

NexTW Column in Semiconductor - August 2024

Sovereignty in the semiconductor supply chain- Taiwan's role in the geo-technology battlefield

Sovereignty in the semiconductor supply chain- Taiwan's role in the geo-technology battlefield



Sovereignty in the semiconductor supply chain- Taiwan's role in the geo-technology battlefield

By Chung-Yi Lee

The concept of 'sovereignty' in the semiconductor supply chain has sparked significant debate. This article will first explain the semiconductor supply chain and then explore why 'sovereignty', traditionally a political term, is applied in this commercial context. Moreover, it addresses the role of Taiwan in the current technological battle between the US and China emphasizing the importance of robust technology manufacturing in this rivalry.

Global Value Chains Shape Semiconductor Manufacturing

Semiconductors, commonly known as "chips," are essential components that power electronic devices. Their applications span both civilian and military sectors. These crucial components are integrated into a diverse array of products, including computers, mobile phones, vehicles, and household appliances. Their manufacturing process is closely connected to the global value chain (GVC), indicating that semiconductor production is distributed across various regions worldwide, making it a cornerstone of globalisation. Supply chains, whether in the semiconductor industry or other sectors, function based on Ricardo's Principle of Comparative Advantage (Irwin, 2017). If a country excels in producing a specific type of product, it should focus on manufacturing that product to maximise profits. Most semiconductor design companies are in the US. American designers excel in semiconductor R&D and own critical intellectual property rights.

East Asia Dominance In Semiconductor Manufacturing

While American companies excel in semiconductor design, they do not handle production. The primary high-end producers, called foundries, are located in East Asia, with Taiwan Semiconductor Manufacturing Company (TSMC) in Taiwan and Samsung in South Korea being notable examples. TSMC and Samsung account for 70% of global semiconductor manufacturing (53.6% and 16.3%, respectively) (Financial Times, 2022). TSMC is the leading manufacturer of 'advanced logic chips' as of April 2024 and has the capacity for volume production of 3nm technology (N3) (TSMC, 2022). Samsung, on the other hand, is making significant efforts to catch up with TSMC. Samsung started volume production of 3nm chips in June 2022 (Hwang, 2023), a few months before TSMC. However, Samsung's yield rate was much lower than TSMC's. Therefore, despite Samsung commencing production earlier, it is actually TSMC that has maintained a much larger global market share in the advanced 3nm technology sector.

US-China Tech War Intensifies Focus on Semiconductor Sovereignty

How did the concept of 'sovereignty' become intertwined with the supply chain? It is closely linked to the notion of decoupling, particularly evident in the efforts of both the US and China. Both nations seek to decouple from each other, primarily motivated by concerns for national security. The movement towards economic nationalism accelerated with the onset of the trade and technology war in 2018. In the US, this trend was initiated by Trump's trade war and later reinforced by the Biden administration's export controls on strategic industries associated with China. This policy affects American companies and their international trade partners. In China, the goal to decouple is highlighted by initiatives such as Made in China (MIC). This bilateral intention to decouple underscores the complexities of global economic relations and the evolving dynamics of sovereignty in the context of supply chains. This policy's objective is to bolster China's own research and innovation capabilities. Notably, the inspiration for MIC came from Germany's 'Industry 4.0' (I40) strategy, a state-led initiative launched in 2013 aimed at maintaining German leadership in technology and mechanical engineering (Anonymous contributor, Background, June 2018). It's crucial to acknowledge that the Made in China (MIC) initiative is comprehensive in scope. Additionally, while the policy underscores the integration of IT and industry, it also aims

to enhance China's capabilities in innovation, quality, value, and environmentally friendly industrial practices. Notably, the cultivation of indigenous technology and innovation began after President Xi assumed office in 2013. This initiative aligns with Xi's vision for modernising China's military force, which includes reducing the number of military personnel and enhancing capabilities in 'smart warfare,' such as strategic and tactical missile operations, as well as cyber, space, and electronic warfare under the strategic support force. All these intentions of 'levelling-up' require China's technology development to rely more on indigenous technology because of the direct impact on national interests and security.

The Complete Ecosystem Behind Taiwan's Semiconductor Dominance

No matter how fierce the US and China are rivals in the field of semiconductors, neither can mass-produce advanced chips. As mentioned earlier, the key producer is TSMC, headquartered in Taiwan. There are several reasons why advanced semiconductor production in Taiwan is inimitable. Firstly, it stems from the strategic business decisions made by TSMC's former CEO, Morris Chang, in the 1990s. TSMC decided against branding any devices with its name and instead focused on supplying chips to major global brands, including Apple, Intel, Huawei (until 2020)¹, and Samsung. This decision reassured customers that they would not face competition from TSMC when contracting for chip design. The second reason is

¹ TSMC stopped servicing orders from Huawei in 2020 (Hille and Stacey, Financial Times, June 9 2020).

² Access to Intel was secured partly through the personal connection and professional background of Morris Chang (Wu et al, 2006:442).

TSMC's strong focus on research and development in manufacturing. TSMC has created a vast network that serves as a repository of chip manufacturing knowledge. This collective knowledge base is constantly evolving and updating in real-time, something companies like Samsung or Intel, which have fewer customers, may struggle to match. TSMC's extensive customer network is a testament to years of effort in earning and maintaining customer trust. Trust between designers and manufacturers is the final crucial element. To cultivate this trust, TSMC places great emphasis on exceptional customer care. In its early years (the early 1990s), TSMC underwent a series of rigorous certification procedures by major US semiconductor firms such as Intel.

Taiwan's comprehensive semiconductor ecosystem, with a deeply embedded supply chain, supports and enhances TSMC's operations.

This certification was essential in establishing customer faith and confidence in TSMC's manufacturing quality.² TSMC demonstrates its dedication to customers through personalized service, assigning a dedicated team to each customer. Engineers at TSMC concentrate exclusively on their specific projects, ensuring focus and efficiency. Engineer teams are not privy to production details from other sections. Moreover, Taiwan's comprehensive semiconductor ecosystem, with a deeply embedded supply chain, supports and

enhances TSMC's operations.

Taiwan's Semiconductor Industry Thrives under Democratic Principles

It is essential to understand that TSMC operates independently and is not a state-owned enterprise. Even though TSMC plays an indispensable role in advanced semiconductor manufacturing, the Taiwanese government does not dictate its investment or development strategies. As a democracy, Taiwan's government has limited control over business operations. Nevertheless, Taiwan is home to TSMC and a thriving semiconductor manufacturing ecosystem, with most high-skilled engineers being Taiwanese and advanced chip production centered in local foundries. It is because of these reasons, rather than any mandates from the Taiwanese government (which likely has minimal influence on TSMC and related semiconductor industries), that Taiwan's robust advanced semiconductor production will remain a key advantage in the ongoing geo-technological rivalry.

References

Anonymous contributor. (2018, June). Made in China 2025. Development Policy, Institute for Security and Development Policy. Retrieved August 10, 2023, from <https://isd.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf>

Financial Times. Samsung slips further behind TSMC in the chipmaking race. (2022, July 17). Retrieved July 22, 2022, from <https://www.ft.com/content/bb13d912-773a-4c1a-bf33-358b3c40ca5a>

Hille, K. & Stacey, K. (2020, June 9). TSMC falls into line with US export controls on Huawei. Financial Times. Retrieved June 6, 2023, from the Financial Times website

Hwang, J.-S. (2023, April 30). Samsung foundry backlogs top \$74.6 bn for logic chip biz goal. The Korean Economic Daily. Retrieved August 17, 2023, from The Korea Economic Daily website

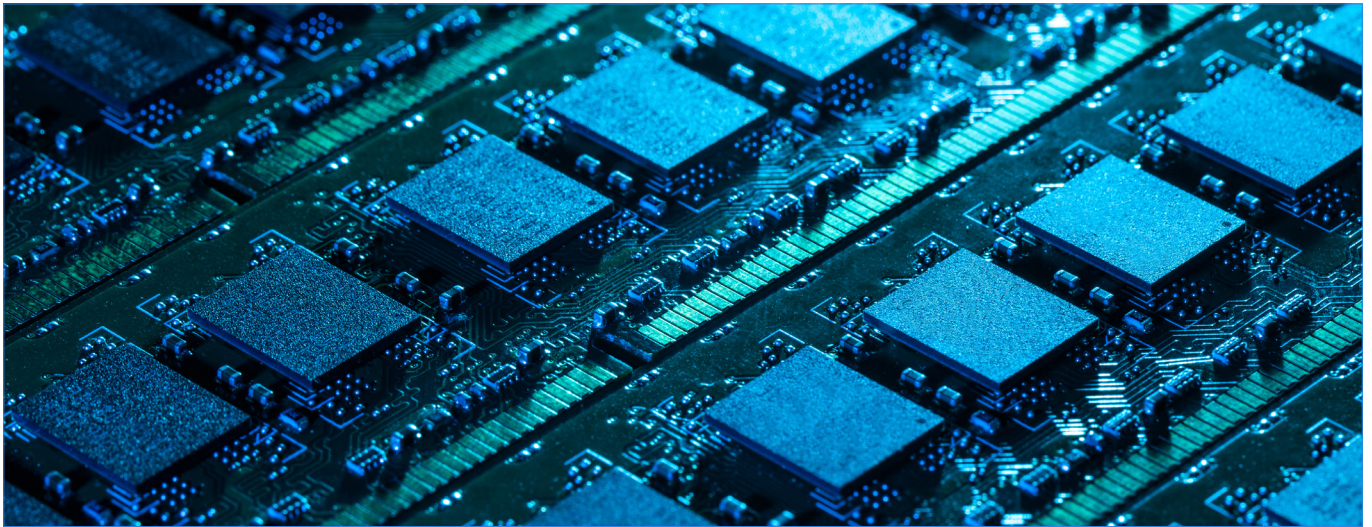
Irwin, D. (2017, April 19). Ricardo and comparative advantage at 200. Retrieved August 12, 2023, from the Center for Economic and Policy Research (CEPR) website

TSMC News. (2022, December 6). Retrieved February 4, 2023, from <https://pr.tsmc.com/english/news/2977>



**Dr. Chun-Yi Lee is
Associate Professor at
school of Politics and
International Relations,
University of Nottingham.**

She is also the Director of Taiwan Research Hub at Nottingham. Chun-Yi's first book was published by Routledge in 2011: *Taiwanese Business or Chinese Security Asset*. The book is under Leiden Series in Modern East Asia History and Politics. In 2010, Chun-Yi received the Economic and Social Research Council (ESRC) standard grant with Prof. Andreas Bieler on a three-year project, 'Globalisation, national transformation and workers' rights: An analysis of Chinese labour within the global economy'. In 2014, Chun-yi received a two-year research grant from the Chiang-Ching-kuo (CCK) Foundation in Taiwan in relation to 'Chinese Investment in Taiwan: Challenge or Opportunity for Taiwan's Industrial Development'. Chun-yi edited numerous books since 2018, most recently In 2023, along with Michael Reilly, Chun-yi edited a book: *China, Taiwan, UK and the CPTPP: Global Partnership or Regional Stand-off?* published by Palgrave. Currently, Chun-yi is working on her second single authored monograph on the topic of 'Sticky Decoupling: Geopolitics and Semiconductor supply chain'.



Sovereignty in the semiconductor supply chain- Taiwan's role in the geo-technology battlefield

By Chung-Yi Lee

The concept of 'sovereignty' in the semiconductor supply chain has sparked significant debate. This article will first explain the semiconductor supply chain and then explore why 'sovereignty', traditionally a political term, is applied in this commercial context. Moreover, it addresses the role of Taiwan in the current technological battle between the US and China emphasizing the importance of robust technology manufacturing in this rivalry.

Global Value Chains Shape Semiconductor Manufacturing

Semiconductors, commonly known as "chips," are essential components that power electronic devices. Their applications span both civilian and military sectors. These crucial components are integrated into a diverse array of products, including computers, mobile

phones, vehicles, and household appliances. Their manufacturing process is closely connected to the global value chain (GVC), indicating that semiconductor production is distributed across various regions worldwide, making it a cornerstone of globalisation. Supply chains, whether in the semiconductor industry or other sectors, function based on Ricardo's Principle of Comparative Advantage

¹ TSMC stopped servicing orders from Huawei in 2020 (Hille and Stacey, Financial Times, June 9 2020).

² Access to Intel was secured partly through the personal connection and professional background of Morris Chang (Wu et al, 2006:442).

(Irwin, 2017). If a country excels in producing a specific type of product, it should focus on manufacturing that product to maximise profits. Most semiconductor design companies are in the US. American designers excel in semiconductor R&D and own critical intellectual property rights.

East Asia Dominance In Semiconductor Manufacturing

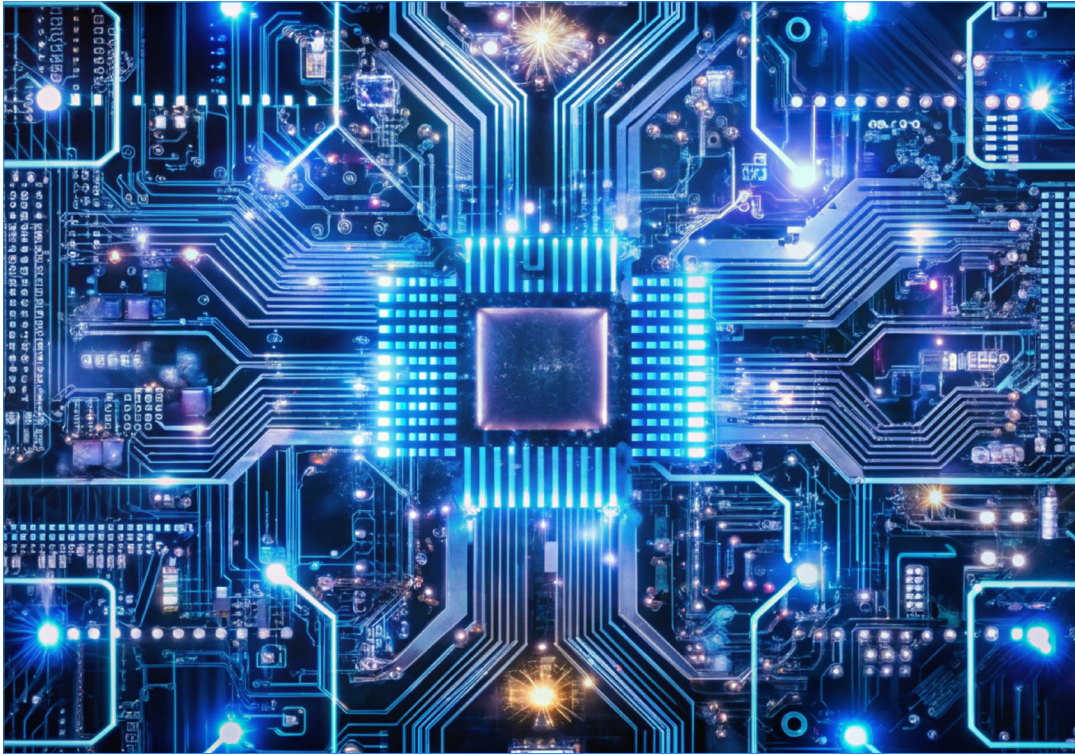
While American companies excel in semiconductor design, they do not handle production. The primary high-end producers, called foundries, are located in East Asia, with Taiwan Semiconductor Manufacturing Company (TSMC) in Taiwan and Samsung in South Korea being notable examples. TSMC and Samsung account for 70% of global semiconductor manufacturing (53.6% and 16.3%, respectively) (Financial Times, 2022). TSMC is the leading manufacturer of 'advanced logic chips' as of April 2024 and has the capacity for volume production of 3nm technology (N3) (TSMC, 2022). Samsung, on the other hand, is making significant efforts to catch up with TSMC. Samsung started volume production of 3nm chips in June 2022 (Hwang, 2023), a few months before TSMC. However, Samsung's yield rate was much lower than TSMC's. Therefore, despite Samsung commencing production earlier, it is actually TSMC that has maintained a much larger global market share in the advanced 3nm technology sector.

US-China Tech War Intensifies Focus on Semiconductor Sovereignty

How did the concept of 'sovereignty' become intertwined with the supply chain? It is closely linked to the notion of decoupling, particularly evident in the efforts of both the US and China. Both nations seek to decouple from each other, primarily motivated by concerns for national security. The movement towards economic nationalism accelerated with the onset of the trade and technology war in 2018. In the US, this trend was initiated by Trump's trade war and later reinforced by the Biden administration's export controls on strategic industries associated with China. This policy affects American companies and their international trade partners. In China, the goal to decouple

Taiwan's comprehensive semiconductor ecosystem, with a deeply embedded supply chain, supports and enhances TSMC's operations.

is highlighted by initiatives such as Made in China (MIC). This bilateral intention to decouple underscores the complexities of global economic relations and the evolving dynamics of sovereignty in the context of supply chains. This policy's objective is to bolster China's own research and innovation capabilities. Notably, the inspiration for MIC came from Germany's 'Industry 4.0' (I40) strategy, a state-led initiative launched in 2013 aimed at maintaining German



leadership in technology and mechanical engineering (Anonymous contributor, Backgrounder, June 2018). It's crucial to acknowledge that the Made in China (MIC) initiative is comprehensive in scope. Additionally, while the policy underscores the integration of IT and industry, it also aims to enhance China's capabilities in innovation, quality, value, and environmentally friendly industrial practices. Notably, the cultivation of indigenous technology and innovation began after President Xi assumed office in 2013. This initiative aligns with Xi's vision for modernising China's military force, which includes reducing the number of military personnel and enhancing capabilities in 'smart warfare,' such as strategic and tactical missile operations, as well as cyber, space, and electronic warfare under the strategic support force. All these intentions of 'levelling-up' require China's technology development to rely more on indigenous technology

because of the direct impact on national interests and security.

The Complete Ecosystem Behind Taiwan's Semiconductor Dominance

No matter how fierce the US and China are rivals in the field of semiconductors, neither can mass-produce advanced chips. As mentioned earlier, the key producer is TSMC, headquartered in Taiwan. There are several reasons why advanced semiconductor production in Taiwan is inimitable. Firstly, it stems from the strategic business decisions made by TSMC's former CEO, Morris Chang, in the 1990s. TSMC decided against branding any devices with its name and instead focused on supplying chips to major global brands, including Apple, Intel, Huawei (until 2020)¹, and Samsung. This decision reassured customers that they would not face competition from TSMC when contracting for chip design. The

¹ TSMC stopped servicing orders from Huawei in 2020 (Hille and Stacey, Financial Times, June 9 2020).

² Access to Intel was secured partly through the personal connection and professional background of Morris Chang (Wu et al, 2006:442).

second reason is TSMC's strong focus on research and development in manufacturing. TSMC has created a vast network that serves as a repository of chip manufacturing knowledge. This collective knowledge base is constantly evolving and updating in real-time, something companies like Samsung or Intel, which have fewer customers, may struggle to match. TSMC's extensive customer network is a testament to years of effort in earning and maintaining customer trust. Trust between designers and manufacturers is the final crucial element. To cultivate this trust, TSMC places great emphasis on exceptional customer care. In its early years (the early 1990s), TSMC underwent a series of rigorous certification procedures by major US semiconductor firms such as Intel. This certification was essential in establishing customer faith and confidence in TSMC's manufacturing quality.² TSMC demonstrates its dedication to customers through personalized service, assigning a dedicated team to each customer. Engineers at TSMC concentrate exclusively on their specific projects, ensuring focus and efficiency. Engineer teams are not privy to production details from other sections. Moreover, Taiwan's comprehensive semiconductor ecosystem, with a deeply embedded supply chain, supports and enhances TSMC's operations.

Taiwan's Semiconductor Industry Thrives under Democratic Principles

It is essential to understand that TSMC operates independently and is not a state-owned enterprise. Even though TSMC plays an indispensable role in advanced semiconductor manufacturing, the Taiwanese government does not dictate its investment or development strategies. As a democracy, Taiwan's government has limited control over business operations. Nevertheless, Taiwan is home to TSMC and a thriving semiconductor manufacturing ecosystem, with most high-skilled engineers being Taiwanese and advanced chip production centered in local foundries. It is because of these reasons, rather than any mandates from the Taiwanese government (which likely has minimal influence on TSMC and related semiconductor industries), that Taiwan's robust advanced semiconductor production will remain a key advantage in the ongoing geo-technological rivalry.



AI x Digital Sovereignty x Economic Security

Definition of Digital Sovereignty

How Insecurity Fuels the Push for Sovereign AI

The concepts of insecurity and de-risking are closely linked. As nations become more aware of the vulnerabilities posed by data and AI, the focus has shifted toward managing key points of control. In particular, data storage and data processing have emerged as areas where governments can exert some influence. By controlling where data is stored and processed, countries aim to reduce the risks associated with external dependencies.

De-risking comes from the concept of insecurities, and these are actually intertwined.

Kai-Chi Chang
School of Law, Soochow University

The Evolving Role of Data

Traditional Perspectives on Data Sovereignty

Traditionally, discussions on data sovereignty revolve around the circumstances in which states should assert control over data, particularly from regulatory and enforcement standpoints. These conversations often aim to justify governmental actions related to personal data protection and privacy, which are fundamental rights that states have a duty to uphold. For a country to exert jurisdiction over data, it must be stored within its borders, allowing governments to exercise control and safeguard these rights. The development of regulations like the GDPR underscores the link between data sovereignty and the protection of fundamental rights.

The Evolving Role of Data in Digital Economies

In the broader context of digital economies, the role of data is evolving significantly. No longer just an asset to be stored, data is increasingly regarded as a raw material, particularly in applications like artificial intelligence training. In this sense, data serves as a foundational element/raw material within a supply chain, where its value emerges not from mere possession but from processing and utilization.

Data is not the subject of development but rather serves as raw material for training and the entire supply chain.

Kai-Chi Chang
School of Law, Soochow University

Historically, countries have claimed sovereign rights over natural resources; similarly, states may seek control over data as a crucial economic resource. This perspective emphasizes the need for countries to harness data to generate new economic opportunities and revenues.

Varying Priorities in Digital Economic Security

The rising discussion of data sovereignty highlights the challenges faced by countries that overly rely on foreign entities. In the EU, sovereignty is increasingly framed as jurisdictional control rather than citizen empowerment, with a strong focus on enhancing competitiveness through AI technologies. The EU

seeks to assert its digital sovereignty by reducing dependence on US tech giants like Amazon, Google, and Microsoft, which currently manage 90% of the EU's data.

Similarly, Japan faces challenges in data center development, where over-centralization in regions like Tokyo and Osaka poses risks due to natural disasters and geopolitical instability. To address this, Japan is promoting decentralization to enhance resilience.

These issues underline the global need for strategic measures to safeguard digital infrastructure and reduce reliance on dominant external actors in the AI and cloud computing landscapes.

Diverging Approaches to Digital Economic Security

Diverging approaches to digital economic security are shaped by differences in infrastructure investment, data governance, and policy frameworks. Countries prioritize securing digital infrastructure, managing data flows, and creating policies that safeguard economic interests, reflecting varied national strategies in response to global technological challenges.

Digital Infrastructure

To enhance its AI capabilities, the EU is investing heavily in quantum technologies, recognizing the synergy between quantum computing and AI solutions. This focus is outlined in the EU's Digital Decade strategy, which sets ambitious goals for cutting-edge quantum advancements by 2030. Quantum AI is an emerging sector

where these technologies converge, and the EU aims to position itself as a global leader in this space.

To lessen its dependence on U.S. hyperscalers, the EU introduced the GAIA-X initiative, a sovereign cloud project designed to unite European cloud providers into a competitive alternative to dominant U.S. companies like Amazon and Microsoft. However, despite these efforts, GAIA-X has struggled to achieve meaningful progress, with many participants withdrawing due to challenges in fostering interoperability among smaller European firms.

Data Governance

Japan's "Data Free Flow with Trust" initiative offers a promising framework for addressing the challenges of data sovereignty in the digital age. This model promotes cross-border data flows while addressing security and privacy concerns by emphasizing the need for a trusted environment.

To facilitate global data free flow, effective data governance is crucial. Regulations like the EU's General Data Protection Regulation (GDPR) have set important benchmarks for data privacy. However, there is growing recognition that regulation alone may not be enough. Many believe that complementary strategies, such as industrial policies and proactive measures, are needed to protect digital ecosystems and ensure secure, free data flows worldwide.

Policy Framework

Despite the perception that the internet transcends borders, data is still physically stored and processed in specific locations, giving countries jurisdiction over that data. Sovereignty still applies, and nations exercise control within their territorial space. Although the internet feels boundless, data remains subject to the laws of the countries where it is stored.

The EU's Strategy to Reclaim Data Sovereignty

For the EU, digital sovereignty is particularly important due to its reliance on US companies.

Currently, 90% of the EU's data is managed by three dominant US cloud hyperscalers: Amazon, Google, and Microsoft. As European firms increasingly digitize, this dependency is becoming more pronounced. In the context of the AI supply chain, cloud computing is poised to become a significant competitive bottleneck, further deepening the EU's reliance on these US firms unless proactive measures are taken to change the trajectory.

EU's Efforts to Protect Its Data

Traditionally, the EU has focused on regulation to safeguard its data, as seen with the General Data Protection Regulation (GDPR). This law aims to enforce European values and standards on the data processing of EU citizens, regardless of where that data is handled. However, a growing debate suggests that regulation alone may not be enough. There is increasing consideration of whether more

robust measures, possibly through industrial strategies or other approaches, are needed to ensure stronger control over Europe's digital future.

EU Obsession with the Brussels Effect

In recent years, the EU has been highly proactive in passing a wide range of legislation, not only focused on personal data protection, such as the GDPR, but also targeting digital competition, online safety, the promotion of data flows within Europe, and various cybersecurity laws. European policymakers often see this as a successful strategy, proudly citing the "Brussels effect"—the idea that foreign companies adopt European standards when operating globally. Moreover, EU regulations frequently serve as benchmarks for other countries developing their own frameworks.

Growing Concern about Data Regulation in Europe

There is increasing concern over the trend toward heightened data regulation in Europe.

1) Market Concentration

One significant issue is market concentration, particularly in cloud computing, where a few hyperscalers dominate. This raises concerns about resilience and the EU's vulnerability to foreign government influence. Despite attempts to introduce digital competition laws aimed at opening the cloud market, success has been limited. New competition is more likely to come from American companies rather than European

ones due to the current business environment in Europe.

2) Global Regulatory Landscape

Europe is not alone in seeking to regulate data flows; many countries assert their right to control data within their jurisdictions. A particular concern is the US Cloud Act, which allows US authorities to access data from companies with minimal connections to the US. In response, the EU has enacted laws to prevent European firms from complying with the Cloud Act, creating conflicting legal obligations that complicate business compliance. Additionally, movements within the EU aim to exclude sensitive data from US jurisdiction, leading to stringent requirements such as storing data solely within Europe and ensuring data management companies are entirely European-owned and operated.

3) Challenges from Non-European Companies

Most Western, like-minded democratic countries recognize the need for pragmatic data protection standards. However, there are concerns that the EU's approach may be becoming overly dogmatic. The United States has made considerable efforts to align with EU data protection standards, but if European courts continue to find these efforts insufficient, it raises questions about how much further the US can realistically go. Legislative changes in the US could address these issues, but navigating the current political landscape makes this a challenging endeavor.



There is growing apprehension that large non-European companies may sidestep European regulations due to their size and influence. Ongoing disputes with companies like Twitter and Telegram highlight concerns that American firms are not fully complying with EU laws, particularly under the Digital Markets Act.

4) Disparity Between EU and Non-EU Standards

Another important factor is that the EU often imposes stricter conditions on foreign countries receiving data than it does on member states. Within the EU, free data flows are generally guaranteed, even though some member countries do not fully adhere to EU fundamental rights regarding data protection, particularly in areas like law enforcement and intelligence gathering. Consequently, various international mechanisms are being explored to facilitate free data flows that extend beyond the confines of the GDPR and the EU framework.

5) Challenges to Alternative International Networks

While these alternative international networks are emerging, it is unlikely that any will gain significant traction.

For most American firms, the EU remains their largest foreign market, accounting for approximately 25% of their international revenues. Many of these alternative frameworks still contain exceptions for domestic public policy objectives, which can effectively reintroduce GDPR-like standards through indirect means.

Given these complexities, the most viable path forward may involve convincing the EU that the GDPR is too stringent and may require revision. This could help create a more balanced approach that facilitates both data protection and international cooperation.

6) Impact on Innovation and Entrepreneurship

Arguably the most critical issue for the EU's long-term future is the potential negative impact of regulation on innovation and entrepreneurship. A recent report by a former Italian prime minister attributes the EU's slow productivity growth to an overreliance on regulation as a problem-solving tool, recommending a period of deregulation and simplification to foster innovation.

Japan's Data Free Flow with Trust (DFFT) Initiative

Japan introduced the concept of "Data Free Flow with Trust" (DFFT) during the G20 Osaka Summit under former Prime Minister Shinzo Abe. This initiative seeks to create a trusted environment for the free flow of data across borders, reflecting Japan's commitment to global digital cooperation while ensuring that data is managed securely.

• Key Challenges

1. **Sovereignty and Data Control:** In Japan, discussions about sovereignty are typically limited, yet the growing importance of data governance has sparked debates around government control versus private sector autonomy. Japan is grappling with how much authority the government should have over private data held by companies. Defining the boundaries of this control remains a key challenge.
2. **Trust as a Foundation:** The principle of DFFT emphasizes trust among various stakeholders—between the private sector, government, and international partners. Building this trust requires open, transparent, and candid discussions. However, translating trust into actionable frameworks is a major obstacle for Japan and its global partners.
3. **Operationalizing DFFT:** The operationalization of DFFT remains an ongoing challenge. Despite widespread support for the concept from leaders like Japan's Digital Minister, Taro Kono, and international counterparts, real progress has been slow. While there have been numerous agreements and declarations of intent, turning DFFT into concrete, actionable policy has proven difficult.

The initiative represents Japan's attempt to navigate the complexities of digital sovereignty while fostering international cooperation in a way that balances security and economic openness.

Japan's Data Free Flow with Trust (DFFT) initiative is an ambitious attempt to lead global discussions on data governance. However, the real challenge lies in turning the concept into a practical framework that can be implemented both domestically and internationally. Achieving trust, while essential, requires more than dialogue—it requires concrete steps to bridge the gap between government control, private sector autonomy, and international agreements.

The Challenges of Implementing Policy

To be continued...

International Collaboration

As we consider economic security,

the concept of de-risking becomes critical. Countries must carefully evaluate their partnerships in developing digital economies, which may lead to the formation of distinct tracks or blocs with varying business models. A more sensible path forward

may involve adopting a multilateral and open approach.

While this may not perfectly address many countries' concerns, it acknowledges the reality that cross-border data flows are essential for modern commerce. Cooperation and the establishment of common standards among multiple countries will be vital.

The Economic Value of Free Data Flows

As countries grapple with economic security in the digital landscape, concerns about interruptions in data flows and supply chains become paramount. Just as chips are subject to export controls, data flows may face similar regulations that could hinder business operations.

Data Free Flow with Trust (DFFT) launched by Japanese Prime Minister Shinzo Abe during the G20 Osaka Summit. This initiative highlights the importance of data flow in a trusted environment.

The principle of Data Free Flow with Trust underscores the necessity of trust among various stakeholders. This includes trust within companies, between government and industry, and among like-minded countries.

To cultivate this trust, sincere and candid discussions are essential.

From the perspective of the economic importance of free data flows. This is especially relevant for Europe, where concerns about low productivity and stagnant economic growth are on the rise. Europe's share of global GDP continues to decline year after year, underlining

the need for greater openness and collaboration in the digital economy.

The economic importance of free data flows for every country is incredibly high ... particularly for Europe, where we have this increasing concern about why productivity and economic growth is so low.

Zach Meyers
Centre for European Reform

For Taiwan, the principles of Data Free Flow with Trust (DFFT) hold important implications. The core idea is that free data flows can occur even with partners who may not be fully trusted, as long as a sufficient level of openness is maintained.

More trust, more openness. Very simple.

Hosuk Lee-Makiyama
European Centre for International Political Economy

This concept reflects a practical conditionality often highlighted by government officials and trade negotiators. For instance, Japan and the EU exemplify this principle through their mutual, unconditional access to each other's data.

Mutual Interdependency as Leverage in Global Cooperation

Rethinking data sovereignty involves acknowledging that while states desire control, it is no longer feasible for them to dominate every aspect of data management, including storage and processing. This reality

parallels the business landscape, where no single entity can possess all the data or computing power necessary for operation.

Take GAIA-X as an example, which is designed to foster interoperability among European cloud providers and has struggled to produce significant results, with many companies withdrawing due to the difficulty of aligning diverse cloud services.

This highlights the necessity of collaboration, as interdependency in the digital landscape is a reality. The involvement of US companies in GAIA-X, though controversial, reflects a pragmatic acknowledgment of the scale-driven business models that US hyperscalers like Amazon and Microsoft employ. These companies leverage their massive primary businesses to offer low-cost cloud services, quickly achieving market dominance. European firms, lacking comparable scale, find it difficult to compete under the same model, underscoring the need for cooperation rather than isolation.

While US companies play a crucial role in GAIA-X, the initiative still faces obstacles. Achieving interoperability standards across different providers has proven complex, and the development of uniform standards remains elusive. The reality is that no single region or set of companies can fully operate independently, making collaboration essential for success in the global digital economy..

...having standards for interoperability and cloud computing is a really difficult thing to achieve when the services that different companies offer are not the same

Zach Meyers
Centre for European Reform

Lessons from the UK's Sovereignty Debate

Considering the question of data sovereignty, the UK's experience with Brexit offers a valuable lesson. As someone from the UK, I have witnessed how the sovereignty debate led to the country's withdrawal from the European Union—a decision that many now regard as neither sensible nor successful. Brexit stemmed from a belief that sovereignty is an all-or-nothing concept, achievable only through complete control and isolation from external negotiation.

However, this approach ignores the realities of an interdependent world. True sovereignty, in today's context, requires a willingness to compromise. Stubbornness in the name of control risks undermining the very autonomy we seek to protect.

Brexit was the result of a discussion where sovereignty was thought about as something that is black and white, and the only way to get it is to completely take back control... That's not the reality of a mutually interdependent world. ... the best way to protect sovereignty is to recognise that you have to compromise and not to be too stubborn.

Zach Meyers
Centre for European Reform

Digital Sovereignty is not Protectionism

Despite the emphasis on data sovereignty, many countries are open to developing international partnerships, offering a more optimistic outlook for those concerned that digital sovereignty equates to protectionism.

First of all, recognizing dependencies. For example, the EU can build leverage by taking the approach that several East Asian countries have taken of becoming an indispensable partner in certain parts of the technology stack, rather than attempting to control all aspects. This approach requires accepting certain dependencies, such as in cloud computing, while focusing on Europe's strengths, like high-end chip-making tools.

Cooperation in the Digital Economy: Bridging Data and Computing Gaps

As countries around the world increasingly engage in digital economy cooperation agreements and free trade initiatives, a key theme that emerges is the imbalance in resources among nations—some are rich in data, while others possess significant computing capabilities.

For instance, countries with smaller populations inevitably generate less data compared to those with larger, more active populations. In such cases, nations that are rich in computing power but limited in data production can benefit from cooperation. However, computing power alone is not sufficient without the data required for training, processing, and deriving value from these resources. On the other hand, having abundant data without the necessary computing infrastructure offers limited advantages.

This disparity in resources presents an opportunity for cross-border collaboration. Southeast Asian countries, for example, are developing cooperative models where those with advanced computing technologies can make use of the vast data produced in other nations. Since each country has its own distinct economic structure and infrastructure, these collaborations can be tailored to maximize mutual benefits, fostering innovation and progress in the digital economy.

Barriers to Break Through

While a global data-free flow framework offers significant economic benefits, there are critical challenges that need to be addressed before cooperation can be fully realized.

Operationalizing DFFT

The concept of Data Free Flow with Trust (DFFT) faces significant challenges, particularly in its operationalization. Much like the broad and often ambiguous notion of a "free and open Indo-Pacific," DFFT remains a widely discussed but poorly defined idea. The practicalities—its implications, costs, and opportunities—are still difficult to grasp.

Despite numerous agreements and statements from global leaders, the concrete steps required to turn these discussions into actionable policies remain elusive, highlighting the complexities of moving from principle to practice.

If we're looking at a trend where regulations are becoming harmonized or have already been implemented uniformly across certain areas, that would be something worth discussing. However, as of now, I don't think we're seeing that trend yet.

Kai-Chi Chang
School of Law, Soochow University

To move toward a harmonization of data regulations, it does not yet align with the current reality. Today, data governance remains fragmented, and the prospect of a uniform global

regulatory framework is still distant.

Here are the key issues that need to be addressed to facilitate a more effective and secure global data free flow:

The Challenge of Unified Regulations for Personal and Non-Personal Data (free flow)

Laws and regulations are deeply influenced by the cultural backgrounds and contexts of each country, reflecting their distinct values—especially regarding personal data. For instance, many may wonder why Europeans place such a strong emphasis on data protection, a concern that might seem puzzling or excessive to those from other regions. However, this focus stems from deeply rooted cultural values that have shaped Europe's regulatory approach.

While nations uphold different values, there is potential for convergence through cooperation. The aim should be to harmonize regulatory frameworks by recognizing what is important to each country while preserving the unique cultural values that inform these regulations. By respecting others' priorities, we can find ways to adapt our policies without compromising our own principles.

The Ambiguity Between Personal and Non-Personal Data in Europe (free flow)

The distinction between personal and non-personal data remains highly ambiguous and undefined in Europe. As a result, businesses often err on the side of caution, treating all data as personal. While this

¹ They end up treating all data as if it's personal data, which naturally kind of increases the cost and complexity of doing business in Europe.

approach may reduce legal risk, it also significantly increases the cost and complexity of doing business within the European market.¹

You end up in a situation where data is kind of mixed together and there's not much you can do about it.

Zach Meyers
Centre for European Reform

This issue is becoming increasingly problematic for two main reasons.

First, there is a growing recognition within Europe that personal data regulation is extremely intricate. In response, efforts are underway to promote the commercialization of industrial or non-personal data, with the aim of giving Europe a competitive advantage in that sector. The goal is to facilitate data transfers to entities that can derive the most value from it. However, the lack of clear boundaries between personal and non-personal data undermines these efforts, making it more difficult to capitalize on non-personal data effectively.

Second, this ambiguity poses particular challenges in areas like AI training. While legal professionals may focus on the precise definitions of personal and non-personal data, in practice, it is nearly impossible to design AI models that adhere strictly to these legal distinctions. The result is often a blending of data types, with little that can be done to fully segregate them.

You end up in a situation where data is kind of mixed together and there's not much you can do about it.

Zach Meyers
Centre for European Reform

Pathways for Taiwan's Future

Risk Management Considerations for Businesses in Cross-Border Operations

For businesses engaging in cross-border operations, a risk-managed approach is essential. Regulatory risk, in particular, should be a primary consideration. As businesses expand internationally, they are exposed to legal and regulatory frameworks in multiple jurisdictions, each presenting its own set of challenges.

Governments also play a crucial role in shaping the business landscape.

For companies in Taiwan, it is vital to first ensure full compliance with domestic regulations. A clear understanding of the regulatory environment at home is the foundation upon which successful international expansion can be built. However, understanding foreign regulations is only one part of the equation.

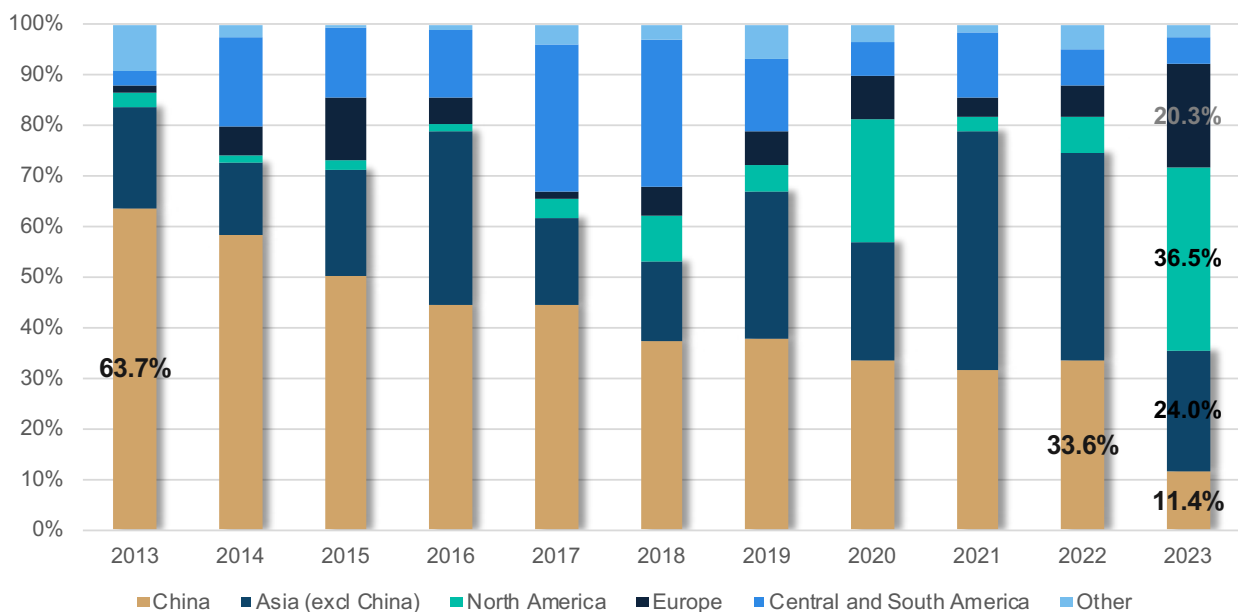
In today's geopolitical climate, economic security concerns and geopolitical dynamics increasingly influence business decisions. For example, it was once assumed

that free trade in semiconductors would remain unaffected due to agreements like those governed by the World Trade Organization (WTO). Yet, national security concerns have shifted the landscape, with countries now prioritizing partnerships with like-minded nations over global free trade.

These geopolitical shifts have significant implications for how businesses choose their markets and partners. By carefully assessing regulatory and geopolitical risks, companies can chart a clearer path for international expansion and ensure long-term success in foreign markets.

Responses to Geopolitical Hits are Industry Varied

Share of Taiwan Outbound FDI by Destinations



3 Pillars of Generative AI

