International Journal of Computer Science and Engineering Development
Volume 1, Issue 2 | May – June 2026 | www.ijcsed.com
ISSN: 3139-0862

Technological Development in China under Great Power Rivalry

A Critical Review of Security Consequences and the Evidence Threshold

Ir Dr Samuel Kwok Piu LIP [#1], Dr. Wing Cheung TANG [*2]

[#1] Founder and Managing Director of Lordray Engineering Company Limited, Hong Kong, China

[*2] Adjunct Professor of Spectrum International University College, Malaysia

[1] samuel@lordray.com.hk , [2] tang957031@gmail.com

Abstract—
This article offers a critical review of a text on China's technology policy amidst the backdrop of greater power rivalry, especially its conceptual framing, evidential choices, and causal claims concerning security implications. The review argues that while the source convincingly contextualises China's innovation trajectory in terms of techno-industrial governance and dual-use "omniuse" technologies, it does not sufficiently operationalise "security implications" or establish empirical benchmarks for causal attribution, nor does it prove (at an acceptable evidentiary level) the alleged effects of military-civil fusion (MCF) and technology-driven supply-chain leverage. The article provides a typology of security-relevant mechanisms (direct military capability, defense-industrial resilience, coercive supply-chain leverage, intelligence or surveillance applications, and escalation risk from technological asymmetry) and applies it to evaluate the coherence and evidential support of the source's arguments. The review also points to deficits in methodological transparency (especially absent case-selection logic, evidence-to-claim mapping, and counterfactual reasoning) and suggests concrete research designs to move beyond plausibility towards measurable security outcomes. The article ends on a sober note: techno-industrial policy can enable capability-building, even as it creates governance bottlenecks, inefficiencies and geopolitical friction; that said, the claims about security consequences need more robust empirical and methodological underpinnings than the source provides.

Keywords—military-civil fusion, political governance, security implications, techno-nationalism, technology policy

I. Introduction

The source under review presents itself in a way that reads more like an analytical policy synthesis than a transparent research article. We do not consider this a purely procedural complaint but rather evaluate the text as if it were a research article (i.e., with a threshold appropriate for security-relevant causal claims). This higher bar is warranted because the document makes not only interpretive claims about governance and innovation, it makes claims about measurable security consequences of China's technology policy and institutional architecture in the context of a great-power rivalry [1].

The passage sets out three connected propositions. First, it conceptualises modern technologies as "omniuse" and argues that "overall technological development directly shapes countries' military capabilities and security," making it analytically difficult to disentangle civilian innovation trajectories from military relevance. Second, it conceptualises techno-industrial policy [2] as state-guided but not entirely top-down, emphasising an increasing political governance that co-exists with continued company-led R&D. Third, it covers how export controls and countermeasures (especially regarding advanced AI chips and critical minerals) change security dynamics, like China's emphasis on self-reliance [3] and adversaries' operational restrictions.

The methodological limitation is not just the absence of a "methodology." More importantly, the text does not specify (i) how claims are selected and delimited, (ii) what type of evidence is required for each security mechanism, (iii) how causal pathways are adjudicated rather than asserted, and (iv) how "security implications" are operationalised into empirically assessable outcomes. The purpose of this review is therefore to enhance the interpretative value of the source and to strengthen the evidential and analytic foundations needed to support its security-level findings.

II. Merging Omniuse Framing with Security

A. Omniuse technologies and the shift from platforms to ecosystems

The omniuse premise of the source reframes security from a domain of defence procurement alone to the outcomes of broader industrial and innovation systems. Such framing is consistent with mainstream dual-use and civilian-military [4] convergence scholarship, where boundaries are blurred by technical spillovers and can be propagated into military capability through procurement, adaptation or operational learning.

The major flaw, however, is the lack of an evidentiary standard that distinguishes between generic dual-use potential (security relevance by possibility) and substantiated military integration (security relevance by demonstrable linkage).

The security pathway remains conceptually plausible but empirically underdetermined absent an explicit criterion for when "direct shaping" is established (e.g., documented integration into defence programs, procurement records, or validated capability adoption).

B. Security outcomes require operationalization

As omniuse technologies can be security-relevant for various reasons, it is analytically necessary to define what "security consequences" are in measurable terms. The source discusses military capability, industrial limitations, and

 ISSN: 3139-0862

geopolitical leverage but does not consistently translate these into operational indicators. In the sections that follow, this review seeks to fill that gap by proposing a typology of security implications matched to types of evidence.

Without such specification, analysis risks mixing separate threat channels, e.g., the effect of a dual-use component on battlefield lethality and the effect of a dual-use component on vulnerabilities in the semiconductor supply chain. The typology identifies three measurable dimensions. The first is a change in the timelines of military deployment or the survivability of systems. The second is quantifiable bottlenecks in industrial production, such as a loss in yield or substitution costs. The third is a change in interstate bargaining power that can be observed in export control lists, delays in technology transfer, or R&D investment patterns. Each dimension has a corresponding type of evidence: respectively, wargame simulation data, industrial capacity audits, and diplomatic procurement records.

This systematic approach translates vague concerns about "strategic risk" into propositions that can be falsified. The typology underpins security consequences in observable metrics, allowing comparative case studies, risk scoring and early warning indicators. It also points out where evidence is lacking at present and gives direction for further intelligence gathering or technical audit. In the end, putting omniuse technology into practice can move the discussion from abstract securitisation to a policy-relevant analysis that can be tested.

III. The Evolution of China's Techno-industrial Policy

The source outlines three changes in the extent of state involvement over time:
(a) Reform and Opening Up (1978–2003): a move towards more market orientation, less intervention.
(b) Policy U-turn in techno-industrial (since 2003): actively identifying priority sectors and targeting resources.
(c) The Xi-era intensification (especially after 2016/2017): focus on high quality development and strategic sectors, while limiting others.

It also discusses two "policy peaks" of industrial direction, a 2006 medium/long term S&T program with megaproject funding and a 2010 Strategic Emerging Industries program cut across multiple technology domains. It points to ongoing megaproject financing under Xi-era governance, as well as specific initiatives (e.g. AI development plans and strategic semiconductor/telecom emphasis). Institutional governance is emphasised in the reorganisation of the Ministry of Science and Technology and the creation of a Party organ that is apparently hierarchically superior to it, giving the Party "ultimate authority over research priorities".

A. The state-business interaction problem

A recurrent theme is the coexistence of strengthened political control alongside continued company-led innovation and R&D. The source backs this up with a statement that firms account for "some 78% in 2024" of R&D expenditure and with an Open Innovation Platform [5] model that aims to boost diffusion through national "champions."

Yet the basic analytical problem is that the source does not build a rigorous theory of how state guidance and company initiative interact across regimes. It suggests that political control can increase effectiveness in strategic sectors, while allowing for innovation through infrastructure and scaling capacity. It also acknowledges limits (MCF limited success; mismatch between industrial policy and local implementation; overinvestment concerns). It does not specify when state direction is enabling rather than distortive.

This gap is important for the security argument. If governance is tightened, but firms still have considerable agency over R&D, then the effect of policy on security consequences is a function of mechanisms (incentives, constraints, procurement channels, talent allocation, performance metrics) that need better causal articulation and evidence standards.

IV. Technology Crackdown as a Turning Point

The source says that a crackdown on technology in the early 2020s was a turning point: managing elevated political risk, rather than rapid growth, shifting away from corporate focus on entertainment platform business models to strategic technologies.

This is a plausible mechanism. Regulatory and political risks can alter firm strategy, capital allocation and talent flows. Still, the security-relevant claim requires stronger adjudication:
(a) Does the crackdown increase R&D output in defense-relevant strategic technologies (AI, semiconductors), or is it largely a matter of resource reallocation and business model restructuring?
(b) What would be the appropriate counterfactual, i.e., would strategic innovation have accelerated anyway, regardless of crackdown conditions?

From the above, causal inference remains underdetermined. There is no comparative evidence or counterfactual reasoning in the passage. This review therefore treats the crackdown to generate hypotheses, not as an empirically closed causal story, unless additional evidence can show changes in defense-relevant innovation outputs associated with the crackdown in a way that is better than alternative explanations.

V. Military-civil Fusion (MCF)

A. Institutionalization of MCF

The source traces MCF from earlier mention to greater visibility in the Xi era. It identifies references in defence white papers [6] and identifies promotion intensification in 2017 by means of specialised planning and establishment of oversight structures. It presents the MCF as a national system for the joint development of innovations by the military and civilian sectors based on multipurpose civilian technologies. This framing highlights the systematic integration of research pipelines, procurement and talent cultivation across previously separate industrial bases.

It also says that terminology for MCF was removed from the 14th Five-Year Plan (2021-2025), which it sees as a strategic downgrade to avoid external scrutiny, including in response to U.S. investment restrictions targeting companies linked to MCF in dual-use sectors. The source said the dropping of the term does not mean abandoning the policy but continuing to operate under less transparent branding. This

 ISSN: 3139-0862

implies that although the official language shifted to broader terms like "integrated national strategic system and capabilities", the basic coordination mechanisms (joint funding, technology transfer protocols, and cross-sector review boards) were retained or even enhanced. The source says rebranding is defensive: it helps with fingerprinting sanctions while keeping the bureaucracy moving.

B. Limited demonstrated outcomes

The source notes that overall MCF success has been limited and cites one specific limitation: security-relevant military R&D has not seen the participation of civilian companies as envisioned, partly because existing suppliers oppose opening markets to new entrants. It also points out that there is evidence in the AI space that non-traditional vendors can contribute to the defence industrial base but emphasises that state owned enterprises remain relevant and receive the most lucrative contracts.

This is a relevant partial qualification: it moves MCF from an abstract top-down integration story towards a more industrial-competitive reality in which procurement structures, incumbency and supplier incentives shape what "fusion" can realistically mean.

But there is no systematic evidence on important evaluative questions:

(a) level of civilian involvement over time,
(b) comparative performance across sectors (AI, semiconductors, quantum, advanced manufacturing), and
(c) definition-based metrics of "success" (speed, cost efficiency, adoption, operational performance).

Without these pieces, the reader cannot judge whether limited success is due to structural constraints (procurement system design, supplier incentives) or strategic recalibration (moving away from term-promoted fusion to other policy instruments).

At a minimum, a security-focused review would require evidence that MCF is linked to operational or procurement relevant outcomes. As written, the text makes plausible institutional claims and provides partial industrial evidence but does not establish the empirical magnitude and defense-relevant significance of MCF outcomes with comparable rigour.

VI. Innovation Metrics and Deep Infrastructure

The source uses a variety of proxies: manufacturing shares (solar modules; lithium-ion batteries), EV shares (70% made by Chinese brands in 2024), R&D spending comparisons (just under 96% of the U.S. on a PPP basis), global innovation rankings, and AI patent/publication shares (e.g., almost 70% of global AI patents granted from 2010 to 2023 originated in China). It also uses an infrastructure argument. Grids, digital networks, industrial workforce, enable scaling.

A. Proxy-based empiricism

A methodological strength of the source is that it is not based solely on qualitative statements and uses measurable proxies for innovation inputs and outputs. The analysis is made verifiable and comparable by quantifying R&D spending, patent filings and technology transfer volumes. For these indicators, it grounds the argument in observable trends, minimising interpretive bias. It also allows replication or critique based on hard data rather than assertion.

B. Metric validity, attribution, and selection bias

Three methodological weaknesses are common to a security-consequence review:

(a) Metric validity -- patents/citations do not necessarily map well onto deployable military capability.
(b) Attribution -- innovation outputs may be driven by economic scale, learning-by-doing or structural advantages rather than by particular policy instruments.
(c) Indicator selection -- Focusing on sectors where China is strong risks cherry-picking, especially if the security claims are broad.

To link innovation proxies to dual-use deployment, the source would need to either document adoption by defence entities, procurement patterns, defence sector integration, or observe changes in capability indicators associated with policy periods.

VII. Causal Attribution Challenges

Earlier drafts correctly point out that counterfactuals and causal attribution [7] are missing again. This should be brought together in one place and developed as an explicit methodological issue rather than repeating the phrasing. A common criticism would be that without a counterfactual baseline of what would have happened in the absence of MCF, observed outcomes cannot be causally attributed to the policy. Repeated mentions dilute the impact and a single developed section on causal inference would make the review sharper. A section like this could talk about selection bias, omitted variables, and the difficulty of disentangling MCF's unique impact from broader trends in defence modernisation.

A. Export controls and semiconductors

The semiconductor case offers a somewhat more coherent causal chain: export controls → reduced access → substitution/self-reliance efforts → longer-term strategic outcomes. But the evidence is not yet quantified enough. First, there is no estimate of the share of delays that are attributable to export controls versus other bottlenecks. These include constraints on foundry capacity, vulnerabilities in the supply chain of equipment (e.g. lithography tools from restricted jurisdictions), shortages in the talent pipeline in advanced process nodes, limitations on materials (ultra-pure chemicals, speciality gases) and gaps in the policy coordination among ministries. Without disaggregating these factors, any attribution of delay to export controls alone risks overstatement.

Secondly, the analysis does not look at how much self-reliance investment offsets short-term impediments which are security significant. The key measure for a security assessment is not whether domestic alternatives will emerge, but whether they will emerge in a militarily relevant timeframe and at an acceptable level of performance parity. If substitution costs you five years of 50% performance degradation, the net effect on security is drastically different than two years of catch-up at 90% parity. The source does not provide any such threshold analysis.

 ISSN: 3139-0862

It also introduces governance risks that are evident in allegations of corruption and institutional purges in Ministry of Industry and Information Technology (MIIT) and semiconductor-related funding contexts, governance challenges of managing strategic investment. These allegations, if proven, suggest that some self-reliance funding may be diverted to wrong uses thereby lowering the effective R&D yield. But the source does not quantify purge rates or link purges to specific program delays.

A rigorous critical review would involve time-series analysis and comparative baselines: pre- verse post-control fab construction timelines, control region comparisons (e.g. China versus South Korea under similar restrictions), and firm level performance trajectories (yield rates, defect densities, time-to-volume). They are not present in the excerpted material. But without this evidence, the causal chain is plausible but not proved, a hypothesis rather than a finding.

VIII. Critical Minerals and Countermeasures

The source contends that upstream choke points in critical minerals enable China to choke high-tech production in adversary countries, and that China tightened controls in response to U.S. export control policies. Policy milestones include controls on Gallium and Germanium in July 2023; controls on graphite and processing technologies for rare earths in late 2023; controls on antimony for military applications and dual use items in 2024; and controls on additional rare earths in April 2025. They are pitched as calibrated retaliation, not blanket bans, at specific stages of processing in which China has near-monopoly positions.

It also has a licensing conditionality that requires foreign companies to certify that rare earths will not be used for defence purposes, a verifiable end-use attestation that adds administrative delays and legal risks for buyers. Defence companies are warning of production cuts because of the challenges and costs of substituting precision-guided munitions, radar systems and optoelectronics, the source said. It cites impacts on F-35 production as an example of Europe's security exposure, with European subcontractors reliant on gallium compounds from China having to overcome certification challenges for alternative suppliers.

The source does not quantify the extent of production pauses or the cost differential between Chinese and non-Chinese supply chains. In the absence of such metrics, the alleged strategic deceleration is believable but untuned for risk assessment. It also has a licensing conditionality that requires foreign companies to certify that rare earths will not be used for defence purposes—a verifiable end-use attestation that adds administrative delays and legal liability risks for buyers. Defence companies are warning of production cuts because of the challenges and costs of substituting precision-guided munitions, radar systems and optoelectronics, the source said. It cites impacts on F-35 production as an example of Europe's security exposure, with European subcontractors reliant on gallium compounds from China having to overcome certification challenges for alternative suppliers. The source, however, does not quantify the extent of production pauses or the cost differential between Chinese and non-Chinese supply chains. In the absence of such metrics, the alleged strategic deceleration is believable but untuned for risk assessment.

A. Linking policy to operational security outcomes

Upstream material control can affect defence supply chains, arguably the most security-direct mechanism in the excerpt. Unlike downstream technology restrictions, which are subject to substitution and reverse engineering, critical mineral chokepoints depend on geologic concentration and long certification cycles. Disrupting supplies of gallium or antimony would have a direct effect on radar, night vision and munitions guidance systems. The mechanism avoids loopholes in export compliance because there are few alternative sources for refined materials, making production halts measurable in weeks rather than years. This makes trade policy an immediate vulnerability in terms of military logistics.

B. Operational specificity and evidentiary precision

Impacts to F-35 output, production timelines and verified supply chain disruptions are not quantified. It says Europe is vulnerable, but no figures are given on how many deliveries of F-35s were delayed, by how much, or whether any airframe remained unfinished because of shortages of Gallium or Germanium. Without such figures the claimed effect is just speculation.

Second, the source does not explain how licensing works in practice: how often it is denied, the compliance burdens it imposes, or the enforcement results. Is China denying 5% or 95% of defence end-use attestations? Do denials cluster around suppliers or countries? How long does a licence review take – weeks, months or indefinite? These parameters determine whether the mechanism delivers symbolic pressure or real supply interruption. Compliance costs (auditing, reporting, legal liability) for foreign firms are mentioned but not cost.

Third, no estimates are made of substitution timelines, recycling rates, and stockpile availability. For example, gallium can be recovered from LED and IC manufacturing waste, but the scale and lead time of the recycling infrastructure are not included. The source does not believe stockpiles in the hands of defence contractors or allied governments could cushion months of disruption. Fourth, the role of alternative sourcing from Australia, Canada or existing stockpiles is not evaluated. Is non-Chinese supply technically possible but economically impossible, or simply not available?

The excerpt treats "chokepoints" as likely degraders of capability, but it does not build the intermediate step that chokepoints translate into measurable harm to defence readiness. Without industry statements that include precise production metrics and verified disruption timing, this is an empirically incomplete security claim, more threat scenario than verified intelligence.

XI. Typology-driven Evaluation of Security Implications

To enhance the review, include a typology mapping the claims of the source with the categories of security mechanisms and the respective evidence requirements. Such a typology would turn impressionistic statements of risk into propositions to be tested. Take the "material chokepoints" category, for example (upstream control of critical minerals) which requires three types of evidence: the first is verified stoppages of production at specific defence facilities (e.g., F-

 ISSN: 3139-0862

35 radar assembly lines that were idled due to gallium shortage), with the duration and output loss quantified; the second is estimates of the costs of substitution, including the recertification costs for alternative suppliers and the diminished performance of substitutes; the third is the timeline for depletion of stockpiles, estimating how many months existing inventories will buffer the disruption before production actually stops. Without all three, a chokepoint claim is still a hypothetical leverage rather than a demonstrated capability degradation.

The "technology denial" category, export controls on semiconductor equipment or design tools, requires quantified attribution of R&D delays. This entails removing the additional months or years added to a competitor's advanced node timeline due to limited access, while controlling for internal bottlenecks like talent shortages or yield learning curves. Evidence standards include counterfactual modelling or comparative case studies (e.g., pre- verse post-control project schedules).

Governance corrosion category (corruption and purges in strategic investment agencies) needs corruption leakage rates (estimated percent of funds diverted) and program audit trails indicating whether purges coincide with project delays or cost overruns. Each mechanism ought to define what enough proof is what counts as verified disruption versus speculative leverage. Then, holes in evidence can be systematically criticised. This typology requires the source to show where the evidence meets the bar and where it fails to meet the bar and thereby increases analytical rigour.

A. Proposed typology

For the operationalisation of security consequence analysis, the review suggests five mechanism categories and associated evidence standards:

(a) Enhance direct military capability -- Needs documentation of military procurement of specific technologies, performance demonstrations relevant to defence use (e.g. gains in range, precision, survivability) and timelines for integration from civilian R&D to fielded system. There is no way to verify claims of capability without serial numbers or deployment data at the unit level.

(b) Defence industrial base resilience -- Must show supply chain redundancy and continuity for defence manufacturing: substitution capability (alternative suppliers qualified within relevant military timeframes); production variance (standard deviation in times of component delivery); domestic manufacturing reliability (yield rates, defect densities). Resilience claims require statistical comparisons of pre- versus post-intervention.

(c) Supply-chain leverage, weaponized -- Demands measured changes in partner production—recorded output reductions at specific facilities—and licensing or constraint results (denial rates, delay time, compliance costs). Most importantly, causality needs to be established: the disruptions must be shown to be caused by the coercer's policy change, and not by unrelated logistics failures or demand shocks.

(d) Intelligence/surveillance uses -- Requires documented deployment in intelligence or surveillance systems (e.g., government procurement contracts, operational use cases with timestamps, or transfer records to relevant defence or internal security entities). Vague references to 'dual-use potential', without evidence of deployment, do not meet this standard.

(e) Risk of escalation via technological asymmetry -- Requires credible routes from technological preeminence to threat perception escalation, supported by breakdowns in strategic doctrine (e.g., changes in official policy language), evidence of crisis communication (diplomatic cables, signalling), or modelled escalation risk based on empirical indicators such as force posture changes or alert status changes. Hypothetical escalation scenarios do not suffice.

B. Applying the typology to the source

The omniuse framing can in principle plausibly accommodate category, but it lacks a consistent evidentiary standard for distinguishing potential from adoption. A lot of the technologies that are labelled "dual-use" never make the transition from civilian lab demonstrations to military fielding. Without adoption metrics, such as procurement contracts, completion of integration testing, or the deployment date of individual units, the security implication is speculative.

The MCF narrative most directly addresses both categories, but the evidence does not establish magnitude or operational outcomes. Collaboration mechanisms exist, but the source does not provide data on the number of projects funded by the MCF that have transitioned to production, the performance gains they have achieved, or the impact on wartime sustainment timelines.

They matter only if the tech crackdown can be shown to divert R&D into measurable outputs relevant to defense, for example, more patent filings in guidance systems or radar components. It is still underdeveloped. The source states intent but does not change output.

This is most directly implicated by semiconductor export controls, and partially, but quantification and counterfactual baselines are missing. And what would be the timelines for semiconductor self-sufficiency without controls? No comparative estimate can be made.

The excerpt does not provide operational measures that connect licensing and controls to the continuity of defence production including the claimed F-35 vulnerability. No production stoppage data, no inventory draw-down curves, no indication of substitution timings.

It is this typology that enables the review to shift from general critique to mechanism-specific evidentiary assessment, which is what a security-consequence journal article demands.

X. Synthesizing Techno-nationalism

The source's unifying theme is techno-nationalism [8], or the idea that technological advancement is a national security project, one that can intensify geopolitical rivalry. Techno-nationalism, it argues, can stymie innovation by reducing international collaboration, breaking up supply chains and duplicating R&D costs. But it also leads to strategic substitution and domestic capability building – particularly under export restrictions where denied access gives way to indigenous innovation. The result is a paradox. The policies that slow near-term technological progress might speed up long-term self-reliance. The source does not

 ISSN: 3139-0862

empirically resolve this tension, and it is unclear under what conditions the net security effect is positive or negative.

A. Theoretical strength

The system's view is internally consistent. Reciprocal constraints can fragment global knowledge networks and raise R&D costs, undermining near-term innovation, but can also lead to adaptive substitution and domestic capability building. This creates a dynamic where early efficiency losses may be more than offset by longer term gains in indigenous capacity and supply chain redundancy. The net effect could be security enhancing or security undermining, depending on the substitution time scales, cost differentials, and strategic patience of investing states, none of which are quantified by the source.

B. Theoretical weakness

In some places the excerpt suggests directional certainty, e.g., export restrictions "may even accelerate" development in the long term, but do not specify conditions (scale of investment, organisational reform, talent retention, alternative market access, or governance capacity) under which acceleration occurs. Claims that techno-nationalism stifles innovation also fail to sufficiently account for adaptation mechanisms such as selective internationalisation through sanctioned channels.

In a journal article these would be turned into conditional hypotheses and spelt out in terms of what evidence would falsify or confirm them. The security logic as presented is more plausibility-oriented than evidence-adjudicated.

XI. Limitations of the Study under Review

As quoted, the review itself concedes that the source is limited in method, evidence operationalisation and causal inference. To meet the standards of the journal, revise this section from a list of omissions to a set of transparency and replicability requirements that a stronger policy review should meet. These include specifying measurable indicators for each security mechanism; providing counterfactual baselines for causal attribution; disclosing data sources and collection protocols; providing replicable coding rules for qualitative evidence. Such requirements transform critique from a subjective judgement into objective and actionable quality criteria of security-consequence research.

A. Minimum transparency standards

It should suggest a minimum set of standards, which turns criticism into useful methodological guidance.

Firstly, the criteria for case selection need to be explicit: why AI, semiconductors and minerals are selected and why they are representative of security consequences. Case selection risks the danger of cherry-picking [9] without justification. To allow for generalisability, the criteria should have variation on at least one dimension (supply chain structure, military dependence, substitution feasibility).

Second, a causal logic diagram is needed, tracing instruments (export controls, MCF funding, mineral licensing) → intermediate mechanisms (R&D delay, production substitution, supply interruption) → security outcomes (capability degradation, resilience loss, coercive leverage). This diagram is a way of forcing theoretical clarity and showing where evidence is lacking.

Third, a claim-to-evidence table should describe the major claim, the type of evidence (policy documents, procurement data, industry statements, licensing statistics, time-series outputs), and the reasoning standard used – distinguishing between "plausible" (consistent with theory) and "demonstrated" (empirically verified). This prevents the hypothesis and the finding from being equivocated.

Fourth, we need operational definitions of security outcomes: readiness (e.g., equipment availability rates), procurement continuity (i.e., delivery variance), capability adoption (i.e., fielding dates), escalation risk (i.e., doctrine changes), coercion feasibility (i.e., compliance rates). They all must be tied to measurable proxies.

Fifth, a counterfactual strategy [10] needs to consider alternative explanation structural constraints (global demand for chips), learning dynamics (firm adaptation), global market effects (price shifts), or internal domestic organisational changes (reforms unrelated to external pressures). These standards transform critique from a checklist of omissions to a replicable methodological contribution that raises the bar for security-consequence research.

XII. Recommendations for Future Research

This section advances the previous "suggestions" document to journal-ready research designs by substituting vague critique with specific methodological standards. The original only asked for missing evidence, but the revised version requires case selection criteria, causal logic diagrams, claim-evidence tables, operationalised security outcomes, and counterfactual strategies. These factors turn casual suggestions into reproducible, peer reviewable procedures that can be published in security research.

A. Process tracing on a specific MCF pilot project

(a) Research question -- Did civilian companies really get involved in a particular defence initiative? What institutional barriers influenced this involvement? This question moves from aggregate MCF claims to observable behaviour at firm level.

(b) Design -- Select one defence program that is said to involve MCF collaboration (e.g., a dual-use sensor or communications system). Create timelines from procurement announcements, corporate filings, contracting records and interviews or expert sources.

(c) Identify specific barriers -- supplier reluctance (fear of IP leakage or regulatory burden), procurement gatekeeping (restricted bidding criteria), IP and security classification mismatches (civilian verse military disclosure rules), and contracting incentives (profit margins, liability terms). A mechanism-level causal story about why fusion works or doesn't in practice, whether due to bureaucratic friction, risk aversion, or incentive misalignment. Unlike aggregate correlation studies, this design yields falsifiable, traceable evidence of actual collaboration constraints, directly testing the operational reality of the MCF model.

B. Event-study design around export controls and countermeasures

 ISSN: 3139-0862

What are the measurable causal effects of export controls on firm-level innovation capacity and strategic adaptation? So, this is a design that must be quantified, not qualitative claims as the source does.

We apply event-study methods (with proper robustness checks) to Chinese semiconductor firms and related supply-chain companies. Pinpoint critical dates of control announcements (e.g. October 2022, July 2023) and analyse stock price reactions for any abnormal returns. Then follow-up changes in R&D announcements (patent filings, new project announcements), capital expenditure (equipment orders, fab construction), hiring (specialised engineer recruitment) and output milestones (yield rates, tape-out announcements). One could use a difference-in-differences specification to compare firms directly exposed to controls vs those less exposed.

The excerpt provides stories, not the data pipeline. This would necessitate granular firm-level data (quarterly financial reports, patent databases, job postings, and industry association bulletins) and careful identification assumptions (parallel trends, no anticipation effects). Without such data, claims of "strategic adaptation" remain plausible storytelling rather than causal evidence. Robustness checks should control for confounding by global demand cycles or domestic policy changes.

C. Comparative case study

(a) Research Question -- When do supply-chain chokepoints [11] become operational security constraints? This moves from saying there are chokepoints to saying when they do constrain behaviour.

(b) Design -- Comparative analysis of four variables across two domains, rare-earth supply leverage verse AI chip export dependence. (i) Substitution feasibility (availability of alternative suppliers/materials); (ii) Procurement time horizons (lead times for new supplier qualification); (iii) Inventory and stockpile dynamics (duration of buffer stocks under normal consumption); (iv) Licensing enforcement (denial rates, compliance costs, circumvention channels).

To explain variation in evidentiary demonstrability, not merely to assert it. Substitution is slow for rare earths, but stockpiles may buffer months; substitution for AI chips in design tools is nearly impossible but smuggling offers circumvention. This comparison allows the design to generate conditional hypotheses about when chokepoints translate into quantifiable production stoppages versus simply price effects, moving from descriptive assertions about leverage to testable logic about security.

XIII. Conclusion

The source offers a coherent synthesis of China's technology development and its security implications in the context of the great power competition. Its conceptual framing (especially technology as omniuse and innovation ecosystems as co-determinants of military capability) is analytically compelling. It also captures institutional dynamics: political governance has increased while companies remain major drivers of R&D; MCF is institutionalised but delivers limited integration; and techno-nationalism shapes both chips and critical minerals supply chains.

But a critical assessment shows that often plausibility replaces operational proof. Security implications (direct capability boost, industrial resilience, coercive leverage, surveillance applications, escalation risk) are not consistently operationalised, and causal claims are not supported with comparative baselines, counterfactual reasoning, and mechanism-specific evidence. The debate on China's techno-security will be vulnerable to assertion rather than adjudication until scholars go beyond plausibility arguments and use transparent, operationalised measures of security outcomes. This review has demonstrated the areas where the evidentiary bar needs to be raised and how future research designs can translate broad security logic into empirically accountable causal claims.

References

[1] Loke, B. (2023). Great Power Rivalry. In *Security Studies* (pp. 169-185). Routledge.

[2] Anguelov, D. (2026). Steering FinTech: Techno-industrial policy for the data-driven economy in China's Greater Bay Area. *Environment and Planning A: Economy and Space*, *58*(2), 274-302.

[3] Cowshish, A. (2024). Defence Acquisition Procedure for Self-Reliance. *Journal of Defence Studies*, *18*(3), 136-149.

[4] Khorram-Manesh, A. (2020). Facilitators and constrainers of civilian–military collaboration: the Swedish perspectives. *European Journal of Trauma and Emergency Surgery*, *46*(3), 649-656.

[5] Osorno, R., & Medrano, N. (2020). Open innovation platforms: A conceptual design framework. *IEEE Transactions on Engineering Management*, *69*(2), 438-450.

[6] Jennings, P. (2013). The politics of defence white papers. *Security Challenges*, *9*(2), 1-14.

[7] Hamann, K., Pilotti, M. A., & Wilson, B. M. (2021). What lies beneath: The role of self-efficacy, causal attribution habits, and gender in accounting for the success of college students. *Education Sciences*, *11*(7), 333.

[8] Luo, Y. (2021). Illusions of techno-nationalism. *Journal of international business studies*, *53*(3), 550-567.

[9] Wolbring, G. (2021). Cherry-Picking and demonizing abilities. *Zeitschrift für Disability Studies*, *1*(1), 1-10.

[10] Georgousis, D., Lymperaiou, M., Dimitriou, A., Filandrianos, G., & Stamou, G. (2026). Evaluating Counterfactual Strategic Reasoning in Large Language Models. *arXiv preprint arXiv:2603.19167*.

[11] Crane, K. (2020). *Choke Points: Logistics Workers Disrupting the Global Supply Chain. Edited by Jake Alimahomed-Wilson and Immanuel Ness.* London: Pluto Press, 2018.