March 23, 2023. (https://www.voanews.com/a/china-russia-target-audiences-online-with-deep-fakes-replica-front-pages-/7018918.html). Note: the study sampled 100 cases of information manipulation related to the conflict.

[23] Grzegorz Stec and Eva Seiwert, "China on peace in Ukraine: What to expect based on the track record of Beijing's narratives," *EUvsDiSiNFO* (Belgium), March 03, 2025. (https://euvsdisinfo.eu/china-on-peace-in-ukraine-what-to-expect-based-on-the-track-record-of-beijings-narratives); "China's Position on Russia's Invasion of Ukraine," *U.S.-China Economic and Security Review Commission*, August 31, 2025. (https://www.uscc.gov/research/chinas-position-russias-invasion-ukraine)

expansion; similar patterns of narrative alignment are visible in parts of the European information space.[24]

On Gaza and Middle East crises, Chinese and Russian narratives often stress Western double standards and human rights hypocrisy.[25] In European debates, these narratives can divert attention from Chinese and Russian actions, heighten polarization inside EU and NATO countries, and erode support for a sustained focus on Ukraine and Indo-Pacific security.

Chinese influence operations also target the transatlantic relationship itself. Messaging frames U.S. export controls and investment restrictions as protectionist efforts that harm European firms, while presenting China as a champion of globalization and an essential market for European industry. When Washington urges Europe to reduce dependencies on Chinese technology or critical minerals, Chinese narratives suggest that the United States is using security arguments to gain a commercial edge.[26]

European institutions are starting to respond. The EU's External Action Service has issued a series of threat reports on foreign information manipulation, explicitly naming China alongside Russia as a source of coordinated disinformation campaigns.[27] The European Commission is pursuing a so-called "democracy shield" that includes a new Centre for Democratic Resilience to coordinate responses to hybrid threats, including Chinese propaganda and fake news websites that mimic legitimate outlets. These are important steps, but they underscore the scale of the challenge.

For NATO and the United States, the risk is clear. If Chinese and Russian information operations succeed in casting NATO deterrence as warmongering, sanctions as economic self-harm, and U.S. policy as the chief obstacle to peace, then European political appetite for sustained transatlantic cooperation will shrink. Hybrid warfare in the information domain is not about a single viral lie. It is about slowly shifting political trendlines so that, when hard decisions arise, allied governments face a headwind of skepticism at home.

Section III. Strategic Dependencies — Where Europe Is Most Exposed

China's penetration of Europe's cyber networks and information space would matter less if it were not paired with something more tangible: hard leverage over Europe's infrastructure and supply chains. Beijing has spent the last decade converting presence into dependence in sectors

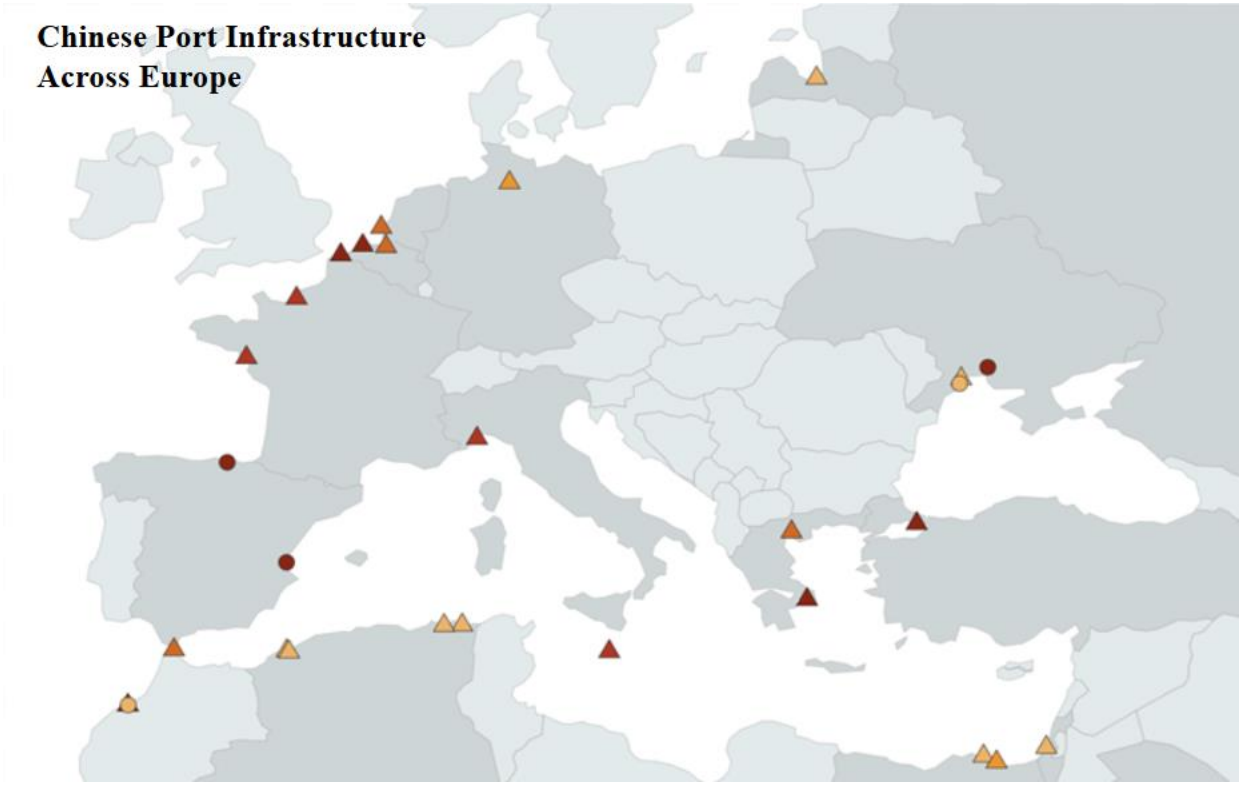
[24] "The Fact-Checked Disinformation Detected in the EU," *European Digital Media Observatory*, accessed December 8, 2025. (https://edmo.eu/thematic-areas/war-in-ukraine/the-fact-checked-disinformation-detected-in-the-eu).
[25] "Capitalising on crisis: Russia, China and Iran use X to exploit Israel-Hamas information chaos," *Institute for Strategic Dialogue*, October 25, 2023. (https://www.isdglobal.org/digital_dispatches/capitalising-on-crisis-russia-china-and-iran-use-x-to-exploit-israel-hamas-information-chaos); Amar Jallo, "China Exploits the 'War on Gaza' in its Power Struggle with Washington," *The Wilson Center*, January 31, 2024. (https://www.wilsoncenter.org/article/china-exploits-war-gaza-its-power-struggle-washington); "US annual human rights circus show exposes its hypocrisy and political bias," *China Daily* (China), August 13, 2025. (https://www.chinadaily.com.cn/a/202508/13/WS689c8beba310b236346f17ed.html); Adriel Kasonta, " China's Gaza ceasefire call reveals the West's hypocrisy," *CGTN* (China), February 17, 2024. (http://eng.chinamil.com.cn/OPINIONS_209196/Opinions_209197/16286915.html).
[26] Jennifer Rankin, "EU plans hub to tackle disinformation threat from Russia and others," *The Guardian* (UK), November 7, 2025. (https://www.theguardian.com/world/2025/nov/07/eu-plans-centre-for-democratic-resilience-to-fight-online-disinformation); Tamás Matura, "Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies," *Center for European Policy Analysis*, June 30, 2025. (https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference).
[27] "3rd EEAS Report on Foreign Information Manipulation and Interference Threats," *European Union External Action Service*, March 19, 2025. (https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf).

that matter for NATO's resilience, from ports and telecom networks to green technologies and critical minerals. These are the points where hybrid warfare moves from the abstract to the acute.

I would highlight four domains where Europe's exposure is most consequential for U.S. and NATO interests: ports and logistics, telecom and digital infrastructure, the green transition, and critical minerals and manufacturing inputs.

A. Ports, logistics, and maritime chokepoints

Chinese firms have acquired stakes in a number of European ports and terminals, especially along key trade corridors linking Europe to Asia and the Mediterranean.[28] In many cases, but not all, these investments are commercially motivated and legally transparent. The strategic concern lies less in day-to-day operations than in the coincidence of ownership, data access, and dual-use potential.



Source: Council on Foreign Relations. Please see footnote for graphic key.[29]

Port stakes, even minority ones, can give Chinese entities:

[28] Grant F. Rhode, "China's Emergence as a Power in the Mediterranean: Port Diplomacy and Active Engagement," *Diplomacy & Statecraft*, May 4, 2021. (https://www.tandfonline.com/doi/full/10.1080/09592296.2021.1913352); Kaki Bali, " In Greece's largest port of Piraeus, China is the boss," *Deutsche Welle* (Germany), October 30, 2022. (https://www.dw.com/en/greece-in-the-port-of-piraeus-china-is-the-boss/a-63581221.)

[29] Zongyuan Zoe Liu, "Tracking China's Control of Overseas Ports," *Council on Foreign Relations*, accessed December 8, 2025. (https://www.cfr.org/tracker/china-overseas-ports). Note: the triangles denote whether the port can handle military traffic; the intensity of the hue corresponds to the share owned by a Chinese firm or the Chinese government (more intense corresponds to a higher ownership stake).

- Visibility into cargo flows**,** including military or dual-use shipments transiting European hubs
- Influence over investment decisions, digitalization projects, and vendor choices for cranes, sensors, and logistics software
- Opportunities to shape how port authorities think about future cooperation with NATO navies, U.S. forces, or defense-related cargo

The risk is not that Beijing will suddenly shut down European ports in peacetime. The more realistic concern is that, in a crisis, Chinese companies and their home government could use regulatory delays, labor disputes, targeted maintenance, or selective denial of services to complicate military logistics or pressure specific allies. Even the perception of such leverage can deter governments from making decisions Beijing dislikes.

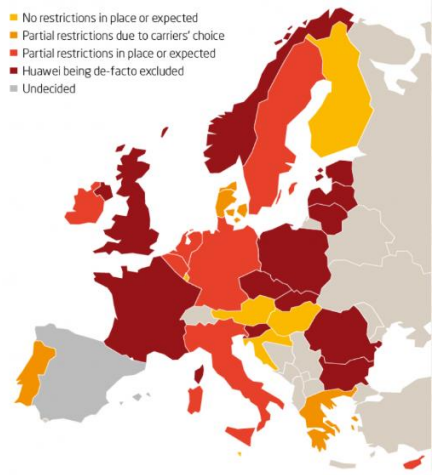
Europe has begun to reassess some of these arrangements. Several governments have tightened foreign-investment screening and, in a few cases, limited or blocked new Chinese stakes in critical ports.[30] But existing ownership structures and long-term leases will remain in place for decades. That creates a lag between recognition of the problem and reduction of the risk.

B. Telecom, cloud, and the digital backbone

Europe's digital backbone remains another area of strategic exposure. Over the past 15 years, Chinese vendors became deeply embedded in European telecom networks, undersea cables, and cloud infrastructure. Many European states have since moved to restrict high-risk suppliers from 5G cores and sensitive segments of their networks, yet large volumes of legacy equipment and contracts remain in place.

[30]Agatha Kratz, Max J. Zenglein, Alexander Brown, Gregor Sebastian and Armand Meyer, "Chinese FDI in Europe: 2023 Update," *Rhodium Group*, June 6, 2024. (https://rhg.com/research/chinese-fdi-in-europe-2023-update); Raphaël Glucksmann, Svenja Hahn, and Pascale Piera, "Revision of the foreign direct investment (FDI) screening regulation," *Commission 24-29*, January 24, 2024. (https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-revision-of-the-fdi-screening-regulation); Francesca Ghiretti, Jacob Gunter, Gregor Sebastian, Meryem Gökten, Olga Pindyuk, Zuzana Zavarská, and Plamen Tonchev, "Chinese Investments in European Maritime Infrastructure," *Policy Department for Structural and Cohesion Policies*, September 2023. (https://www.europarl.europa.eu/RegData/etudes/STUD/2023/747278/IPOL_STU(2023)747278_EN.pdf); Frank Röhling, Lara Steinbach, and Uwe Salaschek, "German approval of Chinese stake in Hamburg container terminal – a veto in disguise?" *FreshFields*, November 3, 2022. (https://riskandcompliance.freshfields.com/post/102i0m9/german-approval-of-chinese-stake-in-hamburg-container-terminal-a-veto-in-disgui); Linton Nightingale, "Strategic stakes: EU sharpens focus on Chinese port ownership," *Lloyd's List*, February 20, 2025. (https://www.lloydslist.com/LL1152631/Strategic-stakes-EU-sharpens-focus-on-Chinese-port-ownership)

Map of Restrictions on Huawei Technology



Source: Mercator Institute for China Studies[31]

From a hybrid-warfare perspective, the concern is twofold:

- First, where Chinese equipment and software remain in key parts of national networks, they may provide persistent access and intelligence-gathering opportunities for Chinese state actors. Even if there is no "kill switch," deep technical knowledge of network architecture is valuable in a crisis.
- Second, heavy reliance on low-cost Chinese vendors can warp future procurement decisions, especially in financially constrained environments. When governments or operators face pressure to expand coverage or cut costs, they encounter a built-in bias toward familiar Chinese suppliers, which can prolong dependence.

The same logic applies to cloud services, data centers, and so-called smart infrastructure**.** As European cities digitize transport, utilities, and public services, Chinese companies are competing to supply sensors, cameras, and management platforms. These systems generate rich, real-time data on how European societies function. They also create new attack surfaces and linkages between what were once separate domains, such as traffic management and police communications.

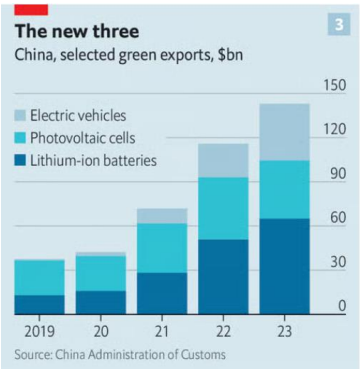
For NATO, digital dependencies matter because modern defense is data-driven defense. If parts of Europe's digital backbone are designed, maintained, or upgraded by firms subject to China's National Intelligence Law (which requires support for state intelligence work), the alliance must assume that sensitive traffic, patterns, or vulnerabilities may be visible to Beijing in ways they are not to Moscow or other adversaries. That knowledge can shape Chinese calculations about escalation, deterrence, and the costs of supporting Russia or threatening Taiwan.

[31] Lucrezia Poggetti, "EU-China Mappings: Interactions between the EU and China on key issues," *Mercator Institute for China Studies*, January 20, 2021. (https://merics.org/en/comment/eu-china-mappings-interactions-between-eu-and-china-key-issues). Note: the map reflects 2021 data; some equipment likely remains in countries which have since banned Huawei from their networks.

C. The green transition: batteries, solar panels, and grid hardware

Europe's most acute strategic dependence on China sits in the heart of its green transition**.** To meet climate targets and reduce reliance on Russian energy, EU member states have accelerated deployment of electric vehicles (EV), batteries, solar panels, wind turbines, and grid-scale storage. In each of these sectors, Chinese firms dominate key parts of the supply chain.

China produces the majority of the world's solar modules and cells**,** a large share of global lithium-ion batteries**,** and critical components for wind and grid equipment. European manufacturers exist and are trying to scale, but they often struggle to compete on price against heavily subsidized Chinese competitors.



Source: The Economist[32]

This dependency poses several hybrid-warfare risks:

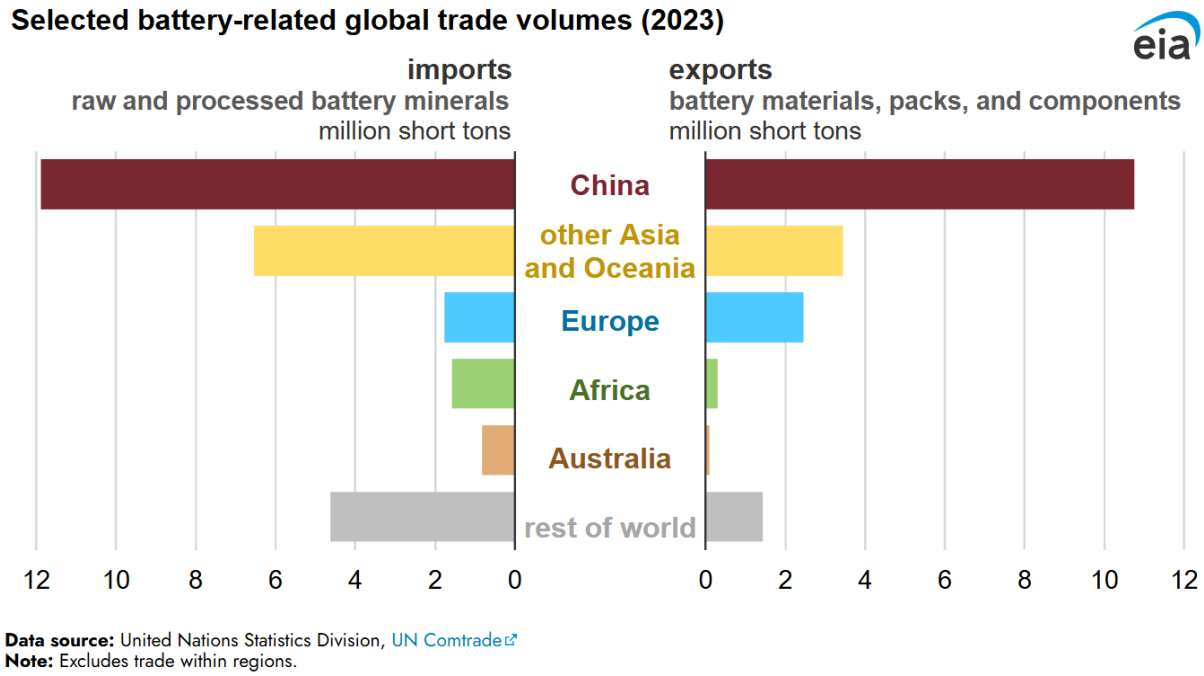
- In a future crisis, Beijing could slow or restrict exports of key components, delaying projects, increasing costs, and undermining public support for energy policies that have become politically sensitive.
- Chinese firms embedded in European energy infrastructure, including inverters, grid controls, and storage systems, may provide additional vectors for data collection or disruption.
- The perception that Europe cannot meet its climate and industrial targets without Chinese technology gives Beijing a powerful political talking point whenever Brussels considers tougher trade remedies, investment restrictions, or export controls.

In effect, China has positioned itself as Europe's green gatekeeper**.** That role gives Beijing latent leverage over everything from EV deployment to renewable buildout timelines, with direct implications for NATO's energy security and resilience.

[32] "Is China a climate saint or villain?" *The Economist* (UK), March 12, 2024. (https://www.economist.com/china/2024/03/12/is-china-a-climate-saint-or-villain)

D. Critical minerals and manufacturing inputs

Behind ports, telecom, and green technologies lies another layer of dependence: critical minerals and manufacturing inputs. China controls significant shares of global processing capacity for rare earth elements, lithium, cobalt, graphite, and other materials crucial to defense systems, electronics, and clean technologies. Even when the raw ore comes from other regions, it often passes through Chinese refineries and component factories before reaching European industry.



Source: U.S. Energy Information Agency[33]

That concentration gives Beijing substantial choke-point power. China has already used export restrictions on rare earths in the past to signal displeasure with foreign governments, including the United States. More recently, Beijing has tightened controls on exports of gallium, germanium, and certain graphite products in response to U.S. and allied semiconductor controls. Each move is calibrated to remind trading partners that China can disrupt supply chains in ways that carry immediate industrial and political costs.

For Europe, whose defense-industrial base is now under pressure to ramp up production of artillery, air-defense systems, and precision munitions, while also meeting green-industrial goals, these dependencies represent a hybrid vulnerability. If China were to impose targeted export restrictions or slowdowns during a crisis, the effects would ripple through:

- Defense production, by delaying or increasing the cost of components for missiles, sensors, and platforms

[33] U.S. Energy Information Agency, "China dominates global trade of battery minerals," May 21, 2025. (https://www.eia.gov/todayinenergy/detail.php?id=65305)

- Energy and industrial policy, by raising costs for EVs, batteries, and renewables at the very moment governments are asking voters to absorb higher security expenditures
- Economic cohesion, by hitting some member states and sectors harder than others, thereby creating political fissures that Beijing and Moscow could exploit.

Chinese firms also supply a wide range of intermediate goods and capital equipment to European manufacturers, from machine tools and electronics to chemicals and automation hardware. Many of these items are not unique to China, but once integrated into production lines, they create switching costs and technical dependencies that are hard to unwind quickly.

E. Why these dependencies matter for NATO and U.S. strategy

Taken together, these strategic dependencies mean that in a serious crisis — whether over Ukraine, Taiwan, or a broader confrontation with Russia and China — Europe would confront not only Russian military pressure but also Chinese economic and technological leverage. Beijing would have multiple options to:

- Target specific allies with discriminating economic pain**,** for example by slowing exports of components critical to one country's defense or energy sector
- Signal that continued alignment with U.S. sanctions or military measures will carry long-term industrial and employment costs, particularly in sectors like autos, chemicals, and clean tech
- Exploit friction among European states with different exposure profiles, turning a shared vulnerability into a source of intra-alliance tension

Hybrid warfare is about shaping the choices available to an adversary. By entrenching these dependencies, Beijing has made sure that any European government contemplating tougher measures against China — or even sustained support for Ukraine and Taiwan — must factor in the risk of Chinese retaliation that hits not just abstract GDP figures but specific factories, jobs, and projects.

IV. From Presence to Pressure: China's Coercive Playbook and Performance

China's hybrid strategy in Europe does not end with penetration and pre-positioning. Beijing has already shown that it is willing to turn presence into pressure, using economic tools, regulatory harassment, and indirect support to Russia's war to shape European choices. These actions provide an early look at how China might wield its leverage in a broader crisis that directly implicates NATO and U.S. interests.

I would highlight two main strands of this playbook: direct economic coercion against European states, and indirect coercion via support to Russia's war machine. Both reveal how Beijing thinks about cost imposition, deterrence, and transatlantic cohesion.

A. Economic coercion against European states: the Lithuania precedent

The clearest European case of Chinese economic coercion to date is a recent event in Lithuania. In late 2021, after Vilnius allowed the opening of a "Taiwanese Representative Office," China responded with a campaign of informal trade restrictions and regulatory pressure.[34] Lithuanian exports were stalled at Chinese customs. European companies using Lithuanian components reported pressure from Chinese authorities and saw their products delayed or blocked.[35]

Crucially, Beijing did not announce formal sanctions. Instead, it relied on opaque customs practices, pressure on multinationals, and unofficial signals. This ambiguity is characteristic of Chinese hybrid coercion. It allows Beijing to deny wrongdoing while still sending a clear message to European capitals: crossing political red lines on Taiwan or human rights can trigger highly targeted economic pain.

The European Union responded by launching a World Trade Organization (WTO) case in early 2022, arguing that China's measures against Lithuanian trade and EU products with Lithuanian inputs amounted to discriminatory and coercive treatment.[36] In parallel, Brussels accelerated work on a new Anti-Coercion Instrument**,** which entered into force on December 27, 2023. Regulation (EU) 2023/2675 now provides a framework for EU action in cases of economic coercion by third countries, including the possibility of countermeasures such as tariffs, restrictions on services, or procurement limits.[37]

This episode illustrates both the strengths and weaknesses of Beijing's approach. On the one hand, Lithuania faced real short-term costs, and other small states drew the lesson that standing up to China can be punishing. On the other hand, Beijing's coercion helped catalyze an EU-wide shift toward de-risking, supply-chain diversification, and new tools designed explicitly to counter economic pressure. The EU has now withdrawn its WTO case after trade flows with Lithuania largely normalized, but it has done so against the backdrop of a more muscular anti-coercion regime and a written commitment to activate that tool if coercion resumes.

Beyond Lithuania, Beijing has used or hinted at economic pressure against European states over 5G decisions, meetings with the Dalai Lama, human-rights statements, and sanctions on Chinese officials. These measures range from import slowdowns and tourism curbs to regulatory scrutiny of specific companies. They rarely appear as formal embargoes. Instead, they operate as calibrated signals, designed to make other governments think twice about policies that Beijing labels "anti-China."

For NATO and U.S. strategy, the lesson is clear. China does not need to coerce the entire EU to shape outcomes. It can focus on one or two exposed states — often those with fewer resources or more concentrated economic ties — and use them as warning beacons for the rest of Europe. The

[34] William Yuen Yee, "China-Lithuania Tensions Boil Over Taiwan," *The Jamestown Foundation*, January 28, 2022. (https://jamestown.org/china-lithuania-tensions-boil-over-taiwan)
[35] Thomas J. Shattuck, "Is Taiwan Fever Breaking in Lithuania*?" Foreign Policy Research Institut*e, February 14, 2025. (https://www.fpri.org/article/2025/02/is-taiwan-fever-breaking-in-lithuania)
[36] Valbona Zeneli, "Lithuania's policy on China: An unlikely EU trailblazer," *The Atlantic Council*, November 10, 2025. (https://www.atlanticcouncil.org/in-depth-research-reports/report/lithuanias-policy-on-china-an-unlikely-eu-trailblazer)
[37] European Commission, "Protecting against coercion," accessed December 8, 2025. (https://policy.trade.ec.europa.eu/enforcement-and-protection/protecting-against-coercion_en)

question is whether EU instruments such as the Anti-Coercion Regulation, and political backing from Washington, can raise the cost of this behavior enough to blunt its deterrent effect.

B. From leverage to restraint: has Beijing's coercion worked?

China's track record in Europe is mixed. In the short term, economic signals have sometimes deterred or delayed specific decisions. Governments that are heavily exposed to the Chinese market or dependent on Chinese inputs often move cautiously. Business lobbies push back when they see contracts or supply chains at risk. This is especially true in sectors that rely on exports to China or on Chinese technology for the green transition and automotive industry.

Over time, however, Beijing's behavior has produced a counter-reaction.

- The EU now speaks openly about de-risking from China and has rolled out an economic security strategy that blends trade defense, investment screening, and export controls. For instance, Brussels has created new tools — such as the Anti-Coercion Instrument — to confront future coercion with coordinated EU-wide responses rather than leaving individual member states isolated.
- Awareness of Chinese hybrid threats has risen significantly in NATO and key national security communities, which now treat economic and technological dependence as core security issues, not just trade questions.

In my assessment, Beijing has succeeded in raising the perceived cost of crossing its political red lines, but it has also accelerated Europe's search for resilience. The result is a more cautious and sometimes inconsistent European approach. Some capitals are more willing to push back; others, including France, still hope to compartmentalize security concerns from economic ties. This uneven response is a vulnerability China can exploit, but it is not the one-way street Beijing might have hoped for.

C. Hybrid warfare by proxy: China's support to Russia's war machine

China's most consequential hybrid action affecting Europe today is not a customs delay or a tourism warning. It is Beijing's role in sustaining Russia's war machine in Ukraine.

Public assessments by NATO and the EU now state that China supplies Russia with dual-use goods and components that feed directly into the Kremlin's defense industrial base. NATO declarations have highlighted Chinese provision of materials and equipment that serve as inputs for Russian weapons production, and warned that China "cannot enable the largest war in Europe in recent history" without consequences for its interests and reputation.[38]

U.S. and European analyses point to a sharp rise in Chinese exports to Russia of machine tools, microelectronics, and telecommunications equipment — all categories critical to manufacturing missiles, armored vehicles, aircraft, and drones. One detailed study estimates that Chinese

[38] NATO, Press Release, "Washington Summit Declaration," July 10, 2024. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration).

suppliers now account for the vast majority of Russia's imports of certain high-priority dual-use goods, and that up to 90 percent of Russia's microelectronics imports come from China.[39]

Recent investigative reporting has gone further, documenting how Chinese businessmen and companies have taken direct stakes in Russian drone manufacturers and supplied hundreds of millions of dollars' worth of drone components, including batteries, motors, and controllers, to the producers of systems used against Ukrainian forces.[40]

From Beijing's perspective, this approach has several advantages:

- It enables Russia to continue a high-intensity war that drains European defense budgets, depletes stockpiles, and tests political cohesion, without China firing a shot in Europe
- It allows China to present itself as formally neutral, avoiding open arms transfers while insisting that its exports are civilian or dual-use items
- It provides real-time lessons in sanctions evasion, alternative payment channels, and logistics networks that could be repurposed in a future crisis involving China directly

For Europe and NATO, the effect is hybrid warfare by proxy. China is not only observing the West's response to Russia's aggression; it is actively shaping the conflict's trajectory by keeping Russia's defense industry supplied. That prolongs strategic pressure on Europe's eastern flank, complicates efforts to rebuild ammunition and missile stocks, and forces allied governments to balance immediate war support against long-term modernization needs.

Beijing's support to Moscow also has an important signaling function. It demonstrates to Russia that China will not leave its partners isolated under Western sanctions, and it signals to European capitals that any future attempt to isolate China over Taiwan or human-rights abuses will likely confront a counter-coalition of authoritarian states willing to help each other endure Western pressure.

D. A candid assessment of where China's hybrid campaign stands

Taken together, China's economic coercion and indirect support for Russia reveal a hybrid campaign that is serious but not yet decisive in Europe.

On the one hand, Beijing has:

- Established real leverage through strategic dependencies in ports, telecoms, green tech, and critical minerals
- Demonstrated a willingness to weaponize trade and investment against European states, as seen in the Lithuania case

[39] Nathaniel Sher, "Behind the Scenes: China's Increasing Role in Russia's Defense Industry," *Carnegie Politika*, May 6, 2024. (https://carnegieendowment.org/russia-eurasia/politika/2024/05/behind-the-scenes-chinas-increasing-role-in-russias-defense-industry)
[40] Chris Cook, Charles Clover, William Langley, and Haohsiang Ko, "Chinese parts supplier takes stake in leading Russian drone maker," *Financial Times*, November 29, 20245. (https://www.ft.com/content/e907c2fa-2d3b-4269-bc6c-b2fee4d9f688); Christian Shepherd and Rudy Lu, "Behind Russia's battlefield drone surge in Ukraine? Chinese factories," *The Washington Post*, October 13, 2025. (https://www.washingtonpost.com/world/2025/10/13/china-russia-drone-parts-ukraine).

- Become a central external enabler of Russia's war effort, thereby shaping the security environment that NATO must manage

On the other hand, China's actions have:

- Accelerated Europe's shift toward de-risking and economic security, including new instruments focused explicitly on countering coercion
- Hardened attitudes in some key capitals and Brussels, where officials now speak more openly about China as a systemic rival and a source of hybrid threats alongside Russia
- Increased transatlantic awareness that Chinese behavior in Europe is not an economic sideshow, but a core part of the strategic challenge from Beijing

In my view, China's hybrid playbook in Europe is still in experimentation mode. Beijing is probing for weaknesses, testing tools, and calibrating how far it can go without triggering a unified Western response. It has learned that coercion can impose costs but also generate backlash. It has seen that supporting Russia offers leverage but also draws scrutiny from NATO and the EU.

For the United States and its European allies, this is a window of opportunity. China's campaign is advanced enough to be visible but not yet entrenched beyond correction. If we use this period to strengthen resilience, coordinate responses, and send clear signals about the costs of coercion and sanctions circumvention, we can shape Beijing's expectations before a more direct crisis over Taiwan, cyberattacks, or European infrastructure.

V. Recommendations

I will close with four concise sets of recommendations for the committee's consideration. They align with HFAC's core tools: oversight, authorizations, reporting, and strategic signaling.

1. Make Chinese hybrid warfare in Europe a standing line of U.S. diplomacy

- Direct the State Department to treat Chinese and Russian hybrid activity as a single, linked challenge in Europe, not two parallel issues
- Require regular classified and unclassified briefings to the committee on how U.S. embassies, the U.S. Mission to NATO, and the U.S. Mission to the European Union are integrating Chinese hybrid threats into their work on Russia, Ukraine, and European security
- Direct the State Department to designate a clear hybrid-warfare lead for Europe and Russia/China within the department's new Emerging Threats Bureau, so this problem does not fall between regional and functional bureaus

2. Support European de-risking from Chinese leverage in critical sectors

- Use hearings, letters, and report language to publicly back Europe's de-risking agenda, especially in ports, telecom, green tech, and critical minerals where Chinese leverage is greatest

- Encourage State and the U.S. International Development Finance Corporation to prioritize co-financing alternatives to Chinese capital and technology in European infrastructure and energy projects that have direct implications for NATO's ability to conduct military mobility
- Request regular reporting on U.S.-EU coordination on investment screening, export controls, and research security related to Chinese entities of concern
- Press for a dedicated U.S.-EU/NATO supply-chain working track on China, focused on mapping and mitigating dependencies in defense-related and modern energy system inputs that Beijing could weaponize in a crisis

3. Strengthen cyber resilience and information sharing with Europe

- Direct the State Department's Bureau of Cyberspace and Digital Policy, in coordination with the regional bureaus, to brief HFAC on a plan to expand joint cyber resilience efforts with European allies against Chinese cyber-threat actors, including hardening ports, energy grids, and telecom networks where Chinese hardware or software is present
- Encourage closer NATO–EU–U.S. information sharing on Chinese cyber campaigns in Europe, including common attribution language, shared red lines for disruptive activity, and agreed response options short of armed conflict
- Support initiatives that help allies identify and remediate Chinese-origin cyber and hardware risks in critical infrastructure, including through joint assessments, exercises, and targeted assistance where exposure is highest

4. Raise the costs of Chinese coercion and support to Russia

- Mandate a recurring public report from State, in coordination with Treasury and Commerce, identifying Chinese entities that materially support Russia's defense-industrial base, with recommendations for sanctions, export controls, or other measures
- Signal, through authorizing language and oversight, that economic coercion against European partners — including informal trade blockages or pressure on firms using European components — will be treated as a strategic issue for the United States, not a bilateral trade dispute
- Encourage the administration to ensure that any future Russia-related negotiations explicitly account for China's role in sustaining Russia's war machine, rather than treating Beijing's contribution as a peripheral issue

5. Strengthen the information and research front with Europe

- Press State to use its existing public diplomacy, intelligence, and democracy-support authorities to systematically track and expose Chinese information operations in Europe, especially where they mirror or launder Russian narratives about NATO, Ukraine, and U.S. policy
- Encourage joint U.S.-European work on research and campus security, including common principles for transparency around Confucius Institutes and their successors, joint labs, and partnerships with Chinese institutions linked to military-civil fusion

- Support initiatives that help European partners map and publicly disclose their own exposures — in ports, telecom networks, green technologies, and universities — so that hybrid vulnerabilities are visible to parliaments and publics, not buried in classified annexes

Thank you for the opportunity to testify.