What is 'national' security in a globally connected digital economy?

WORKSHOP PROCEEDINGS

Internet Governance Project

www.internetgovernance.org

Table of Contents

Introduction

Dr. Karim Farhat, Assistant Director, IGP

During the pandemic, my dissertation analyzed how the US cybersecurity regime was being driven by the threat of China. A bipartisan alliance of China hawks was promoting the notion that all Chinese Information and Communications Technologies (ICT) are Trojan horses that will be used to undermine US national security. At the time, one would have been tempted to dismiss the trend as an ideological distrust of globalization. But listening to countless Congressional hearings made me bet that the incoming Biden Administration would perpetuate this narrative. Today, the securitization of ICTs has indeed turned out to be a consistent and bipartisan trend across both administrations. Increasingly, "Bidenomics" looks like protectionism with a social agenda. It continued some of the same policies as the Trump administration with the assumption that a regime of allies could somehow contain China's economy.

I am convinced that if the United States can one day regain its preeminent role as a bastion of freedom, prosperity, and abundance, a blue or red White House matters little. What does, is the long-term strategy adopted to handle the world's most important bilateral relationship. And it starts by addressing the false narratives in this dysfunctional couple.

In 2022, my mentor and boss, Dr. Milton Mueller referred to the fusion of a state's power and security with economic development in the digital economy as *digital neo-mercantilism*. On November 10, 2023, we convened a balanced meeting of experts to make the public aware of this trend, and to subject many of its premises to critical examination. We prepared and edited this summary as a factual account of what occurred during the workshop. What follows is a summary of those discussions validated by workshop participants for accuracy. It starts with opening remarks from IGP's founding Director Dr. Milton Mueller.

Opening Remarks by Dr. Milton Mueller

The digital economy is globalized. It relies on Internet connectivity, common operating systems and software applications, and a multinational supply chain for semiconductors and digital devices. Complementing and fueling this shared computational infrastructure and transnational data flows are transnational capital flows, which finance research and development and invest in new online services and products.

That globalized digital economy is now becoming an instrument of geopolitical competition. The US-China rivalry was the main catalyst, but not the only one. Policymakers are advancing a more general linkage between the digital economy, national security and national sovereignty. This linkage encourages nationalistic interventions in the digital economy. And in fact, practically all digital goods, services and technologies can contribute some way, however indirectly, to military power as well as economic benefit, and thus can be considered dual use.

This fusion of ICT and national security policy greatly expands the scope of national security. Threats are no longer defined as armed attacks or emergencies that threaten the existence of the state. They now can emerge from the semiconductor trade, from the extraction and distribution of minerals, from private business's decisions to buy network infrastructure from foreign firms. Threats can also be seen in incoming and outgoing capital investment, either because of fears of foreign control, foreign acquisition of advanced technologies, or because we fear that the networks and applications will be used as tools of espionage or ... mind control!

The equation of digital goods and services with national security threats is politically consequential. It obliterates the line between civilian and military uses, making practically everything we do within the digital ecosystem subject to surveillance, economic regulation, and export and import restrictions. Restrictions imposed in the name of national security take priority over other claims, and face fewer democratic checks and balances. Free trade in ICT goods and services, and its supporting infrastructure of open, global interconnection and the free flow of data, are casualties of this linkage. It encourages nationalistic and protectionist interventions in the digital economy, and

rolls back or abandons the international agreements meant to support nondiscriminatory, global exchanges.

We can see the new logic in action by reviewing an extensive (but not exhaustive) list of policy measures enacted by the United States alone from 2018 to October 2023. The US is the most extreme example because of its purported rivalry with China, but similar lists of other countries' measures could be found:

- April 2018: Export controls on semiconductors imposed on ZTE
- August 2018: The Foreign Investment Risk Review Modernization Act expands the remit of the Committee on Foreign Investment in the U.S. (CFIUS) authorizing it to detect foreign investments in "emerging technologies;" the foreign entity need not take majority control
- August 2018: Section 889 of the 2019 NDAA prohibits procurement of equipment and services by 5 named Chinese ICT companies and forbids federal agencies from working with any contractors using their ICTs.
- May 2019: Huawei is added to the entity list, preventing it from acquiring US-origin chips or any chips reliant on US intellectual property. The objective of this action was not to address a cybersecurity threat but to cripple Huawei economically.
- May 2019: the FCC denies China Mobile its Section 214 authorization, which it needs to operate in the U.S. This decision was made after sitting on its application for nearly a decade
- November 2019: CFIUS initiates a retroactive review of ByteDance's acquisition of Musical.ly, the app which became Tiktok, two years after the fact.
- March 2020: Secure and Trusted Networks Act (2020) expands the US government's list of "untrusted vendors," naming 9 Chinese firms and Kaspersky. The Act authorizes expenditure of $3 billion to "rip and replace" Huawei equipment in rural telecom networks
- December 2020: The FCC revokes China Telecom's Section 214 authorization, preventing it from continuing to operate telecom services in the US
- March 2022: The FCC denies authorization to a US-owned cable linking the US and Hong Kong because of minority ownership by a Chinese firm. (*Pacific Networks Corp. and ComNet (USA))*
- October 2022: Export controls on semiconductors. The purpose is to hobble China's tech development over the long term, not to address a direct military threat.

- August 2023: Treasury Department NPRM proposing limits on outgoing investment (August 2023). The controls address three broad categories of "national security technologies," two of them (semiconductors and microelectronics; artificial intelligence) central to the digital economy.
- October 2023: As news of work-arounds spread, U.S. export controls on semiconductors to China are tightened.

These new barriers and controls are global in their effect, but were also supplemented by five Executive Orders characterizing trade in digital goods and services as subject to a "national emergency." That claim justified intervention by the executive branch under the terms of the International Emergency Economic Powers Act (IEEP). Between 2019 and 2021 five Executive Orders – from both the Trump and Biden administrations – invoke the IEEP.

- EO 13873 – Supply chain
- EO 13942 – Banning Tiktok
- EO 13943 – Banning WeChat
- EO 13971 – Banning Chinese software applications and restricting export of data to adversaries
- E.O. 14034 – Evaluating the risk of connected software applications, and giving the Commerce Secretary the power to prevent any ICT transactions with Chinese firms.

The premise underlying this flurry of EOs, sanctions, and regulatory actions was summarized in this paragraph that is used by several of them in both the Trump and the Biden administrations:

"the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."

Note how all these EOs group "national security, foreign policy, and economic objectives" together. The digital economy should be subordinate to military defenses and forms of weaponization required to participate in Great Power conflicts in cyberspace. Note also the massive transfer of power from the people (acting in the market) and the legislatures (elected by the people) to the executive branch (specialized agencies, interagency committees, the President, the Departments). We need to subject this trend to critical analysis and that is why we convened this workshop.

Session 1: National Security and Tolerable Risks in ICTs

The first session asked: When and how do Information and Communications Technology interactions among the market economies of the US and China constitute a national security threat and when do they not? Related questions included: when ICT trade with an adversary nation is simultaneously mutually beneficial and raises potential security risks, how should the two be balanced? Are there identifiable
thresholds at which ICT products and services trigger national security concerns? In exploiting ICT vulnerabilities for espionage or attacks, how much difference does the national origin of the device/software vendor make? How can policymakers differentiate special interests seeking protectionism from actual national security threats?

Exploration of these questions began with claims by some participants that the internet and cybersecurity threats are far more central to the functioning of our economies than they used to be. Some characterized these threats as "existential." While it is true that we are more dependent on information systems, very few cyber threats pose threats to the entire social system. Most are minor and localized in effect, and there is no evidence that states can control or magnify the kind
of cyber threats needed to rise to an existential level. A discussant said, "Hyperbolic descriptions of existential crises aren't helpful. We can't both be part of a global digital economy and also live in perpetual fear of it."

Eventually, this led the participants to recognize and accept the inherently dual-use nature of ICTs and work within those parameters (see conclusions, below). The question of how to separate genuine national security claims from protectionist economic lobbying was not resolved. There was an assertion that "the line between national security and protectionism will always remain blurry. Some factors can push things to one side of the line or the other, but ultimately it will always remain a judgment call, and the goal should be to narrow down the range of the judgment call." The group all recognized that protectionist claims and rent-seeking interest groups will affect the lobbying around national security-related industrial policies, and decision makers should take that into account.

Some participants insisted that we do need clear thresholds, standards, or criteria to determine when something rises to the level of a threat to national security or prosperity and deserves direct government intervention. The question of an identifiable threshold was connected to the problem of deterrence. Finding a clear threshold for assessing national security threats helps us decide how to respond to threats.

What actions should trigger retaliation for the perpetrator, and which should get a milder response? This could be seen as contributing to the evolving language of 21st century deterrence mediated by the digital economy. Accurate and effective retaliatory or punitive actions can deter future adversary actions, but systemic overreaction to every threat, or pre-emptive actions against threats that are hypothetical or extremely implausible, diminishes the power of any retaliatory action at best and escalates tensions between nation-states at worst. Subjecting a claimed threat to some objective test of its severity is necessary if our response is to be proportionate and intelligent. After the boy cries wolf falsely five times, no one gets the real warning.

One framework for arriving at a national security threat determination was suggested:

- How widely used is the technology or service?
- How much access does it give you?
- How much societal dependence on its functions is there?
- How easy or difficult is it to detect malicious activities?

Another participant added a useful observation drawn from military planning. In a conflict, one must consider not just the most dangerous adversary course of action, but also the most likely adversary action. It is often not just suboptimal, but self-damaging to define policy by reference to the most dangerous adversary course of action. This session also witnessed a challenge to the commonly accepted premise that the economic gains from digital openness always increase national security risks. Cutting off data flows between countries shuts off an enormous source of mutual intelligence. It reduces our ability to monitor what's happening in China and impairs our ability to compete by severing relationships with expert workers, private companies at the cutting-edge of ICT services in China, and Chinese capital investment.

Three clear points of consensus emerged from Session 1 discussions:

EVERYTHING DIGITAL IS DUAL USE

The digital ecosystem is a globally shared infrastructure and everything it does can be both beneficial and an attack vector; an economic boon or a security risk. If it is all dual use, general cybersecurity standards and best practices apply, and it is vitally important to find the proper balance between trade, economic growth, and innovation on the one hand, and security on the other.

BALANCE STAKEHOLDERS

Our methods of assessing threats from ICT interactions should involve a balanced set of stakeholders, representing economic benefit and other countervailing concerns, not just national security.

CHANGE THE DEFAULT

In making these tradeoffs, we need to carefully consider what we define as the default position. Some processes focus decision makers only on potential identifiable threats, not on the benefits of allowing a transaction. That default favors restrictions that may not be in our interest.

On dual use, *the dual* capability of modern digital technology heightens the importance of finding the proper balance between trade, economic growth and innovation and security. As one participant put it, "it's going to be increasingly difficult to distinguish between economic and national security interests, because **so** much of the innovation that's relevant for national

are pursuing objectives that are not driven by government interest and government funding, but by commercial realities and opportunity. *Anything that is useful in ICT will largely be dual use.*" Indiscriminate militarization of the entire digital ecosystem involves a refusal to benefit from transnational flows of capital, data, ideas and people. This will stifle growth in all countries and likely only increase the risks of conflict.

On Stakeholder balance: According to one participant, "the balance between national security and economic benefit, whatever that balance is, must be clearly embodied in the decision-making framework of the regulatory or statutory mechanism. If the standard for balance is not set in the framework for the regulatory or statutory mechanism, then you're going to end up with decisions that in almost every instance will skew overly restrictive." The way the process is structured has a lot to do with the output. A discussant noted that the Treasury Department is the chair of CFIUS, not the Defense Department, and that this was deliberate. Several agencies in the committee are security agencies, but others are economic agencies, and their role was to hold the security agencies to their statutory mandate. Treasury is supposed to be the honest broker and facilitator. That structure worked properly for a long time, according to one participant, but the balance broke down around 2018, when the Commerce Department, the US Trade Representative and the State Department stopped playing that balancing role. That change can be attributed to a policy or political shift in the administration. But it also indicates that formal balances in the composition of a committee will not work as intended if certain agencies do not hold up their end of the bargain.

On the default: The Vulnerabilities Equity Process (VEP) was cited as an example of shifting the default. (VEP refers to the decision by military and intelligence agencies whether to disclose software vulnerabilities to vendors and the public to improve public security, or to keep them secret so they can be used against foreign adversaries.) Before 2012, the default position was "we're going to keep this vulnerability secret; convince me why we should disclose it." In 2012 the default position was flipped; it became "we are going to disclose this vulnerability, convince me why we shouldn't." Arguably, the new default serves the public interest, not just the national security interest, by making it possible to patch more of the vulnerabilities that might be exploited by real adversaries.

Session 2: Keynote address by Dr. Abraham Newman

Dr. Newman's keynote summarized his co-authored book with Dr. Henry Farrell, *Underground Empire: How America Weaponized the World Economy*. Dr. Newman said the international community does not yet have norms or a set of principles to help guide how tools of weaponized interdependence should or should not be used. Currently, these tools are used for mere incremental crisis management." To emphasize that point, Dr. Newman relayed a personal communication with a senior member of the United States (US) export control apparatus, noting that the responsibility of assessing the downstream consequences of US export controls has not been assigned to anyone in the US government (USG).

One of Dr. Newman's key takeaways was that the international liberal order needs new institutions to manage weaponized interdependence for the era of great power competition. Such a framework could also be used to inform network-based diversification of supply chains for critical technologies, which he believes is a superior industrial policy to home-shoring. The most important considerations for the framework to help determine would be:

1. What is the nature of the threat: is it a cybersecurity threat, an economic threat, a military threat, or the intersection of multiple threats?
2. When is it appropriate to weaponize economic interdependence? There should be checks and balances on weaponization especially given the abuses revealed by the Snowden revelations.
3. How can these tools be confined to a small set of the economy so the larger set can prosper?
4. A new framework should also include jointly agreed-upon inducements, as opposed to mere restrictions. For example, joint purchasing agreements can affect pricing such that allied governments favor Ericsson as a replacement for Huawei.

One participant pushed back at the notion of inducements, highlighting that the US Congress allocated billions to jumpstart 5G research to "catch up" in the 5G "race". The result was a reduced amount of Independent Research and Development (IRAD) spent by private companies for their own Research & Development (R&D). Dr. Newman also highlighted the need for employing talent trained in logistics, cybernetics, and management structures to better understand complex supply chains and assess network vulnerabilities in supplier networks.

He asserted that there is an institutional gap in the current application of industrial policy. Between the Infrastructure Investment and Jobs Act, the CHIPS and Science Act, and the Inflation Reduction Act, there is not a clear organizational system to coordinate across these various efforts. On the sanctions side of the framework, we have learned that export controls are no longer expected to completely prevent a specific behavior or capability like exporting oil. They can only raise the transaction costs of the targeted economic exchange. In the case of Russian oil, a Rupee exchange with higher transaction cost was created. One participant noted that sanctions create incentives for alternative pathways via a substitution effect for capital and services to flow where lower transaction costs exist. Dr Newman expressed a related concern that any short-term benefit of sanctions is outweighed by the long-term risk of collateral damage, including a complete loss of their effectiveness—for example, by US adversaries reducing reliance on the US dollar and the SWIFT system.

Dr. Newman noted how the invasion of Ukraine was a turning point for Information and Communications Technology (ICT) firms. Before the Ukraine war, Microsoft had set up the Digital Geneva Convention specifically as an attempt to bind private ICT firms into neutrality and refrain from assisting governments in data sharing or other sorts of what might be perceived as coercion. After the war, Brad Smith decided to forgo neutrality and support the Ukrainian war effort in cyberspace. One participant, however, reminded Dr Newman that the governance of internet names and numbers could not be weaponized by nation-states because of the privatization of the Internet Corporation for Assigned Names and Numbers (ICANN) in 2016. ICANN rightfully denied Ukraine's request to remove Russian IP addresses and top-level domains from the DNS root. Should this new institutional framework also refrain from following state-based competition?

Finally, Dr. Newman put forward policy recommendations that could be implemented in the short term until a more complex, long-term framework is developed:

- First, the USG should appoint double-hatted members of the National Security Council (NSC) and National Economic Council (NEC) such that benefits and harms are evaluated simultaneously using appropriately developed metrics. This recommendation mirrors insights from the first session, that "stakeholder balance" should be formally codified in statute.
- Second, the USG should conduct assessments modeled after the EU's European Economic Security Strategy from June 2023.

Competing Narratives in the US political economy

Discussions in the workshop reflected two competing narratives regarding the relationship between national security and ICTs. We can simplify them as *digital neomercantilism* (DNM) and *neoliberal globalization* (NLG) (figure 1). Both narratives embed assumptions about the broader international political economy that were unpacked during the workshop (table 1). Most of the workshop participants varied in the extent to which they espoused the principles of one school of thought over the other. However, each narrative emerged as a distinct, internally coherent worldview. For example, both perspectives have different accounts for what explains China's economic development in the 21st century. Both narratives also shared points of agreement and disagreement summarized in the coming sections. Figure 1 and Table 1 provide a quick primer on how both schools differ in their political economic assumptions.

Digital Neomercantilism

Digital neo-mercantilism (DNM) represents a modern adaptation of mercantilist principles for the information age where ICTs replace physical resources as the key drivers of power and wealth. Motivated primarily by the pursuit of relative geopolitical power, digital neo-mercantilists believe that government control of industrial policy, trade, and ICT capabilities can significantly affect relative prosperity and state power. In this narrative, private economic interests are fused politically with the military and national security interests of the state. In a globalized world economy, states' interdependence should be increasingly weaponized in the service of state power.

Neoliberal Globalization

Neoliberal globalization (NLG) considers the competitive forces of open markets and cooperative international institutions as the engines of economic prosperity and peaceful co-existence. Countries specialize in what they produce best and trade to access goods and services they cannot produce efficiently. Specialization and comparative advantage benefit trading partners by expanding the size of the markets in a positive sum game. Openness, competition, and globalization support technological progress and make the national economy stronger and more resilient. Interdependence reduces the gains from military conflict. In this narrative, peace is achieved through the strength of a national economy and the rising opportunity cost of warfare.

Contrasting political economic assumptions

Digital Neomercantilism

- Relative gains and growth matter more than global gains.
- Firms are identified with their home country
- The primary public policy objective is to optimize for high-wage and value-added industries such as services and the advanced technology and manufacturing sectors
- International competition in high-tech sectors is zero-sum; one country's gain in market share is another's loss
- While industries with high fixed costs and low marginal costs must globalize to reinvest their gains in innovations they should remain primarily on home territory to receive protection and inducements from the state
- Global interdependence is a security weakness because it can be weaponized
- The state should consider all possible interventions in its "toolkit" to influence security and economic gains

Neoliberal Globalization

- Absolute gains and growth matter more than relative gains
- Firms compete in global markets
- The primary public policy objective is to optimize for economic efficiency and the free movement of capital and labor International competition in high-tech sectors is positive-sum; while terms of trade and market share shift to where comparative advantages exist, specialization and innovation will expand the size of the global pie
- The distributed supply chains of high fixed-cost, low marginal-cost industries enable positive feedback loops between trading countries through reciprocal foreign direct investments (FDI).
- Global interdependence promotes cooperation and mitigates conflict because trade raises the opportunity cost of war When national security is defined in practice as protectionism, the result is a degenerative game of tit-for-tat. Therefore, the state should only interfere where clear market failures exist

Session 3: Global value chains and ICT trade

Session three was designed to focus on global value chains and ICT trade. However, it became clear that US-China geopolitical tensions were defining the parameters of ICT trade globally, and therefore became the the main subject of discussion.

One participant shared their insights on the WTO regime noting how the USG has been using security exceptions broadly and permissively. Further, the USG has refrained from presenting critical judgments on WTO dispute resolutions when other countries invoke the security exception to protect trade interests or national security. By continuing its use of a broad national security exception, the USG is encouraging other countries to keep invoking those exceptions at will, thereby undermining the "rules-based order" it built in the process. Another participant noted this trend renders US foreign investments a fair target for retaliation on a similar basis of equivalence.

This participant also discussed how since 2017, the WTO's Joint Initiative on E-commerce had managed to achieve small breakthroughs in services trade such as e-contracting, e-invoicing, paperless trading, consumer protection, spam prevention, and others. While more challenging issues like data localization, custom duties on digital transfers, source code, and encryption disclosures still presented significant areas of divergence between the US, the EU, and China, those areas were actively negotiated. However, in October 2023, the Biden Administration reversed decades of US precedent by formally abandoning its demands for free trade in services from the WTO's Joint Statement Initiative. This change was said to have occurred for two reasons. First, the USG can no longer afford to preference its long-term interests in a rule-based system as it once did. Instead, it is expected to increasingly opt for bilateral or plurilateral agreements as a peer competitor. According to workshop participants, this position may be self-serving to the US in the short term but will be detrimental in the long term if the US abdicates its leadership position as a rule maker at the WTO.

The second reason was said to be an alliance of anti-trade interests. Progressive localists such as Senator Elizabeth Warren and others have been aiming for government crackdowns on "big tech." These actors assert that international trade agreements stand in the way of top-down regulation of the digital economy. Similarly, DNMs aiming to decouple the US-China digital economy are finding unlikely allies with progressive localists. Workshop participants noted that US businesses considered this change in US policy to be determinantal to their global competitiveness.

Workshop organizers asked whether the lack of reciprocity in ICT services hurts a closed economy more than an open one. One workshop participant noted that the US market is not harmed by access to Chinese propaganda but that the CCP would be harmed by open exposure to Western media. Another participant disagreed, noting that Chinese elites are exposed to multiple media sources alongside Chinese propaganda and yet are still more aligned with the commercial interests of Chinese companies and the state.

Finally, a consensus was reached that if China pursues a policy such as censorship, it does not mean the US should seek reciprocity since many Chinese CCP policies are ultimately harmful to China. However, participants also concluded that recent actions by the Office of the United States Trade Representative (USTR), specifically the US's withdrawal from the WTO Joint Initiative on E-commerce have undermined the US's ability to negotiate market access reciprocity with China, and that will be harmful to US interests.

Session 4: Comparing the US and Chinese political economies

On Chinese state-ICT firm relations: Workshop participants highlighted how the Chinese ICT environment is marred by broader political-economic tensions between private sector actors and the Chinese Communist Party (CCP). They discussed how some private companies with global ambitions like ByteDance have devised novel institutional arrangements in an attempt to avoid being caught in a geopolitical tug-of-war like Huawei.

Workshop participants on the DNM side conceded that private ICT firms are indeed profit-maximizing and therefore less likely to openly serve CCP interests when compared to state-owned enterprises. However, they still concluded that all Chinese companies will be more or less state-influenced and serve CCP interests regardless due to the nature of the Chinese legal system, particularly the Cybersecurity and National Intelligence laws. One participant pushed back at this notion, recalling their interactions with Chinese delegates in Hong Kong.
They noted that China's cybersecurity law was created as a response to the growing domestic instability and cybercrime prevalent in its digital economy.

DNMs regarded domestic Chinese firms as more eager recipients of the mercantile strategies of the CCP. For example, one participant explained how PLA Unit 61398 hacked Coca-Cola to "get its top bid price for a Chinese soft drink Company." The same participant said it would be inconceivable for Western intelligence services to perform industrial espionage to aid Western multinationals.

DNMs also noted how some of the Chinese firms with close ties to the state are embraced as "national champions", and therefore receive large subsidies. These subsidies were said to be a product of the mercantile economic goals laid out in the CCP's Made in China 2025 policy. This CCP policy is aiming for import substitution and more self-reliance in various industries, including ICTs. Some participants asserted that Huawei acquired the capabilities to create in-house technological solutions by subterfuge in the late 1990s.

A combination of IP theft and state subsidies was said to have enabled them to replace their foreign competitors in the domestic market, such as Nortel and Lucent, and increasingly in global markets. NLGs disagreed with this version of history, instead highlighting that Huawei's growth was a product of large investments in R&D and competitive forces in a large domestic market. Domestic ICT firms in China expanded outwards with the benefit of a cheap labor force, starting with a labor-intensive, copycat economy. They later became more competitive as they leveraged local know-how and reinvested earnings into R&D.

Both points of view conceded that Huawei produces for the PLA and is present at defense industry events in China. DNMs considered Huawei's relationship with the CCP as a constant while NLGs considered Huawei's rapprochement with the CCP to be a more recent and unfortunate product of US-China's ongoing economic decoupling and a result of US actions. NLGs participants also insisted that the US firms have a similar relationship; they benefit from major government contracts and if the USG invokes national security, ICT firms cannot say "no" to handing over data or technology.

High-tech trade with China and national security: Proponents of NLG acknowledged concerns about China using industrial policy to erode the US competitive advantage in the ICT sector. One participant characterized Chinese mercantilism since the 19th Party Congress as "dual-circulation" where an internal economy is largely protected from the outside world.
They noted the existence of an implicit market share cap designed to prioritize domestic firms in China, but that simultaneously allows foreign firms to set up R&D facilities because China wants to be integrated with global supply chains.
While these mercantile tendencies present significant concerns, NLGs regarded some of them as catalyzed by USG actions during the Trump administration. Consequently, the US should not impose short-term sanctions since these will only accelerate China's efforts to develop substitutes for US ICT products. If China forces import substitution at an accelerated rate, the ensuing market distortions would come at a great cost to its economy. However, unlike the US economy, China's surplus savings will work to its advantage in a long-term race to the bottom.

Market access barriers and limitations on incoming Chinese investments in the US were regarded by NLG as the wrong solutions to counter protectionist measures on digital trade. Such measures only decrease economic efficiency and reinforce China's nationalistic tendencies. For example, the US cannot reduce trade deficits with China by ordering its chip companies to stop selling to Huawei, where billions in surplus exist, while subsidizing laggard semiconductor firms. NLGs also noted that the US cannot gain freer trade with China by asserting that every Chinese provider is an agent of the Chinese state and that any use of their products exposes America to Communist infiltration. Those types of arguments can easily be applied to US firms by the Chinese and lead to an unproductive race to the bottom.

DNMs conceded that the current application of technology sanctions is counterproductive stating "We need to do it [apply sanctions], but if we're going to do it, let's not do it in ways that are just dumb (…) the big risk of the foreign direct product rule is that companies around the world will redesign out American products." Notably, one prominent DNM conceded that companies like Huawei and ZTE were not targeted because of their insecure hardware, which was the nominal pretext, but because they were an economic threat to US telecommunications providers. They noted that the cybersecurity risks of Huawei are likely less of a concern than Nokia and Ericsson given that Chinese ICT firms are some of the most heavily scrutinized in the world. One participant even asserted that Nokia's core and base station equipment may be less technically secure than Huawei's. China hawks did not disagree. For DNM participants, the concern was not the cyber insecurity of Chinese ICT but their potential weaponization as an economic and informational tool by the CCP.

Workshop participants noted how the Chinese telecom giant has been scrutinized for more than a decade. They agreed that if "cybersecurity" was the real concern as the USG insists, then threats must be concretely defined. One participant recalled their experience during the Obama and early Trump administrations when regulators realized a large amount of Huawei and ZTE was emerging in rural networks. As participants in classified national security discussions, they noted that a "smoking gun" for Huawei was never found.

Despite that fact, this participant revealed that politicians wanted to provide "infrastructure money out there for people that backed [their] campaigns." The same participant concluded stating that most Huawei equipment has neither been ripped nor replaced, but so far, no breaches, data theft, or worse scenarios have occurred in these areas. Another participant added that the National Security Agency (NSA) conducted Operation ShotGiant to hack into Huawei headquarters but never found the "smoking gun' it was looking for.

NLGs concluded that concerns about Huawei and ZTE were motivated by their market dominance and the political expediency to scapegoat foreign threats. US interests, including China hawks in Congress, the telecommunications lobby, and the Trump administration, crafted a narrative of China's ICT as a major national security threat. This narrative initially targeted hardware but later expanded to platforms. The vagueness of the security claims served to make the narrative more palatable to the public.

Another voice highlighted how shutting out China can harm national security. The USG's decoupling policies are undermining Signals Intelligence (SIGINT) capabilities. Huawei was forced to rupture from Android and develop a bespoke operating system, HarmonyOS. For this participant, the loss in SIGINT capabilities presents a more direct and tangible risk that is often ignored by those advocating for decoupling both ICT economies.

Another participant made a point that too often, security theater tends to overshadow real cooperation over security objectives. They shared an anecdote describing how Huawei cooperated with the US military in Iraq to dismantle Improvised Explosive Devices. In the aftermath of the Iraq war, insurgents were using IEDs against US troops triggered via Dual-tone multi-frequency (DTMF) signaling. The US military had asked local telecommunications operators and manufacturers for help. They were denied by Ericson but found a cooperative partner in Huawei, which helped save US servicemembers' lives in the process.

Session 5: The Costs & Risks of Weaponized Interdependence

In this session, workshop organizers asked: when does weaponizing interdependence begin to break down the networks of interdependence? One participant noted that weaponizing interdependence risks breaking down the networks of interdependence as soon as they are used. They noted that the geopolitical cost of weaponizing interdependence has not played out well for the US. From a trade standpoint, the lack of ICT market access reciprocity with China implies losing 20% of the world's addressable market. Adding countries that aren't the closest US allies that align with China on trade brings that loss to at least 35%.

On top of the economic disadvantages, large diplomatic costs have been accruing because of China's development strategy in the third world and emerging economies. According to this participant, China is using the phrase "China builds, America bombs," which may be compelling for the global south. They noted China is taking an approach that it is ready to provide "better, faster, cheaper" development for the rest of the world.

For another participant, the solution to uncoupling geopolitical tensions from the digital economy rests in comprehensive legislation on data governance and privacy. They noted that while surveillance used to be confined to war zones, the war on terror accelerated the convergence of civilian communications and intelligence collection. The change to continuous global surveillance occurred after FISA section 702. This change authorized threats to be searched in private domestic networks as well as foreign. However, the problem with pervasive dual-use technologies is that civilian and military lines are blurred and involve trade-offs. Undermining strong encryption to solve a localized security threat opens up a general threat for all devices relying on the same strong encryption. For example, targeting a foreign cyberhacker with a zero-day exploit creates vulnerabilities for devices at home in the civilian infrastructure. One global network with multiple public policy goals now requires agencies with different areas of expertise in the same room to make public policy decisions.

In a rule-of-law democracy, government access to data can be constrained by safeguards for privacy and civil liberties (like the 4th amendment). The EU-US data privacy framework is an example of how safeguards can be applied transnationally. Human rights can be built into international legal arrangements, as the second Max Schrems trial demonstrated. Another example is the OECD's Declaration on government access to personal data in the private sector. This declaration is based on similar safeguards among the members on arbitrary government access to data held in the private sector.

For this participant, there exists a significant legal challenge with EU-China trade that is bound to affect US market access reciprocity negotiations. The EU's legal structure says personal data can only be transferred to these other countries if government access is limited by law, a requirement for a democratic society. This implies that under European law and given reciprocity agreements with other OECD members, there are no lawful transfers of personal data from the EU to China today at all. China's domestic privacy law, the PIPL, leaves open the government access to personal data that is the basis for the EU limitations on data transfer. According to this participant, such irreconcilable differences between authoritarian regimes and OECD members can be pragmatically solved with a "data allies" model. Such a model can allow democratic nations to address security and privacy risks posed by non-democracies while keeping the door open on global trade when risk is manageable. The participant noted that such a model could allow democracies to reconcile liberal values and rights in light of the convergence of civilian and national security ICT because rule of law surveillance limits can be harmonized accordingly.

However, real legal and diplomatic challenges in the "data allies" model were highlighted. What would such a framework look like for the 100 to 150 non-aligned nations that don't look like Europe or China? Does the absence of such rule of law safeguards be the basis for limiting trade with non-democracies? Another participant highlighted that the US is different from the EU because some of its most important trading partners are non-democratic nations such as Saudi Arabia and other Gulf Cooperation Council countries.

Session 6: The Road Ahead

In this session workshop participants compared the viability of mercantilism and liberalism as distinct strategies to contend with the rise of China. They highlighted how positive versus zero-sum trade debates are not new. From the American Revolution to the peak of the British Empire, the US engaged in protectionism. After World War Two, the US championed free trade. It invested in the Bretton Woods system and the Marshall Reconstruction Plan to counter the threat of the Soviet Union. The US had a national security interest that allies recover from the war and remain prosperous. It created a globalized trading system that transformed agricultural societies into highly industrialized economies. Even though the US's share of global GDP was reduced in relative terms as its allies reconstructed, the corresponding reductions in global poverty were a net good that expanded the size of the global "pie" benefiting all trading partners including the US. Participants illustrated how this period in history was proof that autarky does not work even for a country as large in land and resources as the Soviet Union. They noted that both perspectives today consider the pursuit of power, prosperity, and wealth to be interwoven but are at odds when it comes to how to prioritize these values, and how to configure domestic and international institutions to achieve them. On one hand, DNM requires bold action to contain China and fragment the trading system. On the other hand, NLG stresses the way US firms and citizens benefited from globalization and implicitly assumes that absent any course corrections, China can be its own worst enemy.

When it comes to DNM, participants described how the Trump and Biden administrations have bundled policy outcomes deemed in the public interest to justify applying protectionist policies. While AI safety, cybersecurity, privacy, human rights, and jobs are worth pursuing, they were said to be used as convenient pretexts by an alliance of opportunistic politicians, military intelligence interests, and private rent-seeking businesses. Another participant disagreed with the premise that mercantilism involves special interests protecting their industry using national security as a pretext. They stated "There's this narrative that somehow this [US-China trade issues] is about mercantilism and protecting our own companies. It's actually the opposite. You know, we're pretty much the only country in the world that takes policy choices that intentionally damage our own companies (...)"

NLGs responded that it may be natural to expect winners and losers after public and private sector entities bargain and a political equilibrium is reached. However, they insisted some US firms have played into the overly broad national security argument tied to their products. These US firms then created artificial links tying dual-use and even commodity ICT products to national security with a tenuous link to undefined military capabilities. For NLG participants, the securitization of Chinese ICT trade was said to be oversimplifying and harmful. First, because the link of Chinese ICTs to undefined military or intelligence capabilities is tenuous at best. Second, because the narrative overlooks the real drivers of innovation in the face of complex supply chain and geopolitical challenges.

Participants followed by questioning the two rounds of chip restrictions by the Department of Commerce's Bureau of Industry and Security (BIS). In the last round of sanctions in October 2023, BIS assumed a direct relationship between a chip's so-called performance density threshold and the extent to which it can enable military capabilities. Participants questioned the scientific basis for that assessment. They asked a series of rhetorical questions to illustrate the inherent ambiguity motivating the restrictions on leading-edge chips:

- Are chip restrictions intended to solve supply chain cybersecurity about the feared kill switch or do they assume Chinese chips facilitate global surveillance?
- Do AI frontier models require higher performance density or better-trained algorithms and data?
- Will AI military capabilities create an offset of such magnitude that it is worth pursuing at all costs and at the detriment of the entire chip ecosystem?

Participants noted that USG policies are not addressing more genuine security concerns about industrial resilience and the availability of older chips in the event of a conflict. One participant also asked: if Russian cruise missiles contain US-made chips, can older Chinese-made chips not be used in conventional US weapons systems? These ambiguities highlight the importance of defining and articulating clear problems and purported solutions.

Moving to the Chinese political economy, participants highlighted how CCP trade policy since Xi Jinping ascended to power involves varying degrees of state and private ownership that leverages mercantilism to achieve its goals.

NLGs highlighted the contradictory nature of a model that uses strict capital controls, protected domestic markets and heavy regulation of tech firms yet expects to have consistent growth, especially given declining demographics, political instability, and a middle-income trap.

One participant highlighted how many public Chinese firms listed in Hong Kong raise capital using financial instruments called variable interest entities (VIE). These instruments allow Chinese firms to register in tax havens to raise capital and get around Chinese regulations. For NLGs, Chinese capital should be encouraged to offshore instead of actively discouraging it. One participant noted that while capital controls limit how much Chinese individuals can invest overseas, elites have used Bitcoin to transfer their savings abroad before it was banned. Today, they use exchange-traded funds in Japan and the United States to transfer their savings to foreign markets.

Another participant described the protectionist Jones Act of 1920 as an example of why the cost of propping up infant industries bears heavy on the rest of the economy. The Jones Act protected the US shipping industry from foreign competition by requiring any cargo shipped between US ports to be carried by US ships with at least 75% American crews. By limiting competition, the law made the cost of shipping goods between US ports about two to three times what it would cost using foreign competitors. These costs transferred to the rest of the economy and disincentivized investment in new fleets, preserving less fuel-efficient and slower ships as the industry was shielded from competition.

Proponents of the Jones Act argued it was essential for national security to maintain a domestic shipbuilding industry and a trained maritime workforce. While national security is a legitimate concern meaningfully invoked when a clear military capability is on the line, the maritime industry is commercial. The artificial protection of an inefficient domestic fleet might offer illusory security gains, it does so at the expense of overall economic efficiency, a much stronger contributor to national security. This participant concluded that the protection of the maritime industry is not unlike the modern chip industry where national security is a pretext used by an alliance of special interests lobbying for protection. A globally competitive domestic shipping industry can be vital for military logistics just as a competitive US ICT ecosystem can be beneficial to US SIGINT.

Session 7: Reaching Consensus

In this session, a workshop moderator summarized consensus points and disagreements. A consensus was reached that security concerns justifying ICT market interventions require specific demarcation, as discussed in session 1. A simple claim that national security is threatened should not be used as the basis for ICT restrictions. Broad claims of insecurity were said to be off the mark and harmful because they do not materially improve security and encourage tit-for-tat retaliations.

A significant point of agreement was that the **USG should stop making country-of-origin the primary risk criterion in cybersecurity discussions**. One major neo-mercantilist advocate even admitted that he didn't care about the cybersecurity of Huawei; keeping it out of US markets was all about unfair trade competition to him. Another more liberal-leaning participant with expertise in cybersecurity said that objectively, Nokia 5G equipment may be less secure than Huawei's. The current
discourse about “trusted vendors,” “secure clouds,” or “clean networks,” when based entirely on the country of the producer or investor, confuse ICT security discussions with trade protectionism in a way that is not conducive to rational decision-making.

As relates to US trade with China, workshop participants agreed that the USG should narrow its techno-economic security focus to **negotiate for greater openness** of China’s ICT and data markets. Further, the US should **not mirror China's restrictions on information flows** as a way of punishing China’s restrictions on US information firms or external information flows. The US media environment thrives on openness and free expression is a fundamental value enshrined in the Constitution. There is evidence that China’s economy is hurt by its attempts to tightly control information.

Points of disagreement: DNMs claimed to be in favor of genuine reciprocity of market access as a way forward with China. However, they remained skeptical that a fair exchange would ever be possible with the CCP in power. One participant said, if “Germany can’t buy a Chinese port, China shouldn’t be allowed to purchase ports in Germany. If an American ICT company isn’t allowed in China, Chinese companies shouldn’t be allowed in the US”, and so on.

NLGs instead considered that even if negotiations risk failing, the USG should still make a good-faith offer for free trade. One particularly informative exchange on ICT reciprocity occurred between a dovish participant and a hawkish participant. The dovish one asked what would happen if the CCP offered US companies a deal similar to TikTok's Project Texas compromise with CFIUS? In this scenario, a company like Meta would be presented with the option of operating competitively in China if a Chinese citizen was assigned to the board of its domestic subsidiary to represent the national security interests of CCP, and all data on Chinese citizens would be hosted on a Chinese cloud, and Chinese firms and the government would have the power to approve and even modify any software updates. Would US firms and/or the USG ever agree to the conditions required of TikTok in the US? If not, is reciprocity really the goal?

The hawkish participant said the premise was misguided because, unlike Chinese firms, US firms have a history of saying "no" to the USG, and cited Apple's rejection of the Federal Bureau of Investigation's request to unlock the phone of the San Bernardino terrorist. Tim Cook didn't suffer the fate of Jack Ma, the co-founder of Alibaba Group. Google's workforce forced the company to drop its collaboration with the Department of Defense in Project Maven on the use of artificial intelligence to enhance image processing. Both participants understood one another's position.

Conclusion

Our workshop asked: What is 'national' security in a globally connected digital economy? The discussion was global in scope but focused on the US-China relationship given that it is defining the parameters of ICT trade. Participants provided a range of answers on the trade-offs and complementarities that exist between national security and ICT trade. Some answers were a product of consensus, while others revealed divergences. The proceedings revealed digital neomercantilism and neoliberal globalization as distinct narratives with different perspectives on how to address US trade relations with China.

Participants from both perspectives unpacked internal tensions in the US and Chinese political economies, revealing complex internal bargains between private actors and the state. They addressed how both systems perceive their mutual interdependence. The workshop also uncovered how the dominant US narrative, digital neomercantilism, causes an intermingling and bundling of policy issues leading to an inability to engage in compartmentalization and pragmatism. The consequences of a lack of clear demarcation of policy problems are such that problems of the US's own making are often attributed to China, and vice versa. Our workshop proceedings revealed how both dominant US narratives had several blind spots.

We summarized them as a series of rhetorical questions in the appendix. Disagreements remain over whether free trade is a source of economic growth or whether economic development is a precondition for free trade. Today, while China never fully liberalized, be it historical resentments or weariness of openness, its GDP was 78% the size of the US economy in 2021 ($18 trillion) and the gap is closing. The years of sustained double-digit growth and corresponding investment in infrastructure and education at the turn of the century gave substance to the Thucydides trap argument. At the same time, the risks of China's rise today are often overstated in the US. China faces many barriers to its development that make it an unlikely candidate to replace the US as the dominant global power anytime soon.

That said, Washington's China containment strategy is severely misguided. Beijing will not sit idly by with the US crippling its industries without retaliating. It has already hit back with a licensing and controls regime for rare earth elements that threaten the current administration's green agenda. Not only will the degenerating relationship come at severe costs to global stability and prosperity, but USG is also undermining neutral global governance structures and standards development organizations that are relatively favorable to US firms and US economic pre-eminence. As the USG pulls back from the WTO and politicizes institutions like the US dollar and SWIFT, it is undoing the very networks that made it so successful historically. Recent shifts in United States Government rhetoric from "decoupling" the United States and China's digital economies to "de-risking" them are commendable as a step in the right direction. A resumption of military communication and cooperation on climate change are also good starts creating diplomatic capacity to better manage a relationship in decline. But a lot more is needed. This temporary détente is not built on a solid foundation.

Recommendations for reconciling national security and global economic competition in ICT markets

- The USG should appoint double-hatted members of the National Security Council (NSC) and National Economic Council (NEC) such that benefits and harms are evaluated simultaneously using appropriately developed metrics. This recommendation mirrors insights from the first session, that “stakeholder balance” should be formally codified in statute.The US’s new WTO position is tantamount to admitting an early defeat with China on trade issues. Instead of pulling out of the WTO Joint Initiative on E-commerce, the US should advocate for WTO reforms to address issues like state-owned enterprises, digital trade, and dispute settlement mechanisms, and aim to make the organization more effective in dealing with China's economic practices. The US should also reform its practice of using the national security safeguard/escape clauses.

- The US should aim for reciprocity of bilateral trade with China or a close approximation instead of a race to the bottom. US-China negotiations should start seeking redress and establish new rules and terms of trade.

- The US is actively seeking to de-risk from Taiwan but should refrain from further subsidies. Adjustment costs are temporary, they affect the profit margin of US manufacturers if they are slow to innovate or adapt their business models. If China wants to subsidize and artificially prop up infant industries, US DNMs should have no objections to the CCP inefficiently draining its surplus savings.

- Joint national security threats should be addressed such as sovereign debt and instability in the Eurodollar financial system.

Workshop Composition

Abraham Newman, Georgetown University; **Aimen Mir**, Freshfields Bruckhaus Deringer; **David Simpson**, Virginia Tech; **Andreas Kuehn**, Observer Research Foundation America; **Dean Cheng**, Lincoln Policy Center, US Institute for Peace; **Gregory Touhill**, Carnegie Mellon University; **Harry Oppenheimer**, Georgia Institute of Technology; **John Lash**, DarkHorse Global; **Jyoti Panday**, **Karim Farhat**, Georgia Institute of Technology; **Karl Grindal**, University of New Hampshire at Manchester; **Letian Cheng**, Georgia Institute of Technology; **Nadiya Kostyuk**, Georgia Institute of Technology; **Michael Daniel**, Cyber Threat Alliance; **Matt Butkovic**, Carnegie Mellon University; **Milton Mueller**, Georgia Institute of Technology; **Peter Swire**, Georgia Institute of Technology; **Benjamin Grazda**, AccessNow; **Robert Atkinson**, Information Technology Industry Council; **Samm Sacks**, Yale University, New America; **William Drake**, Columbia University.

Observers

Alex Mueller, University of Pennsylvania; Esra Caliskan, University of Istanbul; Ishan Metha, CommonCause; Le Yang, Tsinghua University; Seungtae Han, Vagisha Srivastava, Georgia Institute of Technology

Annex: Ideological gaps

Our workshop proceedings revealed how both narratives had a number of blind spots. Some were idiosyncratic and others were based on incomplete information or faulty assumptions by participants. With the benefit of hindsight, we summarized a holistic picture of US-China trade tensions with rhetorical questions to both political economic narratives. Addressing those gaps may help forge a better path ahead for the world's most important bilateral relationship.

Digital Neomercantilism

- If reciprocity can be achieved, would the US not benefit from having China become an advanced digital economy with high-end manufacturing capabilities as it did with Japan?
- How can we assume to know what the demand for advanced manufacturing will look like in the face of rapid innovation?
- If Chinese manufacturing is increasingly advanced and capital flows freely, wouldn't innovation and knowledge transfer back into the US market and advance the US economy?
- If trade is zero-sum, why would anyone join a US-led plurilateral regime unless the US coerced its allies? Why would Europeans or other countries not fill the void left by US firms in China?
- If rent-seeking and cronyism have impacted the US policy position on Chinese ICTs since around 2010, how can CFIUS and the intelligence community better distinguish genuine threats of industrial espionage or worse from legitimate joint ventures or other profit-seeking enterprises?

Neoliberal Globalization

- How can globalized division of labor account for nonreciprocal mercantilism when the market isn't able to self-correct? Will that not create long-term national security vulnerabilities in critical technology industries that are offshored?
- If the market for advanced manufacturing leads to concentration creating dependencies on risky foreign producers in places like Taiwan, what would the appropriate policy response be?

About IGP

Founded in 2004, the Internet Governance Project is the leading source of independent analysis of global Internet governance. IGP is a group of professors, postdoctoral researchers, and students hosted at the School of Public Policy at the Georgia Institute of Technology, one of the world's leading engineering universities.

IGP conducts scholarly research, produces timely policy analyses and public comments, blogs on current events in Internet governance, and brings ideas and proposals directly into Internet governance processes at the United Nations, agencies of the US government and the European Commission, the Internet Corporation for Assigned Names and Numbers (ICANN), the Regional Internet Address Registries (RIRs) and other venues. IGP also educates professionals and young people about Internet governance in various world regions, which it reaches via classes taught by its professors, public events, and publications.

IGP is devoted to decentralized, multistakeholder governance of the Internet, an open and competitive digital economy, free trade in information services and technologies, peace, and free expression.