hinrich foundation
advancing sustainable global trade

Techno-nationalism and diplomacy:

The US-China race to reshape alliances, institutions and standards

BY ALEX CAPRI
RESEARCH FELLOW, HINRICH FOUNDATION

hinrich foundation

Contents

Contents

Introduction

The Clean Network Program is a reflection of techno-nationalism. Techno-diplomacy is the realpolitik behavior of advancing a nation's techno-nationalist agenda.

American diplomats have been persuading other nations to block Chinese technology from their digital networks.

In August 2020, Washington launched the Clean Networks program, an initiative that seeks to expunge Chinese technology from carrier networks, data storage, mobile apps, cloud networks and undersea cables.[1]

These actions have created an existential crisis for Chinese companies, which have come under fire as they are increasingly viewed as de facto proxies of the Chinese Communist Party (CCP). In the broader context of a US-China technology cold war, Chinese companies' linkage to Beijing has relegated them to the status of malign actors.

Techno-nationalism

The Clean Network program is a reflection of techno-nationalism: mercantilist-like behavior that links tech innovation and enterprise directly to the national security, economic prosperity and social stability of a nation. [2]

According to the US State Department, thirty countries have signed up to this program, including the UK – which, itself, is calling for a 5G alliance of ten democratic countries to provide an alternative to Huawei, the Chinese telecoms equipment maker. These ten countries include India, Australia, South Korea, France, Canada, Germany, Japan, Italy, the US, and the UK.[3]

When viewed together with Washington's ongoing campaign of export controls, these developments have put Beijing's diplomats in crisis management mode. In August 2020, for example, shortly after Washington's announcement of the Clean Network program, Beijing dispatched foreign minister Wang Yi and other diplomats on a five-nation European tour to assuage a growing China backlash.

Beijing's imposition of the national security law in Hong Kong as well as its internment of ethnic Muslim minorities in China's western Xinjiang autonomous region were just several of the latest provocations causing European policy makers to rethink relations with China.

Thus, for Beijing, it has become increasingly difficult to find sympathy in Europe regarding Washington's campaign to crush Huawei.[4] Four of the five countries visited by the Chinese foreign minister were linked to Huawei: the Netherlands (to try and obtain access to vital semiconductor manufacturing equipment) and France, Italy and Germany (to persuade them not to block Huawei 5G technology from their telecoms networks).

Shortly after Mr Wang's five-nation European tour, Washington dealt another blow to China's technology ambitions when it announced export restrictions on Semiconductor Manufacturing International Corp (SMIC), China's most advanced micro-chip company.[5]

The rise of techno-diplomacy

Techno-diplomacy is the realpolitik-behavior of advancing a nation's techno-nationalist agenda through

enticements, partnerships, and concessions, as well as through the threat of negative outcomes. Techno-diplomacy plays out across a range of different forums and institutions, including, increasingly, on social media platforms and other forms of digital media. This behavior is rooted in realpolitik practices, but techno-diplomacy is tied to core ideological values, which will be discussed throughout this study.

In September 2020, China's Ministry of Foreign Affairs announced the Global Initiative on Data Security (GIDS), a project aimed at defining global standards for data security. Its real purpose, however, could be construed as an attempt to deter others from signing up to Washington's Clean Network program.

Under the GIDS, China calls on all countries to handle data security in a "comprehensive, objective and evidence-based manner."[6] The initiative also denounced "mass surveillance against other states" and condemned the use of "backdoors in products and services to illegally obtain users' data…"

More importantly, however, Beijing's high-profile rollout of the GIDS underscores the role that techno-diplomacy will play in the winning of hearts and minds during the next phases of the US-China technology war.

Underlying themes of techno-diplomacy

As the US-China technology cold war escalates, techno-diplomacy will play an increasingly important role in advancing the strategic interests, values and policies of China, the US, Europe, and a host of other international stake holders.

Techno-diplomacy between nations is motivated by four underlying themes.

1. **Digital democracy versus techno-authoritarianism**
   The linkage of technology to fundamental ideological values has become a defining issue in the global technology landscape. The authoritarian use of data and artificial intelligence (AI) to conduct censorship, surveillance and mass monitoring of populations is in direct conflict with democratic standards regarding privacy and freedom of expression.

   These contrasts will accelerate decoupling, fragmentation and realignment throughout the digital economy. Governments will devote increasing amounts of time and resources to shaping public opinion regarding these values.

2. **The emergence of international technology alliances and partnerships**
   Like-minded democratic nations will coalesce around the formation of public-private partnerships and alliances dealing with AI ethics, cyber security and defense, R&D and innovation. Techno-diplomacy will increase government-to-government engagement as policy makers increasingly look to draw upon common values and leverage each other's markets, resources, and firms.

   Techno-diplomacy will see the US and European Union (EU) set aside differences over tariffs, defense costs and tech regulations to cooperate and refocus on the long-standing transatlantic relationship. Key priorities will include addressing Beijing's techno-nationalist

Techno-diplomacy will play an increasingly important role in advancing the strategic interests, values and policies of China.

The linkage of technology to fundamental ideological values has become a defining issue in the global technology landscape.

Rules frameworks must be updated to define and enforce appropriate governance standards.

Balancing the appropriate amount of offensive cyber-military tactics with other "softer" approaches will become a core focus of techno-diplomacy.

and mercantilist practices. Other democracies, including India and Japan, will join these alliances and partnerships.

Although the EU will maintain substantial trade ties with China, Brussels is rebalancing its relationship with Beijing – treating it as a systemic rival[7] which will result in further "strategic decoupling" from Beijing. Thus, Beijing's efforts to pull the EU closer into its orbit will become less successful, particularly in light of China's increased authoritarian leanings.

3. **The spread of hybrid warfare**
Hybrid warfare involves a mix of economic, cyber, diplomatic, information and security related actions, all of which are designed to disrupt or disable an opponent without engaging in open hostilities.

Since the outbreak of the global Covid-19 pandemic, intelligence agencies in democratic countries report an increase in Chinese hybrid warfare activity, particularly regarding the use of digital media. As Beijing's influence, censorship and disinformation campaigns become more widespread, countries will begin to adopt new regulations – an outcome which could see major ramifications for the media industry, particularly as China looks to increase the presence of its state-backed TV entities in local markets, such as its expansion of CGTV and other networks in the EU.

Balancing the appropriate amount of offensive cyber-military tactics with other "softer" approaches, therefore will become a core focus of techno-diplomacy.

4. **New international institutions and rules frameworks**
As the world undergoes a fundamental realignment around technology standards and values, existing institutions must accommodate these changes. Rules frameworks must be updated to define and enforce appropriate governance standards involving trade in data and e-commerce, for example.

Regarding the EU-US transatlantic alliance, NATO will be revamped to address hybrid warfare threats from China, Russia and other state and non-state actors. Regarding the need for new rules frameworks, countries will explore alternatives to the World Trade Organization (WTO), which is struggling to address, among other things, today's challenges regarding digital trade, e-commerce, and Chinese mercantilism.

Alternatives to the WTO will include bilateral digital trade agreements, digital carve-outs into larger multilateral free trade agreements – such as the CPTPP – or even the creation of new multilateral frameworks involving like-minded members.

As it prosecutes its techno-nationalist objectives, for example, the US will look to influence multilateral alliances such as the Wassenaar Arrangement[8], the international voluntary framework that includes the EU and other member countries, which seeks to control the dispersal of "dual use" technologies, such as semiconductors.

Overview of report

Techno-diplomacy will drive important outcomes that lead to the creation of new institutions and rule frameworks.

This study is the third in a series of Hinrich Foundation essays on US-China techno-nationalism, authored by Research Fellow, Alex Capri.

The first essay in this series – which followed a ground breaking study on semiconductors – covered US-China strategic decoupling and focused on the re-shoring and ring-fencing of critical supply chains as well as on "in-China-for-China" planning and risk scenarios.

The second essay focused on the US-China techno-nationalist competition and the pursuit of the "innovation advantage." It examined the underlying dynamics and tensions between markets, non-state actors and governments.

This study looks at how the above developments are compelling governments to pursue strategic alliances and partnerships, and how inherent ideological differences between the Chinese system and those of open market, liberal democracies will influence outcomes.

Techno-diplomacy, therefore, will drive important outcomes that lead to the creation of new institutions and rules frameworks, or produce outcomes that profoundly influence existing institutions.

This report is comprised of three sections:

I. The US-EU transatlantic alliance and China

In this first section, the focus is on the current US-EU state of affairs and why the partnership has sunk to historically low levels of trust.

We also examine Europe's current relationship with China and reveal that, despite deep trade ties, China's recent geopolitical and techno-nationalist behavior has exposed deep fissures in the Sino-European relationship. As a deep dive, we look at how China's so-called 17+1 platform in Eastern Europe has backfired – amplified by occurrences in social media and the digital landscape, in general.

Next, we examine how the exportation of China's model of techno-authoritarianism around the world has accelerated the rebalancing of Europe's relationship with China and motivated its pivot to the values of digital democracy.

In the final part of Section I, we do a snapshot of "Transatlantic Alliance 2.0," which features new partnerships and alliances around AI and standards that promote digital democracy.

II. How techno-diplomacy is changing multilateral institutions

This section does a deep dive into the revamping of NATO and addresses how new technology-driven threats such as hybrid warfare and cyber-security are spurring new levels of teamwork between the EU and the US. We examine how NATO's mission is increasingly being re-oriented to address a rising technology powerhouse, China, and what this means for the world.

Washington's proactive cyber defense posture is being embraced by NATO,

Must new rules frameworks be created exclusively for open market, liberal democracies?

and we look at how techno-diplomacy will be required to manage challenges regarding NATO's Cyber Pledge and Article 5.

Next, we examine how China has been working to influence multilateral institutions such as the International Telecommunication Union (ITU), the International Standards Organization (ISO) and others to adopt Chinese standards for both hard and soft (virtual) technologies, and how the US and its allies are adopting techno-diplomatic countermeasures.

Finally, we do a deep dive into the Wassenaar Arrangement, another historical Cold War multilateral treaty, and examine how the US is using its influence within the alliance to achieve a more coordinated effort regarding export controls on semiconductor and other "dual use" technology.

III. How techno-diplomacy will change rules-based frameworks

In this final section, we examine the impact that techno-nationalism and related diplomatic developments are having on multilateral rules frameworks, such as the World Trade Organization (WTO). We attempt to answer the question whether new frameworks must be created exclusively for open market, liberal democracies.

Finally, we discuss how digital trade and cross-border data flows require new kinds of rules and standards, and we explore how new rules regarding technology standards and ethics are being baked into multilateral FTAs, bilateral FTAs and "digital-only" agreements.

I. The US-EU transatlantic alliance and China

Europeans and Americans have differing views when it comes to the regulation and taxation of the digital landscape.

The GDPR has disrupted the business models of the large American digital companies and data capitalism.

US-EU disagreements

US-EU relations are at their most disharmonious juncture since the creation of the Bretton Woods Accords[9], near the end of the Second World War. At that time, America and more than forty of its allies came together to plan a new rules-based order. This resulted in the creation of multilateral institutions such as the World Bank, the International Monetary Fund (IMF), and, sometime later, the General Agreement on Tariffs and Trade (GATT) – the forerunner of today's embattled WTO.

Since the 2016 election of US President Donald Trump – who ran on a platform of populism and anti-globalization – his administration has targeted the EU in a series of Section 301[10] investigations and trade disputes that have eroded trust and tested goodwill amongst longtime friends. These investigations have included tariff increases on more than 100 categories of European goods, for example.

Beyond tariffs, in 2018, the US President went so far as to question the value of NATO, which has been the bedrock of the transatlantic security alliance since 1947. The importance of NATO, as a cyber-oriented institution, will be discussed in more detail later in this report.

EU digital regulations

In addition to grappling with the trade disputes, the Europeans and Americans have differing views when it comes to the regulation and taxation of the digital landscape.

With the passage of General Data Protection Regulation (GDPR) legislation, the EU has taken an assertive posture regarding citizen data privacy rights. These regulations, which apply to the private data of EU citizens, mandate that companies must obtain an EU citizen's consent before using or selling data, and must also expunge any private data from their systems at the request of an EU citizen.

The GDPR has disrupted the business models of the large American digital companies and data capitalism, in general. No longer can data be sent across borders without appropriate measures in place to scrub, remove or block the sharing of private data.

The European Court of Justice's decision on the Privacy Shield System

The Court of Justice of the European Union headquarters in Luxembourg.
(Source: Gwenael Piaser/Flickr)

The EU is breaking new ground with anti-trust legislation, much of it aimed at Silicon Valley's dominant companies.

In September 2020, the need for constructive EU-US techno-diplomacy became more acute after the European Court of Justice (ECJ) struck down "Data Shield," a system that allowed US companies to effectively comply with the GDPR standards when transferring the data of EU citizens outside the EU to the US. Under Data Shield, US companies could transfer data as long as they had "appropriate safeguards" in place, something that was rather vague and hard to ascertain.

The EU-US Privacy Shield arrangement allowed some 5,300 US companies – most of which are small-medium enterprises (SMEs) or tech start-ups – to sign up to higher privacy standards and conduct transatlantic business.[11]

But a privacy advocate challenged the agreement on the grounds that US national security laws, which allow law enforcement agencies access to private citizen data and the right to perform surveillance, violate the EU's GDPR.

As a result of the ECJ ruling, US companies, like other foreign companies, are required to sign "standard contractual clauses" (SCC) – non-negotiable legal contracts drafted by European authorities.

But if US laws regarding law enforcement, national security and public interest override Europe's new data privacy standards, as defined in Europe's SCC contracts, large amounts of transatlantic digital commerce could be blocked by the EU for non-compliance with GDPR.

US digital companies have commoditized personal data to the point that "surveillance capitalism," a term attributable to the author, Shoshana Zubof, has become common place. The challenge of data privacy, in general, has become a matter that will require special attention discussions for regulators in both the EU and the US. Here, the EU has the power to influence regulatory trends across the Atlantic.

The ruling by the ECJ, which followed a series of US Section 301[12] investigations and the subsequent levying of higher tariffs against European goods, looks like retaliation. In this case, privacy standards are at issue, rather than export subsidies or tit-for-tat tariffs. This underscores the importance of techno-diplomacy, going forward.

Aerial view of Apple Park, the corporate headquarters of Apple Inc., located in Cupertino, California. (Source: Daniel L. Lu/Wikimedia Commons)

Large differences regarding digital trade between the US and the EU are unlikely to be resolved soon.

Confronting Silicon Valley

Beyond data privacy, the EU is breaking new ground with anti-trust legislation, much of it aimed at Silicon Valley's dominant companies.

After assessing US$8 billion in fines against Google – which have not diminished Google's stranglehold on the market – the EU's Digital Services Act (DSA) is on the verge of implementing new measures: forcing big tech firms to offer smaller rivals access to their data on standardized and non-discriminatory terms.[13]

Margrethe Vestager, the EU Commissioner for competition, has signalled that Apple and Amazon, for example, could face anti-trust measures for using merchant data to compete with, displace and supplant these same companies on their platforms.[14] Under new legislation, the fine could be as high as 10% of Amazon's global revenues. Facebook, meanwhile, could face fines regarding "fake news" standards.

On matters of digital taxation, the EU is pushing new boundaries that are aimed at the US tech giants as well,

with a digital services tax ranging from between 2% and 7.5%, depending on the country.[15]

Despite all these differences, the Americans and the Europeans share common underlying democratic and market practices when compared to the EU's second largest trading partner, China. Even with seemingly large differences regarding digital trade between the US and the EU unlikely to be resolved soon, when it comes to data privacy, cooperation between Brussels and Beijing will be even more problematic.

Overview of EU-China relationship

At a time of strained US-EU relations, Europe's complicated relationship with China is also at a crossroads. China is Europe's second largest trading partner after the US, while the EU is China's largest trading partner, and trade volumes are predicted to increase in the coming years. The EU is currently running a trade surplus with China in services.[16]

The EU has cooperated with China in ways that the US presently does not, including G2G collaboration and research regarding the Covid-19 pandemic,[17] and, more broadly, B2B and G2B collaboration on climate change. By contrast, the US, under the Trump administration, famously pulled out of the Paris Climate Accord in 2019, and has eschewed any public-private partnerships on the issue.[18]

Despite strong commercial ties, however, in 2019, the EU labelled China a "systemic rival," a reaction to China's growing geopolitical assertiveness and expanding influence within Europe's economic and political landscape.

The Covid-19 epidemic has opened up existing fissures in the relationship which will likely become permanent. One seemingly small public relations event, in April 2020, will end up having big repercussions for EU-China relations. At the time, Beijing allegedly pressured EU civil servants to change the language in a report regarding the assessment of the origins and early spread of the coronavirus.

Chinese Premier Li Keqiang speaking at the EU-China Summit, 2013.
(Source: Herman Van Rompuy/Flickr)

Language in the original draft document stated that Beijing had used both overt and covert tactics to engage in "a global disinformation campaign to deflect blame for the outbreak of the pandemic and improve its international image."[19] Chinese diplomats allegedly threatened economic reprisals if the EU published the document, and they were successful in getting the original language removed from an edited, later publication.

The consensus was that the EU had been coerced into putting commercial interests and fear of Chinese economic reprisals ahead of its commitment to civil society. This event marks the beginning of a fundamental reassessment on a broad range of issues which is likely to result in a significant adjustment of Sino-EU relations.

Confronting techno-authoritarianism

Three themes will define how supply chains, data and the internet continue to fragment and coalesce around competing techno-nationalist systems:

– Privacy
– Free speech
– Surveillance

China's system of digital authoritarianism – in which the state relies upon hard technology, digital platforms, and data from Chinese tech companies to engage in censorship, surveillance and citizen control – is fundamentally incompatible with the liberal democratic model.

In 2016, at the second World Internet Conference, Chinese President Xi Jinping outlined what China considered the cornerstones of internet governance:[20]

– Respect for cyber sovereignty
– Safeguarding peace and security
– Fostering open cooperation
– Building good order

The need for control and "good order" have been baked into Beijing's model of techno-authoritarianism. According to a report from Freedom House, an NGO, along with the building of telecommunication networks and infrastructure, China has been cultivating the political and media elites in client states, and is providing training and instruction on how to manage cyberspace and citizen behavior in a manner that mirrors Beijing's modus operandi.[21]

> China's system of digital authoritarianism is fundamentally incompatible with the liberal democratic model.

Surveillance cameras installed in Tiananmen Square, Beijing (Source: Jack Hynes/Flickr)

176 countries are actively using AI technologies for surveillance purposes.

Beijing has hosted, for example, two week-long seminars on "Cyberspace Management for Officials along the Belt and Road Initiative" which, according to Freedom House, covers topics such as "big data public-opinion management systems," and tools for "positive energy public-opinion guidance system."[22]

Chinese surveillance AI

According to a working paper by the Carnegie Endowment for International Peace, globally, 176 countries are actively using AI technologies for

surveillance purposes and sixty-four countries are using facial recognition systems.

Chinese companies, including Huawei, Hikvision and Dahua – all on the US restricted entity list – supply AI surveillance technology in sixty-three countries, thirty-six of which are part of China's Belt and Road Initiative (BRI). Huawei, alone, is responsible for providing AI surveillance technology to at least fifty countries worldwide.[23]

Figure 1 – Global use of Chinese AI surveillance technology

Regions using Chinese AI surveillance technology

Regions using other AI surveillance technology
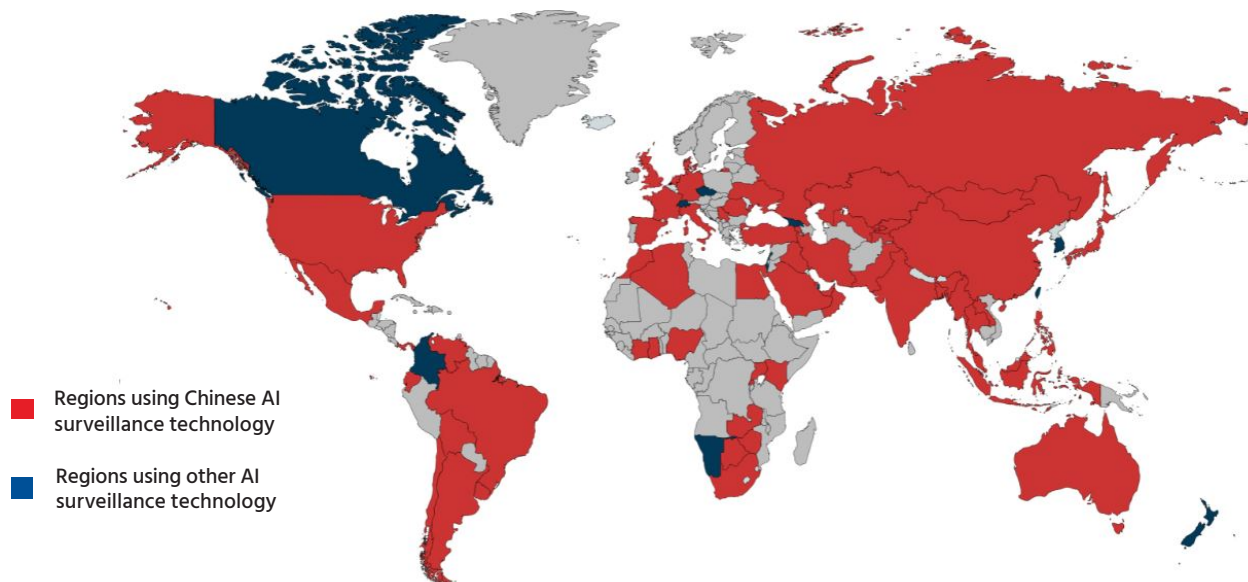
Countries using Chinese companies to supply their AI surveillance technology					
Algeria	China	Iraq*	Mexico	Rwanda*	UAE*
Argentina	Denmark	Italy*	Mongolia*	Saudi Arabia*	UK
Armenia*	Ecuador	Ivory Coast	Morocco*	Serbia*	US
Australia	Egypt*	Japan	Netherlands	Singapore*	Uruguay
Bahrain*	France	Kazakhstan*	Nigeria	South Africa*	Uzbekistan*
Bangladesh*	Germany	Kenya*	Oman*	Spain	Venezuela*
Bolivia*	Ghana	Kyrgyzstan*	Pakistan*	Tajikistan*	Zambia
Botswana	Hong Kong	Laos*	Panama*	Thailand*	Zimbabwe
Brazil	India	Malaysia*	Philippines*	Turkey*	
Myanmar*	Indonesia*	Malta	Romania*	Uganda	
Chile	Iran*	Mauritius*	Russia*	Ukraine*	

*Countries included in China's Belt and Road Initiative

Chinese AI surveillance companies		
CEIEC	Megvii*	Huawei*
CloudWalk*	SenseTime*	ZTE*
Dahua*	Yitu*	Hikvision*

*Companies on the US Entity List

Source: https://carnegieendowment.org/publications/interactive/ai-surveillance

The spread of techno-authoritarianism

As Chinese technology becomes more widely used around the world, delinking it from Beijing's overarching value system has become increasingly difficult, if not impossible. A number of examples involving developing countries have added to this view.

The Philippines – Under the Duterte regime, media groups have attended courses in China on "Socialist Journalism with Chinese Characteristics." The Philippines has ignored US pressure to block Huawei from building the country's 5G networks.[24] The spread of both the censorship and the repression of journalists in the Philippines under the Duterte regime has been linked directly to Beijing's techno-authoritarian model.

Malaysia – In Malaysia, another country that has embraced Huawei's 5G infrastructure, the police wear facial recognition cameras provided by Yitu, a Chinese company that makes surveillance technology, which has been placed on the US restricted entity list along with other Chinese AI surveillance-tech firms such as SenseTime, Megvii and HikVision on the grounds that that these companies have been complicit in human rights violations against the Uighur population in China's Xinjiang province.

Bolivia – Authorities in Bolivia have deployed more than 2,500 facial recognition cameras as part of the country's BOL-110 Integrated System of biometric surveillance technology for "Citizen Security."[25] Surveillance tech companies like Dahua and HikVison are part of a Chinese ecosystem including Huawei, which is also building Bolivia's 5G network.

Zimbabwe – In Zimbabwe, the government has partnered with CloudWalk, a Chinese company, to implement a real-time surveillance system that utilizes facial recognition technology.[26] Long known for its oppressive rule under strongman Robert Mugabe, Zimbabwe's new regime, under Emmerson Mnangagwa, has continued in the vein of authoritarian rule and is representative of how surveillance technology is being used in less developed countries to monitor and silence political opponents and critics.[27]

The African Union headquarters, Addis Ababa – In what is considered an early catalyst to Washington's campaign against China technology companies, the French newspaper, Le Monde, reported that a China-built computer network, used in the African Union building in Addis Ababa, allegedly had a "backdoor" inserted that allowed for the direct transfer of data to a server in Shanghai.[28] The African Union building, which was completed in 2012, was built at a cost of US$200 million, and was a "gift" from the Chinese government. This reflected a common practice throughout Africa, where Beijing has been building infrastructure and public facilities such as stadiums, hospitals and roads in countries where it has commercial and geopolitical interests. In 2017, some five years after the network had been installed at the African Union building, technicians noticed a peak in data usage between midnight and

2:00 am every night when the building was empty. An investigation revealed that the African Union's confidential data was being copied onto servers in Shanghai.

All of these examples demonstrate a clear linkage between the use of technology and the extension of Beijing's distinct political and ideological techno-nationalist objectives. From a European perspective, growing awareness of this phenomenon is accelerating its "rebalance" with China.

EU policy makers have grown increasingly proactive in suspending existing EU-China initiatives.

Clashing values and diverging geopolitics

As a reaction to China's expanding model of techno-authoritarianism, EU policy makers have grown increasingly proactive in either suspending existing EU-China initiatives or looking to create new constraints on Chinese behavior within Europe.

Since the EU's coronavirus document affair, described above, Beijing's ongoing actions regarding the internment and forced "education campaigns" of ethnic Uighur Muslims in Xinjiang province and the imposition the national security law in Hong Kong have galvanized EU policy makers to take further actions regarding the rebalancing of Sino-EU relations.

In June 2020, members of the European Parliament adopted a resolution condemning China's security law in Hong Kong, and called for the filing of a case against the Chinese government in the International Court of Justice.[29]

The EU's crisis of conscience over human rights issues has also shifted to other more market oriented challenges: after more than seven years of negotiations, the EU-China Comprehensive Agreement on Investment (CAI), has been put on hold, indefinitely. EU policy makers have concluded that Beijing is unlikely to change its practices regarding state subsidies, market access, technology transfer and IP protection.

The EU is now fully engaged in weighing the costs and benefits of having a major economic partner that is not only a "systemic rival" but a regime whose political values are increasing at odds with EU core values.

China's 17+1 strategy in Europe

Figure 2 – Confucius Institutes in the "17+1" countries

Number of Confucius Institutes in each country

Members of the 17+1 format

■ EU 17+1 members ■ Non-EU 17+1 members ■ EU member states ■ Non-EU member states

Source: https://chinaobservers.eu/wp-content/uploads/2020/04/CHOICE_Empty-shell-no-more.pdf

Beyond techno-authoritarianism, ubiquitous digital media have amplified and exacerbated geopolitical fears regarding a rising China.

In August 2020, the EU's foreign policy chief, Josep Borrell, accused Beijing of employing a "divide and rule" tactic with its member states. One of the issues driving Mr Borrell's assertion was China's so-called "17+1" arrangement with the smaller Central and Eastern European countries, many of which have been targeted for strategic infrastructure and investment, including the education, telecommunications and tourism sectors – all areas that would increase Chinese influence and political leverage.

Additionally, Chinese investments in ports throughout Europe, including COSCO's majority ownership in Greece's Piraeus port, and its pressing efforts to invest in Lithuania's port of Klaipeda, have set off alarms in European capitals.

Hungary, Poland, the Czech Republic and Slovakia have been recipients of the majority of Chinese money. Greece recently joined the platform in 2019, which is seen as an important link in Beijing's Belt and Road Initiative.

Policy makers, thought leaders and the general public throughout the 17+1 group have become disenchanted with Beijing, concluding the relationship has been one-sided and less about reciprocal trade than about advancing China's geopolitical ambitions.

Much of this discourse has played out along with allegations of digital influence campaigns and the weaponization of social media.

Some key events which have effectively dented the 17+1 platform:

China trade imbalances and deficits
In 2018, the value of accumulated deficit with China, within the group, totaled some US$75 billion.[30]

Disinformation and influence campaigns
In 2019, the Chinese embassy in Prague surreptitiously financed a course at the most prestigious university in the country, the Charles University, with the aim of spreading the official Chinese party narrative regarding the BRI – which external experts called propaganda.[31]

Also included in the operation: funding for a series of Charles University branded BRI conferences, designed to promote CCP content, again, for which the Chinese embassy remained a silent promoter.

Utilizing social media for political influence and coercion
In 2019, in Vilnius, Lithuania, a public gathering in support of pro-democracy protest in Hong Kong, was met by a crowd of pro-Beijing counter protesters which engaged in heckling and intimidation. The event had been organized and directed over social media by Chinese diplomats, who were on the scene.

These seemingly small, inconsequential events, when magnified on social media, have exacerbated broadly held negative perceptions of Beijing's agenda in Europe and have paved the way for further rounds of geopolitical recalibration.

As Sino-US relations deteriorate, Washington will accelerate efforts to block Chinese tech firms from expanding into overseas markets.

Europe's pivot to digital democracy

Differences in the application of technology around privacy, free speech and surveillance have driven the world's democracies to collaborate in advancing common standards. The US and the EU will form the bedrock of this block, which will draw in Canada, Australia, New Zealand, Japan and others. India, despite a record of heavy-handed treatment of internet freedoms, is tilting toward joining this pro-democracy camp, a development that will have historic consequences for China and the world's techno-nationalist landscape.

As Sino-US relations deteriorate, Washington will accelerate efforts to block Chinese tech firms from expanding into overseas markets, through, for example, its Clean Networks initiative.[32] Beijing will respond by accelerating is own supply chain "de-Americanization" efforts. It will also try to pull Europe more closely into its orbit and in general, drive a wedge between America and its historic allies.

But the chances of Beijing achieving this last objective are decreasing substantially.

New international technology alliances and AI partnerships

The US and the EU, together, account for more than 30% of the world's GDP. If Japan, the UK, South Korea, Canada, Mexico and Australia are added, the world's leading democracies contribute more than 45% of global GDP. With India included, this number jumps to more than 50% of global GDP. China is now at about 17% of global GDP, based on purchasing power parity, making it the world's largest economy, just barely edging out the US.[33]

In terms of R&D, as we detailed in a previous Hinrich Foundation study, if the US and EU R&D investment expenditures are combined, these two markets dominate the world's innovation landscape. Furthermore, the majority of the world's top ranked research universities are in North America and the EU, in high concentrations, making the possibilities of successful EU-US technology alliance very high.
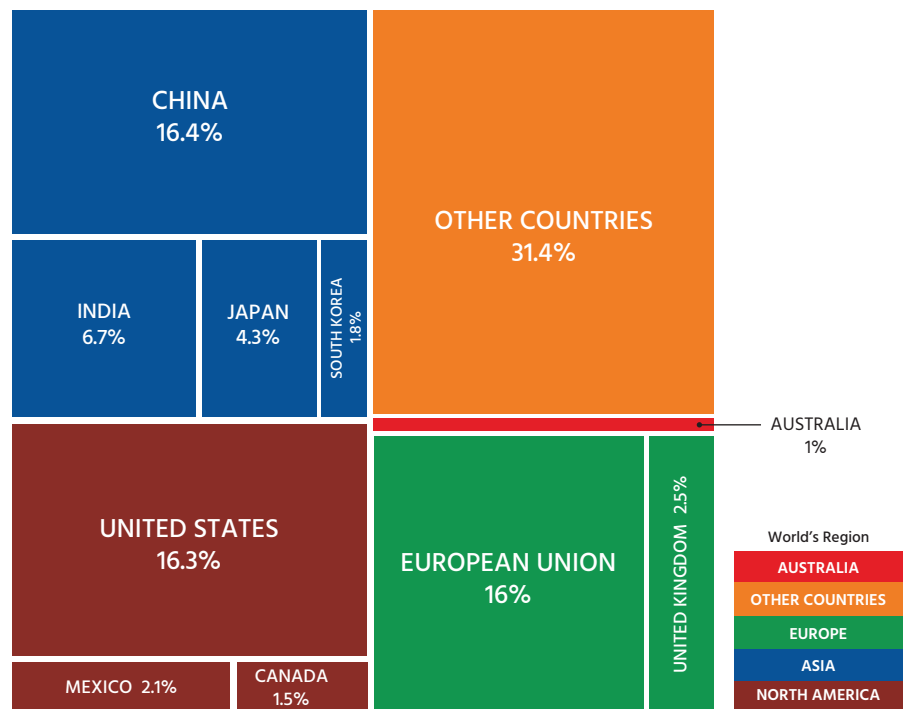
US-EU technology partnerships

A series of international partnerships and collaborative alliances have emerged, all with the objective of promoting democratic standards and values around the use of technology.

The G7 AI Pact
In May of 2020, the US joined other G7 members – Canada, France,

A series of international partnerships have emerged with the objective of promoting democratic standards and values around the use of technology.

The US and the EU, together, account for more than 30% of the world's GDP.

Figure 3 – Digital democracies equal approximately 50% of global GDP (PPP basis)

CHINA 16.4%

OTHER COUNTRIES 31.4%

INDIA 6.7%

JAPAN 4.3%

SOUTH KOREA 1.8%

AUSTRALIA 1%

UNITED STATES 16.3%

EUROPEAN UNION 16%

UNITED KINGDOM 2.5%

MEXICO 2.1%

CANADA 1.5%

World's Region
AUSTRALIA
OTHER COUNTRIES
EUROPE
ASIA
NORTH AMERICA

Note: Graph not to scale

Source:
https://howmuch.net; https://ec.europa.eu/eurostat/documents/2995521/10868691/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e

Germany, Italy, Japan and the UK, in a technology-focused pact with the purpose of studying and providing recommendations to encourage the creation of AI technologies that respect privacy and civil liberties.

The US, under the Trump administration, had not been appreciative of the effectiveness of multilateral organizations, in general, but the group's objective of serving as a countermeasure to China's techno-nationalist model, in particular, finally moved the US to join the pact.[34]

The Global Partnership on AI (GPAI)
Similar to the G7 AI Pact, the GPAI is an international initiative created by France and Canada along with Australia, the EU, Germany, India, Italy, Japan, Mexico, New Zealand, the Republic of Korea, Singapore, Slovenia, the UK and the US.[35]

The GPAI's mission is to guide responsible development and use of AI in a distinctly democratic way. In the same spirit of the EU's other "progressive" agreements involving, for example, trade, the GPAI emphasizes:

– Inclusion
– Diversity
– Innovation
– Economic growth

The GPAI also seeks to instigate a series of funded public-private research partnerships focused not only on AI technical standards but also on privacy, free speech, and surveillance.

Issues of data privacy and data ownership are also problematic in today's data capitalism model.

Other factors driving technology alliances

Even as the US and the EU work to form partnerships around common standards as countermeasures to Chinese techno-nationalism, they will pursue transatlantic techno-diplomacy on other matters, particularly to sort out differences over digital taxation and European anti-trust regulations against the big American "FAANG" (Facebook, Alphabet, Amazon, Netscape, Google) companies.

Issues of data privacy and data ownership are also problematic in today's data capitalism model – or as Shoshana Zuboff calls it: "surveillance capitalism."[36] But these differences will not deter the EU from recalibrating its commercial ties with China or stop it from its pivot to the US.

As the G7 AI Pact, the GPAI and other coalitions – such as NATO's cyber defense organizations – evolve, they will tap into key trends that are driving today's economic and political zeitgeist.

These include the establishment of new sovereign wealth funds to boost innovation in industries of the future and other initiatives designed to protect key sectors. These "neo-mercantilist" measures are a direct response to China's state-centric model and its economic practices. While these measures are anathema to the laissez-faire economic mind-set – despite that model having been upended by decades of Beijing's economic policies and trade practices – they are a necessity in today's techno-nationalist landscape.

European sovereign technology fund

Having lacked a sovereign wealth fund in the past, the EU has established its EUR100 billion "Future Fund"[37] which is designed to promote a new generation of European tech companies, and protect existing local companies – some of which are currently in a distressed state because of the economic effects from the coronavirus – from acquisition by foreign tech giants including the American FAANG and the Chinese BAT (Baidu, Alibaba, Tencent) companies.

From a US perspective, this is not necessarily a bad thing, considering Europe's sovereign fund will also trigger an increase in transatlantic public-private partnerships around ongoing AI initiatives, such as the GPAI and NATO's cyber – partnerships, which, in turn, will bring together new ecosystems of companies, including start-ups, venture capital funds and universities.

Regardless of which party and candidate wins the 2020 US presidential election, techno-nationalism will continue to drive investment in new digital infrastructure, partnerships, and alliances.

US "repair & prepare" technology initiatives

US presidential candidate Joe Biden has proposed a US$300 billion technology fund[38], which would include investment in next generation wireless networks and other digital infrastructure in the US. This is part of a larger proposed US$700 billion plan that would seek to not only "repair" aging infrastructure, but "prepare" for the future by investing in education, R&D and building a new digital infrastructure.

One major component of this plan involves the development of "clean-tech", as a policy response to climate change. Here, the EU – which, from a competitive standpoint, missed out on the first wave of the tech innovation around the digital economy – has a burgeoning clean tech sector that could participate in America's public spending initiatives.

The same applies for other US spending initiatives, including the US$100 billion Endless Frontier Act[39], designed to develop AI and other leading-edge technology in the US. EU and US G2G efforts will produce partnerships that will be, like the GPAI and G7 AI Pact, inclusive of companies pursuing democratic values.

Here, for example, Nokia and Ericsson, two European telecommunication equipment manufacturers, could see increased involvement in the US technology landscape – particularly as they step up open-sourced collaboration around 5G networks.

Regardless of which party and candidate wins the 2020 US presidential election, techno-nationalism will continue to drive investment in new digital infrastructure, partnerships, and alliances. Meanwhile, China's ongoing Made in China 2025, Digital Belt and Road and other initiatives will underscore the importance of a revived transatlantic partnership.

Successful partnerships and alliances, however, require transparent and functional rules frameworks.

II. Impact of techno-diplomacy on international institutions

Liberal democracies are especially vulnerable to hybrid warfare.

The world of 2020 presents NATO with an entirely new kind of threat.

NATO

For the past seventy years, the North Atlantic Treaty Organization (NATO) has been the bedrock of the transatlantic security alliance, which now includes thirty member countries, most of which are in Europe. Led by the United States, NATO was instrumental in assuring conventional military preparedness on land, sea and in the air during the Cold War with the former Soviet Union. This war effectively came to an end in 1989, when the Berlin Wall, an emblem of decades of super-power rivalry, was torn down.

Hybrid warfare

The world of 2020 presents NATO with an entirely new kind of threat, one for which missiles and aircraft carriers are of little or no use: hybrid warfare.

Hybrid warfare occurs below the threshold of armed conflict and involves a mix of economic, cyber, diplomatic and information-related actions, all of which are designed to disrupt or disable an opponent without engaging in open hostilities.

Liberal democracies are especially vulnerable to hybrid warfare as hostile actors have learned, in particular, to weaponize open political systems and free speech by leveraging social media platforms to sow disinformation and stoke social disharmony. Recent documented events regarding attempts to influence elections in the US and in Europe, for example, have been attributed to Russia.[40]

Hybrid warfare and the media

Chinese diplomats are becoming more active on western social media platforms. (Source: Pixabay)

A major component of China's soft power and influence projection involves the scaling up of its foreign broadcasting presence overseas

In 2019 and 2020, events involving China's imposition of the national security law in Hong Kong, and the spread of the coronavirus, resulted in Chinese diplomats and other officials migrating to western social media platforms such as Twitter, WhatsApp and Facebook. A review of social media messages by more than 100 Chinese diplomats, as reported by the media company, POLITICO, revealed a four-fold increase in online posts by Chinese officials from a year earlier.[41]

This so called "wolf-warrior" digital messaging campaign was oriented towards promoting Beijing's narrative of pro-democracy protests in Hong Kong and discrediting unfavorable views on China's handling of the initial coronavirus outbreak in Wuhan. The campaign included the circulation of conspiracy theories, including one that stated the coronavirus was a creation of the US military.[42]

In general, social media has become an increasingly toxic arena. But as state-actors have learned to conduct influence operations in this space, NATO has doubled down on its efforts to build new frameworks for pursuing info-war countermeasures.

Traditional television broadcasting is also becoming a fixture in the hybrid warfare landscape. A major component of China's soft power and influence projection involves the scaling up of its foreign broadcasting presence overseas. According to a report from The Economist, Beijing is spending billions[43] to position its TV broadcasting in local markets around the world.

China Media Group, for example, one of China's largest state-owned media companies, is looking to set up headquarters in Brussels. Known as "the voice of China," it acts as the umbrella organization for CGTN, another rapidly expanding state-owned network.[44]

In June 2020, the American government required China's major media news agencies in the US to register as "foreign missions," due to being "substantially owned and effectively controlled" by the CCP.[45]

This development has been watched closely in the EU as it deliberates on how to regulate foreign companies that receive state funding while operating in the EU. The European commission may eventually audit and vet such companies to determine if they merit an operator's license. Among other things, fair reporting, transparency and independence may become criteria for approval of a broadcasting license in the EU.

NATO's cyber defense response

NATO's transition to a cyber-oriented defense institution began in 2016, when the organization declared cyberspace a domain of warfare. This transition is occurring increasingly through techno-diplomacy, which involves member countries' military, government officials and non-state actors, such as cybersecurity firms.[46]

At a summit in 2018 of NATO Leaders, it was divulged that cyber security threats had become more "frequent, complex, destructive and coercive."[47] NATO's Cyber Defense Pledge calls for the defense of critical national networks and infrastructure. Each ally has the responsibility to improve its resilience and ability to respond quickly and effectively to cyber-attack and other hybrid warfare threats.

Figure 4 – Distribution of cyber-attacks in selected global regions during 1st half 2020, by category
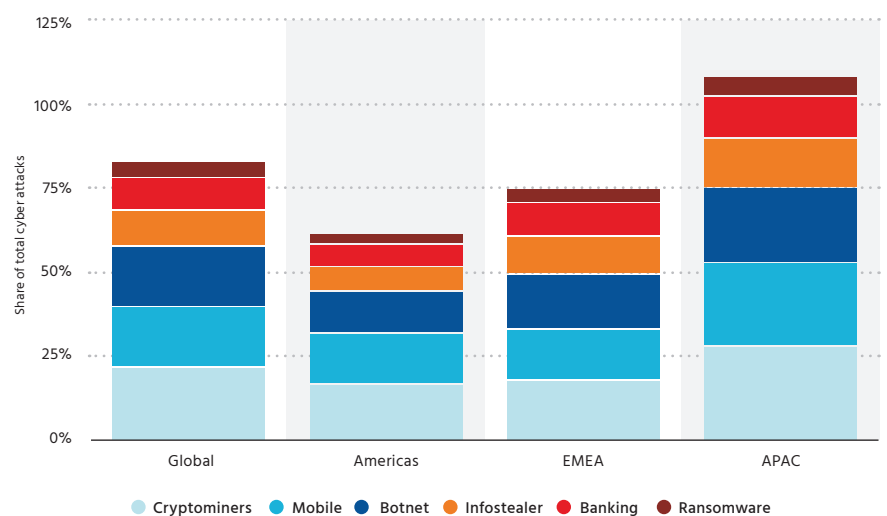
Source: Check Point Software Technologies, Statista

Additional information: Worldwide; Check Point Software Technologies; H1 2020

Since 2016, this pledge has been the catalyst for a series of initiatives designed to facilitate NATO's transition, including:

Cyberspace Operations Center (CYOC)

A fully dedicated entity charged with strategic planning, coordination, intelligence gathering and oversight of key cyber operations.

NATO Cooperative Cyber Defense Center of Excellence

Responsible for developing human capital and talent through education, training and innovation programs.

Cyber Coalition

Organizes and oversees NATO's joint exercises and manages scenario preparedness and crisis management exercises.

NATO Industry Cyber Partnership

Facilitates and enables public-private partnerships with technology companies, cyber security firms, academic institutions and other stake holders.

Just as hybrid warfare combines information, economic, security, diplomatic and other elements, cyber-defense requires more public-private partnerships that blur the line between commercial and military objectives. This outcome mirrors the rationale behind the concept of "dual-use," which applies to export controls designed to control or block the flow of controlled technologies to restricted entities.

In the context of NATO's cyber defense efforts, non-state actors will be pulled into strategic partnerships, which will also make them targets of cyber-attack. We will cover this topic, in more depth, in a subsequent report in this series on techno-nationalism and cyber-security.

NATO Article 5 Collective Defense Commitment

Under Article 5 of the NATO Charter, an attack against any one member of the alliance constitutes an attack against all, requiring other members to come to another member's defense. In 2019, NATO Secretary General Jens Stoltenberg stated that in the event of

> Cyber-defense requires more public-private partnerships that blur the line between commercial and military objectives.

First NATO Council meeting at the new NATO headquarters in Brussels.
(Source: NATO/Flickr)

"serious" cyber-attack, the collective commitment under Article 5 would be triggered.

The techno-diplomatic challenges of cyber warfare

The US and its NATO allies are confronted with two fundamental challenges, both of which are being addressed through techno-diplomacy. In the first instance, there is the question of what constitutes a "serious threat" regarding cyber security, and, in the second instance, how is "sovereignty" defined in cyberspace? Both questions are important as they will need to be properly answered before NATO establishes clear rules – for friend and foe alike – for triggering Article 5.

The US and its NATO allies are confronted with two fundamental challenges, both of which are being addressed through techno-diplomacy.

Meanwhile, in 2018, the US Congress and the White House expanded the rules regarding cyber warfare and the kinds of methods US Cyber Command – under the US Department of Defense – could employ in hybrid warfare.[48] The laws produced two concepts that will change the way NATO engages in cyber warfare:

– Forward presence
– Persistent engagement

Both allow offensive and pre-emptive cyber operations aimed at state and non-state actors. Thus, as the US and its allies increase these types of offensive activities, they are likely to accelerate

decoupling in other areas of the technology landscape, from perceived "non-secure" threats such as Chinese social media platforms and cloud infrastructure.

According to numerous reports, in 2018, US Cyber Command launched a preemptive attack on the Internet Research Agency in St Petersburg – an alleged Russian troll[49] factory – during the US November mid-term elections, effectively shutting down its networks and preventing it from spreading misinformation.[50]

A less lethal form of techno-diplomacy involves old fashioned public attribution: when a bad actor is exposed, it is publicly named and shamed. More powerful states in the alliance can resort to other punitive actions, including sanctions, export controls, cancellation of investment and other types of diplomatic and economic reprisals. A perfect case of public attribution involves the US campaign against Huawei.

Within NATO, the US, the UK, Netherlands, Denmark and Estonia and Lithuania – two Baltic States that suffered massive cyber-attacks – have used public attribution after being targets of cyberattacks. Public attribution is increasingly linked to social media campaigns.

"China Standards 2035"

The spread of Chinese technical standards would facilitate techno-authoritarian practices such as "social credit scores" and biometric ID and surveillance practices.

One of China's most grandiose – some would say, unrealistic – techno-nationalist ambitions involves its "China Standards 2035" plan. This medium-term strategy compliments the Made in China 2025[51] plan which outlines Beijing's goal of dominating manufacturing in 10 leading emerging and foundational industries of the future, including 5G, robotics, machine learning and semiconductors.

China Standards 2035 takes things a step further, beyond just dominating manufacturing, by enabling Chinese companies to dictate global interoperability standards and functions for hard technologies as well as systems and platforms. This would confer huge advantages to China, by perpetuating a virtuous cycle of up-scaling its home grown technology ecosystems around the world, and, simultaneously, by giving Beijing the ability to weaponize its digital monetary systems, surveillance and censorship technologies, and other commercial systems.

China Standards 2035 is focused on two dimensions:

Hard technologies
Beijing wants to set international standards regarding the technical aspects, functions, and interoperability of key types of equipment and "hard" systems. This includes autonomous vehicles, advanced manufacturing systems and robotics, machine learning and quantum computing, additive manufacturing (3D printing), advanced materials, 5G communications infrastructure and more.

Soft technologies
Soft technologies include AI algorithms, encryption for cyber security, social media and other digital platforms and apps.

Taking advantage of ubiquitous underlying "hard" technologies and infrastructure – made by state-backed companies – China Standards 2035 would allow Beijing to scale-up its technology footprint around the world and push out competing systems. As these hard technology ecosystems dominate, the CCP would use them to standardize practices around censorship, surveillance, and citizen monitoring – as is documented elsewhere in this report.

As such, the spread of Chinese technical standards would facilitate techno-authoritarian practices such as "social credit scores" and biometric ID and surveillance practices, which would be linked to commercial inclusion or marginalization, for example.

China, multilateral institutions and technology standards
Beijing's central planners have made it a priority to gain influence in multilateral technology standard setting institutions. For the past several decades, the CCP has been placing Chinese techno-diplomats in key international standards bodies such as:

- International Telecommunication Union (ITU)

- The International Standards Organization (ISO)

– the International Electrotechnical Commission (IEO)

– The Institute of Electrical and Electronics Engineers (IEEE)

These multilateral standards-setting institutions have been – until now – disproportionately lobbied by Chinese companies.

US techno-diplomacy and international standard setting institutions

The US Department of Commerce recently revised its rules regarding US companies' interaction with Chinese restricted entities in order to allow for increased participation and lobbying at international technical standards institutions.

Huawei, in particular, has been very active in influencing international standards setting at the ITU and IEEE, largely because, as a restricted entity, US companies were prohibited from interacting with it, without a special license. Thus, American firms stayed away from important public events and meetings, thereby ceding influence to their Chinese rivals.[52]

Now that the US, the EU and the world's other digital democracies are beginning to coalesce around common digital standards and practices, they are turning their attention to multilateral standards setting institutions.

These collaborative campaigns between Washington and its allies will make it virtually impossible for Beijing to see China Standards 2035 through to fruition – another sign of the growing efficacy of US techno-diplomacy.

Washington is pivoting away from a one-dimensional approach of export control enforcement and moving towards leveraging institutions.

Wassenaar Arrangement: Techno-diplomacy and export controls

Washington is pivoting away from a one dimensional approach of export control enforcement and moving towards leveraging institutions. Despite the Trump Administration's disdain for international organizations, American unilateralism has turned to selective multilateralism – if and when it can be used to thwart China's techno-nationalist agenda.

Despite America's turning away from its historic leadership role in the world's international institutions, for many of which the US was the chief architect,

its influence over these institutions remains relatively strong.

One such entity is the Wassenaar Arrangement.[53] This group of forty-two member countries has been entrusted with a voluntary export control regime. Its members exchange information on transfers of conventional weapons and dual-use goods and technologies.[54]

Through these exchanges, Wassenaar was designed to promote "greater responsibility" among its members regarding the exports of weapons and, increasingly, to monitor and control the disbursement of dual-use goods,

---

Figure 5 – Wassenaar member countries & US techno-diplomacy semiconductor export licensing

■ Key semiconductor global value chain countries and key US allies

■ Historic US allies & digital democracies. *India has done a recent techno-nationalist pivot toward the US, despite having a poor record regarding internet freedoms.

■ Non-EU and/or non-NATO

Argentina	Estonia	Japan	Norway	South Africa
Australia	Finland	Latvia	Poland	Spain
Austria	France	Lithuania	Portugal	Sweden
Belgium	Germany	Luxembourg	South Korea	Switzerland
Bulgaria	Greece	Malta	Romania	Turkey
Canada	Hungary	Mexico	Russia	Ukraine
Croatia	India*	Netherlands	Slovakia	United Kingdom
Czech Republic	Ireland	New Zealand	Slovenia	United States
Denmark	Italy			

Source: https://www.wassenaar.org/participating-states/#contact-links-box-AR

Source: https://chinaobservers.eu/wp-content/uploads/2020/04/CHOICE_Empty-shell-no-more.pdf

with the aim of preventing hostile actors from receiving these controlled technologies.[55]

The Wassenaar Arrangement utilizes virtually the same nomenclature for export control classification numbers (ECCN) as the American system and mirrors Washington's controlled commodities and technologies lists. The system serves as a harmonized international export control and licensing framework that governments and businesses have been using for compliance enforcement and corporate governance since 1995.

Wassenaar's Cold War origins

Wassenaar's roots go back to the end of World War II, to the US and Soviet Union cold war-era, where it was known as the Coordinating Committee for Multilateral Export Controls (COCOM). It was created to restrict exports to the former Soviet Union and Eastern bloc, and motivated by concerns that the Soviet Union

would acquire controlled technologies that would further its advancement of nuclear weapons capabilities.

Unlike COCOM, in today's Wassenaar, members lack veto authority over other members' proposed exports, a power that COCOM members exercised – and through which the US used to exert its will on a regular basis.

Washington's renewed interest in Wassenaar is driven by a host of realpolitik conclusions:

– Unilateral actions by the US regarding technology transfer to China are far less effective than multilateral efforts exercised through strategic partners.

– Joint enforcement of export controls requires harmonization of functional rules and procedures among members – something Wassenaar provides in abundance.

Washington's renewed interest in Wassenaar is driven by a host of realpolitik conclusions.

Soviet nuclear missiles being paraded through the Red Square at the height of the Cold War, circa 1963. (Source: Reddit)

– Export controls, alone, will delay but not prevent technology transfer to hostile actors, thus they should be accompanied by targeted diplomacy, purpose-driven alliances and cooperative ventures.

Despite not having a veto mechanism in Wassenaar, the US has been effectively influencing the organization, primarily to leverage its techno-nationalist weapon of mass destruction: semiconductor technology.

Washington has leveraged its Wassenaar partnerships to tighten its chokehold on US technology in semiconductor value chains.

Washington has leveraged its Wassenaar partnerships to tighten its chokehold on US technology in semiconductor value chains. As we have documented in previous reports in this techno-nationalism series, US companies dominate key components of the global semiconductor value chain, including research and design capabilities and specialized manufacturing and tooling equipment, all of which are vital for production of microchips.[56]

China, by contrast, lacks these capabilities and Beijing's tech-champions, from Huawei to Tencent, remain highly vulnerable to losing access to US semiconductor technology. At the time of this publication, Washington's campaign to block Huawei's access to semiconductor technology has put the company in "survival mode," and Huawei's 5G infrastructure and smart phone businesses in existential crisis.[57]

China's top techno-nationalist priority, therefore, centers on developing its own domestic semiconductor capabilities and reducing its dependence on American businesses. To do so, however, it must obtain critical IP, technology, and talent from abroad, at a time when the US and its allies are turning to multilateral institutions to block these efforts.

Semiconductors and Wassenaar

The latest changes to the Wassenaar Arrangement reflect growing consensus around the US's intentions to cut off semiconductor technology to Chinese interests.

Within the Wassenaar group, the US and its historic allies UK, France, Germany, Japan and others were instrumental in revising export controls on military-grade cyber software and semiconductor manufacturing technology. This action was a countermeasure to an increase in cyberattacks and cyber intrusions with suspected links to China.[58]

Japan threw the full weight of its support behind this action, as Mitsubishi Electric Corp. and NEC Corp., – both, major players in the nation's semiconductor and defense and infrastructure industries – are frequent targets of cyber intrusion and corporate espionage.

The latest changes to the Wassenaar arrangement reflect growing consensus

around the US's intentions to cut off semiconductor technology to Chinese interests. Blocking access not only delays Beijing's use of technology to further its broader geopolitical objectives, it retards the CCP's corporate espionage and cyber intrusion capabilities.

The two latest revisions are aimed at highly specialized portions of the semiconductor value chain:

1. **Computational software designed for the development of patterns on extreme ultraviolet lithography.** Computational lithography allows semiconductor manufacturers to simulate real circuit models and correct deviations during wafer manufacturing. It is mainly used to solve problems such as nano-

Figure 6 – Share of the global semiconductor industry by country in 2018 and 2019
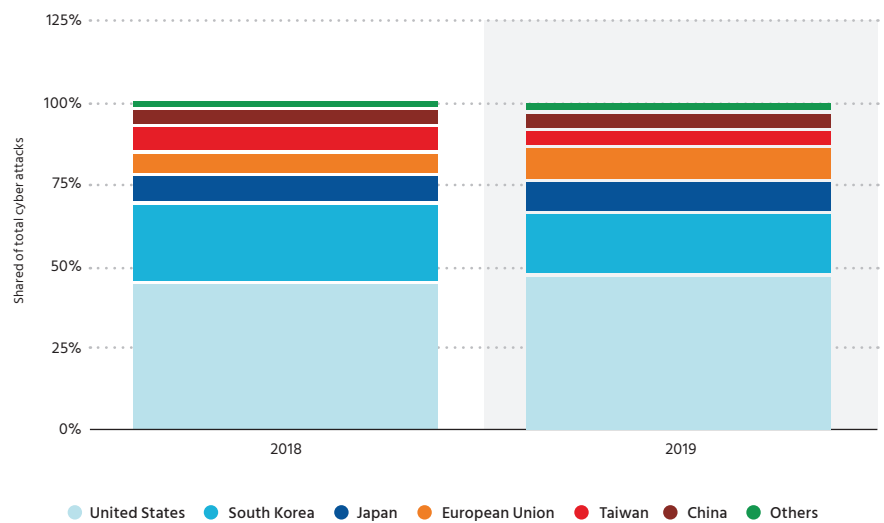
Source: SIA, Statista 2020

Additional information: Worldwide; SIA; 2018 to 2019

The door is closing for Chinese companies when it comes to alternatives to US tech.

scale mask repair, chip design/ manufacturing defect detection and correction during semiconductor manufacturing.[59]

A small handful of companies dominate the technology in this space, namely, the Dutch and the Americans. ASML, in the Netherlands, owns specialized software, as do KLA Tencor, Synopsis, Mentor Graphics and Ansys, all American companies. Another American software company, Cadence Design, was recently acquired by Siemens of Germany, representing another Wassenaar member country that has been formulating countermeasures to Chinese techno-nationalism.

In the case of the Netherlands, the US government has turned to diplomatic pressure, in order to prevent the issuance of an export license by the Dutch government to ASML, for the sale of extreme ultra-violet lithography machines to China. Thus, by adding software to the list of controlled items, the door is closing for Chinese companies when it comes to alternatives to US tech.

2. **Technology required for the slicing, grinding and polishing of 300 mm (12 inch) silicon wafers.** A wafer is a thin slice of semiconductor, such as a crystalline silicon, used for the fabrication of microchips. The wafer serves as the substrate for microelectronic technology built in and upon the wafer.

China currently has no capabilities for mass producing high yield (the margin of error is almost impossible to achieve) 300 mm wafers.

The market for slicing and grinding silicon wafers is controlled by five companies: Shin-Etsu and Sumco of Japan, Global Wafer from Taiwan, Germany's Sitronic, and SK Siltron from South Korea. Japanese companies control more than half the market.[60]

An equally small number of American, European, and Japanese companies dominate the market for wafer polishing.

These actions represent increased multilateral efforts, let by the US, to counteract Beijing's techno-nationalist agenda. More broadly, they demonstrate how the US and its allies are collectively leverage international institutions such as the Wassenaar Arrangement to achieve their own objectives.

III. Techno-diplomacy's impact on international rules frameworks

The WTO has failed to produce the necessary rules framework, and the world needs to find ways to create and execute new rules frameworks.

When it comes to governance of trade, the digital economy has upended the world's existing institutions and rules frameworks.

The world requires new rules frameworks to address the challenges of the digital economy. New rules addressing e-commerce, digital taxation, e-identities, dispute resolution and data privacy have not been harmonized or universally defined.

The world needs to find ways to create and execute these new rules frameworks. This could involve revamping existing organizations such as the WTO, to take on, for example, the function of an "e-WTO." Otherwise, more realistically, groups of countries would take it upon themselves to establish new agreements and mechanisms to define and enforce their unique values and standards.

These types of arrangements could include:

– Multilateral FTAs with specified digital/technology focused rules and standards

– Bilateral FTAs with specified digital/technology rules and standards

– Digital-only agreements (more narrow than an FTA with digital sub-sections) between specific parties

Can the WTO be revamped and rehabilitated?

Since 1995, the modern-day WTO has been the designated multilateral institution charged with facilitating the rules for international trade. It has set and enforced harmonized rules around customs valuation and rules of origin, for example, and has provided a dispute resolution mechanism for trade disagreements between countries.

Another role of the WTO involves its function of providing a forum for trade liberalization. Here, when viewing trade liberalization in the context of the digital economy, the WTO has failed to produce the necessary rules framework.

In 2019, about half of the 164 member WTO countries launched discussions on new rules to accommodate digital commerce – dealing with issues such e-signatures and identities, the banning of duties on e-commerce and on-line services transactions, cyber-security and other issues.[61] These talks continue but the large number of participating countries involved make it unlikely that a consensus will emerge. And, even if agreement was possible, with such a large group of countries participating, the amount of time it takes to reach any agreement is simply too long.

China as a digital rules obstructionist

More fundamentally, because of Beijing's export model of techno-authoritarianism, which relies on technology and AI for censorship and surveillance, China has obstructed efforts of other countries to craft digital standards tied to transparency, privacy rights and free speech.[62]

In 2001, China became a member of the WTO on the grounds that it would commit to liberalizing its economy. Many erroneously believed that China's ascension to the WTO would lead to

its adoption of free market behavior as well as a shift toward a more open, democratic political process.

China has doubled down on its state capitalist model of massive government subsidies, protectionism and forced technology transfer.

China's Communist Party has, however, doubled down on its state capitalist model of massive government subsidies, protectionism and forced technology transfer. Politically, the CCP hardened its repressive practices as well, thus the WTO seems an unlikely forum for the world's open market democracies to press their case for a new digital rules' framework.

The US has also placed its own national priorities ahead of compliance with WTO rules.

The US has also placed its own national priorities ahead of compliance with WTO rules. In September 2020, a WTO panel announced that the US had violated WTO rules by imposing tariffs on China, the EU and others, under the Section 301 Investigations undertaken by the USTR. Washington's response was unequivocal: the US would ignore the WTO ruling and proceed as it wished.

Should US presidential candidate Joe Biden win the 2020 election, there is speculation that this new administration would seek to reform the WTO. Perhaps the dispute resolution mechanism would be bolstered. Nonetheless, the future status of the WTO remains uncertain.

Coalitions of the willing

A question that has begun to circulate in trade policy circles is: could a coalition of willing nations form a new global trade institution with standards that require open market principles and democratic ideals? Such a forum would have to exclude China and other nations with "non-market" economies.

Countries are more likely to utilize free trade agreements (FTAs) or other standalone agreements to define and frame their digital rules.

These ideas were recently proposed by Mogens Peter Carl, a former European Commission Director General for Trade

and the Environment.[63] Such a move would signal a paradigm shift back to an era of "managed trade," something which is anathema to the liberalized trade model. Yet China's mercantilist model of managed trade has already effectively upended the liberal, open trading system, thus continuing with the status quo would only perpetuate Beijing's unfair trade advantages.

Free trade agreements with digital rules and frameworks

Rather than trying to reengineer or create new rules frameworks at large bureaucratic institutions such as the WTO, or create an alternative institution to the WTO, countries are more likely to utilize free trade agreements (FTAs) or other standalone agreements to define and frame their digital rules.

Multilateral FTAs
Multilateral FTAs require all members to adhere to a harmonized set of rules, which would make digital trade a more seamless experience.

The Comprehensive and Progressive Transpacific Partnership (CPTPP), for example, currently with eleven existing member countries, including Japan, Singapore, Vietnam, Canada and Australia, has specific chapters devoted to digital trade. Thus, in the future, techno-diplomacy efforts may gravitate towards multilateral agreements, given the seamlessness of having one set of rules that applies across a wide area and many nations. This encourage more countries to aspire to join these trade blocks.

However, if new rules or standards are proposed and must be negotiated, the amount of time it takes for multiple governments to agree could take years.

Bilateral FTAs

The forging of trade agreements between just two countries may present the better option when it comes to negotiating rules that apply to a rapidly changing digital landscape. The time it takes for two parties to negotiate the terms of a bilateral deal is much faster than what is required for a multi-lateral negotiation.

Ideally, a bilateral trade deal would include a section that addresses standards and rules for digital commerce. Even if one does not exist, it might be added at a later date. Again, this would be much easier to do between two countries, than in a multilateral setting.

Digital-only agreements

Rather than embedding a chapter on digital trade inside a more comprehensive multilateral or bilateral free trade agreement, some countries are resorting to "digital only" agreements.

Trade ministers from 11 countries gathered in Chile, Santiago, March 2018 to sign the CPTPP. (Source: Subsecretaría de Relaciones Económicas Internacionales de Chile/Flickr)

The Digital Economy Partnership Agreement

An example of digital-only agreements is the Digital Economy Partnership Agreement (DEPA)[64], which includes New Zealand, Singapore, and Chile. The DEPA is ground-breaking in that it incorporates a robust rules framework that addresses:

– Data privacy and security
– Transparency
– Digital identities
– AI ethics
– Payment platforms and Fintech standards
– Dispute settlement mechanisms

The DEPA, which incorporates interoperability through digital platforms, such as Singapore's Networked Trade Platform, could well become the prototype of larger multilateral digital trade agreements and could also be replicated in other bilateral digital-only agreements.

DEPA is an example of successful techno-diplomacy, in this case to promote standards that enable open markets and digital democracy.

The US State Department's Blue Dot program[65] represents a further attempt to create rules frameworks for digital finance. The Blue Dot program brings together governments, the private sector and civil society under shared standards for global infrastructure development. Certification by the Blue Dot Network would serve to validate market-driven, transparent, and financially sustainable development projects.

Blue Dot Network was designed to attract private capital to infrastructure projects in developing and emerging economies, and aims to serve as a countermeasure to China's model of government funded infrastructure, such as the digital Belt and Road, which has been spreading techno-authoritarianism.

Yet another multilateral arrangement with forward looking rules involves India, Australia and Singapore, and their efforts to create a resilient supply chain initiative that would include digital trade rules[66]. Here, again, we see techno-diplomacy at work, this time in a coalition of the willing involved in efforts to build digital trade rule frameworks into supply chains.

As the US-China technology cold war continues to spill over into politics, economics and society, policy makers and business leaders will become further affected by the many variations of techno-diplomacy.

This will require not only new rules frameworks and the modification of existing institutions, it will demand an entirely new way of executing corporate good governance – across physical supply chains and the management of data and digital platforms.

This will be the featured topic of the next Hinrich Foundation report in our ongoing series on techno-nationalism.

Researcher bio:
Alex Capri

Alex Capri is a research fellow at the Hinrich Foundation and a senior fellow and lecturer in the Business School at the National University of Singapore. He also teaches at the NUS Lee Kuan Yew School of Public Policy.

He is the author of *Techno-Nationalism: How it's reshaping trade, geopolitics, and society* (Wiley), due out in 2021.

From 2007-2012, Alex was the Partner and Regional Leader of KPMG's International Trade & Customs Practice in Asia Pacific, based in Hong Kong. Alex has over 20 years of experience in global value chains, business and international trade – both as an academic and a professional consultant.

He advises governments and businesses on matters involving trade and global value chains. Areas of focus include: IT solutions for traceable supply chains, sanctions, export controls, FTAs and trade optimization.

Alex has been a panelist and workshop leader for the World Economic Forum. He writes a column for Forbes Asia, the Nikkei Asian Review and other publications and is a frequent guest on global television and radio networks. He holds a M.Sc. from the London School of Economics, in International Political Economy. He holds a B.Sc. in International Relations, from the University of Southern California.

Alex Capri

Research Fellow,
Hinrich Foundation and
Visiting Senior Fellow,
The NUS Business School

Endnotes

1 "Announcing the Expansion of the Clean Network to Safeguard America' Assets", US State Department press statement, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

2 Capri, A., "Techno-Nationalism: What Is It And How Will It Change Global Commerce?", Forbes, 20 December 2019, https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-is-it-and-how-will-it-change-global-commerce/#6a9deb1710f7

3 "UK seeks alliance to avoid reliance on Chinese tech: The Times", Reuters, 29 May 2020, https://www.reuters.com/article/us-britain-tech-coalition/uk-seeks-alliance-to-avoid-reliance-on-chinese-tech-the-times-idUSKBN2343JW

4 Since placing Huawei on the restricted entity list in May of 2019, Washington has effectively crippled the company. As of September 2020, the US has choked off Huawei's access to critical American microchip technology, which it needs to build smart phones and 5G network infrastructure. Once Huawei burns through an emergency stockpile of microchips, the world's largest manufacturer of telecoms equipment will lose its capability to service existing 5G contracts and to build new networks.

5 Whalen, J., "US restricts tech exports to China's biggest semiconductor manufacturer in escalation of trade tensions", The Washington Post, 27 September 2020, https://www.washingtonpost.com/technology/2020/09/26/us-restricts-exports-chinas-smic/

6 Wong, C.H., "China Launches Initiative to Set Global Data-Security Rules", The Wall Street Journal, 8 September 2020, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974#:~:text=Under%20its%20new%20%E2%80%9CGlobal%20Initiative,a%20text%20released%20by%20the

7 Burchard, H., "EU slams China as 'systemic rival' as trade tension rises", POLITICO, 3 December 2019, https://www.politico.eu/article/eu-slams-china-as-systemic-rival-as-trade-tension-rises/

8 The Wassenaar Arrangement, https://www.wassenaar.org

9 Federal Reserve History, Creation of the Bretton Woods System, https://www.federalreservehistory.org/essays/bretton_woods_created

10 Congressional Research Service, Section 301 of the Trade Act of 1974, 31 August 2020, https://crsreports.congress.gov/product/pdf/IF/IF11346

11 "EU-US Privacy Shield for data struck down by court", BBC, 16 July 2020, https://www.bbc.com/news/technology-53418898#:~:text=A%20major%20agreement%20governing%20the,Court%20of%20Justice%20(ECJ).&text=US%20Secretary%20of%20Commerce%20Wilbur,deeply%20disappointed%22%20by%20the%20decision

12 In September 2020, a dispute panel at the WTO ruled that the US's imposition of duties on China, the EU and other countries violated WTO rules. Perhaps more significantly, however, the US has publicly stated it will ignore the WTO's verdict, a sign that the WTO is in danger of becoming irrelevant. This will be explored later in the report.

13 Chee, F.Y., "EU throws new rule book at Google, tech giants in competition search", Reuters, 1 July 2020, https://www.reuters.com/article/us-europe-tech-google-antitrust-analysis/eu-throws-new-rule-book-at-google-tech-giants-in-competition-search-idUSKBN242623

14 Chee, F.Y., "Amazon may face EU antitrust charges over merchant data in coming weeks: source", Reuters, 12 June 2020, https://www.reuters.com/article/us-eu-amazon-com-antitrust/amazon-may-face-eu-antitrust-charges-over-merchant-data-in-coming-weeks-source-idUSKBN23I2V7

15 Asen, E., "What European OECD Countries Are Doing about Digital Services Taxes", Tax Foundation, 22 June 2020, https://taxfoundation.org/digital-tax-europe-2020/

16 European Commission, "China", Trade policy by countries and regions, https://ec.europa.eu/trade/policy/countries-and-regions/countries/china/

17 European Commission, "The EU's Response to COVID-19", 24 February 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_307

18 Friedman, L., Trump Serves Notice to Quit Paris Climate Agreement, The New York Times, 4 November 2019, https://www.nytimes.com/2019/11/04/climate/trump-paris-agreement-climate.html

19 Apuzzo, M., "Pressured by China, EU Softens Report on Covid-19 Disinformation", The New York Times, 24 April 2020, https://www.nytimes.com/2020/04/24/world/europe/disinformation-china-eu-coronavirus.html?auth=login-email&login=email

20 Wang, C., "Four principles on Internet governance reflecting a global norm based on international law", ResearchGate, February 2016, https://www.researchgate.net/publication/300046593_Four_principles_on_Internet_governance_reflecting_a_global_norm_based_on_international_law

21 Shahbaz, A., "The Rise of Digital Authoritarianism", Freedom House, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

22 Ibid

23 Feldstein, S., "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace, 17 September 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

24 Heydarian, R., "Ignoring the US, Philippines goes with Huawei", Asia Times, 18 July 2019, https://asiatimes.com/2019/07/ignoring-the-us-philippines-goes-with-huawei/

25 Burt, C., "Chinese biometric surveillance technology deployed internationally amid criticism", Biometric, 23 October 2019, https://www.biometricupdate.com/201910/chinese-biometric-surveillance-technology-deployed-internationally-amid-criticism#:~:text=Authorities%20in%20Bolivia%20have%20deployed,China%20to%20export%20its%20citizen

26 Ibid

27 Zimbabwe's Mnangagwa vows to 'flush out opponent', BBC, 4 August 2020, https://www.bbc.com/news/world-africa-53642492

28 Dahir, A., "China 'gifted' the African Union a headquarters building and then allegedly bugged it for state secrets", Quartz, 30 January 2018, https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/

29 Timsit, A., "Parliaments are on the frontlines of Europe's face-off with China", Quartz, 20 June 2020, https://qz.com/1870052/eu-parliaments-are-shaping-their-countries-china-policy/

30 Elmer, K., "Europe's '17+1' countries dissatisfied with China relations, report says, as summit is postponed", South China Morning Post, 7 April 2020, https://www.scmp.com/news/china/diplomacy/article/3078830/europes-171-countries-dissatisfied-china-relations-report-says

31 EURACTIV Network, "China funded 'propaganda' course at Czech University", 31 October 2019, https://www.euractiv.com/section/politics/news/china-funded-propaganda-course-at-czech-university/

32 US Department of State, The Clean Network, https://www.state.gov/the-clean-network/#:~:text=The%20Clean%20Network%20program%20is,as%20the%20Chinese%20Communist%20Party

33 Eurostat, "China, US and EY are the largest economies in the world", 19 May 2020, https://ec.europa.eu/eurostat/documents/2995521/10868691/2-19052020-BP-EN.pdf/bb14f7f9-fc26-8aa1-60d4-7c2b509dda8e

34 Chafkin, M., "US Will Join G7 AI Pact, Citing Threat From China", Bloomberg, 28 May 2020, https://www.bloomberg.com/news/articles/2020-05-28/g-7-ai-group-adds-u-s-citing-threat-from-china?sref=jeNvC3eC

35 French government, "Launch of the Global Partnership on Artificial Intelligence", 17 June 2020, https://www.gouvernement.fr/en/launch-of-the-global-partnership-on-artificial-intelligence

36 Naughton, J., "The goal is to automate us': welcome to the age of surveillance capitalism", The Guardian, 20 January 2019, https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

37 Financial Times, "EU floats plan for €100bn sovereign wealth fund", 23 August 2019, https://www.ft.com/content/033057a2-c504-11e9-a8e9-296ca66511c9

38 "Joe Biden proposes a $700 billion-plus 'Buy American' campaign", CNBC, originally from Associated Press, 9 July 2020, https://www.cnbc.com/2020/07/09/biden-proposes-a-700-billion-plus-buy-american-campaign.html

39 Mervis, J., "US lawmakers unveil bold $100 billion plan to remake NSF", Science, 26 May 2020, https://www.sciencemag.org/news/2020/05/us-lawmakers-unveil-bold-100-billion-plan-remake-nsf

40 Simmons, A., "Russia's meddling in other nations' elections is nothing new. Just ask the Europeans", Los Angeles Times, 30 March 2017, https://www.latimes.com/world/europe/la-fg-russia-election-meddling-20170330-story.html

41 Scott, M., "Chinese diplomacy ramps up social media offensive in COVID-19 info war", POLITICO, 29 April 2020, https://www.politico.eu/article/china-disinformation-covid19-coronavirus/

42 Myers, S., "China Spins Tale That the US Army Started the Coronavirus Epidemic", The New York Times, 13 March 2020, https://www.nytimes.com/2020/03/13/world/asia/coronavirus-china-conspiracy-theory.html

43 The Economist, "China is spending billions on its foreign-language media", 14 June 2018, https://www.economist.com/china/2018/06/14/china-is-spending-billions-on-its-foreign-language-media

44 Parrock, J., "Voice of China's European ambitions", POLITICO, 8 September 2020, https://www.politico.eu/article/china-europe-media-voice-ambitions-global-television-news-cgtn-global-television-news/

45 US Department of State, "Designation of Additional Chinese media Entities as Foreign Missions", 22 June 2020, https://www.state.gov/designation-of-additional-chinese-media-entities-as-foreign-missions/

46 Brent, L., "NATO's role in cyberspace", NATO Review, 12 February 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html#:~:text=The%20CyOC%20serves%20as%20NATO's,coordination%20for%20cyberspace%20operational%20concerns

47   NATO, "Defending against cyber-attacks", https://www.nato.int/cps/en/natohq/topics_118663.htm?selectedLocale

48   American Journal of International Law, "US military undergoes restructuring to emphasize cyber and space capabilities", Vol. 1143, Issue 3, July 2019, pp. 634-640, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/us-military-undergoes-restructuring-to-emphasize-cyber-and-space-capabilities/CE983ACA46178DBCB0CD7DBE50DE8FF4

49   The Cambridge Dictionary defines a troll as "Someone who leaves an intentionally annoying message on the Internet, in order to get attention or cause trouble." The goal is to trigger emotional or sometimes violent reactions, which, when applied at scale to social groups and populations, can stoke antagonisms, spread lies, and lead to political instability and social unrest.

50   Nakashima, E., "US Cyber Command Operation disrupted Internet access of Russian troll factory on day of 2018 midterms", The Washington Post, 27 February 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

51   Made in China 2025 (MIC 2025) was released by the Ministry of Industry and Information Technology in 2015.

52   Wei, H., Murphy, F., "Update: US to Allow Cooperation With Huawei on 5G Standards", Caixin, 8 May 2020, https://www.caixinglobal.com/2020-05-08/update-us-to-allow-cooperation-with-huawei-on-5g-standards-101551250.html

53   The Wassenaar Arrangement, https://www.wassenaar.org

54   Dual use goods are products or technologies that have been designed for commercial uses but could also be used for military applications. This covers the majority of the world's emerging and foundational technologies for the industries of the future.

55   "The Wassenaar Arrangement at a Glance", Arms Control Association, December 2017, https://www.armscontrol.org/factsheets/wassenaar#:~:text=The%2042%20participating%20states%20in,Netherlands%2C%20New%20Zealand%2C%20Norway%2C

56   Capri, A., "Semiconductors at the heart of the US-China tech war", Hinrich Foundation, 17 January 2020, https://www.hinrichfoundation.com/research/wp/tech/semiconductors-at-the-heart-of-the-us-china-tech-war/

57   Cheng, T.F., Li, L., "Huawei in 'survival mode' as suppliers race to beat US deadline", Nikkei Asian Review, 25 August 2020, https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-in-survival-mode-as-suppliers-race-to-beat-US-deadline#:~:text=%22Huawei%20is%20in%20a%20chaotic,survival%20for%20the%20Chinese%20company.&text=%22Huawei%20is%20battling%20for%20survival.%22

58   Kyodo News, "Int'l group agrees to control military software exports", 23 February 2020, https://english.kyodonews.net/news/2020/02/36cfd58a338e-intl-group-agrees-to-control-military-software-exports.html

59   Ariat Technology, "New Wassenaar agreement 'arranges' Chinese semiconductors, increase export controls on computational lithography software and large silicon technology", https://www.ariat-tech.com/news/New-Wassenaar-agreement-arranges-Chinese-semiconductors-increase-export-controls-on-computational-li.html

60   Ibid.

61   European Commission, "76 WTO partners launch talks on e-commerce", 25 January 2019, http://trade.ec.europa.eu/doclib/press/index.cfm?id=1974

[62] Peker, E., "US, China Face Off Over Digital-Market Regulation", The Wall Street Journal, 6 March 2019, https://www.wsj.com/articles/u-s-china-to-face-off-over-digital-market-regulation-11551878261

[63] Stewart, T., "A new WTO without China? The July 20, 2020 Les Echos opinion piece by Mogens Peter Carl, a former EC Director General for Trade and then Environment", WITA, 25 July 2020, https://www.wita.org/blogs/a-new-wto-without-china/

[64] New Zealand Ministry of Foreign Affairs and Trade, DEPA Modules, https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/digital-economy-partnership-agreement/depa-modules/

[65] US Department of State, Blue Dot Network, https://www.state.gov/blue-dot-network/

[66] The Straits Times, "Japan, India and Australia working on achieving supply chain resilience", originally from Bloomberg, 2 September 2020, https://www.straitstimes.com/asia/east-asia/japan-india-and-australia-working-on-achieving-supply-chain-resilience

hinrich foundation
advancing sustainable global trade

The Hinrich Foundation is a unique Asia-based philanthropic organization that works to advance mutually beneficial and sustainable global trade.

We believe sustainable global trade strengthens relationships between nations and improves people's lives.

We support original research and education programs that build understanding and leadership in global trade. Our approach is independent, fact-based and objective.

MEDIA INQUIRIES

Ms. Berenice Voets,
Director of Public Affairs
T: +852 9081 8210
berenice.voets@hinrichfoundation.com

There are many ways you can help advance sustainable global trade.
Join our training programs, participate in our events, or partner with us in our programs.
inquiry@hinrichfoundation.com

Receive our latest articles and updates about our programs by subscribing to our newsletter

hinrichfoundation.com

 hinrichfdn
 hinrichfoundation
 hinrich foundation
 hinrichfoundation