Military Cyber Affairs

Volume 3 | Issue 2 Article 2

2018

# Countering "Made in China 2025": Strategy for Western Powers in a Cybered World

David Mussington
*University of Maryland, College Park*, bmussing@umd.edu

# Countering "Made in China 2025": Strategy for Western Powers in a Cybered World[1]

David Mussington[2]

**Abstract:** Cyber capabilities have diffused disruptive potential to new actors and locations around the world. The engine for diffusion, however, is the economy, not politics. Interactions in trade, global product development systems and digital services spreads patterns of mutual dependence – and vulnerability – worldwide. Access to this global economy equates to participation in wealth creation and technological progress. Denial of access creates disadvantages and imposes costs. For nation-states, this environment is full of both risk and opportunity. Confronting a Chinese government strategy that targets Western economic advantages, the democracies face a series of questions: what is the best strategy for successful protection of assets and infrastructures of value? What should be done about authoritarian states that both participate in the cybered world, yet oppose the open, transparent and democratic norms of cyberspace's originators?

[1] Please cite as: Mussington, David, "Countering 'Made in China 2025': Strategy for Western Powers in a Cybered World," in Demchak, Chris C. and Benjamin Schechter, eds. Military Cyber Affairs: Systemic Cyber Defense 3, no. 2 (2018).

[2] Director of the Center for Public Policy and Private Enterprise and Professor of the Practice in the School of Public Policy, University of Maryland, College Park

## Introduction

Cyber capabilities have diffused destructive and exploitation potential to new categories of actors. Beyond nation-states, cyber technologies empower whole categories of hacktivists, terrorist groups, and predictably – private sector businesses. Where these businesses operate critical infrastructures, their awareness of risk factors and operational capabilities can exceed that of national governments. A second feature of this environment is the assembly, disassembly and re-combination of digital service providers, software companies and device fabricators – in a shifting ecosystem of old and new enterprise and company formations – as investors and entrepreneurs seek new market opportunities, launch new starts and dismantle failed businesses.

National governments seek to manipulate and reshape this global environment to their own economic and security ends. Conflict in cyberspace – over jurisdiction, data confidentiality, integrity, availability and over conditions of access – expands as does problematic attribution over particular events and trends. Authoritarian states and a diminishing number of democracies contend for control and influence in the global system. What possible strategies and options exist for Western democracies to defend their current positions and perhaps regain lost momentum in shaping the cybered future?

## Legacy Presumptions

It is commonly assumed that the success of authoritarian countries – most prominently China – but also countries such as Iran and North Korea – in generating cyber capabilities and successfully exfiltrating high value data and intellectual property (IP) - means that the freedom of action and advantages enjoyed by Western democratic nations are in eclipse. Russia is also of primary concern – though not for economic reasons. Further, the point is not simply that the democracies are going to be a diminishing minority among the world's nation states, but that the future poses a new challenge – where economic growth and technological dynamism characteristic of western capitalist countries may now be superseded by alternate governance models deriving from Asia. In addition, states not typically thought of as challengers to Western countries have gained an ability to leverage IT advances to disrupt or exploit infrastructures and digital services – posing a cyber as well as physical threat. This reality, among all others, has begun to reduce the West's confidence that it can compete effectively without a right-ward political turn — further



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055

undermining the old certainties of national security and a predictable international setting led by liberal capitalist democracies. Finally, the innovative capacities of firms based in the industrialized West are said to be diminished through predatory technology and IP acquisition processes leveraged by the government of China. As the new proto-hegemon arises, all others must adapt or perish in the face of its strategic preferences. [3]

This is a frightening vision. But is it accurate? And what does this say about the strategies still available to Western states? Is decline inevitable. This paper examines some aspects of this strategic dilemma, aiming to deconstruct some of the assumptions of this declinist frame of reference. It also seeks to define the space available for the democracies to save themselves and others whose world order preferences parallel their own. All may not be lost, but neither is change avoidable.

## How We Got Here

Western capitalist democracies advocated for – and fostered – the emergence of the cybered world. That world provided seeds that now empower authoritarian competitors. After all, the rise of cyber power asymmetrically advantages (rising) weaker states – allowing them to leverage dominant states' technical and economic models to launch growth-oriented competing strategies for themselves. This approach does not mimic western frameworks, it cherry-picks them in pursuit of mercantilist and exclusionary goals.

The Western vision of this broader distribution of technology, wealth creation, and independence was (and remains) that positive and mutual gain is possible through free exchange. In trade, global markets for digital services, and a sophisticated division of labor aligning production factors in MNE (multinational enterprise) systems of asset and value transfer, "all boats are said to rise together". A crucial enabler for this framework was the stability of great power politics reinforced variously by the Cold War, the post-Cold War, and global power dynamics favoring the dominance of the West. Access to resources and markets was secured behind the

[3] For an interesting analysis of Japan's hedging strategies for a rising China, see Ll. López i Vidal & Àngels Pelegrín (2018) "Hedging Against China: Japanese Strategy Towards A Rising Power", Asian Security, 14:2, 193-211, DOI: 10.1080/14799855.2017.1333983; for an older and less rigorous articulation of this idea, see Fareed Zakaria "A 'Hedge' Strategy toward China" Washington Post November 15 2010. (url: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/14/AR2010111403883.html) Accessed 25 September 2018.

defenses offered by US power. For much of the world this stability – even if viewed as problematic – became both familiar and a predictable backdrop for planning and investment.

Overtime, however, as US and western technological and economic advantages over rising powers diminished, the composition of production inside Western economies also began to change – generating unemployment, maldistribution of wealth, and political forces in opposition to open trade and immigration. Our current era is characterized by these forces – and by the reemergence of class, race, and geostrategic divergences of view that erode expectations of safety and security in the West. For China and other beneficiaries of the emerging technology and cyberspace landscape, however, optimism and future oriented visions of new status and opportunity abound. This thrust collides with recently resurgent Western suspicion and insecurities. For cyberspace, this means that a legacy of innovation and wealth creation may be producing a return to competition and concern with absolute – not relative –gains from trade. As the mercantilist strategies of China find success – and envy, Western nations may seek to close markets and production systems. Relative gains are either diminished – or not aligned with the established distribution of benefits to established constituencies within national borders.

Today globalized technology development cycles and cybered production processes no longer deliver predictable gains to western economies in the way they do to China and other emerging powers (at least, that is the emerging perception). This has led to a reduction in support for liberal and open trade, and to the emergence of a constituency that favors unilateralism and "brute" reciprocity over the current rules-based system governing world trade.[4]

## The Requirement for Strategy in a Cybered Environment

However, the discovery by Western countries that their advantages are no longer automatic need not mean inevitable decline. What it does signify is that the West needs to adopt explicit strategies for protection and catalytic investment – leaving behind "invisible hand" attitudes which

[4] Current trade disputes involving the United States and its principal allies (e.g., the European Union and Canada) exemplify this emerging trend. See Yasmeen Serhan "US Allies are helping Trump Undermine Global Trade", The Atlantic (https://www.theatlantic.com/international/archive/2018/06/europe-mexico-canada-trump/562382/) Accessed 25 September 2018.



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055

inhibit timely response to evidence of predatory behavior. Evidence of a geostrategic challenge by an emerging peer competitor requires a response at the *scale of the risks presented.*

Concerns with a downturn in the positive returns to technology investments and market participation need to be addressed by identifying their root causes. This does not mean that Western countries should turn a blind eye to violations of accepted trading system rules including intellectual property rights protections. It does mean that flexibility needs to be found through *a strategic redefinition of the rules* to protect those areas deemed to be central to active and beneficial participation in a cybered global economy. In other words, picking winners may be necessary – with all of the risk, misaligned incentives, and potential for corruption such a path engenders. The only question is, in what areas should we focus our attention.

Our rising competitors provide us ready guidance to the elements of the cybered world that may hold the key to shaping the global economic system in a Western friendly direction. National strategies that *leverage participation in technology research to "seed" the formation of business firms and wealth creation* are clearly ascendant. China has adopted this approach, setting stretch goals for progress (if not global dominance) in key technology areas seen as vital to preserving growth opportunities for domestic firms. That country's analysis may be flawed, but their pursuit of advantage through a deliberate and structured planning process is nonetheless validated by their recent success. China is not to be blamed for the refusal of others to take steps to recognize shifting conditions and areas where they can be disadvantaged. Rather than mimicking China's strategy, we need to take note of their actions, evaluate the impact of a relative (or absolute) loss of US and Western capacity in key technologies, and conduct a horizon scan on the risks of different states of the world where China's stretch goals are achieved (largely at our expense). Once identified, these cases can be ranked, analyzed and selectively countered using cyber and cross-domain capabilities. (See the schematic of this sort of ordered approach in Figure 1 below).

*Any counter-measures would of necessity need to be well coordinated, and multilateral.* A point to be noted is that, whichever strategy we choose, investments in science, technology and STEM education will empower populations to participate in an economy where income levels for the more educated are rising relative to those in less skilled or de-skilled occupations. We can help ourselves through a *rediscovery of the technical and educational excellence* that we more recently have taken for granted.

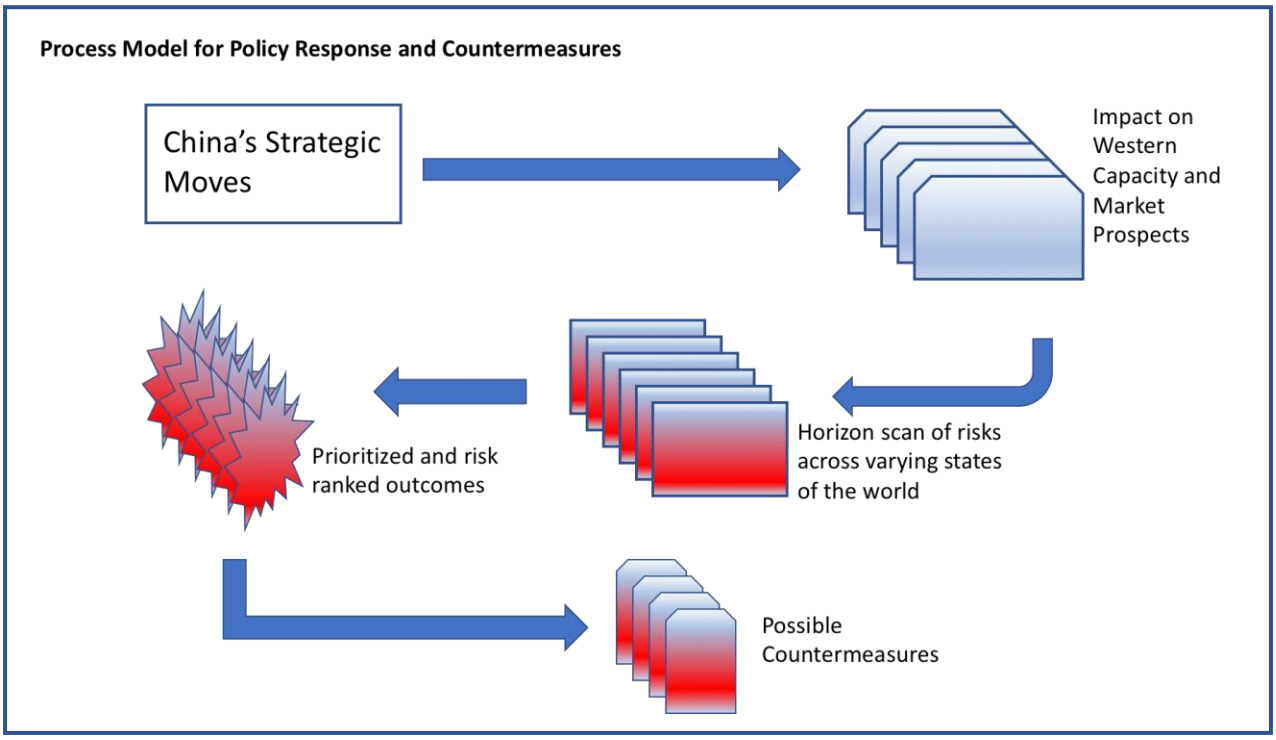



**Figure 1. Process Model for Policy Response and Countermeasures**

## China's Goals and Strategic Approach

The "Made in China 2025" program identifies a list of technologies and industries where China seeks not only a competitive position, but outright dominance. Targeted areas include[5]:

1) advanced information technology;
2) robotics and automated machine tools;
3) aircraft and aircraft components;
4) maritime vessels and marine engineering equipment;
5) advanced rail equipment;
6) new energy vehicles;
7) electrical generation and transmission equipment;
8) agricultural machinery and equipment;
9) new materials; and
10) pharmaceuticals and advanced medical devices.

[5] Office of the United States Trade Representative, *findings of the investigation into china's acts, policies, and practices related to technology transfer, intellectual property, and innovation under section 301 of the trade act of 1974* (Washington DC: Executive Office of the President, March 22, 2018), p. 19.



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055

For this analysis, two market impacts are important: first, is the impact of China's internal market on the setting of global technology standards; second is the explicit import substitution strategy adopted by China that violates WTO rules and disadvantages established industries in Western countries, potentially costing them both global market share and employment.[6]

China uses a number of mechanisms and policy tools to achieve its objectives. These include mandatory joint venture partnerships for foreign firms seeking to do business in China in designated industries;[7] loans at less than market rates to domestic manufacturers that create excess capacity (used for "dumping" product on international markets at lower than the cost of production)[8], regulatory barriers to foreign participation in leading infrastructure projects and government procurements; de facto designation of "national champions" in key technology areas – with supporting programs of investment, protection from foreign competitors, and subsidization of R&D activities.[9] An aligned foreign data and IP exfiltration campaign that supports the creation of new industrial competitors, and a myriad of parallel measures rounds out China's aggressive data and technology acquisition efforts.[10]

Needless to say, this activity also contributes to China's defense industrial capabilities, consistent with the military industrial complex approach adopted by that country – leveraging

---

[6] For a survey of key impacts, see the US-China 2017 Report to Congress of the US-China Economic and Security Review Commission, 115th Congress, November 2017. Chapter 4. "China's High Tech Development," pp. 507-537. (https://www.uscc.gov). Accessed 28 April 2017; and Jessica Myers, "How 'Made in China 2025' became the real threat in a trade war." Los Angeles Times 24 April 2018 [Briefing], http://www.latimes.com/world/asia/la-fg-china-2025-20180424-story.html; and, Scott Kennedy, "Made in China 2025," https://www.csis.org/analysis/made-china-2025. Accessed 28 April 2018.

[7] For an example of the arc of such a partnership, see Nicole Perlroth and John Markoff, "Symantec Dissolves a Chinese Alliance." New York Times 26 March 2012. https://www.nytimes.com/2012/03/27/technology/symantec-dissolves-alliance-with -huawei-of-china.html. Accessed 28 April 2018. The authors note Symantec's fear that continuing the joint venture would limit its access to classified US information. Also, see China Briefing: Challenges Facing German Investors 23 April 2018, https://www.china-briefing.com/2018/04/23/china-germany-relations-opportunities-emerge-investment-ties-grow-html. Commentators observe shifting regulatory schemas and threats to German intellectual property as berries to further investment.

[8] See Megan Geuss, "Chinese Solar Exports Fall in 2016 with global Anti-Dumping Measures," Ars Technica 27 February 2017, https://arstechnica.com/ 2017/02/Chinese-solar-exports-fall-in-2016-with-global-anti-dumping-measures/; and Matthew Wald, "US Imposes Duties on Chinese Wind Tower Makers," NY Times, 30 May 2012 https://www.nytimes.com/2012/05/31/business/energy-environment/US-imposes-duties-on-chinese-wind-towers.html. Accessed 28 April 2018.

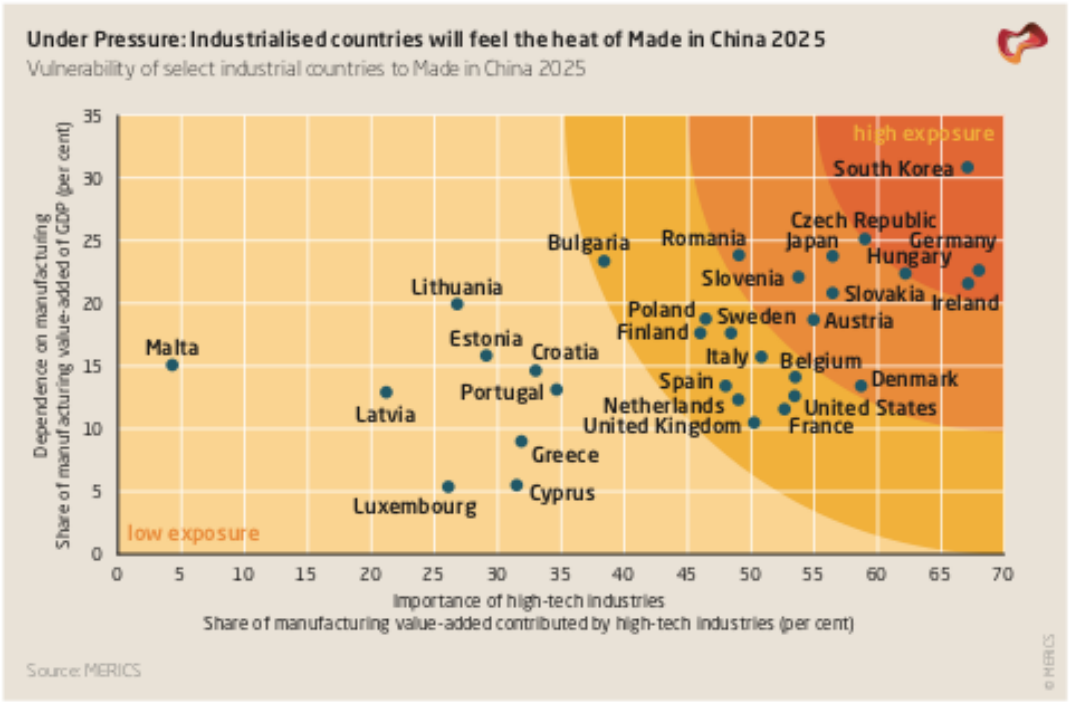
[9] See Harold Furchtgott-Roth, "Chinese Government Helps Huawei with 5G." https://www.forbes.com/haroldfurchtgottroth/2017/05/08/chinese-government-helps-huawei-with-5G/; and "EU Commissioner Attacks China's Telecom Subsidies" 27 March 2014 Financial Times https://www.ft.com/content/d6d0bec-b5cb-11e3-b40e-00144feabdc0 Accessed 28 February 2018

[10] Sam Frizell, "Here's What Chinese Hackers Actually Stole from U.S. Companies," Time 20 May 2014 https://time.com/106319/heres-what-chinese-hackers-actually-stole-from -u.s.-companies/. Accessed 28 April 2018.

civilian technology progress to jump-start secular improvements in weapon systems and platforms sophistication.

Countries affected by China's industrial policy approach are indicated on the graphic provided by the Mercator Institute for China Policy below.[11] Supply chain impacts are likely even more widespread. This is an example of a national government deciding to dramatically restructure a global cybered economic ecosystem – to its own ends. It is no surprise that other actors – perceiving a potentially negative impact on their own situations – will likely respond. The net effect of these iterative challenge and response cycles may not reflect the intentions of either initiating or responding actors. Indeed, identifying which is which is itself controversial.

Figure 1




MADE IN CHINA 2025 CHANGES THE TERMS OF THE GAME

[11] Jost Wubbeke, Miriam Meissner, Max J. Zenglein, Jacqueline Ives and Bjorn Conrad Made in China 2025: The Making of a High-Tech Superpower and the Consequences for Industrial Countries. Mercator Institute for China Studies, 2016), p. 7.



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055

## Conceptualizing the Link between Technology Competition and World Order Strategies

Technology alone does not create strategic potential or defense capabilities. Organization of capabilities, and the coordination of efforts with allies and partners can contribute important leverage useful for shaping risk assumptions and managing escalation.

Actors impacted by China's strategy are tightly interconnected. Indeed, entities *within China* may gain or lose depending on the opposition that China's policies provoke. This creates potential leverage that Western governments can use to complicate the implementation of China's import substitution strategy. *Selective engagement with Chinese firms* that creates an interest in positive and mutually advantageous economic interaction is an element of any sensible counter strategy. Carrots and sticks have a place at this level – where individual transactions – both procurement or mergers and acquisitions (M&A) are being evaluated.

The flip-side of a renewed emphasis on a rules-centric approach is red-lines that identify behavior and policies that run counter to a newly defined consensus on acceptable behavior. Like-minded governments interested in the survival of an open global trading order will need to *reconsider some long-settled rules* and judgments to avoid a rapid erosion of support for a world trade regime widely perceived as ossified and unable to respond to the challenge posed by China.

World order strategy requires the adoption by governments of *closer collaboration with industrial and technology businesses* based within their borders, but with global operations. Western countries that seek to maintain the competitiveness of their economies need to achieve consensus on new rules that preserve the viability of value creation in their own economies – and the accessibility of global supply chains that they require for profitability (and cost control). National targeting of these supply chains by China merits *coordinated reprisals at the same scale as the aggressive* – indeed predatory — campaigns that seek to undermine them – as is best exemplified by Made in China 2025. TPP countries, the EU, and other parties interested in open rules-based trade relations are the logical grouping for what amounts to a nascent countervailing coalition.

## The Limits of Strategy: Less Theory and More Plans and Practice

Strategy involves choice. Informed choices require systematic examination of decision dependencies in the short, medium and long term. Such a point of view is well known to military planners and grand strategists. We don't need a new grand strategy, however. What we need is a memory and a plan for a near term path forward. The historical legacy of US leadership during the Cold War and post-Cold War – while imperfect – allowed for global growth and prosperity almost unparalleled in the human experience. A memory for what prudential, consistent policies can deliver over decades long time horizons may help to reinforce cohesion among the like minded – especially in the face of short term reversals. That this prior period coincided with the emergence of the most destructive weapons ever created is an irony not lost on those with a long view of our limited powers of prediction.

Nuclear deterrence provided stability at the global level, interrupting the cycles of Great Power warfare that characterize the international system. This did not end warfare (obviously) or organized violence. It did, however, facilitate the emergence an internationaL order that allowed for mutual gain – and reinforced rules set that justified limited aims and preserved the possibility of positive change without the resort to violence. The US-led Western community deserves some credit for this achievement and legacy. Its preservation requires a strategy that reconciles a new global capability distribution that empowers authoritarians, while at the same time reducing support in Western nations for the very achievement that led to unprecedented economic growth and wealth creation.

## Options

Policy options for dealing with this emerging situation need to be flexible, multilateral, and to the greatest degree possible coordinated in terms of both timing and intensity of application. The environment for "easy alignment" among Western nations will be challenged by interest conflicts among historical allies – tied to desires for ongoing market access to China. Collective action by western states that allow the pursuit of objectives that preserve global supply chain flexibility and choice are most advisable as these minimize the effectiveness of likely "divide and conquer" countermeasures from China and its leading firms. Potential counters include:



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055

- Coordinated Counter-Measures – responses designed to protect domestic consumers and industrial enterprises from the impact of anti-competitive effects of China's policy approach
- Tactical "mirror-imaging" of China's Market Access Rules – A series of structured quid pro quo measures subjecting China-origin products and investments to reciprocal treatment depending on the openness of its markets to foreign competition and investment
- Investment Surveillance and National Champions: Targeted Industrial Policy Interventions for designated strategic areas
- Segmented Governance in the Information Sphere: Renewed attention to Internet governance and "public core" infrastructure issues
- Selective "Militarization" of Cyberspace and Reciprocal Cyber Domain CBMs: Defense Investments as a Catalyst
- Special rules for critical infrastructures – including collaborative active cyber defense for NATO and its partners

## Conclusions

The Western democracies confront the rise of authoritarian countries with considerable economic potential. Worse still, the democracies are interdependent with China for complex global product chains and technology development systems that yield both new products, but also markets for digital services. This means that whatever challenges are presented, the relationship between the West and its new Asian competitors – principally China – will be both cooperative *and* competitive. This constrains the use of countermeasures and complicates strategic choice. Nonetheless, some actions can be taken to reduce the gains from theft of intellectual property, or the adoption of mercantilist economic policies that threaten to damage industrial competitiveness in North America and Europe.

The list of six focus areas for policy identified above is not in priority order. A strategy needs to knit such activities together into coherent frameworks for defending access to technology markets and developmental processes for both products and platforms. For defense this means preserving industrial capabilities critical to weapon system and integrated platform development. For commercial activities this means preventing the leakage – or seeking to minimize the leakage and destruction – of core competencies held by named Western-based technology companies and their suppliers.

Some will dismiss the viability of this kind of approach, asserting that it amounts to "picking winners" in competitive markets — thereby negating the discipline of real competition. This is certainly a risk. Another risk is assuming that global technology markets can remain competitive when China adopts an aggressive technology acquisition strategy – alongside a mercantilist international trade approach that leverages IP theft and aggressive targeting of Western companies. Balancing these risks (among others) is the task of public and private sector stakeholders interested in reforming global economic governance to deal with the emerging challenge.



https://scholarcommons.usf.edu/mca/vol3/iss2/2
DOI: https://doi.org/10.5038/2378-0789.3.2.1055