CEPA

Injecting Security into European Tech Policy

ABOUT CEPA

The Center for European Policy Analysis (CEPA)'s mission is to ensure a strong and enduring transatlantic alliance rooted in democratic values and principles with strategic vision, foresight, and impact. Through cutting-edge research, analysis, and engagement, we provide innovative insight on trends affecting democracy, security, and defense to government officials and agencies; we help transatlantic businesses navigate changing strategic landscapes; and we build networks of future leaders versed in Atlanticism.

Cover Illustration: Michael Newton/Center for European Policy Analysis. Illustration Photos: A wafer is seen at the new Bosch 300-millimeter wafer fab for silicon chips in Dresden, Germany, May 31, 2021. Credit: REUTERS/Matthias Rietschel; Thierry Breton, February 23, 2023. Credit: Bogdan Hoyaux/European Commission; Export shipping containers and commercial electronics with dual use semiconductor microchips. Credit: Unsplash

Contents

FOREWORD

When Washington discusses new regulations, it always considers security. When the European Union (EU) ponders similar new regulations, it almost never does. This gap, while understandable, is unfortunate.

The EU is not a military alliance. It leaves national security priorities to NATO and its 27 member states. EU regulations have historically been enacted without proper security vetting. This results in high risks.

CEPA's series, *Injecting Security into European Tech Policy*, highlights and details these risks, which are becoming more dangerous as the EU moves ahead with a broad range of significant tech regulations. The EU has imposed drastic restrictions on the largest US tech companies, limiting what businesses and activities they can pursue. It is on the verge of imposing new, protectionist cybersecurity rules that could eject US cloud companies from the continent. And now, it is adopting new rules to restrain the rise of artificial intelligence.

The regulatory offensive coincides with a critical time in transatlantic relations. Russia's full-scale invasion of Ukraine highlights the importance of technology on the battlefield — and in protecting critical infrastructure. China's aggressive rise threatens Western technological leadership.

In response, both the EU and the US are bolstering domestic production of semiconductors and tightening sanctions and export controls. While positive, these moves need to be coordinated. Instead, protectionism and a quest for "digital sovereignty" on both sides of the Atlantic threaten transatlantic cooperation.

The US, for its part, has ceded much tech policy leadership to the EU. There is still no US federal privacy law. There are still no new federal rules for dealing with disinformation and illegal online content. There is an antitrust push against large US tech companies, but courts are pushing back. And the US has provided no effective opposition to potentially threatening European regulations.

Transatlantic relations suffer. US and European views on pushing back against Russian aggression and Chinese authoritarianism converge. We need to build on this alignment when it comes to a democratic vision for tech policy that puts innovation and competitiveness first. This means working together, not unilaterally. It means addressing, not ignoring, our differences over digital regulation. Above all, it means realizing that technology is central to our joint security.

Dr. Alina Polyakova
President and CEO
Center for European Policy Analysis

EXECUTIVE SUMMARY

It's been a dramatic one-two punch. Russia invaded Ukraine. China ramped up its authoritarian ambitions. On both sides of the Atlantic, these national security crises and challenges spotlight policies governing digital technology, from cybersecurity and export controls to semiconductor production and artificial intelligence.

The transatlantic alliance depends on deep coordination on the rules governing tech — and yet, unfortunately, the US and EU find themselves moving in different, contrary directions. *Injecting Security into European Tech Policy* is a series of policy papers examining the increasing distance in five areas — competition policy, cybersecurity, semiconductor subsidies, artificial intelligence, and export controls.

Europe and the US enjoy complimentary instincts. Both want to bolster domestic protection of key technologies. Both want to limit Russian and Chinese access to the same key technologies. Both even use the same vocabulary to describe their goal vis-à-vis China — de-risking, not de-coupling. And yet, differing priorities and political systems often lead to divergent and conflictual policies, preventing effective coordination.

Start with cybersecurity. As Janna Brancolini recounts in "*Europe Upgrades its Cybersecurity Arsenal — Frightening the US*," Russia's invasion of Ukraine created a cybersecurity crisis. European leaders feared that Russian hacking would bring down Ukraine's infrastructure. This catastrophe was averted. Ukraine's banks kept operating. Trains continued to run. Although cruise missiles hit the Ukrainian government's data center, Microsoft, VMware, and other Western companies protected the data by dispersing it outside of the country.

Ukraine's success depended on strong private-public partnerships and a willingness to put aside counterproductive ideas about data localization and digital sovereignty. Instead of learning these lessons, Brancolini writes that European policymakers are focusing on an arbitrary crusade against private tech companies. They are preparing to impose a certification scheme on cloud computing companies that will make it difficult for the three biggest providers, Amazon, Microsoft, and Google, to do business on the continent simply because they are American.

Like the EU, the US is making cybersecurity a priority. Russian and Chinese hackers have launched numerous cyberattacks on US infrastructure and even the email accounts of US Secretary of Commerce Gina Raimondo. The Biden Administration has responded with a new National Cybersecurity Strategy, setting concrete timelines and goals for the defense of critical infrastructure. But the US plan omits specifics around data privacy, digital identity, and cloud risk. Fundament changes require congressional approval, unlikely with a paralyzed House of Representatives.

Photo: United States Secretary of Commerce Gina Raimondo and European Commissioner for Competition Margrethe Vestager (left) and European Commissioner for Internal Market Thierry Breton and European Commissioner for Trade Valdis Dombrovskis (right) speak during a Transatlantic Tech Council Meeting in Paris, May 15, 2022. Credit: Jean-Louis Carli/European Commission.

A similar story is playing out with semiconductors. As Christopher Cytera writes in *"Confronting China and Catching Up on Chips,"* the EU and the US are aligned on the security risks of an unstable semiconductor supply chain. Both are responding by supporting domestic industries. They need to coordinate — or risk competing against each other rather than against China.

Success is far from certain. Timelines differ. The US raced ahead of the EU in approving its legislative proposal and spending billions of dollars on subsidies. Critics fear overlap and that the funding could be spent on white elephant projects. Instead of building giant new chip manufacturing foundries, Cytera concludes that the funds should be used on overcoming "choke points." The EU should concentrate on its competitive advantage in chip design, optics, and chemicals. The US should emphasize its software strengths.

Competition policy poses less discussed but perhaps equally important security risks. Both the EU and the US are concerned about the potential excessive power of the largest tech platforms. The Biden Administration has launched a series of antitrust cases against Google, Microsoft, and Amazon. But courts have pushed back and blocked much of this aggressive antitrust enforcement.

Europe has gone much further, passing a potentially revolutionary new law, the Digital Markets Act. As Bjorn Lundqvist writes in *"Reining in the Gatekeepers and Opening the Door to Security Risks,"* the new rules target the world's largest digital platforms, almost all American, from Alphabet, Amazon, and Apple to Meta and Microsoft.

The restrictions are far-reaching. As an example, Apple must unlock its App Store, and Google must no longer collect data from Maps and YouTube and combine it with Google Search data without users' specific consent. Meta must allow its WhatsApp messaging service to accept calls from competitors such as Signal and Telegram. Violators face penalties of up to 20% of their global revenue for repeated violations.

These requirements and restrictions hold potentially far-reaching dangers. Gatekeepers must give away data — potentially to enemies. They can no longer vet their operating systems and app stores for security. Almost anyone — even Russian and China — can obtain access. When gatekeeper messaging apps — Skype, WhatsApp, and iMessage — open up their interfaces to other messaging services to provide interoperability, their own services risk becoming disarmed against security breaches.

While the US tech leaders rush to comply with the Digital Markets Act, they are also rushing to adopt artificial intelligence. The emergence of ChatGPT which can explain complex concepts in a flicker, has catapulted the technology to the front page. The EU is responding with broad, sweeping legislation, now in its final negotiations, while the US is enacting only voluntary commitments.

The disconnect is dangerous, write Ylli Bajraktari and Lauren Naniche in "*Transatlantic Community Must Unite to Address AI Risks and Opportunities*." If the US and EU don't work together, China will win, the authors warn. The EU's go-it-alone prescriptive approach will prove difficult to enforce and, faced with a fast-evolving technology, could soon be outdated. Perhaps worse, it threatens to divide the allies, burying hopes for a united democratic approach to AI.

Export controls are perhaps the issue most directly concerned with security. The US and EU agreed on tough sanctions against Russia in response to the invasion of Ukraine. They also agree on "de-risking" from China, working together to limit the exports of the most advanced semiconductors and manufacturing equipment.

But the two sides struggle to coordinate, writes Matthew Eitel in "*Export Controls — The Keys to Forging a Transatlantic Tech Shield.*" The US enjoys well-established regulations to protect its 'economic security.' It imposes controls quickly and unilaterally. In contrast, the EU must forge a consensus among its 27 member states, each of which insists on pursuing its own national prerogatives and sovereignty.

Photo: President Joe Biden delivers remarks on his agenda for “Investing in America”, Tuesday, March 28, 2023, at the Wolfspeed semiconductor manufacturing facility in Durham, North Carolina. Credit: Cameron Smith/White House.

EU and US political priorities also differ. The US now places national security concerns at the center of its international economic agenda, willing to sacrifice trade in the name of protecting US security. While the EU has hardened its view of economic engagement with China, key member states such as Germany remain skeptical of the trade-offs required to closely align their approach with that of the US.

While perhaps the most pressing, the issues addressed in this series are far from exhaustive. The transatlantic alliance faces other key tech-related security challenges. Among them: How to draw Europe away from Chinese telecom infrastructure and how to allow Europe’s desire for increased data sharing without allowing our enemies to take advantage?

Despite persistent American pressure, the EU, particularly Germany, continues to allow China’s Huawei to build its crucial mobile phone infrastructure. At the same time, the EU remains skeptical about an innovative, inexpensive mobile phone operating system called Open RAN — even though Open RAN contains no Chinese parts. Once again, the culprit seems to be Europe’s misguided quest for digital

sovereignty. Asian and American companies lead in the development of Open RAN. The new way of building mobile phone systems threatens European tech heavyweights Ericsson and Nokia.

Data is becoming another key area of divergence. The EU just passed a new Data Act. On the surface, the idea sounds promising and noble — the digital equivalent to the Schengen Area, within which EU citizens are allowed to move and work without restriction. Just as the EU has promoted free travel, it now envisions a series of measures to facilitate data open sharing. But free personal travel looks much less dangerous to achieve than free data transfers. Policymakers did not even consider how the Data Act could leak crucial information, including to Russian and Chinese companies.

Both European and US companies lobbied hard against the Data Act, arguing it jeopardized their own competitiveness as well as national security. European policymakers in Brussels did not listen. The natural venue for transatlantic discussions, the Trade and Transatlantic Council, never was consulted. EU officials, led by EU Commissioner Thierry Breton, say European domestic regulations are not negotiable.

That's a mistake. Both Europe and the US must stop avoiding their differences in tech policies. They must work together, not against each other. Nothing should be off the table when it comes to transatlantic security — including tech policy.

Bill Echikson
Senior Fellow, Digital Innovation Initiative
Center for European Policy Analysis


COMPETITION
ANTITRUST
REGULATIO
Commission européenne

Reining in the Gatekeepers and Opening the Door to Security Risks

By Björn Lundqvist

The EU should not accept every request from digital gatekeepers to avoid regulation, but it should be careful before dismissing legitimate security concerns.

The European Union's (EU's) regulatory offensive against the world's largest digital platforms, from Amazon and Apple to Meta and Microsoft, is designed to increase competition on the Internet. Its new Digital Markets Act (DMA) prohibits these designated "gatekeepers" from sharing data among their various divisions while requiring them to share data with users, businesses, and competitors.[1]

In practical terms, the DMA means Amazon must stop favoring its own goods over those from independent vendors, Apple must unlock its App Store, and Google must no longer collect data from Maps and YouTube and combine it with Google Search data without users' specific consent. Meta must allow its WhatsApp messaging service to accept calls from competitors such as Signal and Telegram. Microsoft might be forced to end tying to the Microsoft 365 Office bundle. Violators face penalties of up to 20% of their global revenue for repeated violations. "We are putting an end to the so-called Wild West dominating our information space," vowed Thierry Breton, the EU commissioner in charge of enforcing the new rules.[2]

Although some of these changes seem justified by conventional antitrust analysis, the DMA has been enacted without proper consideration of the danger of malign entities leveraging the regulation to wage economic or, even worse, military cyber warfare. In this paper, I analyze the potential security challenges stemming from opening up digital platforms and forcing data sharing. When gatekeepers' messaging apps are obliged to allow their subscribers to receive calls from other messaging apps, end-to-end encryption and security protections could be jeopardized. When gatekeepers' app stores are forced to weaken the vetting of their developers, it threatens not just our privacy but also our protection from both private and state-operated hackers.

The landmark regulation fails to address the risk of geopolitical conflict. It falls disproportionately on Silicon Valley while sparing and perhaps benefiting Russian and, most dangerous of all, Chinese tech giants.

Opposite Illustration: Michael Newton/CEPA. Images: Left: Margrethe Vestager, June 9, 2021. Credit: John Thys/Pool via REUTERS; Center: Mobile Phone. Credit: Vojtech Bruzek/Unsplash. Right: Thierry Breton, February 23, 2023. Credit: Bogdan Hoyaux/European Commission.

The Digital Markets Act and the Gatekeepers

The DMA applies to large platforms identified as "gatekeepers." These companies, owing to their size and their importance as gateways for business users to reach customers, play an essential role on the Internet.

The market value, number of users, and turnover thresholds to designate gatekeepers are set high — a market value of more than €75 billion or a core platform counting 45 million European users or a European turnover of €7.5 billion over the past three years. Only a few companies fall within the scope. In theory, the nationality of the gatekeepers is irrelevant. In practice, almost all those targeted are US-based platforms, including Google, Amazon, Apple, and Meta.[3] As we will see, this emphasis on US companies is dangerous.

Dangerous Data Sharing

Among the many new obligations facing the gatekeepers, perhaps the most dangerous is data access. In Article 6 (10), the DMA stipulates that a gatekeeper must "provide business users and third parties authorized by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of" the business user's sale of products and provision of services. Article 6 (11) states the act targets search engines: "The gatekeeper shall provide to any third-party undertaking providing online search engines, at its request, with access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on its online search engines."

These mouthfuls translate into stiff demands and prohibitions: gatekeepers are required to share access to commercial data generated on their platforms with "business users."[4] Google will be forced to share European search queries with rivals that include Russia's Yandex or China's Alibaba.[5] At the same time, the gatekeepers are not generally allowed to make use of the same data in competition with the business user, nor are they allowed to bundle it with other personal data generated elsewhere in their ecosystem unless they receive consent from users.

Competitors and business users are supposed to benefit. They have the right to obtain all data, including aggregated data, that is generated by the users' activities on the gatekeeper platform. According to the act, "business user" refers to any natural or legal person acting in a commercial or professional capacity, who uses the core platform services while providing goods or services to end users.

Photo: Margrethe Vestager, Executive Vice-President of the European Commission in charge of Europe fit for the Digital Age, and Commissioner for Competition, and Thierry Breton, European Commissioner for Internal Market, gave a press conference, February 19, 2020. Credit: Xavier Lejeune/European Commission.

This definition is broad. It includes small firms making use of platforms to boost their business. No exemption exists to exclude companies or even governments originating from unfriendly jurisdictions. Both Russian and Chinese firms would be able to make use of the data access rule to obtain data from the gatekeepers.

This is dangerous. Under a veil of extracting and gaining data from platforms, a malicious actor could create a service to scoop up data from users. The malicious actor might use the brand name of the platform to gain credibility. Authoritarian countries have the means to do this on a large scale.

Companies originating in the EU or the United States do not have a corresponding right to access data from Chinese platforms such as Alibaba or Tencent or from Russia's Yandex search engine under Chinese or Russian law. While business users make use of US platforms in Europe, they may gain access to valuable user data that could give them a competitive edge.

Consider a few concrete examples. If Amazon's Alexa or Amazon's cloud are declared a gatekeeper service, voice assistants from competitors such as Huawei's Celia to Telefonica's Aura might be able to access data stored on them. Or consider cars. Apple and Android car systems generate reams of driving data. If declared gatekeeper services, they could be forced to share this information with other business users. Malign actors — even enemy armies — might be able to procure real-time information on traffic flows and automobile movements.

App Stores

Apple and Google control access to almost all of the world's mobile phones through their iOS and Android software, respectively. Both run app stores on top of these platforms. Three quarters of Android and iOS apps already suffer security vulnerabilities, according to a report by enterprise security company Positive Technologies.[6] Vulnerable storage of app data could allow hackers access to sensitive data such as passwords, financial details, personal data, and communications.

Apps send data to a server, which is hosted by a developer. Few protections exist to protect data stored by such a third party. Apple makes a particular point of emphasizing security for its App Store, saying that it "provides layers of protection to help ensure that apps are free of known malware."[7] Thousands of developers "deliver hundreds of thousands of apps for iOS, iPadOS, and macOS—all without impacting system integrity. And users can access these apps on their Apple devices without undue fear of viruses, malware, or unauthorized attacks."

While the app stores are insecure, the DMA could accentuate these already dangerous vulnerabilities. As gatekeeper services, Google and Apple could be forced to accept requirements to ease "sideloading," the ability of third-party application developers to upload onto the app stores without their approval. Even though this may increase competition, Apple has criticized the DMA for compromising its safeguards, saying the law "will create unnecessary privacy and security vulnerabilities."[8]

Google faces similar challenges to ensure Android's security. Although more vulnerabilities were found in Android than iOS apps, the Positive Technologies report states that "this difference is insignificant, and the overall security level of mobile application clients for Android and iOS is roughly the same." Vulnerabilities classified as "high risk" were identified in 38% of iOS apps and 43% of Android apps.[9]

App store vulnerabilities present potential national security risks that should have been taken into consideration in the DMA. This oversight is not limited to the DMA, it can be spotted in other European regulations as well. While European regulations all are reviewed for their impact on climate and privacy, former Estonian President Toomas Hendrik Ilves worries that "when it comes to security, there's no review of legislation, which is a fundamental flaw."[10] He criticizes regulators for going "after Apple" for vetting and blocking apps uploaded to iPhones that can be "used for surveillance." He said: "We cannot allow apps that help foreign entities listen to your conversations, or even shut down your electricity grid."

Photo: Smartphone app store icon. Credit: James Yarema/Unsplash

Messaging Apps

Messaging apps such Microsoft's Skype, Meta's WhatsApp and Messenger, and Apple's iMessage face stiff security challenges too. The DMA requires messaging apps owned by these gatekeepers to offer users of rival services like Signal or Telegram the ability to send and receive messages.

The goal is to promote competition. At present, it is difficult for users to move away from a service because they lose access to their friends who stay behind. Interoperability offers new services a chance to compete — offering new features and stimulating innovation.

But there are a few hitches.

Many popular messaging services are end-to-end encrypted.[11] Although the DMA says encryption should be maintained, many experts believe interoperability may require breaking this encryption. In addition, there is a tight timeline for finding a technical solution. According to the DMA, the services will be required to make "end-to-end text messaging," including various kinds of media attachments, interoperable on request by a competing service within three months of a request, beginning early in 2024[12]) Group texts will need to be interoperable in two years, and voice and video calls in four years.

These could prove to be tight timelines. Meta announced plans to interconnect WhatsApp with Messenger in March 2019; this project remains unfinished.[13] And that is within the same company, not with competitors.

Upstart messaging apps that would be interested in obtaining access to the gatekeeper's massive subscriber pool are wary because consumers demand encryption on privacy grounds. Groups such as the Electronic Frontier Foundation worry about the threat to human rights, saying encryption is "critical to protecting human rights defenders who depend upon strong security while opposing or exposing abuses in dangerous environments."[14]

Russia's invasion of Ukraine underlines the importance of messaging apps. The Ukrainian government has depended on these apps to communicate with its citizens safely and securely.[15] Its soldiers depend on them for communicating with their superiors. If Russian or Chinese messaging apps can demand interoperability, they could endanger these crucial tools.

Policy Recommendations

The DMA obligations come into effect in early 2024. Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Samsung declared in July 2023 that they meet the gatekeeper thresholds.[16] These companies are preparing compliance plans which could attempt to close these security gaps.

For both app stores and messaging services, the DMA allows gatekeepers to argue that they need to protect the "integrity" of their hardware or operating system.[17] Apple could argue that forcing users and developers to buy and sell through its App Store is the only way to protect them. Meta could argue that traffic from small messaging services could present a similar security threat.

The European Commission will then need to decide whether to accept these arguments. If it does not — and it probably will not — the companies can bring the cases to court. It could then take years to reach a final decision.

Security should not be used as a smokescreen to protect anti-competitive behavior. Yet the DMA was enacted without taking adequate account of potential dangers. The European Commission could and should exempt specific platforms on the grounds of public security, judging that the cost to society disproportionate to the potential benefit.[18] Whether the exemption can be used with the speed and flexibility needed in today's fast-moving digital environment remains unclear.

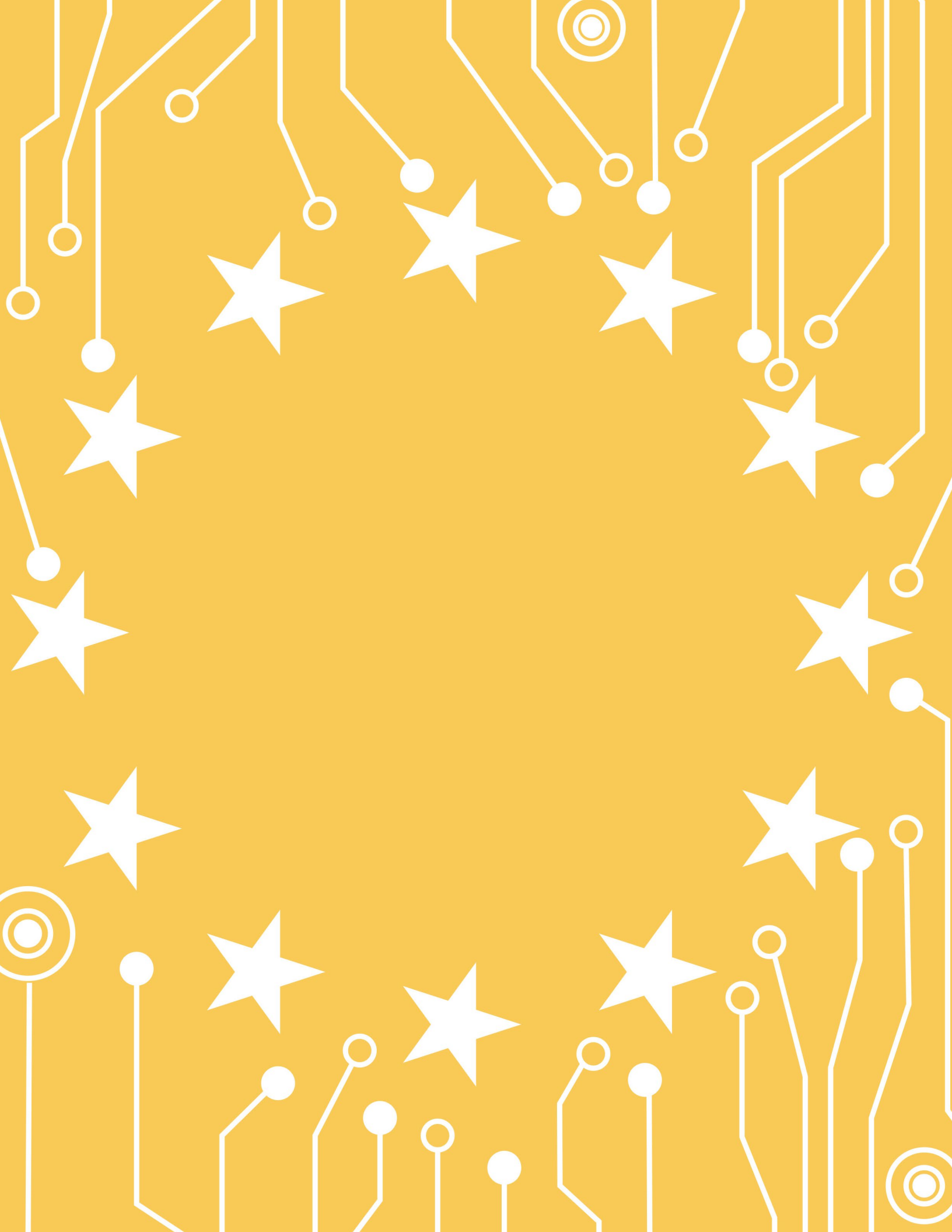
On interoperability, the European Commission should strengthen the security-protective exception for encrypted messaging. It should prohibit any messaging service that "breaks the promise of end-to-end encryption through any means—including by scanning messages in the client-side app or adding 'ghost' participants to chats" from being able to "demand interoperability," says the Electronic Frontier Foundation.[19]

Above all, the European Commission should allow gatekeepers to raise security justifications based on system integrity — even where the DMA does not explicitly allow it. If it is impossible to make encrypted messaging interoperable in the timeframe demanded by the DMA, the commission should initiate a European standards-setting and governance process to solve the issue.

There is another way to accomplish this goal — an express proportionality safeguard. A proportionality safeguard would allow companies to justify their conduct based on security, if they can.[20] In particular, a gatekeeper should be allowed to protect the legitimate security interests of its services, including system integrity. Including such a clause would improve the legitimacy of the DMA, be consistent with fundamental principles of proportionality under EU law, and come with no material downsides for effective enforcement.

Gatekeepers need to retain tools to protect security in their app stores, on their messaging apps, and in their obligations to share data while opening up for competition. The DMA says that the gatekeeper can take "duly justified" and "strictly necessary and proportionate" measures to ensure the preservation of security. As the regulation's enforcer, the European Commission should not accept every request from the gatekeepers to delay. But it should be careful before dismissing legitimate claims.

Björn Lundqvist is a nonresident senior fellow with the Center for European Policy Analysis (CEPA). He is a professor of law in the Department of Law at Stockholm University, the head of the EU Law Research Group, director of the European Law Institute, and director of Ascola Nordic.



Europe Upgrades its Cybersecurity Arsenal — Frightening the US

By Janna Brancolini

The EU's emphasis on privacy and digital sovereignty in its mission to advance cybersecurity is creating transatlantic tensions.

Three days after Russia's full-scale invasion of Ukraine on February 24, 2022, Europe's interior ministers gathered for an extraordinary meeting to address an urgent issue: How would European governments work together to repel a Russian cyberattack that could take down their essential networks?

What happened surprised them and the world: Russia's cyberattacks on Ukraine's digital infrastructure failed. Ukraine's banks kept operating. Trains continued to run. Although cruise missiles hit the Ukrainian government's data center, Microsoft, VMware, and other Western companies had protected the data by dispersing it outside of the country.[21]

Ukraine's success depended on strong private-public partnerships and a willingness to put aside counterproductive ideas about digital sovereignty. Today, the unanswered question is whether European policymakers have learned these lessons. Will they seek to strengthen private-public partnerships? Or will they respond by mandating counterproductive cloud certification and data-localization schemes?

Europe's Legislative Landscape

Europe approaches cybersecurity differently than the US, which sees it primarily as a national security issue. In the European Union, the emphasis is on protecting privacy and warding off economic danger, says Sandra Joyce, head of global intelligence at Mandiant, a cybersecurity leader.[22] Cybercrime costs Europe an estimated €5.5 trillion ($5.9 trillion) per year, according to the European Commission.[23]

In 2016, the European Parliament adopted the Network and Information Systems (NIS) Directive, the first piece of EU-wide cybersecurity legislation. The NIS Directive required member states to shore up defenses in "critical infrastructure" such as energy, transport, water, banking, and health care.[24] Operators of this critical infrastructure must notify national authorities of serious cyber incidents, and member states must share information about ongoing risks and threats.[25]

In 2021, the European Commission proposed an update called NIS 2.[26] It expanded the scope of critical infrastructure to include space, express delivery, food, waste

Illustration: Michael Newton/Center for European Policy Analysis.

management, public administration, telecommunications, and digital services such as social networks and data centers.[27]

Under both NIS 1 and 2, national authorities issue certificates confirming that a product has passed security tests commensurate with the product's risk level: basic, substantial, or high. All

EU countries are obliged to recognize the certificate, easing trade across borders and saving businesses time and money on multiple certifications, according to the European Commission.[28]

The goal of strengthening national security is never mentioned.

The NIS cybersecurity directives contain other significant flaws. They distinguish between critical and noncritical sectors, which critics warn creates a false distinction because it is difficult to impossible to separate and classify dangers in the digital world. If everything is connected, everything becomes critical infrastructure, notes Ot van Daalen, a cybersecurity researcher at the University of Amsterdam. A vulnerable camera could be used to execute a DDoS attack against an energy company, or a hacked router could be used to access a critical health care database.

The New Cyber Resilience Proposal

Europe is attempting to plug these gaps with the Cyber Resilience Act. Proposed in September 2022, it would set common cybersecurity standards for connected devices and services not already covered by regulation. [29] Products running afoul of the rulebook would face fines of up to €15 million ($16 million) or 2.5% of worldwide turnover, whichever is higher.

The act is still under negotiation, but if approved, it would make permanent the European Union Agency for Cybersecurity (ENISA), which was established in 2004 on a temporary basis.[30]Products would be classified as "default," "Class I," or "Class II."

Class I products pose minimal security risks. Their manufacturers must either follow specific standards or complete a third-party certification process. These include browsers, password managers, identity and access software, routers and modems, and mobile device applications.

Class II products present the highest security risk and must receive third-party certification before being put on the market. These include software operating systems, public infrastructure and digital certificate issuers, industrial routers and switches, industrial internet of things devices, robot sensing, and smart meters. About 90% of digital products would fall into this high- risk category, including photo editing software and video games that present no real cyber dangers.

Photo: Margaritis Schinas, Vice-President of the European Commission in charge of promoting our European Way of Life, and Thierry Breton, European Commissioner for Internal Market, gives a press conference on building a Joint Cyber Unit, June 21, 2021. Credit: Lukasz Kobus/European Commission

The Cyber Resilience Act would not apply to devices already covered under dedicated legislation, such as medical devices and automobiles. Additional rules would also be imposed for artificial intelligence systems that would be classified as high risk in a separate law on AI that is under negotiation.[31]

The cyber legislation would take effect in two phases. Within 12 months of adoption, manufacturers would need to report cybersecurity breaches and vulnerabilities, and within 24 months, member states and affected businesses would need to conform.

Business groups and even some member states have expressed serious concerns. By allowing third parties to judge security precautions, any certification process is inherently risky, they say.

Other corporate critics fear that the Cyber Resilience Act could slow or even stall the rollout of essential new technologies and services.[32] “Businesses would have to wait for certification before adopting product security,” says Alexandre Roure of the tech lobby Computer & Communications Industry Association.

The Act remains under negotiation. European parliamentarians, governments and the European Commission are engaged in a "trialogue" to adopt the legislation.[33]

Cloud Services and Data Localization

Another danger is conflating cybersecurity with Europe's quest for "digital sovereignty." The battlefield on this front is cloud services. In 2021, France's national cybersecurity agency, ANSSI, revised its cybersecurity certification and labeling program to disadvantage — and effectively preclude — foreign cloud firms from providing services to government agencies.[34]

ENISA officials are now finalizing a European certification scheme for cloud companies to prove they abide by high cybersecurity standards. The draft requirements could force US cloud giants to disavow Washington's data-access laws. Only European companies could qualify for the highest certification, excluding global leaders Amazon, Microsoft, and Google.[35]

If adopted, this push to develop a European cloud industry promises to be counterproductive. It would force European companies to use high-priced, low-performing local providers. It would, perversely, prove a security risk. The best way to protect data, cybersecurity experts agree, is to distribute, not localize, data, and to store it with the biggest, most technologically advanced providers.[36] Ukraine's success in safeguarding its critical data in multiple centers outside of the country provides strong evidence that data localization is not the best way to protect against cyberattacks.

Cloud services providers, mostly US companies, fear that the changes could be used to keep them out of the European market, which would, in turn undermine the continent's cyber defenses. In a September 2022 white paper, Google called for Europe to rethink its approach and junk closed ecosystems, digital walls, or data localization in favor of what it called "open security," relying on private-public partnerships, threat sharing, and encryption rather than certification.[37]

Many EU governments share these concerns. Estonia, the Netherlands, Greece, and Germany have objected that the proposed ENISA rules would stifle competition.[38]

How this issue is resolved will be key in determining whether a legitimate quest for cybersecurity provides real protection — or whether, perversely, it is just a cover for dangerous protectionism.

Transatlantic Cooperation

The war in Ukraine underlines the importance of public-private partnerships in helping a country anticipate and deal with cyber threats.

In the hours before it sent troops over the border, Russia targeted malware at dozens of Ukrainian agencies. AI helped deflect the attack, allowing defensive software

Photo: The NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) annual cyber defence exercise Locked Shields 2023 took place in Tallinn. Credit: NATO CCDCOE

code to be deployed, according to Microsoft.[39] Such private-sector advances in digital technology, particularly AI, will remain crucial in countering bad actors.

Effective cyber policy requires bringing together a broad coalition of lawmakers, regional bodies such as ENISA, national market surveillance authorities, law enforcement, trade groups, companies, academia, and consumers, says Isabella Wilkinson, a cybersecurity researcher at Chatham House.[40]

Europe should extend cooperation with the United States. At the US-EU Trade and Technology Council, European and US leaders have made cybersecurity a priority. "In the current tense geopolitical environment, risks are increasing for critical internet infrastructures," says the EU readout of the December 2022 meeting in College Park, Maryland.[41] The two sides vowed, "to facilitate projects that strengthen the resilience of infrastructure such as strategic overland and subsea cables."

Yet the EU and US are moving at different speeds. As the EU rushes ahead with its cyber plans, US cyber regulation remains rudimentary. A decade ago, the US Chamber of Commerce spearheaded a campaign to block legislation that would have imposed cybersecurity requirements on private businesses. Since then, the US has relied on voluntary schemes, executive orders, and the federal government's purchasing power to raise cybersecurity standards, all with limited success.

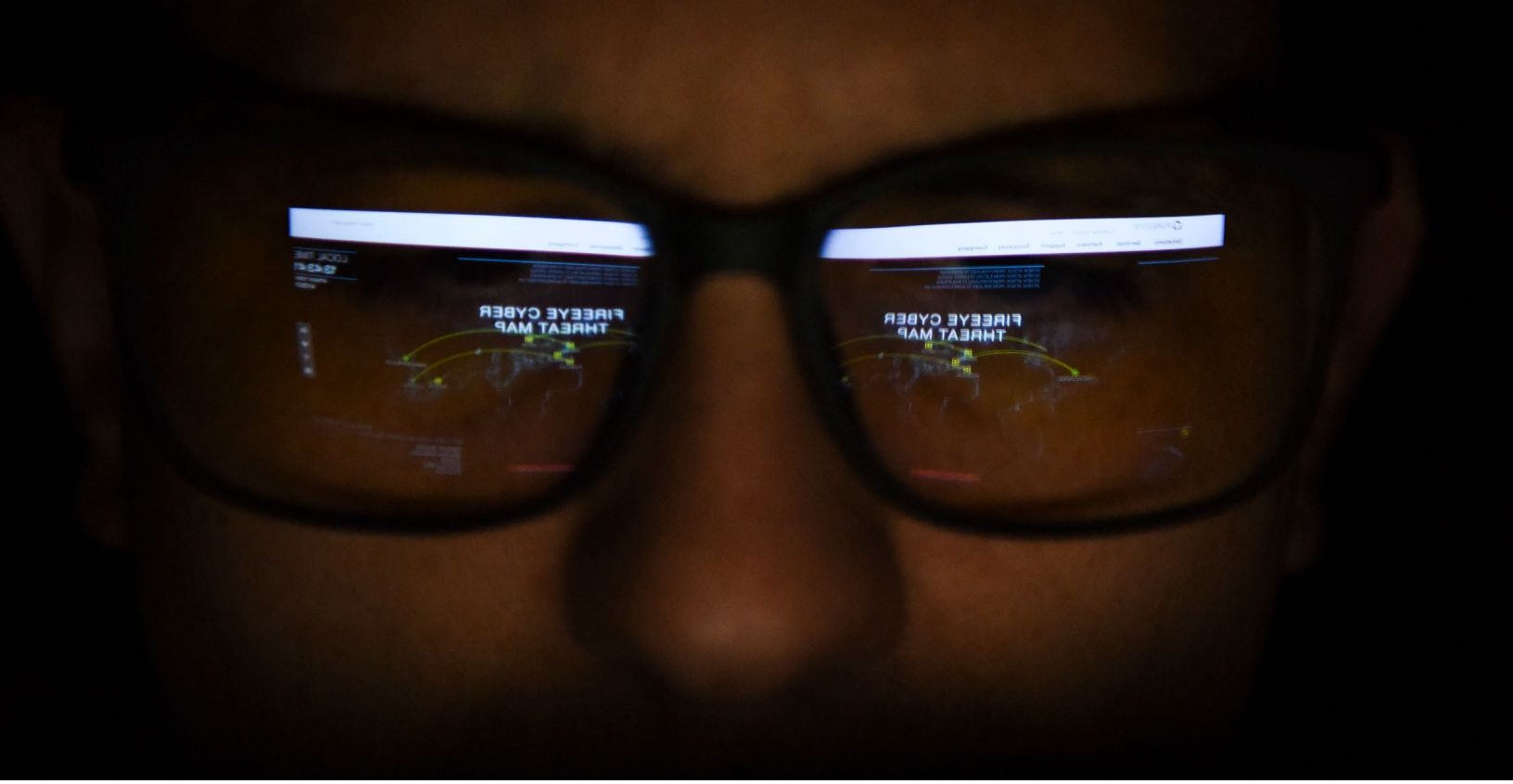


Photo: Air Force Tech. Sgt. Jochen Emrich, of the 189th Airlift Wing, Communications Flight, Arkansas Air National Guard, assesses real-world cyber threats, Dec. 5, 2021, at Little Rock Air Force Base, Arkansas. Credit: Tech. Sgt. Jonathan Porter/Air National Guard

The war in Ukraine, coupled with the May 2021 ransomware attack on the Colonial Pipeline, increased the US appetite for action.[42] In June 2021, the Senate confirmed the country's first national cyber director, and the following year Congress allocated $22 million for the office.[43] In 2022, President Joe Biden imposed the first cybersecurity regulations on oil and gas facilities.[44]

It's not just the Russian threat that creates new urgency to the US cybersecurity push. Chinese hacking is on the rise. In May, 2023, Microsoft disclosed that a Chinese hacking group infiltrated US government agencies, including the email account of Commerce Secretary Gina Raimondo.[45]

The Biden administration has released a new cybersecurity strategy seeking to require companies to report vulnerabilities and intrusions, which had previously been voluntary.[46] An implementation plan was published in July 2023.[47] It sets timelines and outlines steps to protect pipelines, electrical grids and other key infrastructure.

But gaps remain. Specific provisions around data privacy, digital identity and cloud risk, part of the administration's initial strategy, are omitted in the implementation plan.[48] The problem is political. Fundament changes require congressional approval, unlikely with a Republican Party-run House of Representatives.[49] Russia's attack on Ukraine has underlined the importance of effective cyber defense. Chinese hacking ups the danger. Let's hope Europe and the US learn the lessons.

Policy Recommendations

Europe's Cyber Resilience Act should avoid slowing implementation of innovations such as AI that will protect connected services.

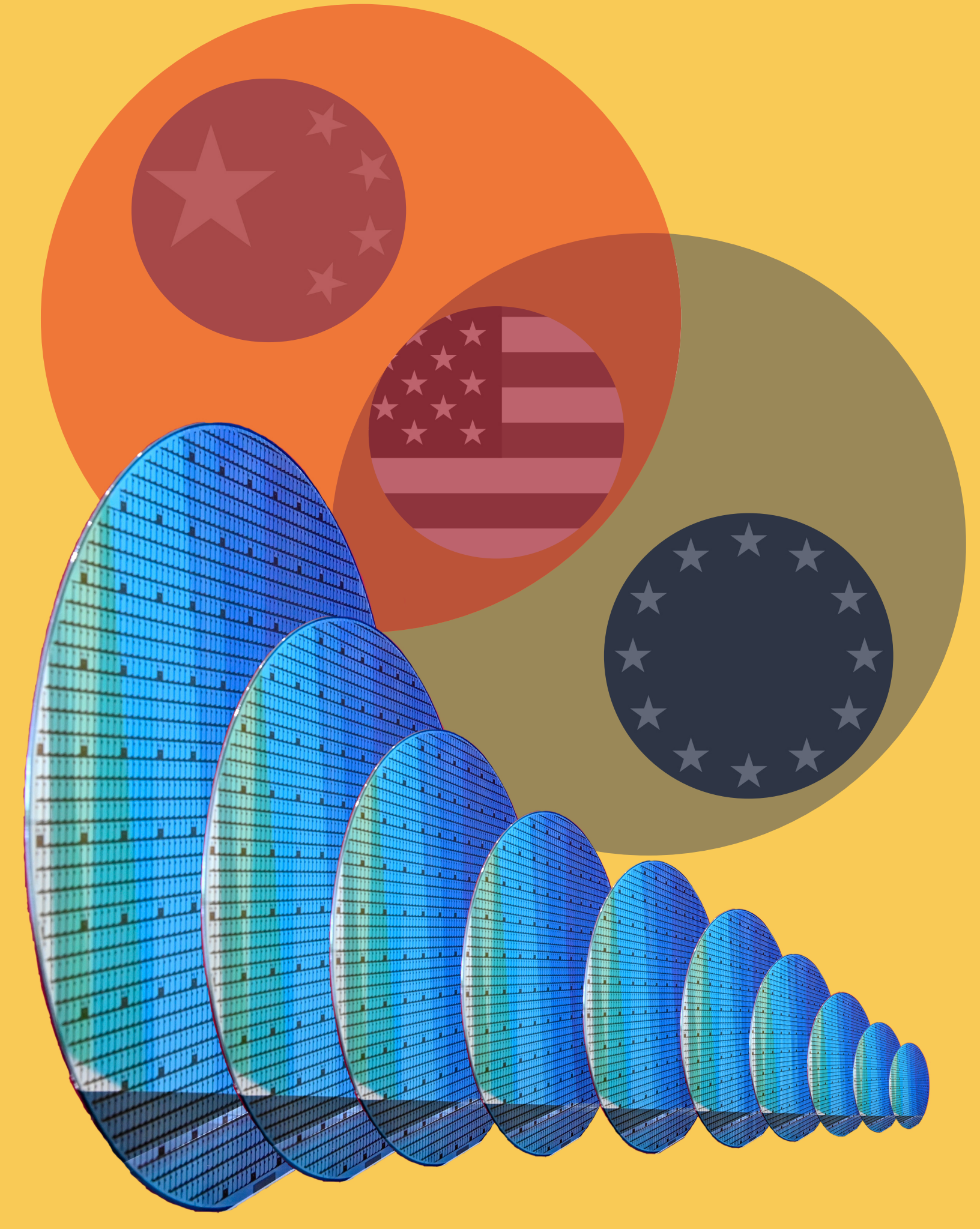
Europe's cloud certification scheme should avoid adopting protectionist measures and imposing data-localization requirements.

Europe's cybersecurity strategy should involve increased stakeholder participation, including industry groups and businesses, to promote public-private partnerships.

The US Congress should move to turn the promising Biden plan into hard law, allowing the Executive Branch to take strong action to protect critical infrastructure.

The US-EU Trade and Technology Council should be used to head off potential conflicts in US and European cybersecurity policies — and to prevent Europe from using cybersecurity to keep US cloud companies out of its market.

Janna Brancolini is a Nonresident Fellow with CEPA's Digital Innovation Initiative. She is an independent journalist based in Milan, Italy, covering legal affairs, business, technology, and sustainability for Bloomberg and the Los Angeles Times.



Confronting China and Catching Up on Chips

By Christopher Cytera

The United States and the European Union (EU) are aligned on the security risks of an unstable semiconductor supply chain—and yet they risk fighting over how to repair it.

Both Washington and Brussels fear that Chinese chips in Western electronics could be used for surveillance and intelligence gathering. Both have launched expensive public-funded programs to build up their own industries. At the EU-US Trade and Technology Council (TTC), a key focus is to ensure these semiconductor support programs are complimentary, not competitive. The TTC is also developing "an early warning system to address and mitigate semiconductor supply chain disruptions."[50]

While it is hard to justify state intervention in most areas of a free market economy, the desire to mitigate security risks justifies extraordinary government intervention. Semiconductors drive the essential tools of contemporary life, from smartphones to automobiles. They are crucial to military prowess, guiding missiles, controlling jets, and running secure communications systems. While the industry is cyclical, demand is expected to boom in the coming decade. The global semiconductor market exceeded $500bn in sales in 2022 and is expected to expand into a trillion-dollar industry by 2030, according to a McKinsey & Company report.[51]

During the COVID-19 pandemic, a shortage of chips wreaked havoc on entire industries, causing deep economic pain and generating geopolitical tensions. In response, the United States, the EU, and China have unveiled ambitious public-funded programs to strengthen their chip industries.

Even so, the EU and US projects entail big risks. The European and US timelines differ: The United States already has approved its chips plan, while the EU continues to debate its legislative proposal. Despite their avowed aim of avoiding duplication, critics fear an inevitable overlap. The giant European and US state-funded subsidy programs could end up spent on white elephant chip-manufacturing facilities, producing a global glut. Signs of a short-term chips glut are already becoming evident.[52]

It would be preferable to use public funds to build up capabilities on "choke points" in the chip development and manufacturing process. The EU should concentrate on its competitive advantage in optics and chemicals. The United States should emphasize its unparalleled design and software capabilities.

Illustration: Michael Newton/CEPA. Photo: A wafer is seen at the new Bosch 300-millimeter wafer fab for silicon chips in Dresden, Germany, May 31, 2021. Credit: REUTERS/Matthias Rietschel

Security Risks

The COVID-19 pandemic has highlighted the semiconductor supply chain's bottleneck-prone nature. With demand soaring for physical goods and foundries shut, global shortages spread, causing economic havoc. Automaking, which depends on advanced electronics, is estimated to have lost the production of almost eight million cars in 2021.[53] Popular products, including the latest Sony PlayStation, became scarce.[54] Beyond generating gaps in consumer products, chip shortages produced security fears, which became accentuated after the Ukraine war depleted Western arsenals.

The Javelin anti-tank weapon, for example, which has proved crucial in Ukraine's resistance to the Russian invasion, requires at least 250 chips. Ukraine requested hundreds of Javelin systems per day at the outset of the war, but US companies struggled to procure the semiconductors needed to meet the demand.

Modern militaries must replace their stockpiles of semiconductor-intensive munitions. To prepare for a potential conflict with China, experts have called for the US military to build up its stockpiles and help countries like Taiwan do the same. These recommendations require a smoothly functioning, resilient semiconductor supply chain.

While many of the most advanced chips are designed in the United States, the EU is strong in the imaging technologies required to miniaturize silicon, and Asia dominates manufacturing. Taiwan produces 65% of the world's semiconductors, while smaller percentages are produced in South Korea, Japan, the United States, and the Netherlands.[55] China produced 5.5% of the world's semiconductors in 2021.[56]

Taiwan's undisputed leadership in advanced chipmaking provokes particular concern. In semiconductors below 10 nanometers—the leading-edge versions of the technology—Taiwan holds more than 90% of the global market share.[57] This dominance introduces several supply chains risks: The island is located just off the coast of China, which claims sovereignty. A Chinese naval blockade of the island, or an outright invasion, would immediately cut off supply of nearly all current production SoCs (System on Chips) designed by the likes of Qualcomm, Broadcom, and Nvidia and supplied by them to Apple, Samsung, Dell, HP, etc. Beyond geopolitics, recent droughts in Taiwan have impacted manufacturing (chip fabrication requires significant amounts of water)[58] and the island is subject to destructive earthquakes.[59] Both the United States and the EU have "zero fabrication capacity for leading-edge logic chips (5 nanometers and below)."[60]

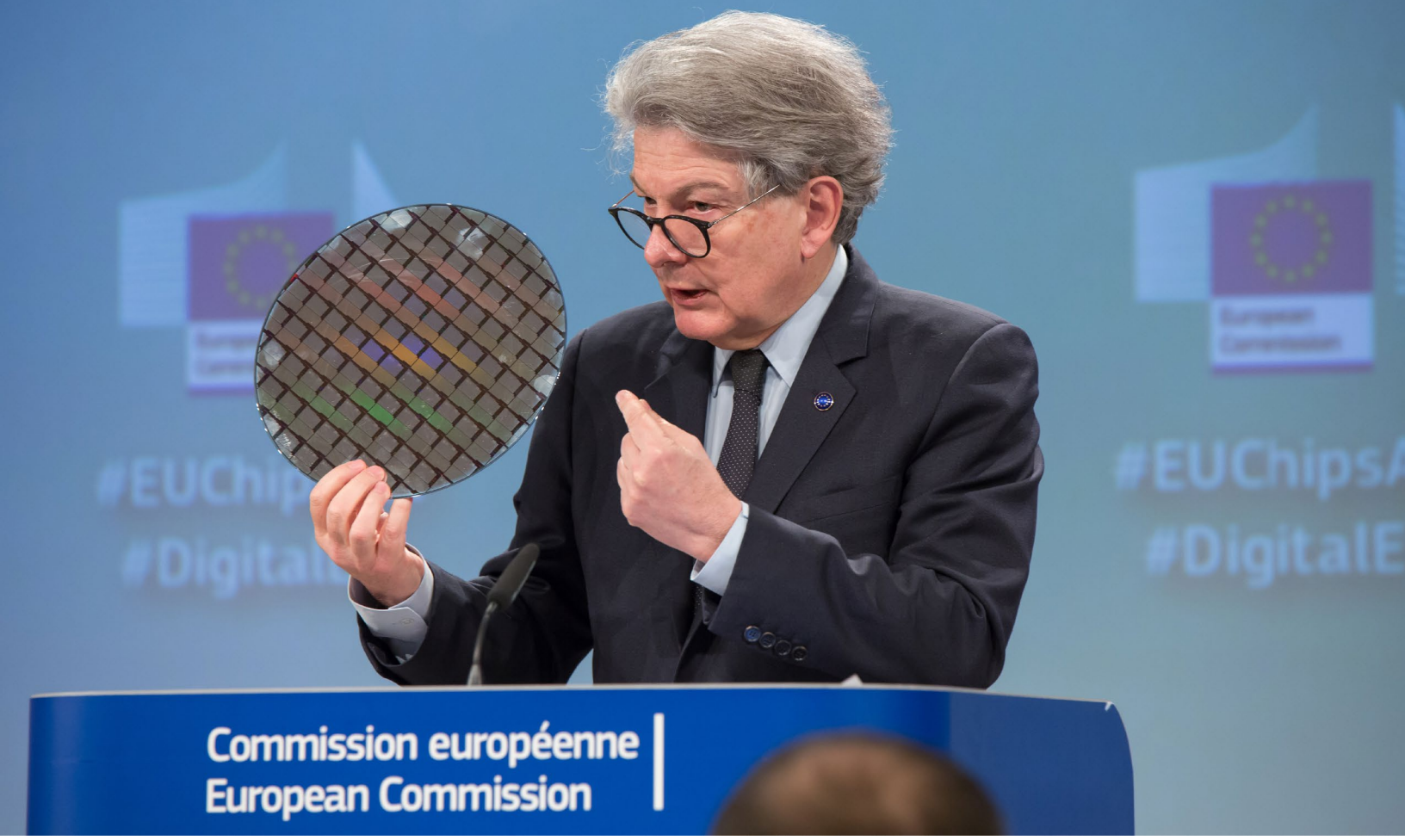


Photo: Commissioner for Competition, Thierry Breton, holds a semiconductor wafer while giving a press conference on the European Chips Act, February 8, 2022. Credit: Aurore Martignoni/European Commission.

The chip industry is capital intensive. It costs billions of dollars or euros to build a modern foundry. Since the start of the century, the number of firms able to offer the most modern technology has fallen from nearly 30 at the turn of the century to just two, Taiwan's TSMC and South Korea's Samsung.[61]

Beyond these risks, both the United States and the EU have identified China's growing semiconductor capabilities as a strategic threat. China is building a competitive semiconductor industry, using extensive state subsidies, intellectual property (IP) theft, and forced labor, they say. US and EU law enforcement and intelligence agencies have voiced concern about the ability of Chinese electronics companies to surveil and gather sensitive data.

Chinese electronics companies, including some which are state-owned, have also sought to purchase or invest in several microelectronic companies, including in the EU and United Kingdom. In late 2022, the German government halted the sale of a semiconductor factory to a Swedish subsidiary of a Chinese electronics company.[62] In the UK, the government mandated the unwinding of the sale of a Welsh company to a Chinese one.[63] Yet Chinese companies remain present in the EU technology space—Huawei, the large Chinese telecommunications firm, has continually pushed for more "partnerships" with EU technology companies.[64]

US and EU Chip Proposals

Both the United States and the EU are gearing up to spend large amounts of public funds to boost domestic semiconductor production. Success is far from certain. The Western efforts are late. China,[65] Taiwan,[66] and South Korea[67] all have provided significant subsidies for years to their semiconductor industries.

The US CHIPS and Science Act

US President Joe Biden signed the Creating Helpful Incentives to Produce Semiconductors and Science Act (CHIPS and Science Act) into **law on August 9, 2022.**[68] The act ensures $280bn in spending over the coming decade. Of that amount, $200bn is slated for research and development (R&D) and commercialization. Another $52.7bn is targeted at semiconductor manufacturing, with $24bn worth of tax credits for chip production. A final $3bn is slated for programs aimed at leading-edge technology and wireless supply chains.

A considerable amount of the funding will give tax incentives to build new chip-manufacturing facilities in the United States, which are planned to be built or expanded in Ohio,[69] New York,[70] and Texas.[71] Additional resources are allocated to boost research, with smaller grants going to improve supply chain security abroad.[72] The legislation subsidizes developers of telecommunications technology with an important condition—recipients of the federal money must not use advanced Chinese chips.[73]

The United States has made security a focus of its chip plans. Both the 2019 and 2021 National Defense Authorization Acts (NDAAs) included steps to boost US chip manufacturing and secure supply chains of semiconductors designed for military use. Chips used for military applications must be more resilient—able to withstand high altitudes and extreme environments—than ones designed for consumer goods. In the 2019 NDAA, a pilot program was introduced to determine the authenticity and security of microelectronic parts in weapons systems.[74] The 2021 NDAA created new incentive programs to boost domestic manufacturing, as well as a new federal center for research and workforce training.[75]

The US government will still struggle to manage chip inventories. The government can only convene the private sector to distribute timely information on supply chain threats and bottlenecks—and set long-term incentives to ease them. The burden of managing chip inventories largely remains on the private sector.[76]

The European Chips Act

In 2022, the European Commission proposed a significant overhaul of its semiconductor industry. The European Chips Act would pump €43bn ($46.58 bn) into research and manufacturing for European chip designers and manufacturers.[77] It aims to double the EU's share of the global semiconductor market from less than 10% today to 20% by 2030.

While most European officials agree on the importance of chips funding, the European Parliament and EU governments still must approve. At the time of writing, the EU had not agreed on how it will raise funds for its Chips Act. European spending looks set to be much lower than US spending.[78] The South Korean government's predicted spending on chips of $400bn through 2030 will dwarf planned European investments of between €20bn and €30bn ($21.67-$32.5 bn) by 2030.

Additional disagreements exist on how the European funds should be spent.[79] Most could end up going to Asian and US firms and, indeed, Intel is slated to receive large dollops of German and EU funding to build a foundry outside Berlin. The plan could increase tensions between EU members. Since funding for these subsidies comes from national budgets, the richest member, Germany, could outspend others, as evidenced by the first large, planned investment linked to the Chips Act — Intel's Magdeburg foundry.[80] Poorer or smaller EU members could be left behind.

Unlike the US focus on national security, the EU's legislation focuses on the "security of supply," the ability of the EU to overcome the gap in its chip supply chain. The European Chips Act would give the EU latitude to direct manufacturers to manufacture critical chip components and to use its bulk buying power as a lever to incentivize manufacturers.[81]

One criticism of the European plan is its focus on the most advanced chips. Since the demise of Nokia as a smartphone supplier, European industry requires few of the most modern chips. It would make more sense to concentrate on the more specialized power semiconductors and micro-controllers required by the continent's strong car and manufacturing industries.

The goal of increasing the EU's share of the global chip market from 10% to 20% by 2030 is arbitrary. Europe does not boast a world-class chipmaker on which to build market share. From being mainstream consumer chip suppliers with top 10 global rankings in the 1990s, Germany's Infineon and French-Italian STM Manufacturers have retreated into niche areas. The European Chips Act will not bring them back into the mainstream nor create the start-ups required for semiconductor innovation and renewed growth in the European ecosystem.

Photo: An employee of chip company Infineon holds a 300-millimeter wafer for demonstration during a press tour in the clean room of the chip factory. Infineon breaks ground for the new Smart Power Fab in Dresden on May 2, 2023. Credit: Robert Michael/dpa/Alamy Live News

Instead, the focus should be on reinforcing European preeminence in key "choke" areas. Europe enjoys impressive chipmaking strengths. Dutch company ASML dominates manufacturing of the lithography machines required to produce the most modern miniature chips. Germany's Zeiss leads in optics. Belgium's Solvay and Germany's BASF provide critical chemicals.

No longer part of the EU, the UK has since released its own semiconductor strategy with a much more modest $1bn support package. The emphasis is on supporting R&D and security, leaving it unclear how supply chains are going to be strengthened.[82]

Export Controls

The United States has taken drastic steps to curb China's efforts to expand its semiconductor industry.[83] In late 2022, the Department of Commerce imposed export restrictions that effectively ban US nationals from working in Chinese businesses associated with chip manufacturing. New licensing requirements make it difficult to export chips from China to the United States, and to ship US equipment to China. Both US and foreign-made products that contain advanced chips with US

inputs must now receive US government approval before being sent to China.[84] The new regulations have shaken the Chinese chip-making industry—experts have noted that the new rules will likely set China back "years."[85]

China consumes more than a third of the world's semiconductors, the vast majority of which are manufactured abroad.[86] Reducing the ability of companies to export to China could have significant consequences for global industry.[87] China may have to invest up to a trillion dollars to make up for the shortfall.[88]

Since these measures were announced, China has retaliated by restricting exports of certain metals[89] used in semiconductor manufacture and banning memory chips from US firm Micron Technologies.[90] We are witnessing the start of what could be protracted "Chip Wars".

While the United States has taken action to reduce the presence of Chinese microelectronics, the EU has not followed suit, partly hamstrung by its own consensus-based foreign policy and trade system. EU semiconductor manufacturers, notably ASML in the Netherlands, complain of US protectionism.[91] Chinese-manufactured security cameras, which have been restricted in the United States, are still common in the EU.[92] Chinese telecommunications firms, notably Huawei, are enmeshed in EU telecommunications—in Berlin, Huawei controls a higher market share of telecom equipment than it does in Beijing.[93]

The United States and the EU look set to continue sparring over just how hard to crack down. Initially, the Dutch government resisted US pressure to ban ASML from exporting its most modern machines to China. In the end, US pressure won out.[94] This could open a new era of transatlantic cooperation.

Policy Recommendations

Blunt policies designed to prevent China from building an advanced chip-manufacturing industry could backfire. In the short term, they will hurt domestic companies by reducing their sales. In the long term, they will have little effect on China. Instead, democratic countries should pursue sanctions that target China's violations of international humanitarian and trade rules.

Enforce Intellectual Property Import Restrictions

Chinese IP theft is widespread and damaging to the United States; 80% of all economic espionage prosecutions brought by the US Department of Justice revolve around actions that would benefit the Chinese state.[95] The estimated cost of these stolen trade secrets is between $225bn and $600bn per year.[96]

Recent reports have detailed Chinese theft of trillions of dollars' worth of IP.[97] In 2019, a California court ordered XTAL, a US subsidiary of Chinese company Dongfang Jingyuan Electron Ltd., to pay ASML $845m to compensate for IP theft.[98] In 2021, ASML voiced concerns that Dongfang Jingyuan Electron Ltd. was using stolen IP to develop competing yield-enhancing products.[99]

The United States and the EU should restrict or tax imports of Chinese technology that depend on stolen Western IP. The United States should reengage with the World Trade Organization to force structural change in China rather than rely solely on the brute force of sanctions.[100]

Increase Forced Labor Import Restrictions

A March 2020 Australian Strategic Policy Institute report identified 83 foreign and Chinese companies that directly or indirectly benefit from Uyghur forced labor.[101] The industries range from electronics to textiles to automobiles. The list is certainly not comprehensive.

In the electronics industry, Apple and other US companies have been implicated in forced labor in China. Seven Chinese suppliers have been accused of forced labor, ranging across the electronics supply chain.[102] Policymakers and experts especially highlight electric vehicle battery[103] and solar panel manufacturing.[104]

The United States and the EU should shift their focus to restricting imports of Chinese technology that has been sourced or manufactured with the use of forced labor. While recognizing that it is often difficult to identify production from forced labor, suspicious solar panels could be taxed based on existing international trade rules that prohibit unfair trading practices.

Increase Scrutiny of Chinese Acquisitions

Western countries have taken steps to examine acquisitions and investments by Chinese companies in critical industries. In the UK, chip company purchases are closely scrutinized. In the United States, the number of Chinese acquisitions reviewed by government regulators over security concerns has skyrocketed.[105]

At the same time, the EU has continued to allow major deals to move forward, including a deal for a Chinese company to purchase a section of an important German port.[106] Democratic countries, and the EU in particular, should take steps to ensure that adequate security oversight exists for foreign investment in critical industries, particularly from China.

Target Chip Funding

The EU and US chips acts represent important steps to boost domestic production. They should focus on R&D for the next generation of semiconductors. Advanced imaging technology will be needed to develop the next generation of chips.[107] New manufacturing equipment, currently built in only a select few locations, will become a critical part of controlling the next generation of the semiconductor supply chain. Money should not exclusively be poured into foundries, but also invested in finding new ways to improve supply chain security, such as integrating artificial intelligence into the semiconductor supply chain.[108]

Avoid Protectionism and Hypocrisy

Unless rethought, US and European public funding of semiconductors could threaten a new transatlantic crisis. President Biden and von der Leyen are working to diffuse a monthslong spat over the US Inflation Reduction Act's electric vehicle tax credits.[109] Both the US Congress and the European Parliament could stand in the way of a solution.[110] Under the US "Buy America" provisions, the CHIPS Act threatens a repeat of the Inflation Reduction Act fight.

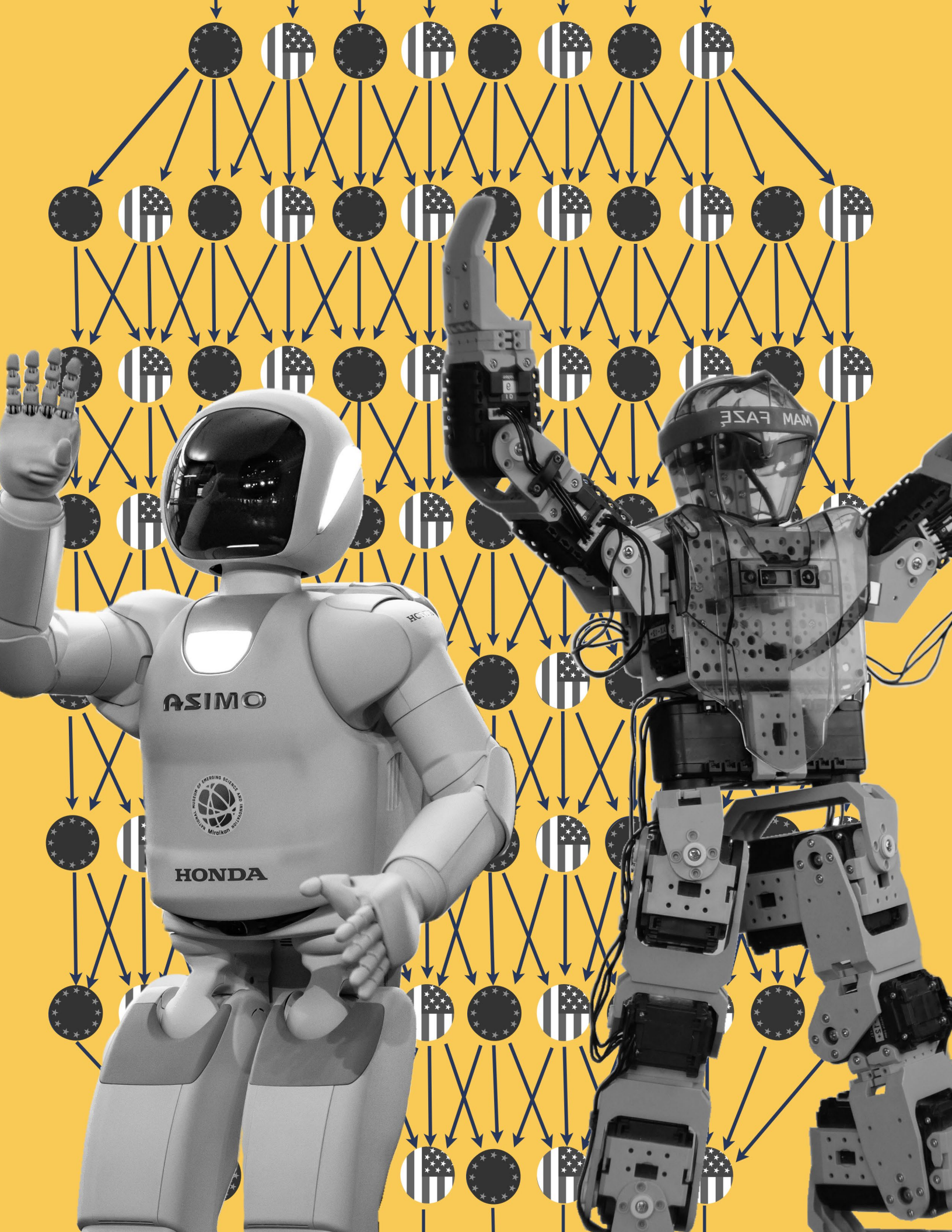
Europe risks falling into a similar trap.

While much of its public funding could go to US and Taiwanese companies to build foundries in Europe, the threat of imposing local manufacturing restrictions is driving these investments.

US and European funds should not only focus on manufacturing chips. The Chinese army flooding into Taiwan is not the only threat, though it remains real. Instead, the United States and the EU should concentrate on building up their respective competitive advantages and synergies with leading-edge semiconductor process development. Together, that is the most effective way to meet the Chinese challenge and secure the semiconductor supply chain.

Christopher Cytera CEng MIET is a Non-resident senior fellow with the Digital Innovation Initiative at the Center for European Policy Analysis and a technology business executive with over 30 years of experience in semiconductors, electronics, communications, video, and imaging.

Alexander Wirth and Bill Echikson contributed research.


ASIMO
HONDA

Transatlantic Community Must Unite to Address AI Risks and Opportunities

By Ylli Bajraktari and Lauren Naniche

Artificial intelligence (AI) has come a long way since 1968 when science fiction imagined the "2001: A Space Odyssey" villain HAL 9000 computer uttering "I'm sorry Dave, I'm afraid I can't do that." Today's chatbot ChatGPT explains complex concepts and generates intriguing ideas. AI is transforming our societies and economies. It powers personalized, precision medicine; gene therapy; vaccine discovery; drug design; and cancer screening. It is revolutionizing crop management.[111] It reduces plastic waste. It is turning futuristic fusion energy into a reality.

The European Union has responded with a broad and sweeping legislative proposal to regulate AI.[112] While the EU's proposed AI Act represents a legitimate attempt to ensure that technology serves society well, European legislators are overlooking its potential security and strategic consequences.[113]

Nations that set the rules of the road for our global digital life will be the leaders in mastering AI. The Chinese Communist Party has made its ambitions clear: It wants to dominate emerging technologies, increasing the world's dependence on China while reducing its own dependence on the outside world. Beijing is devoting enormous state resources to accomplish this objective.[114] Democracies find themselves in competition with China over AI leadership, which will be one of the defining features of our global politics.

What would a world dominated by Chinese technology look like? Our Special Competitive Studies Project report, "Mid-Decade Challenges to National Competitiveness," offers a startling snapshot.[115] China would control the global digital infrastructure, enjoy the dominant position in technology platforms, and harness biotechnology and new energy sources. AI is a key battleground that the transatlantic alliance cannot cede.

If leadership in AI and other technologies ultimately shapes the international order, will the future be one of shared beliefs and democratic values — especially with regard to individual privacy and free speech? Or will we face a future of state surveillance and control? We need to ensure democracies stay ahead to meet these challenges. The United States and the EU must come together rather than drift apart on AI.

Opposite Illustration: Two robots and an artificial intelligence learning model with the flags of the United States and European Union. Credit: Michael Newton/CEPA.

The EU's Proposed AI Regulation Has Negative National Security Implications for Democracies' Position in the Technology Competition.

Europe risks putting regulation and innovation on a collision course. Its proposed AI Act might be the next regulatory miss. "The road to regulation hell is paved with the EU's good intentions," says Oren Etzioni, the founding CEO of the Allen Institute for AI.[116]

The proposed AI Act is based on several assumptions: that it will spur the "right kind" of innovation because of legal certainty and increasing public trust in AI, that companies will be able to implement it, and that the European Commission will be able to enforce it. All three assumptions are misguided.

The EU has yet to demonstrate that its regulatory approach, one seeking to be all-encompassing rather than adaptable, generates innovation. The EU's regulatory history points in the opposite direction. Consider the landmark General Data Protection Regulation (GDPR). Held as a gold standard by many European legislators, the GDPR regulates first and works out the details later.[117] Large, complex compliance requirements hurt European innovation, data shows.[118] Small and medium-sized enterprises (SMEs) are hit hardest.

Compliance with the proposed AI Act will be difficult. Many requirements, especially in regard to the explainability of AI systems, risk being impossible to achieve.[119] A timely example of this is ChatGPT; it is unclear how such large language models will fit in the EU's AI Act risk framework or how the explainability requirements can apply to neural networks.[120] By the time the proposed AI Act is finalized and enforced, one can only suspect that other new AI applications will run into the same issue.

Purist thresholds entrenched in law for emerging technologies are detrimental. They thwart the use of exciting technologies on technicalities. We need to ask ourselves: Do we want to accelerate the use of cutting-edge AI applications or wait for greater AI explainability?

European legislators will struggle to make a broad piece of legislation such as the proposed AI Act "future-proof" or adapted to the fast-paced world of AI innovation.[121] The already wide gap between theory and practice will only increase over time and as technology evolves. Consider cookies. Europe's ePrivacy Directive requires that almost every time a European opens a web page, or anyone opens a web page hosted in the EU, they are confronted with a request to accept or decline cookies.[122] This well-intentioned tool has turned into a time-consuming annoyance. Most users end up clicking "accept all" and sharing their data because it is faster to do so than to consider all their options.[123]

Photo: Visit of Ursula von der Leyen, President of the European Commission, to the Vrije Universiteit Brussel. Credit: Jennifer Jacquemart/European Commission

The proposed AI Act risks downplaying its impact on innovation and, by extension, on Europe's ability to host the next technology breakthroughs. This has larger security implications, particularly since autocratic nations will face few similar restraints

Chinese social media platform TikTok offers a first example: An update to TikTok's privacy policy allowed China-based employees to access European data, even if it did so "by way of methods that are recognized under the GDPR."[124] Greater security concerns eventually led the EU to require a complete ban of TikTok from their staff's devices.[125] Even the GDPR, arguably the strictest data privacy regulatory framework in the world, proved to have limits in enforcing the respect of European fundamental values on a Chinese platform.

ChatGPT offers another striking example of the way values are inscribed in technology by way of innovation rather than regulation. This revolutionary tool has already raised concerns around bias in its answers.[126] The EU will undoubtedly have a harder time regulating and aligning on values-related matters with a Chinese Ernie Bot than a US ChatGPT.

This is not to discourage AI regulation. The United States offers no positive example of harmonized guardrails for AI. The United States falls on the end of the spectrum of dangerous *laissez-faire*. National security is tied to achieving and enforcing proper governance and cannot be overlooked.

But the biggest security threat to democracies ultimately does not come from autocratic states generating their own AI regulations. Yes, China has been drafting laws to define how AI can be used in its own society.[127] But there will not be a "Beijing Effect" on AI governance in the same way the EU is counting on a "Brussels Effect" out of the proposed AI Act.[128]

The fundamental threat to democracies is to fall behind in AI innovation. If we lag, we will not get to dictate how data and algorithms are developed and used. As the EU AI Act moves forward in the "trilogue" process between the European Commission, the European Council, and the European Parliament, lawmakers at the table have an opportunity to course-correct parts of the upcoming AI regulation. During these negotiations, they should strive to answer the following question: How do democratic societies stay ahead and use AI technologies for the betterment of our societies while staying true to our ideals?

Policy Recommendations: The Democratic Path Toward Tech Leadership

Promote pro-innovation, responsible governance.

Technology has become the organizing principle of the contest for the future of the global order. How we govern AI, and how we leverage AI to strengthen our economies and defenses represent important elements of the competition between democracies and autocracies.

We have reached a point across the democratic world where we agree upon the basic principles of what AI should be allowed to do — and not allowed to do. The Organization for Economic Cooperation and Development (OECD) has developed global, high-level principles; the Hiroshima AI process announced at the last G7 seeks to build off that work to expand on generative AI; the White House has also released a Blueprint for an AI Bill of Rights that captures the spirit of the EU's proposed AI Act.[129] Both sides of the Atlantic, and democratic partners beyond, recognize the legitimate concerns about privacy, bias, trust, and reliability that flow from poorly designed AI applications.[130] As a dual-use technology, powerful, well-designed AI systems can harm our societies without a proper set of guardrails.

When it comes to implementation and legislation, a perfect democratic alignment is unreasonable. Its absence should not be the basis for division. The United States and its allies were rarely in perfect alignment during the Cold War or post-Cold War on complicated issues involving tech, trade, and governance. But this did not forestall strategic alignment or deep economic ties.

Photo: Chat GPT illustration displayed on smartphone. Credit: Mojahid Mottakin/Unsplash

Both sides must recognize not only the need for AI regulation, but also the dire need for democratic AI innovation. There is a balance to strike between the two. We must build and use AI systems safely, responsibly, and ethically. As well, time and again, with shorter and shorter time between discoveries, we are witnessing examples of AI breakthroughs in areas critical to our health and well-being. AI's shortcomings should not prevent us from pursuing the opportunities and the progress AI holds. Our approach to AI governance should focus on competitiveness, harnessing the new geometry of innovation, and it should put at its core the strategic stakes of the global tech competition. We welcome initiatives such as the Voluntary AI Code of Conduct for Businesses, proposed by Commission Executive Vice-President Vestager and to be developed jointly with the United States.[131] Self-regulatory frameworks allow for more iterative and nimble AI guardrails.

The private sector represents an invaluable partner. When Russia invaded Ukraine in February 2022, the tech sector stepped up — providing cyber defenses to safeguard Ukraine's infrastructure, mobilizing cloud services to store Ukrainians' data, and keeping Ukrainians connected to the web.[132] As we develop our governance model, we cannot overlook the role of our private sector in supporting democracy.

Do not let the trade tree distract us from the national security forest.

While a timely and necessary transatlantic forum, the US-EU Trade and Technology Council (TTC) has yielded modest deliverables on AI.[133] Last December's TTC meeting rendered a new joint AI road map, which helpfully begins to chart a course on joint

Photo: Margrethe Vestager, Executive Vice-President of the European Commission, speaks on fostering a European approach to Artificial Intelligence. Credit: Aurore Martignoni/European Commission.

standards.[134] However, progress in the meeting was overshadowed by conversations surrounding the US Inflation Reduction Act, which subsidizes domestic production of electric vehicles against European imports.[135] The fourth TTC iteration in May offered little advances on these issues. The work of the transatlantic alliance on tech and joint strategic objectives has been hampered by economic competition and tensions.

Democracies must marshal the resources and diplomatic will to collectively build the digital apps, software, and platforms that support everyday governance, commerce, and life. Concretely, this requires government-supported investment in global digital ecosystem projects. It means aligning on maintaining standards based on technical, not political, criteria. Human rights-abusing regimes should not get to benefit from technologies designed and built in our free societies.

Diplomatically, democracies need to build a new “DemTech alliance” to address the opportunities and risks we face in this new competition. We need a novel alliance

framework to outpace our dated legacy institutions.[136] We should invest in our collective comparative advantages for technologies such as AI but also 5G and chips and build our strategic partnerships to keep control of the digital infrastructure of the future.

After Russia's invasion of Ukraine, it is clearer than ever that the AI partnership must include a strong security dimension. We need European AI companies supporting European security initiatives, working with US companies undertaking similar work.

The strategic landscape has changed, and so should the balance between partnerships and competition.

The rising power and ambition of authoritarian regimes to harness AI and other technologies of the future present a common threat. If we fall behind autocratic states in AI development, it will be bad for our collective security, companies, and economies.

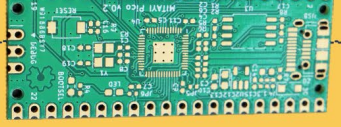
The transatlantic alliance should spend more time on cultivating our rich ecosystems of universities, companies, and innovators, rather than belaboring the risks of innovation. We need to shift our mindsets toward an optimistic view of AI and look forward to harnessing its benefits, rather than automatically hitting the regulation button. How can we unlock data for the good of society while upholding our values? How can we encourage AI researchers to solve our big societal problems? How can we get more of the youth excited about studying to become AI engineers?

The best way for us to engrave our democratic values in technology, and enforce regulatory frameworks that support them over time, is to be innovation leaders. It is time for Europe, hand in hand with the United States and other democratic allies, to lead the way again in these groundbreaking technologies.

Ylli Bajraktari is the President and CEO of the Special Competitive Studies Project (SCSP). Prior to launching SCSP, he served as the Executive Director of the National Security Commission on Artificial Intelligence. Beforehand, Mr. Bajraktari served as Chief of Staff to National Security Advisor Ltg H.R. McMaster, held a variety of leadership roles for former Deputy Secretary of Defense Robert Work, and was a Special Assistant to the Chairman of the Joint Chiefs of Staff.

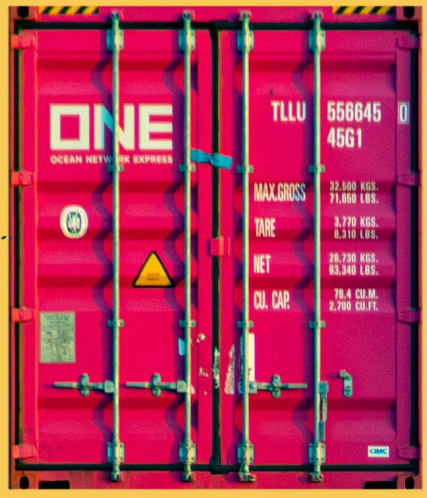
Lauren Naniche is the Associate Director for Research and Analysis at the Special Competitive Studies Project (SCSP). Prior to her time at SCSP, Ms. Naniche worked at the Center for European Policy Analysis (CEPA), the Hudson Institute, and wrote for the McGill International Review.

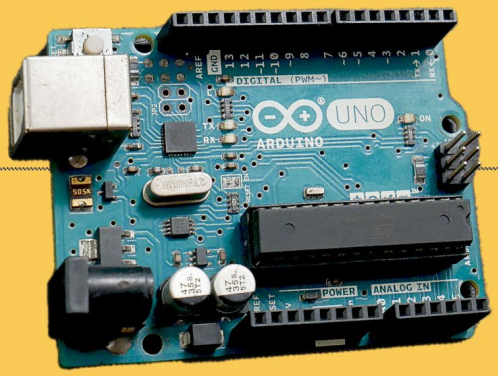
This report was published in partnership with the Special Competitive Studies Project.



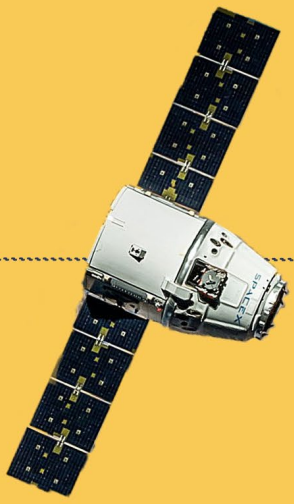

TCNU 427368 9
45G1
MAXGROSS
TARE WT.
PAYLOAD
CU. CAP.
CAUTION
9'6"
HIGH


Canon
EOS
ASAHI OPTICAL CO.


ONE
OCEAN NETWORK EXPRESS
TLLU 556645 0
45G1
MAX.GROSS
TARE
NET
CU. CAP.


DIGITAL (PWM~)
UNO
ARDUINO
POWER
ANALOG IN


TCNU 441766 2
45G1
MAXGROSS
TARE WT.
PAYLOAD
CU. CAP.
CAUTION
96"
HIGH




TRITON
TCNU 624758 6
45G1
MAXGROSS
TARE
PAYLOAD
CUB.CAP.
CAUTION
9'6"
HIGH
CONTAINER


TLLU 553526 0
45G1
MAX.GROSS
TARE
NET
CU. CAP.

Export Controls — The Keys to Forging a Transatlantic Tech Shield

By Matthew Eitel

The United States (US) and the European Union (EU) agree that export controls are a key weapon in the arsenal against authoritarianism. In response to Russia's full-scale invasion of Ukraine, the allies coordinated a comprehensive ban on selling Moscow a variety of dual-use technologies — hardware or software with both civilian and military applications — such as semiconductors and telecommunications equipment.[137] They also align on placing export controls in a central role to "de-risk" supply chains and counter economic coercion from China.[138]

Yet, the differing governance structures of the allies remain a key obstacle. The US benefits from a strong federal executive branch, which can impose financial sanctions and export controls quickly and unilaterally. Some US export controls are effective upon release.[139] The EU, on the other hand, can only act after forging consensus among its member states. Member states, who view export controls as a national security competency, often sideline the Brussels-based European Commission when creating national level controls. It takes about a year to update the EU's export control list.[140]

EU and US political priorities also differ. The US now places national security concerns at the center of its international economic agenda, willing to sacrifice trade in the name of protecting US security interests.[141] The EU has hardened its view of economic engagement with China, but key member states remain skeptical of the trade-offs required to align their approach with that of the US.[142]

Future transatlantic coordination on the rationale and implementation of export controls will require reflection and reform. Washington must remain careful about unilateral action. It must avoid applying too many extraterritorial controls and coercing allies to align their regulations. Europe must update its fragmented export control regime and form a consensus on a strategic approach to technology transfers to China.

Washington Sounds the Alarm and Seeks to "Lead from the Front"

In the late 1940s, the United States began to use export controls as a national security tool in response to mounting tensions with the Soviet Union. The US Congress codified national security and foreign policy considerations as a valid rationale

Opposite Illustration: Export shipping containers and commercial electronics with dual use semiconductor microchips. Credit: Michael Newton/Center for European Policy Analysis

for imposing sanctions.[143] After World War II, NATO members and Japan began coordinating on multilateral export controls to "affect the economic development of the Soviet Union" and restrict its access to sensitive technology and military equipment.[144]

A fear of rising authoritarian power continues to motivate US export control policies. In 2015, China announced its flagship industrial policy plan dubbed "Made in China 2025."[145] It articulated an ambition to dominate global supply chains in strategic sectors such as "new advanced information technology" and "new materials."[146] The plans alarmed Washington policymakers. They view the "Made in China" ambitions as a threat to US leadership in technological innovation. In response, Washington pushed to revitalize the laws that govern the US export controls.

In 2018, Congress passed the Export Control Reform Act mandating the identification of "emerging and foundational" technologies that required export restrictions as a matter "essential to the national security of the US."[147] The Bureau of Industry and Security, housed in the US Commerce Department, won the authority to identify the technologies that warrant export controls, alongside the US Departments of Defense, Energy, and State.

At the same time, the administration of former US President Donald J. Trump launched efforts to curtail Chinese telecommunications firm Huawei's access to US technology. In 2019, the US labelled Huawei a grave national security threat and added the firm and 68 of its non-US affiliates to the Entity List.[148] All non-licensed "exports, reexports, and transfers" to Huawei from US companies were banned.[149]

However, since Huawei continued to acquire restricted tech from non-US firms, Washington introduced an expansive new regulation to address this weakness.[150] The "Entity List foreign direct product rule" represented a substantial shift to reliance on extraterritorial authority on foreign-produced tech transfers in US export control policy.[151] By August 2020, the rule subjected any foreign-produced item using US inputs that could eventually be "produced, purchased, or ordered" by Huawei or its non-US affiliates to US export restrictions.[152]

Although the use of extraterritorial rules is not new, the expansion of this tool given the prevalence of US technology in global supply chains has generated tensions on both sides of the Atlantic. Transatlantic tech trade associations complained that "extraterritorial application of US export controls creates regulatory burdens on European stakeholders and discourages European entities from collaborating with US counterparts, creating incentives to avoid US technology or, in some cases, hire US persons."[153]

Photo: Employees of the Infineon chip group stand in the clean room of the chip factory. Infineon breaks ground for the new Smart Power Fab in Dresden on May 2, 2023. Credit: Robert Michael/dpa/ Alamy Live News

The onset of Russia's renewed aggression against Ukraine in early 2022 forced Washington and Brussels to address tensions over extraterritoriality. Departing from the Trump administration's approach to Huawei-related controls, the administration of US President Joseph R. Biden, Jr. offered exemptions from foreign direct product rules to European allies who joined the Russia/Belarus controls regime.[154] The exemptions incentivized cooperation and reduced the danger that European firms would not use US inputs or switch to non-US suppliers.[155]

The Biden administration has proved more aggressive in countering China's tech ambitions than its predecessor. US intelligence perceives Beijing as a "near-peer" strategic threat, asserting that China is "the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."[156] The US no longer aims to stay only "a couple generations ahead" of China in key technological industries, says US National Security Advisor Jake Sullivan.[157] The goal is to "maintain as large of a lead as possible" by pursuing a "small yard, high fence" approach to limiting to China's ability to "exploit American and allied technologies."[158]

To achieve this ambitious goal, the Biden administration has ratcheted up pressure. On October 7, 2022, the US Commerce Department introduced new export controls aimed at stunting China's ability to manufacture and purchase semiconductors and chip manufacturing equipment above a certain performance threshold.[159] China's technological advancement is now deemed a national security risk by the Biden administration, which asserts that it is impossible to distinguish between China's military and non-military uses of many critical technologies.[160] The US is looking to close loopholes in the October controls with restrictions on Chinese companies' access to US cloud-computing services.[161] Updates could also expand US extraterritorial jurisdiction by lowering the threshold needed for the controls to apply to foreign equipment.[162]

The new export controls strategy has caused consternation, both inside and outside the US. Critics define it as "decoupling" and "an act of [economic] war," worrying that it could hurt Americans and Europeans as much or more than China.[163] The Biden administration has toned down the rhetoric of its security-at-any-cost strategy. In an April speech, US Treasury Secretary Janet Yellen emphasized that US export controls are "motivated solely by our concerns about our security and values," and not to "gain competitive economic advantage."[164] Sullivan echoed the softer tone in a similar speech saying that US export controls are "narrowly focused on technology that could tilt the military balance."[165]

However, the core of the "Sullivan Doctrine" animating US export controls remains intact. As US Undersecretary of Commerce for Industry and Security Alan Estevez stated when describing the rationale for the October controls, the US will "not balance trade with national security."[166]

Most of Europe disagrees.

European Attitudes Are Changing — But Skepticism Persists

The European Union began as a commitment to free trade and an aversion to power politics.[167] During the Cold War, EU member states each formulated their own export control policies. National security remained a national prerogative, outside the scope of the Common Market.

This is changing. European leaders understand the need to reinforce their ability to impose export controls. After nearly six years of negotiations, they adopted a new export control regime in 2021.[168] It reformed controls on dual-use technologies, harmonized licensing procedures across EU member states, and established regular communication channels between national and European Commission officials. The new regulations also crack down on the export of surveillance products that pose

serious risks of a "violation of human rights, democratic principles or the freedom of expression."[169]

Despite this reform, the EU's capacity to control exports remains limited. The final 2021 regulation reflects scaled-down ambitions compared with the original European Commission proposal.[170] The Commission cannot order EU-wide sanctions. It only is allowed to help member states coordinate their policies and to maintain permanent EU-wide lists of restricted exports. The EU's Foreign Affairs chief proposes sanctions but needs the unanimous consent of the 27 to impose them.[171] Any single EU member state can delay or dilute new controls and sanctions in response to Russia's aggression.[172]

European concerns about China are intensifying, driving a new push to reform the EU's export controls policies. The EU has traditionally held a dovish view of China. In 2019, the Commission defined relations with China as a negotiating partner, an economic competitor, and a systemic rival simultaneously, without committing to any of the three definitions.[173] Josep Borrell, High Representative of the EU for Foreign Affairs and Security Policy, seeks to recalibrate EU relations with China in a "clear-eyed but not confrontational" manner that relies on "a more effective export control system (and) the control of inbound (and outbound) investment."[174]

The EU is seeking expanded legal powers to match this hardened view. An upcoming "anti-coercion instrument" aims to bolster the bloc's ability to hit back at China following a trade dispute driven by Lithuania's recognition of Taiwan.[175] The new "European Economic Security Strategy" calls for updates to the EU's dual-use export controls to support European Commission President Ursula von der Leyen's push to "de-risk" European supply chains from China.[176]

Despite growing alignment with the US and calls for reform, significant challenges remain. Many Europeans did not view China as a security risk. The populations of all but four EU member states view China as an "ally" or "necessary partner."[177] Europe's economies remain dependent on China; Ireland is the only EU member state that can boast a trade surplus with China.[178] German Chancellor Olaf Scholz downplayed the importance of Germany's new China strategy, which stopped short of endorsing aggressive controls on advanced tech.[179] France, Germany, Italy, and the Netherlands have expressed concerns that President von der Leyen's "de-risking" strategy will encroach on member states' ability to set national security policies.[180]

US willingness to use extraterritorial application of its export controls as leverage is also a key obstacle. Dutch company ASML has become the symbol of this struggle.[181] It is the world's only manufacturer of extreme ultraviolet lithography systems, a type of semiconductor equipment used to produce advanced chips.[182] In 2018 and

Photo: Shipping containers at a port facility. Credit: Chuttersnap/Unsplash

2019, the Dutch government resisted US pressure before finally accepting a ban on certain ASML exports to Chinese chips manufacturer SMIC.[183]

The US, Netherlands, and Japan engaged in a similar diplomatic dance after the US October 2022 controls. The rules introduced novel restrictions on how US corporations — and individual US citizens — can assist Chinese chipmakers, as well as what types of US inputs warrant an export license for non-US-origin items shipped by non-US firms.[184] The long-term viability of these controls required semiconductor powerhouses Japan and the Netherlands to impose similar restrictions.

Despite initial skepticism, Japan and the Netherlands agreed in January to a confidential deal to impose similar controls.[185] Dutch Trade Minister Liesje Schreinemacher announced the "additional national export control measures" — echoing central tenets of Sullivan's strategy — in March and published the new controls in late June.[186] Japan followed suit, announcing that aligning its high tech export controls with those of the US and Netherlands "[fulfills Japan's] responsibility as a technological nation to contribute to international peace and stability."[187]

A New Venue

Another challenge to transatlantic tech reconciliation is the lack of agreement on the best way to coordinate future controls.

Nations traditionally use multilateral export control regimes to agree on common export restrictions. Member countries meet regularly, draw up a list of technologies and goods to control, and implement the restrictions at the national level. Four of these voluntary, non-binding groups are active: the Nuclear Suppliers Group, the

Missile Technology Control Regime, the Australia Group (for chemical and biological weapons), and the Wassenaar Arrangement (for conventional weapons and associated dual-use technologies). Most of the items and technologies included on EU export control lists were agreed upon under the rules of one of these four groups.[188]

However, skepticism is rising about the relevance of these multilateral regimes.[189] They focus on limiting conventional weapons or weapons of mass destruction rather than broader objectives such as containing another country's technological rise.[190] Decisions require consensus among a large and diverse membership. The Wassenaar Arrangement has 42 members, including Russia.

These limitations have led to proposals to create a new forum restricted to advanced democratic countries and designed to deal with dual-use technology exports to China. After the relative success of democratic coordination against Russia, such a new multilateral group could be effective in imposing "export controls to achieve objectives beyond nonproliferation."[191]

Success is far from assured. The EU remains hesitant to use multilateral forums like the EU-US Trade and Technology Council (TTC) to target China.[192] Many European firms remain suspicious of US companies unfairly benefitting from expansive US controls, although US firms like Micron and NVIDIA are facing steep costs and lost opportunities.[193] European fears of US tech dominance breed worries of export controls threatening the Commission's quest for technological sovereignty.[194] To some, the US is simply acting "without seriously consulting its European allies" and its drive to "[maintain] US tech dominance…runs headlong into European concerns."[195]

Perverse Incentives and Unintended Consequences

In the late 1990s, the US restricted exports of satellite technologies.[196] At the time, US companies generated over 60% of global revenue for the satellite industry. By 2005, that number dropped to 41% with US satellite firms losing more than $500 million annually. The ability of the US satellite industry to lead global innovation was hamstrung while China and other nations found alternative suppliers.

This cautionary tale underlines important lessons. Over time, export controls can undermine national security interests, though designed to strengthen them.[197]

US export controls are only as strong as the world's dependency on US equipment, software, and knowledge. That dependency is not a given. Strict, unilateral controls create incentives to reduce the ability of the US to control the flow of advanced technology.[198] They encourage competitors to develop US-free supply chains to evade US export controls and keep selling to China.

Chinese firms are aggressively pursuing chip supply chains free of Western inputs, while Beijing is striking back with chip manufacturing controls of its own. Yangtze Memory Technologies Corp (YMTC) plans to use domestically sourced equipment for advanced flash memory products.[199] Huawei filed patents for its own extreme ultraviolet technology in 2022, signaling that its lofty ambitions to catch up to ASML — but most Chinese semiconductor firms remain woefully short of Beijing's lofty goals for chipmaking self-sufficiency.[200] China's restrictions on two key chipmaking metals could succumb to similar faults of US chip controls by accelerating Europe's critical minerals "de-risking" efforts.[201]

Adversaries and allies alike are subject to the economic costs of US export controls. After an expedited cybersecurity review, Beijing banned Chinese infrastructure operators from using products made by US chipmaker Micron Technology in Chinese infrastructure.[202] The US urged Seoul to dissuade South Korean chipmakers Samsung Electronics and SK Hynix from cashing in when Micron lost access to upwards of $7.7 billion in annual revenue.[203] Washington possesses strong leverage. The US Commerce Department granted, and recently extended, a one-year exemption from the October 2022 controls to Korean firms who produce 40 percent of their memory chip inventory in China.[204] This dynamic demonstrates that diplomatic pressures from export controls cut both ways. Allies can force carve-outs in US policies that could weaken their impact over time, while also acquiescing to certain US requests.[205]

China's chip self-sufficiency push and the Micron ban illustrate the need for transatlantic alignment on tech export controls regimes. Multilateral implementation of controls can greatly reduce the perverse incentives of unilateral restrictions. The US must shift to a strategy of incentivizing rather than coercing allies to join these regimes. Brussels must make the case to member states that strengthened EU export control rules can increase national security as a necessary component of "de-risking" the continent's supply chains.

The US and the EU share a common interest in ensuring China does not take advantage of Western technology to strengthen its military and commit human rights abuses. The allies must adapt their approaches to export controls to bolster their competitive advantages and exploit chokepoints in advanced tech supply chains. Forging a transatlantic tech shield requires a new, united vision for export controls and enacting the reforms necessary to make it a reality.

Policy Recommendations

Leverage the EU-US Trade and Technology Council (TTC) to align on the rationale for China-focused export controls: Previous EU-US TTC joint statements expressed "shared concerns" that the "civil-military fusion policies of certain actors undermine security interests" but stop short of naming China or citing the concern as a reason to impose controls.[206] Building on the G7's Hiroshima Leaders' Communiqué, the fifth TTC joint statement should explicitly endorse preventing the exploitation of advanced US-EU tech as a legitimate rationale for dual-use export controls.

Improve European export control governance: the European Union should consider proposals to develop a new joint risk framework for bloc-wide export controls and uplift the Dutch government's definition of "public security."[207] The EU should also follow through on a recent draft recommendation of a parliamentary committee to set up a "dedicated European Export Control Agency" to oversee dual-use export controls.[208]

Address the implications of extraterritorial controls for advanced tech supply chains: Recent US export controls create perverse incentives for adversaries — and allies — to reduce their reliance on US tech, potentially threatening the controls' long-term effectiveness and weakening US leverage on China.[209] Congress should mandate the US Bureau of Industry and Security produce a report evaluating how foreign direct product rules affect the presence of US inputs in semiconductor supply chains.

Broaden the discussion and think long term: Europe and the US should expand efforts to work with a wider array of democratic allies, including Japan, South Korea, and Taiwan, when aligning on export controls policy. Together, they should monitor the emergence of new technologies, map key supply chain chokepoints and dependencies, and assess the capabilities of selected countries.[210] This will help build consensus and foster common threat perceptions, with a view to launching further initiatives, including a new multilateral export controls regime to deal with non-traditional security concerns.

Matthew Eitel is Special Assistant to the President and CEO at the Center for European Policy Analysis (CEPA). Matthew was previously a Program Officer for CEPA's Digital Innovation Initiative.

Charles Martinet contributed significant research and editorial support to this policy brief. Charles is a former intern with CEPA's Digital Innovation Initiative and is currently master's student at Sciences Po Paris, where he studies the geopolitics of technology, artificial intelligence governance, and EU tech policy.

Endnotes

1 "The Digital Markets Act: Ensuring Fair and Open Digital Markets," European Commission, October 12, 2022, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

2 Adam Satariano, "E.U. Takes Aim at Big Tech's Power with Landmark Digital Act," The New York Times, March 24, 2022, https://www.nytimes.com/2022/03/24/technology/eu-regulation-apple-meta-google.html.

3 Samuel Stolton, "US Pushes to Change EU's Digital Gatekeeper Rules," POLITICO, January 31, 2022, https://www.politico.eu/article/us-government-in-bid-to-change-eu-digital-markets-act/

4 "Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter into Force," European Commission Press Corner, October 31, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6423.

5 "Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter into Force," European Commission Press Corner, October 31, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6423.

6 "Vulnerabilities and threats in mobile applications, 2019," Positive Technologies, June 19, 2019, https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

7 "App Security Overview," Apple Support, May 13, 2022, https://support.apple.com/guide/security/app-security-overview-sec35dd877d0/web.

8 Sophie Mellor, "Apple and Google Criticize the New EU Digital Markets Act That Will Radically Change the Way They Have Operated for the Past 20 Years," Yahoo News, March 25, 2022, https://www.yahoo.com/now/apple-google-criticize-eu-digital-192134850.html.

9 "Vulnerabilities and threats in mobile applications, 2019," Positive Technologies, June 19, 2019, https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

10 Bill Echikson and Toomas Hendrik Ilves, "Missing in Europe's Tech Regulations – Security," Bandwidth, August 1, 2023, https://cepa.org/article/missing-in-europes-tech-regulations-security/

11 Bojan Jovanovic, "What is Encryption Software?," DataProt, updated May 5 2023, https://dataprot.net/articles/what-is-encryption-software/#:~:text=End%2Dto%2Dend%20or%20the,received%20data%20and%20decrypt%20it.

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

13 Gennie Gebhart, "A Privacy-Focused Facebook? We'll Believe It When We See It.," Deeplinks Blog, Electronic Frontier Foundation, March 7, 2019, https://www.eff.org/es/deeplinks/2019/03/privacy-focused-facebook-well-believe-it-when-we-see-it.

14 Christoph Schmon, Andrew Crocker, and Mitch Stoltz, "The EU Digital Markets Act's Interoperability Rule Addresses An Important Need, But Raises Difficult Security Problems for Encrypted Messaging," Electronic Frontier Foundation, May 2, 2022, https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises.

15 1. Elad Natanson, "How Encrypted Messaging Apps Have Become a Vital Tool for Surviving Warfare," Forbes, April 14, 2022, https://www.forbes.com/sites/eladnatanson/2022/04/13/how-encrypted-messaging-apps-have-become-a-vital-tool-for-surviving-warfare/?sh=4a42c17a106b.

16 "Remarks by Commissioner Breton: Here Are the First 7 Potential 'Gatekeepers' under the EU Digital Markets Act," Press Corner, European Commission, July 4, 2023, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_3674.

17 Ben Lovejoy, "Apple Faces March 5 Deadline for Third-Party App Stores – but Don't Hold Your Breath," 9to5Mac, July 4, 2023, https://9to5mac.com/2023/07/04/third-party-app-stores-deadline/.

18 "Lex – 32022R1925 – En – EUR-Lex; Article 10: Exemption," EUR-Lex, September 14, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925#:~:text=of%20this%20Regulation.-,Article%C2%A010,-Exemption%20for%20grounds

19 Christoph Schmon, Andrew Crocker, and Mitch Stoltz, "The EU Digital Markets Act's Interoperability Rule Addresses An Important Need, But Raises Difficult Security Problems for Encrypted Messaging," Electronic Frontier Foundation, May 2, 2022, https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises.

20 Henry Mostyn, Maurits Dolmans, and Emmi Kuivalainen, "Rigid Justice Is Injustice: The EU's Digital Markets Act Should Include An Express Proportionality Safeguard," Social Science Research Network Electronic Journal, 2022, Ondernemingsrecht, no. 2 (December 10, 2022): 1–22.

21 Brad Smith, "Defending Ukraine: Early Lessons From the Cyber War," Microsoft On the Issues Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

22 Stormy-Anniker Mildner, "German-American Tech and Trade Conference," Landesvertretung Baden-Württemberg, 15 February, 2023, video, 4:21:39, https://www.youtube.com/watch?v=0zm3CtWHI9E&t=15699s.

23 Cyber Resilience Act," Shaping Europe's Digital Future, European Commission, September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

24 "Directive on Measures For a High Common Level of Cybersecurity Across the Union (NIS2 Directive)," European Commission, January 16, 2023, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

25 "NIS Cooperation Group," Shaping Europe's Digital Future, European Commission, June 7, 2022, https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group.

26 "Proposal for Directive on Measures for High Common Level of Cybersecurity across the Union," Shaping Europe's digital future, European Commission, December 16, 2020, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

27 Maria del mar Negreiro Achiaga, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU: Think Tank: European Parliament," Think Tank | European Parliament, The European Parliament, February 8, 2023, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333; "Directive on Measures for a High Common Level of Cybersecurity across the Union," Shaping Europe's digital future, European Commission, May 12, 2021, https://digital-strategy.ec.europa.eu/en/library/directive-measures-high-common-level-cybersecurity-across-union-0

28 "Questions and Answers - Eu Cybersecurity," Press Corner, European Commission, June 26, 2019, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369

29 "Cyber Resilience Act," Shaping Europe's Digital Future, European Commission, September 15, 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

30 "Regulatory Framework", European Union Agency for Cybersecurity, accessed March 24, 2023, https://www.enisa.europa.eu/about-enisa/regulatory-framework.

31 Brando Benifei and Dragos Tudorache, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" Artificial Intelligence Act, The European Parliament - IMCO & LIBE Committees, November 28, 2022, https://artificialintelligenceact.eu/.

32 "New EU Cybersecurity Rules Are Well-Intended, but Introduce Unnecessary Red Tape," CCIA, Computer & Communications Industry Association, September 15, 2022, https://ccianet.org/news/2022/09/new-eu-cybersecurity-rules-are-well-intended-but-introduce-unnecessary-red-tape/.

33 Luca Bertuzzi, "EU Lawmakers Set to Close Deal on Cybersecurity Law for Connected Devices," EURACTIV, July 4, 2023, https://www.euractiv.com/section/cybersecurity/news/eu-lawmakers-set-to-close-deal-on-cybersecurity-law-for-connected-devices/.

34 "Agence Nationale de la Sécurité des Systèmes D'information, accessed March 24, 2023, https://www.ssi.gouv.fr/en/

35 Laurens Cerulus, "Big Tech Cries Foul Over EU Cloud-Security Label," POLITICO, POLITICO, June 14, 2022, https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/

36 Carolina Ramos, Lindsey Sheppard and Erol Yayboke, "The Real National Security Concerns over Data Localization," Center for Strategic and International Studies, July 23, 2021), https://www.csis.org/analysis/real-national-security-concerns-over-data-localization;

37 "Enhancing Cybersecurity and Digital Resilience in Europe," Google, September 2022,https://services.google.com/fh/files/blogs/cybersecurity_and_digital_resilience.pdf

38 Laura Kabelka, "EU's Cybersecurity Agency Chief Warns to Keep Guard Up," EURACTIV, September 27, 2022, https://www.euractiv.com/section/cybersecurity/news/eus-cybersecurity-agency-chief-warns-to-keep-guard-up/.

39 Brad Smith, "Defending Ukraine: Early Lessons From the Cyber War," Microsoft On the Issues, Microsoft, June 22, 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

40 "Undercurrents: The Global Human Rights System, and Responding to Ransomware," Chatham House, August 12, 2021, https://www.chathamhouse.org/2021/08/undercurrents-global-human-rights-system-and-responding-ransomware

41 "EU-US Trade and Technology Council Addresses Common Challenges and Responds to Global Crisis," Press Corner, European Commission, December 5, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7433.

42 Ellen Nakashima, "U.S. National Security Cyber Strategy to Stress Biden to Push on Regulation," Washington Post, Washington Post, January 5, 2023, https://www.washingtonpost.com/national-security/2023/01/05/biden-cyber-strategy-hacking/

43 Stephen Weigand, "Reports: Inglis To Soon Retire From Office of National Cyber Director," SC Media, SC Media, December 24, 2022, https://www.scmagazine.com/news/leadership/reports-inglis-to-soon-retire-from-office-of-the-national-cyber-director.

44 "Fact Sheet: Biden-Harris Administration Delivers on Strengthening America's Cybersecurity," Briefing Room Statements and Releases, The White House, October 10, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/.

45 Julian E. Barnes and Edward Wong, "Chinese Hackers Targeted Commerce Secretary and Other U.S. Officials," The New York Times, July 12, 2023, https://www.nytimes.com/2023/07/12/us/politics/china-state-department-emails-microsoft-hack.html.

46 David E. Sanger, "New Biden Cybersecurity Strategy Assigns Responsibility to Tech Firms," The New York Times, The New York Times, March 2, 2023, https://www.nytimes.com/2023/03/02/us/politics/biden-cybersecurity-strategy.html.

47 "National Cybersecurity Strategy — Implementation Plan," The White House, July 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

48 Trey Herr et al., "The National Cybersecurity Strategy Implementation Plan: A CSI Markup," Digital Forensic Lab, July 19, 2023, https://dfrlab.org/2023/07/18/national-cybersecurity-strategy-implementation-plan-markup/.

49 "Strategic Intent Statement for the Office of the National Cyber Director," The White House, The White House, October 1, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/10/ONCD-Strategic-Intent.pdf.

50 "Fact Sheet: U.S.-EU Trade and Technology Council Advances Concrete Action on Transatlantic Cooperation," The White House, December 5, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/fact-sheet-u-s-eu-trade-and-technology-council-advances-concrete-action-on-transatlantic-cooperation/.

51 Ondrej Burkacky, Julia Dragon, and Nikolaus Lehmann, "The Semiconductor Decade," Our Insights, McKinsey, McKinsey & Company, April 1, 2022 , https://www.mckinsey.com/industries/semiconductors/our-insights/the-semiconductor-decade-a-trillion-dollar-industry.

52 Asa Fitch, "Chip Inventories Swell as Consumers Buy Fewer Gadgets," WSJ, The Wall Street Journal, December 27, 2022, https://www.wsj.com/articles/chip-inventories-swell-as-consumers-buy-fewer-gadgets-11672092605?mod=hp_lead_pos5.

53 Christopher Veitch, "Semiconductor Chip Shortage's Continual Impact," Schneider Downs, Schneider Downs, April 19, 2022, https://www.schneiderdowns.com/our-thoughts-on/semiconductor-chip-shortages-continual-impact.

54 Brian Ashcraft, "Sony Cuts PlayStation 5 Sales Expectations Due to Global Chip Shortage," Kotaku, Kotaku, February 2, 2022, https://kotaku.com/ps5-playstation-5-sony-chip-shortage-semiconductor-supp-1848465342.

55 Saibal Dasgupta, "Race For Semiconductors Influences Taiwan Conflict," VOA News, VOA, August 10, 2022, https://www.voanews.com/a/race-for-semiconductors-influences-taiwan-conflict-/6696432.html.

56 Daniel Slotta, "China's share of worldwide semiconductor manufacturing capacity from 2013 to 2021," Statista, last modified November 3, 2021, https://www.statista.com/statistics/1272188/china-share-of-global-semiconductor-manufacturing-capacity/.

57 Lauly Li, "The Global Microchip Race: Europe's Bid to Catch Up," FT, Financial Times, December 13, 2022, https://www.ft.com/content/b31e27fd-0781-4ffd-bb69-9af985abff41.

58 Eamon Barrett, "Taiwan's Drought is Exposing Just How Much Water Chip Makers Like TSMC Use (And Reuse)," Fortune, Fortune, June 12, 2021, https://fortune.com/2021/06/12/chip-shortage-taiwan-drought-tsmc-water-usage/.

59 Chris Szewczyk, "Taiwan Earthquake Reminds Us How Vulnerable the World's Chip Supply Really Is," PCGamer, Future Publishing, September 20, 2022, https://www.pcgamer.com/taiwan-earthquake-reminds-us-how-vulnerable-the-worlds-chip-supply-really-is/.

60 Vishnu Kannan and Jacob Feldgoise, "After the CHIPS Act: The Limits of Reshoring and Next Steps for U.S. Semiconductor Policy," Carnegie Endowment, Carnegie Endowment for International Peace, November 22, 2022, https://carnegieendowment.org/2022/11/22/after-chips-act-limits-of-reshoring-and-next-steps-for-u.s.-semiconductor-policy-pub-88439

61 "Why is There a Shortage of Semiconductors?" The Economist explains, The Economist Newspaper, February 25, 2021, https://www.economist.com/the-economist-explains/2021/02/25/why-is-there-a-shortage-of-semiconductors.

62 Anna Cooban and Chris Stern, "Germany Blocks Sale of Chip Factory to China Over Security Fears," CNN Business, November 10, 2022, https://edition.cnn.com/2022/11/09/tech/germany-blocks-chip-factory-sale-china.

63 Helen Thomas, "Muddle Over Welsh Semiconductor Company is a Lesson in Strategy," Financial Times, November 22, 2022, https://www.ft.com/content/7467ec0e-9819-4a92-bd69-ca1d0b7762e2.

64 Sophie Batas, "Huawei and European Industry: Natural Powers," POLITICO, December 23, 2020, https://www.politico.eu/sponsored-content/huawei-and-european-industry-natural-partners/.

65 Chris Park, "Potential Dependency Oversight in U.S.-South Korea Chip Policy," Asia Unbound, Council on Foreign Relations, September 19, 2022, https://www.cfr.org/blog/potential-dependency-oversight-us-south-korea-chip-policy.

66 Sarah Wu, "Taiwan Invests in Next Generation of Talent with Slew of Chip Schools," Reuters, Reuters, March 11, 2022, https://www.reuters.com/markets/funds/taiwan-invests-next-generation-talent-with-slew-chip-schools-2022-03-10/.

67 Sebastion Moss, "South Korea to Spend $451 Billion on Becoming a Semiconductor Manufacturing Giant," Data Center Dynamics, May 14, 2021, https://www.datacenterdynamics.com/en/news/south-korea-to-spend-451-billion-to-become-semiconductor-manufacturing-giant/.

68 Chips Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022), https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.

69 "Intel Announces Next US Sight with Landmark Investment in Ohio," Intel Newsroom, Intel, January 21, 2022, https://www.intel.com/content/www/us/en/newsroom/news/intel-announces-next-us-site-landmark-investment-ohio.html#gs.qwk98d.

70 "GlobalFoundries and Qualcomm Announce Extension of Long-Term Agreement to Secure U.S. Supply through 2008," PR Newswire, Cision, August 8, 2022, https://www.prnewswire.com/news-releases/globalfoundries-and-qualcomm-announce-extension-of-long-term-agreement-to-secure-us-supply-through-2028-301601262.html.

71 Debby Wu and Sohee Kim, "Samsung Eyes $200 Billion Expansion of Chip Plants in Texas," Bloomberg, Bloomberg, July 21, 2022, https://www.bloomberg.com/news/articles/2022-07-21/samsung-eyes-sweeping-expansion-of-chip-facilities-in-texas#xj4y7vzkg.

72 Chips Act of 2022, Pub. L. No. 117-167, 136 Stat. 1366 (2022), https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.

73 Debby Wu, Daniel Flatley, and Jenny Leonard, "U.S. to Stop TSMC, Intel From Adding Advanced Chip Fabs in China," Bloomberg, August 2, 2022, https://www.bloomberg.com/news/articles/2022-08-02/us-to-stop-tsmc-intel-from-adding-advanced-chip-fabs-in-china#xj4y7vzkg.

74 National Defense Authorization Act of 2019, H.R. 5515, 115th Cong. (2019), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf.

75 National Defense Authorization Act of 2021, H.R. 6395, 116th Cong. (2021), https://www.govtrack.us/congress/bills/116/hr6395/text.

76 Vishnu Kannan and Jacob Feldgoise, "After the CHIPS Act: The Limits of Reshoring and Next Steps for U.S. Semiconductor Policy," Carnegie Endowment for International Peace, November 22, 2022, https://carnegieendowment.org/2022/11/22/after-chips-act-limits-of-reshoring-and-next-steps-for-u.s.-semiconductor-policy-pub-88439.

77 The European Commission, "European Chips Act," https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

78 Alicia Garcia-Herrero and Niclas Poitiers, "Europe's Promised Semiconductor Subsidies Need To Be Better Targeted," Bruegel, October 17, 2022, https://www.bruegel.org/blog-post/europes-promised-semiconductor-subsidies-need-be-better-targeted.

79 Pieter Haeck, "In the Global Chips Race, EU's Cash Engine sputters," POLITICO, November 15, 2022, https://www.politico.eu/article/budget-squabbles-put-eu-on-the-back-foot-in-the-chips-race/

80 "Intel Announces Initial Investment of More Than €33 Billion for Semiconductor R&D and Manufacturing in EU," Press Releases, Intel, March 15, 2022, https://www.intc.com/news-events/press-releases/detail/1532/intel-announces-initial-investment-of-more-than-33.

81 "The EU Chips Act: Securing Europe's Supply of Semiconductors," Think Tank Briefing, The European Parliament, December 28, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)73359.

82 Christopher Cytera, "The Good, the Bad, and the Missing in the UK's Semiconductor Strategy," Bandwidth, Center for European Policy Analysis, June 7, 2023, https://cepa.org/article/the-good-the-bad-and-the-ugly-in-the-uks-semiconductor-strategy/.

83 U.S. Bureau of Industry and Security, "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," US Bureau of Industry and Security, October 7, 2022, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file

84 Sujai Shivakumar, Charles Wessner, and Thomas Howell, "A Seismic Shift: The New U.S. Semiconductor Export Controls and the Implications for U.S. Firms, Allies, and the Innovation Ecosystem," CSIS Analysis, Center for Strategic & International Studies, November 14, 2022, https://www.csis.org/analysis/seismic-shift-new-us-semiconductor-export-controls-and-implications-us-firms-allies-and.

85 Stephen Nellis, Karen Freifeld, and Alexandra Alper, "U.S. Aims to Hobble China's Chip Industry with Sweeping New Export Rules," Reuters, October 10, 2022, https://www.reuters.com/technology/us-aims-hobble-chinas-chip-industry-with-sweeping-new-export-rules-2022-10-07/.

86 Regina Sukwanto, "China's semiconductor industry: Seeking for self-sufficiency amid tensions with Taiwan and the US chip export ban." DaxueConsulting, last modified September 28, 2022, https://daxueconsulting.com/china-semiconductor-industry/.

87 Max Cherney, "The Biden Administration Issues Sweeping New Rules on Chip-Tech Exports to China," Protocol, Protocol, October 7, 2022, https://www.protocol.com/enterprise/chip-export-restrictions-tsmc-intel.

88 "What do US curbs on selling microchips to China mean for the global economy?" The Guardian, The Guardian News & Media, October 19, 2022, https://www.theguardian.com/world/2022/oct/19/what-do-us-curbs-on-selling-microchips-to-china-mean-for-the-global-economy.

89 "What People Are Saying about China's Chipmaking Export Controls." Reuters, July 4, 2023. https://www.reuters.com/technology/what-people-are-saying-about-chinas-chipmaking-export-controls-2023-07-04/.

90 Christopher Cytera, "Chip Wars: China Strikes Back," Bandwidth, Center for European Policy Analysis, July 5, 2023, https://cepa.org/article/chip-wars-china-strikes-back/

91 Antonia Hmaidi and Rebecca Arcesati, "Why Europe Struggles With US Export Controls on China," The Diplomat Media, December 27, 2022, https://thediplomat.com/2022/12/why-europe-struggles-with-us-export-controls-on-china/.

92 Christopher Cytera, “the Chinese Communist Trojan Horses in Our CCTV,” Europe’s Edge, Center for European Policy Analysis, Center for European Policy Analysis, March 24, 2021, https://cepa.org/article/the-chinese-communist-trojan-horses-in-our-cctv/.

93 Alan Weissburger, ”Strand Consult: Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 31 European Countries,” IEEE ComSoc, IEEE Communications Society, https://techblog.comsoc.org/2022/12/17/1068759/.

94 Matthew Eitel and Bill Echikson, ”Netherlands Joins the US anti-China Tech Chorus,” Bandwidth , Center for European Policy Analysis, March 10, 2023, https://cepa.org/article/netherlands-joins-the-us-anti-china-tech-chorus/.

95 “American is Struggling to Counter China’s Intellectual Property Theft,” Financial Times, April 18, 2022, https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39.

96 Sherisse Pham, “How Much Has the US Lost From China’s IP Threat,” CNN Buiness, March 23, 2018, https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html.

97 “Operation Cuckoobees Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation,” Cybereason, May 2, 2022, https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation.

98 Paul van Gerven, ”Court Quadruples ASML’s Damages in XTAL Case,” Bits & Chips, Techwatch, May 6, 2019, https://bits-chips.nl/artikel/court-quadruples-asmls-damages-in-xtal-case/.

99 Paul van Gerven, ”ASML Suspects Stolen IP is Being Commercialized in China,” Bits & Chips, Techwatch, June 7, 2021, https://bits-chips.nl/artikel/asml-suspects-stolen-ip-is-being-commercialized-in-china/.

100 Jon Bateman, ”U.S.-China Technological ’Decoupling,’” Carnegie Endowment for International Peace, 2022, https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf.

101 “China: 83 Brands Implicated in Report on Forced Labour of Ethnic Minorities from Xinjiang Assigned to Factories Across Provinces; Includes Company Responses,” Business and Human Rights, Business & Human Rights Resource Center, https://www.business-humanrights.org/en/latest-news/china-83-major-brands-implicated-in-report-on-forced-labour-of-ethnic-minorities-from-xinjiang-assigned-to-factories-across-provinces-includes-company-responses/.

102 Wayne Ma, ”Seven Apple Suppliers Accused of Using Forced Labor from Xinjiang,” The Information, The Information, May 10, 2021, https://www.theinformation.com/articles/seven-apple-suppliers-accused-of-using-forced-labor-from-xinjiang.

103 Ana Swanson and Chris Buckley, “Red Flags for Forced Labor Found in China’s Car Battery Supply Chain,” The New York Times, June 20, 2022, https://www.nytimes.com/2022/06/20/business/economy/forced-labor-china-supply-chain.html.

104 “China uses Uyghur Forced Labor to Make Solar Panels, Says Report,” BBC News, May 14, 2021, https://www.bbc.com/news/world-asia-china-57124636.

105 Martin Chorzempa, "US Security Scrutiny of Foreign Investment Rises, But So Does Foreign Investment," PIIE, Peterson Institute for International Economics, September 1, 2022, https://www.piie.com/blogs/realtime-economic-issues-watch/us-security-scrutiny-foreign-investment-rises-so-does-foreign.

106 Finbarr Bermington, "Posts in a Storm: Chinese Investments in Europe Spark Fear of Malign Influence," South China Morning Post, October 30, 2022, https://www.scmp.com/news/china/diplomacy/article/3197723/ports-storm-chinese-investments-europe-spark-fear-malign-influence.

107 "A Fast and Accurate Innovative Imagining Technique to Moniter Modern Semiconductor Devices," SPIE, The International Society for Optics and Photonics, April 20, 2022, https://spie.org/news/a-fast-and-accurate-innovative-imaging-technique-to-monitor-modern-semiconductor-devices?SSO=1.

108 Sebastion Göke, Kevin Straight, and Rutger Vrijen, "Scaling AI in the Sector that Enables It: Lesson for Semiconductor-Device Makers," McKinsey Insights, McKinsey & Company, April 2, 2021, https://www.mckinsey.com/industries/semiconductors/our-insights/scaling-ai-in-the-sector-that-enables-it-lessons-for-semiconductor-device-makers

109 "Joint Statement by President Biden and President von der Leyen," Briefing Room Statements and Releases, The White House, March 10, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/10/joint-statement-by-president-biden-and-president-von-der-leyen-2/.

110 Steven Overly and Barbara Moens, "U.S., EU lawmakers feel cut out of Biden's electric vehicle trade agenda," POLITICO, March 31, 2023, https://www.politico.com/news/2023/03/31/washington-brussels-pushback-patch-trade-rift-00089941.

111 Mark Minevich, "How to Fight Climate Change Using AI," Forbes, July 8, 2022, https://www.forbes.com/sites/charlestowersclark/2023/04/18/should-only-the-rich-be-allowed-purpose/?.

112 The proposed AI Act and recent draft AI Liability Directive directly touch on AI, but other texts such as the Digital Services Act, Digital Markets Act, and Data Governance Act also have implications for AI technologies.

113 European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," COM(2021) 206 final, accessed April 19, 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206.

114 [2] Beijing has been increasingly explicit about its intentions through initiatives such as the National Medium- and Long-Term Program for Science and Technology Development (2006-2020), Made in China 2025, the New Generation Artificial Intelligence Development Plan, and China Standards 2035.

115 Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness," Virginia: Special Competitive Studies Project, 2022, https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf.

116 Kyle Wiggers, "The EU's AI Act could have a Chilling Effect on Open Source Efforts, Experts Warn," Tech Crunch, Yahoo, September 6, 2022, https://techcrunch.com/2022/09/06/the-eus-ai-act-could-have-a-chilling-effect-on-open-source-efforts-experts-warn/.

117 Margaret Taylor, "Data Protection: Threat to GDPR's Status as 'Gold Standard,'" IBANet, International Bar Association, August 25, 2020, https://www.ibanet.org/article/A2AA6532-B5C0-4CCE-86F7-1EAA679ED532.

118 Chinchih Chen, Carl Benedikt Frey, and Giorgio Presidente, "Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally," Oxford Martin Working Paper Series on Technological and Economic Change, No. 2022-1 (2022), https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf.

119 Ashish Kumar Sen, "Eric Schmidt on Confronting China: Stop Regulating and Invent," Europe's Edge, Center for European Policy Analysis, September 30, 2021, https://cepa.org/article/eric-schmidt-on-confronting-china-stop-regulating-and-invent/.

120 Hadrien Pouget, "The EU's AI Act is Barreling Toward AI Standards That Do Not Exist," Lawfare blog, Lawfare, January 12, 2023, https://www.lawfareblog.com/eus-ai-act-barreling-toward-ai-standards-do-not-exist.

121 Iskander Sanchez-Role et al., "Can I opt out yet?: GDPR and the Global Illusion of Cookie Control," Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, Asia CCS '19 (New York: Association for Computing Machinery, 2019), 340-351, https://doi.org/10.1145/3321705.3329806.

122 European Data Protection Supervisor, "ePrivacy Directive," accessed April 19, 2023, https://edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en.

123 "Safer Internet Day: Are you Restricting Cookies," Eurostat, European Commission, February 8, 2022, https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220208-1.

124 Elaine Fox, "Sharing an Update to our Privacy Policy," TikTok Newsroom, Bytedance, November 2, 2022, https://newsroom.tiktok.com/en-eu/sharing-an-update-to-our-privacy-policy.

125 Jamil Anderlini and Clothilde Goujard, "Brussels moves to ban Eurocrats from using TikTok," POLITICO, February 23, 2023, https://www.politico.eu/article/european-commission-to-staff-dont-use-tiktok/

126 Davey Alba, "Open AI's Chatbot Spits Out Biased Musings, Despite Guardrails," Bloomberg, December 8, 2022, https://www.bloomberg.com/news/newsletters/2022-12-08/chatgpt-open-ai-s-chatbot-is-spitting-out-biased-sexist-results.

127 Ylli Bajraktari, "2-2-2: Where are we on AI Regulations?," SCSP 2-2-2, Special Competitive Studies Project, SCSP, February 16, 2022, https://scsp222.substack.com/p/scsp222?s=r.

128 Anu Bradford. The Brussels Effect: How the European Union Rules the World. New York: Oxford University Press, 2020.

129 "OECD Principles on Artificial Intelligence," OECD, accessed April 19, 2023, https://oecd.ai/en/ai-principles; "G7 Hiroshima Leaders' Communiqué," G7, May 20, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/; White House Office of Science and Technology Policy, "Artificial Intelligence Bill of Rights," White House Office of Science and Technology Policy, accessed April 19, 2023, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

130 Cameron F. Kerry and John Villasenor, "Protecting Privacy in an AI-Driven World," Brookings Institution, December 10, 2019, https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

131 Philip Blenkinsop, "EU tech chief sees draft voluntary AI code within weeks," Reuters, May 31, 2023, https://www.reuters.com/technology/eu-tech-chief-calls-voluntary-ai-code-conduct-within-months-2023-05-31/

132 "The First Networked War: Eric Schmidt's Defense Innovation Board and the Future of U.S. Military Technology," SCSP 2-2-2, Special Competitive Studies Project, May 22, 2021, https://scsp222.substack.com/p/the-first-networked-war-eric-schmidts.

133 "U.S.-EU Trade and Technology Council (TTC)," US Department of State, accessed April 19, 2023, https://www.state.gov/u-s-eu-trade-and-technology-council-ttc/.

134 "TTC Joint Roadmap: Trustworthy AI and Risk Management," Shaping Europe's Digital Future, European Commission, accessed April 19, 2023, https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management.

135 European Parliament Research Service, "The EU's New Digital Compass and the Way Forward," European Parliament Research Service, February 2023, accessed April 19, 2023, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739336.

136 Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness," Virginia: Special Competitive Studies Project,2022, page 103, https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf.

137 "Commerce Implements Sweeping Restrictions on Exports to Russia In Response to Further Invasion of Ukraine," Office of Congressional and Public Affairs, U.S. Department of Congress, February 24, 2022, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/2914-2022-02-24-bis-russia-rule-press-release-and-tweets-final/file.

138 "Joint Statement on the EU-US Trade and Technology Council of 31 May 2023 in Lulea", Press Corner, European Commission, May 31, 2023, https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992.

139 "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification", Federal Register, Bureau of Industry and Security, Department of Commerce, October 13, 2022, https://www.federalregister.gov/d/2022-21658/p-5

140 Christian Paul, "Updating the EU Control List: Keeping Up With Technological Change," (presentation, 2022 Export Control Forum, Brussels, December 6, 2022), https://circabc.europa.eu/ui/group/654251c7-f897-4098-afc3-6eb39477797e/library/aebe73fa-52d8-40fb-bd2f-0851a60a5b3f/details.

141 "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution", Briefing Room Speeches and Remarks, The White House, April 27, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/

142 Anchal Vohra, "Europe Is Stuck in a Toxic China Relationship," Analysis, Foreign Policy, June 22, 2023 https://foreignpolicy.com/2023/06/22/europe-is-stuck-in-a-toxic-china-relationship/.

143 Paul Kerr and Christopher Kasey, "The U.S. Export Control System and the Export Control Reform Act of 2018," CRS Reports, Congressional Research Service, June 7, 2021, https://crsreports.congress.gov/product/pdf/R/R46814

144 "Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under EU-US Trade and Technology Council", European Commission, January 14, 2022, https://futurium.ec.europa.eu/en/EU-US-TTC/wg7/posts/public-comments-kevin-wolf-emily-kilcrease-and-jasper-helder-regarding-areas-and-priorities-us-and

145 Scott Kennedy, "Made in China 2025," CSIS, Center for International & Strategic Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025

146 Björn Conrad et al., "Made in China 2025," Merics, Mercator Institute for China Studies, August 12, 2016, https://merics.org/en/report/made-china-2025.

147 Kevin Wolf et al., "The Export Control Reform Act of 2018 and Possible New Controls on Emerging and Foundational Technologies," Akin Gump, Straus Hauer & Feld LLP, September 12, 2018, https://www.akingump.com/a/web/97168/aokrg/international-trade-alert-09-12-2018-the-export-control-refo.pdf

148 David Sanger et al., "In 5G Race with China, U.S. Pushes Allies to Fight Huawei," The New York Times Company, January 26, 2019, https://www.nytimes.com/2019/01/26/us/politics/huawei-china-us-5g-technology.html

149 "Addition of Entities to Entity List", Federal Register, Bureau of Industry and Security, Department of Commerce, https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list

150 "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," Press Release, Bureau of Industry and Security, U.S. Department of Commerce, https://2017-2021.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.html

151 "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General Liscense, and Amendments to the General Prohibition Three (Foreign-Produced Direct Product Rule)", Federal Register, U.S. Department of Commerce, Bureau of Industry and Security, August 20, 2020, https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2593-85-fr-51596/file; Kevin Wolf et al., "US Government Clarifies, Reorganizes, and Renames Descriptions of How Foreign-Produced Items Outside of the United States are Subject to US Export Controls as the US Contemplates New Restrictions on Russia," Akin Gump, Strauss Hauer & Feld LLP, February 9, 2022, https://www.akingump.com/a/web/6SN1Qt9s1tPFQ4h6fjePTq/3BJHNi/international-trade-alert.pdf

152 Kay Georgi and Sylvia Costelloe, "BIS Expands the Huawei Foreign Direct Product Rule to Capture a Wide Swath of COTS Products," AFSlaw, ArentFox Schiff, August 19, 2020, https://www.afslaw.com/perspectives/alerts/bis-expands-the-huawei-foreign-direct-product-rule-capture-wide-swath-cots.

153 "EU-US Trade and Technology Council (TTC) Export Controls Working Group," Bureau of Industry and Security, U.S. Department of Commerce, October 27, 2021, https://www.bis.doc.gov/index.php/policy-guidance/u-s-eu-ttc

154 Emily Kilcrease, "Noteworthy: The New Russia Export Controls," CNAS, Center for a New American Security, March 7, 2022,https://www.cnas.org/press/press-note/noteworthy-the-new-russia-export-controls ; "Resources on Export Controls Implemented in Repsonse to Russia's Invasion of Ukraine",Bureau of Industry and Security, U.S. Department of Commerce, May 19

155 Wolf et al., "U.S. Government Imposes Expansive Novel and Plurilateral Export Controls Against Russia and Belarus," Akin Gump, Strauss Hauer & Feld LLP, March 8, 2022, https://www.akingump.com/a/web/ayCoxfB41bXG1H8Y4jUWup/3FFMet/us-government-imposes-expansive-novel-and-plurilateral-export.pdf

156 "National Security Strategy", The White House, October 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; "Annual Threat Assessment of the US Intelligence Community", Office of the Director of National Intelligence, April 9, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

157 "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy", The White House, October 12, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/

158 "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit", Briefing Room Speeches and Remarks, The White House, September 16, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/; "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy", The White House, October 12, 2022, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/

159 "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)," Bureau of Industry and Security, U.S. Department of Commerce, October 7, 2022, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file

160 Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," War on the Rocks, Metamorphic Media, January 6, 2023, https://warontherocks.com/2023/01/how-to-win-friends-and-choke-chinas-chip-supply/; Emily Benson, "Bargaining Chips: US Allies and Export Controls," the Diplomat, January 1, 2023, https://thediplomat.com/2022/12/bargaining-chips-us-allies-and-export-controls/

161 Yuka Hayashi and John D. McKinnon, "U.S. Looks to Restrict China's Access to Cloud Computing to Protect Advanced Technology," The Wall Street Journal, July 4, 2023, https://www.wsj.com/articles/u-s-looks-to-restrict-chinas-access-to-cloud-computing-to-protect-advanced-technology-f771613

162 Karen Freifeld, "Exclusive: US, Dutch set to hit China's chipmakers with one-two punch," Reuters, June 29, 2023, https://www.reuters.com/technology/us-dutch-set-hit-chinas-chipmakers-with-one-two-punch-2023-06-29/

163 Jon Bateman, "The Fevered Anti-China Attitude in Washington Is Going to Backfire," POLITICO, December 15, 2022, https://www.politico.com/news/magazine/2022/12/15/china-tech-decoupling-sanctions-00071723; Alex W. Palmer, "'An Act of War': Inside America's Silicon Blockade Against China," The New York Times, July 12, 2023, https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html

164 "Remarks by Secretary of the Treasury Janet L. Yellen on the U.S. - China Economic Relationship at Johns Hopkins School of Advanced International Studies", Press Releases, U.S. Department of the Treasury, April 20, 2023, https://home.treasury.gov/news/press-releases/jy1425

165 "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution", Briefing Room Speeches and Remarks, The White House, April 27, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/

166 Martijn Rasser, "A Conversation with Under Secretary of Commerce Alan F. Estevez," CNAS, Center for a New American Security, October 27, 2022, https://www.cnas.org/publications/transcript/a-conversation-with-under-secretary-of-commerce-alan-f-estevez

167 Barbara Moens and Hans Von Der Burchard, "Europe First: Brussels Gets Ready to Dump its Free Trade Ideals," POLITICO, December 5, 2022 https://www.politico.eu/article/ursula-von-der-leyen-joe-biden-trade-europe-first-brussels-gets-ready-to-dump-its-free-trade-ideals/; Zaki Laïdi, «Can Europe Learn to Play Power Politics," CER, Center for European Reform, November 28th, 2019, https://www.cer.eu/publications/archive/essay/2019/can-europe-learn-play-power-politics

168 European Parliament and Council of the European Union, Regulation (EU) 2021/821, Setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), May 20, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0821

169 Publications Office of the European Union, Regulation (EU) 2021/821 setting up an EU regime for the control of exports, brokering, technical assisstance, transit and transfer of dual-use items, January 12, 2023, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=legissum:4532505.

170 Klaui et al., "The Recast Dual Use Regulation - A Missed Opportunity," Akin Gump, Strauss Hauer & Feld LLP, June 11, 2021, https://www.akingump.com/a/web/sMtcSswS9zAkkKzXQrAGkq/2NyXfv/the-recast-dual-use-regulation-a-missed-opportunity.pdf

171 "Frequently Asked Questions: Restrictive Measures (Sanctions)," Press Corner, European Commission, February 26th, 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_1401

172 Jan Strupczewski, "No More EU Sanctions on Russia Needed, Negotiatons Better Option - Hungary," Reuters, June 23, 2022, https://www.reuters.com/world/europe/no-more-eu-sanctions-russia-needed-negotiations-better-option-hungary-2022-06-23/

173 "European Commission and HR/VP Contribution to the European Council: EU-China – A Strategic Outlook," European Commission, March 12, 2019, https://commission.europa.eu/system/files/2019-03/communication-eu-china-a-strategic-outlook.pdf.

174 Alexandra Brzozowski, "EU Proposes to Recalibrate China Strategy," EURACTIV, May 12, 2023, https://www.euractiv.com/section/eu-china/news/eu-proposes-to-recalibrate-china-strategy/; Josep Borrell, "How to Deal With China," EEAS, European Union External Action Service, https://www.eeas.europa.eu/eeas/how-deal-china_en

175 Jessica Parker, "Lithuania-China Row: EU Escalates Trade Dispute with Beijing," BBC News , January 27, 2022, https://www.bbc.com/news/world-europe-60140561; "Trade: Political Agreement on the Anti-Coercion Instrument," Press Release, Council of the European Union, March 28, 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/03/28/trade-political-agreement-on-the-anti-coercion-instrument/

176 "Speech by President Von Der Leyen on EU-China Relations to the Mercator Institute for China Studies and the European Policy Center", PressMarch 30, 2023, https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2063; European Commission, An EU approach to enhance economic security, June 20, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3358

177 Jana Puglieren and Pawel Zerka, "Keeping America Close, Russia Down, and China Far Away: How Europeans Navigate a Competitive World," ECFR, European Council on Foreign Relations, June 7, 2023, https://ecfr.eu/publication/keeping-america-close-russia-down-and-china-far-away-how-europeans-navigate-a-competitive-world/

178 Arendse Huld, "EU-China Relations - Trade, Investment and Recent Developments," China Briefing, Dezan Shira and Associates, April 4, 2023 https://www.china-briefing.com/news/eu-china-relations-trade-investment-and-recent-developments/

179 Guy Chazan, Laura Pitel, and Patricia Nilsson, "Germany warns companies to reduce dependence on China," Financial Times, July 13, 2023, https://www.ft.com/content/3add5745-fbf4-48b3-8638-70a8f912136e

180 Finbarr Bermingham, "EU's 'de-risking' plan for China meets resistance from some members," South China Morning Post, June 10, 2023, https://www.scmp.com/news/china/diplomacy/article/3223619/eus-de-risking-plan-china-meets-resistance-some-members; Philip Blenkinsop, "EU Faces Test to Get Members to Cede Power on Export Controls," Reuters, May 26, 2023, https://www.reuters.com/business/eu-faces-test-get-members-cede-power-export-controls-2023-05-26/

181 Charles Martinet, "Dutch Dilemma: Caught in the Middle of the US-China Tech Cold War," Bandwidth, Center for European Policy Analysis, January 18, 2023, https://cepa.org/article/dutch-dilemma-caught-in-the-middle-of-the-us-china-tech-cold-war/

182 "EUV Lithography Systems," ASML, last accessed June 8, 2023, https://www.asml.com/en/products/euv-lithography-systems

183 Stu Woo and Yang Jie, "China wants a Chip Machine From the Dutch. The U.S. Said No," Wall Street Journal, July 17, 2023, https://www.wsj.com/articles/china-wants-a-chip-machine-from-the-dutch-the-u-s-said-no-11626514513; Alexandra Alper, Tober Sterling, and Stephen Nellis, "Trump Administration Pressed Dutch Hard to Cancel China Chip-Equipment Sale: Sources," Reuters,January 6, 2020 https://www.reuters.com/article/us-asml-holding-usa-china-insight-idUSKBN1Z50HN

184 McCarthy et al., "BIS Imposes New Controls to Limit the Development and Production of Advanced Computing and Semiconductor Capabilities in China," Akin Gump, Strauss Hauer & Feld LLP, October 27, 2022, https://www.akingump.com/a/web/dPkFKYAkdYwpiDGPT5RzQz/4v9EH8/international-trade-alert.pdf

185 Sam Flemming and Andy Bounds, "Dutch Minister Defends Trade Link With China," Financial Times, December 1, 2022, https://www.ft.com/content/d10a2164-b447-4bcf-9e01-e297a5fb423c; Toby Sterling, "Dutch Trade Minister: Won't Summarily Agree to U.S. Rules on China Exports," Reuters, January 16, 2023, https://www.reuters.com/technology/dutch-trade-minister-wont-summarily-agree-us-rules-china-exports-2023-01-16/

186 Matthew Eitel and Bill Echikson, "Netherlands Joins the US Anti-China Tech Chorus," CEPA, Center for European Policy Analysis, March 10, 2023, https://cepa.org/article/netherlands-joins-the-us-anti-china-tech-chorus/ ; Government of the Netherlands, Government publishes additional export measures for advanced semiconductor manufacturing equipment, June 30, 2023, https://www.government.nl/latest/news/2023/06/30/government-publishes-additional-export-measures-for-advanced-semiconductor-manufacturing-equipment

187 Tim Kelly and Miho Uranaka, "Japan Restricts Chipmaking Equipment Exports as it Aligns with US China Curbs," Reuters, March 31, 2023, https://www.reuters.com/technology/japan-restrict-chipmaking-equipment-exports-aligning-it-with-us-china-curbs-2023-03-31/

188 European Commission, Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation Under the US-EU Trade and Technology Council, January 14, 2022 https://futurium.ec.europa.eu/en/EU-US-TTC/wg7/posts/public-comments-kevin-wolf-emily-kilcrease-and-jasper-helder-regarding-areas-and-priorities-us-and

189 Kevin Wolf and Emily Weinstein, Cocom's Daughter?, Center for Security and Emerging Technology, Georgetown University, May 2022, https://cset.georgetown.edu/wp-content/uploads/WorldECR-109-pp24-28-Article1-Wolf-Weinstein.pdf

190 Jon Bateman, "The Fevered Anti-China Attitude in Washington Is Going to Backfire," POLITICO, December 15, 2022, https://www.politico.com/news/magazine/2022/12/15/china-tech-decoupling-sanctions-00071723

191 Emily Weinstein, "Challenges from Chinese Policy in 2022: Zero-COVID, Ukraine, and Pacific Democracy," Testimony before the US-China Economic and Security Review Commission, August 3, 2022, https://cset.georgetown.edu/publication/emily-weinsteins-testimony-before-the-u-s-china-economic-and-security-review-commission-2/

192 Matthew Eitel, "Talking Trade, Tech — and Security?," CEPA, Center for European Policy Analysis, June 22, 2023, https://cepa.org/article/talking-trade-tech-and-security/

193 Marc Hijink, "ASML Chief Executive on Exports to China: We Have Already Surrendered Enough," Mediahaus NRC, December 13, 2022, https://www.nrc.nl/nieuws/2022/12/13/asml-topman-over-export-naar-china-wij-hebben-al-ingeleverd-a4151373; Christopher Cytera, "Chip Wars: China Strikes Back," Bandwidth, Center for European Policy Analysis, July 3, 2023, https://cepa.org/article/chip-wars-china-strikes-back/

194 Bill Echikson, "US and Europe Share Diagnosis on Tech Ills,Yet Risk Confrontation," CEPA, Center for European Policy Analysis, November 7, 2022, https://cepa.org/article/us-and-europe-share-diagnosis-on-tech-ills-yet-risk-confrontation/

195 Jeremy Shapiro, "Transatlantic Trade Disputes are Moving to a New US-Controlled Rhythm," Financial Times, March 9, 2023 https://www.ft.com/content/1a961a58-d6ec-46c4-bec1-e171eb0d8ef1; James Lewis, "Notes on Creating an Export Controls Regime," CSIS, Center for Strategic & International Studies, December 15, 2022, https://www.csis.org/analysis/notes-creating-export-control-regime

196 "U.S. Space Industry "Deep Dive" Assessment: Impact of U.S. Export Controls on the Space Industrial Base", U.S. Department of Commerce, Bureau of Industry and Security, 2014 https://www.bis.doc.gov/index.php/documents/technology-evaluation/898-space-export-control-report/file

197 Martijin Rasser, "Rethinking Export Controls: Unintended Consequences and the New Technological Landscape," CNAS, Center for A New American Security, December 8, 2022, https://www.cnas.org/publications/reports/rethinking-export-controls-unintended-consequences-and-the-new-technological-landscape#fn22

198 Sarah Bauerle Danzman and Emily Kilcrease, "The Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail," Foreign Affairs, Council on Foreign Relations, December 30, 2022, https://www.foreignaffairs.com/united-states/illusion-controls

199 Che Pan and Ann Cao, "Exclusive: Tech War: China's Top Memory Chip Maker YMTC Making Progress in Producing Advanced 3D NAND Products with Locally Sourced Equipment: Sources," South China Morning Post Publishers, April 23, 2023, https://www.scmp.com/tech/article/3217919/tech-war-chinas-top-memory-chip-maker-ymtc-making-progress-producing-advanced-3d-nand-products

200 Iris Deng and Che Pan, "Tech War: Huawei's Stealth Chip Production Plan Becomes a Guessing Game for Industry Leaders as US Sanctions Keep it Hemmed In," South China Morning Post Publishers, January 6, 2023, https://www.scmp.com/tech/big-tech/article/3205730/tech-war-huaweis-stealth-chip-production-plan-becomes-guessing-game-industry-insiders-us-sanctions; Jan-Peter Kleinhaus et al., "Running on Ice: China's Chipmakers in a Post-October 7 World," Rhodium Group, April 4, 2023, https://rhg.com/research/running-on-ice/

201 "Xi's Metal Curbs Risk Backfiring as G-7 Seeks China Alternative," Bloomberg News, July 4, 2023, https://www.bloomberg.com/news/articles/2023-07-04/xi-s-metal-curbs-could-backfire-as-g-7-seeks-china-alternative?sref=SfEXIlDZ#xj4y7vzkg

202 Eleanor Olcott and Demetri Sevastopulo, "China Bans Micron's Products From Key Infrastructure Over Security Risk," Financial Times, May 21, 2023, https://www.ft.com/content/e6a8e034-cbc2-4267-9b41-b7670db7d130

203 Demetri Sevastopulo, "US Urges South Korea Not To Fill China Shortfalls If Beijing Bans Micron Chips," Financial Times, April 24, 2023, https://www.ft.com/content/64c58ee2-a604-4d31-84f4-bc0aa6d8343a

204 Yuka Hayashi, "U.S. to Allow South Korean, Taiwan Chip Makers to Keep Operations in China,» The Wall Street Journal, June 12, 2023, https://www.wsj.com/articles/u-s-to-allow-south-korean-taiwan-chip-makers-to-keep-operations-in-china-5d7d72cc?st=hco7ode3kleod4c; Martin Chorzempa, "How US Chip Controls on China can benefit and cost Korean firms," PIIE, Peterson Institute for International Economics, July 2023, https://www.piie.com/publications/policy-briefs/how-us-chip-controls-china-benefit-and-cost-korean-firms

205 Sam Kim, "South Korea to Avoid Cashing In on China's US Chipmaker Ban," Bloomberg, May 27, 2023, https://www.bloomberg.com/news/articles/2023-05-27/south-korea-to-avoid-cashing-in-on-china-s-us-chipmaker-ban#xj4y7vzkg

206 "EU-US Trade and Technology Council," European Commission, last accessed July 17, 2023, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

207 Tobias Gehrke and Julian Ringhof, "The Power of Control: How the EU Can Shape the New Era of Strategic Export Restrictions," European Council on Foreign Relations, May 17, 2023, https://ecfr.eu/publication/the-power-of-control-how-the-eu-can-shape-the-new-era-of-strategic-export-restrictions/#option-c-augment-the-current-framework

208 "Draft Report: Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Software," European Parliament, August 11, 2022, https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf

209 Paul Scharre, "Decoupling Wastes U.S. Leverage on China," Foreign Policy, January 13, 2023, https://foreignpolicy.com/2023/01/13/china-decoupling-chips-america/

210 Emily Weinstein, "Challenges from Chinese Policy in 2022: Zero-COVID, Ukraine, and Pacific Democracy," Testimony before the US-China Economic and Security Review Commission, August 3, 2022, https://cset.georgetown.edu/publication/emily-weinsteins-testimony-before-the-u-s-china-economic-and-security-review-commission-2/

Center for European Policy Analysis
1275 Pennsylvania Ave NW, Suite 400
Washington, DC 20004
info@cepa.org | www.cepa.org