3.

TECH DIPLOMACY AND TECH GOVERNANCE

— CATHRYN CLÜVER ASHBROOK

With technology becoming the frontline of geopolitical competition and control, this chapter explores the emerging discussion on the shape of technological governance in the context of an accelerating rivalry between democracies and autocracies. With restrictions on access to technology rising and regulations implemented that reflect starkly different appreciations of technology's use in society and a "renationalization" occurring in the West and in China, where even open-source code is actively being replaced by national solutions in a desire for sovereignty, the "Balkanization" of digital ecosystems is occurring. The Western response has been at once to increase bilateral and minilateral cooperation, which might lead to the creation of a "democracy-led" digital tech and regulatory space, providing existing barriers are addressed.

This chapter briefly surveys the existing landscape and examines the possibility and pitfalls of creating a wider, democracy-led T-12/T-14 alliance structure as a coordination and governance model of the near-term future in technology policy terms. It concludes that instead of a linear march toward a wider governance structure, a patchwork of deepening and coordinating nodes on tech governance by and for democracies is more likely in the short-term, to facilitate practical alignment. Key hurdles include the very definition and constitution of a democracy (barriers to entry and conditionality of exit); legal and regulatory differences; differences in domestic technological capabilities and attitudes toward corporate innovation, regulatory and financial provisions as well as strategic evaluation of technology and variations on strategic interests. It recommends that policy-makers in the West become increasingly aware of their own contributions to a global Splinternet, and instead continue a dual approach, whereby they address the tech-trade issues in one set of organizational arrangements, but pursue areas of interoperability in areas in which technological solutions will be vital to addressing questions of the global commons—climate, pandemic prevention, poverty reduction—with a continued, globalist attitude.

THE BATTLEGROUND OF TECHNOLOGY

Technology has is now the pre-eminent battleground of economic leadership—and attendant to that political leadership—in an era of exacerbated great power competition. The conflict over Ukraine's sovereignty has placed a prism on the division between democratic and autocratic stewardship of the technology that will determine economic, political and human thriving over the coming decades, as the globe undergoes accelerated, sweeping transformations. In short: The IT stack is splitting along geopolitical fault lines. The nation—or nations—which best steer supply chains, acquire, adopt and mainstream emerging technologies such as AI, super- and quantum computing, 5G/6G and IoT based on digital networks, run over undersea cables or through independent cloud infrastructure, stabilized by satellite infrastructure while setting norms, rules and standards

for technology to preserve privacy, security and system integrity from outside interference will create edge and hedging power for decades, where power overall has become diffuse.

How will governments negotiate or share power in geopolitical terms with their tech companies? Who assumes responsibility and political liability when things go wrong? Traditional instruments of market access limitations and regulation will prove too blunt a tool. To ensure a successful continuation of liberal democratic nations, countries who aspire to its values will have to cooperate in new ways, anchored in greater openness across sectors, to ensure that technological advantages are shaped toward democratic ends. More importantly, countries working together in this way, sharing sensitive knowledge and policy practice will need to be able to better assess and mitigate risk—both in traditional capital and investment terms—but also in terms of the very nature and definition of what constitutes and stabilizes democracies. In addition, democracies accelerating their collaboration must be aware of the dangers of "bloc building" themselves. Where technological innovation will be critical in addressing issues of the global commons—climate change, energy transformation, pandemic prevention, poverty alleviation—in the medium-term, democracies must be mindful of creating competitive systems that can create global norms and capacities.

This chapter will briefly retrace the development of the technological rivalry between Western countries and China, to examine the realities of early governance attempts across the continuous and rapidly evolving fields of technology, surveying efforts for their structural merits and evaluating them on their functional capacities and shortcomings. Gradual trust-building in regional and allied cooperation and the demands of urgency in competition with a burgeoning community of autocracies will likely create a web of minilaterals with a weighted node structure, rather than the formation of a more static or fully-fledged institutional design of inter-democratic technological stewardship—at least for now. These minilaterals—as illustrated in the chapter by Tyson Barker using the EU-U.S. TTC frame in this volume—will have to overcome a series of significant hurdles both in their substantive breadth, issue-bound overlap, internal power imbalances and in-group/out-group dynamics. Nonetheless, democratic partners should not lose sight of the possibility of building a group of vanguard tech democracies—a T-12 or T-14 structure—to work toward deepening advances on democratic principles in the protection and consolidation of telecommunications hardware, the protection of satellite, cloud and cable-based connectivity, and the interoperability of advanced software systems—all while signaling a desire to achieve "global commons" capacities in addressing threats with global consequences, where technology offers solutions.

THE WEST AND THE REST

The West's reaction to the "China challenge" has been two-fold—strategic outpacing and attempted hermetic closure—decoupling, friendshoring, or attempts at expediting "sovereignty"-fundamentally anathematic to the way in which corporate tech innovation has mapped its own global trajectory.

Democracies and autocracies are in a moment of active competition for members of emerging technological coalitions on either side of a splintering internet and exacerbating competition over control of tech inputs, next generation networks and their stability, hardware sovereignty and software spread.

This race to the bottom has taken its toll: overall internet freedom is in decline for the 12th consecutive year.[1]

Despite deep-seated systemic differences—and their articulation in norms, standards, technological products and usage—both democracies and autocracies will also need to find accommodation in areas of technological development between them for the feeder technologies that would have detrimental effects on human thriving—not unlike the development of nuclear technology and deployment. The possibility of weaponizing dependencies

across the technological stack continues to have dangerous side-effects, particularly for those countries entirely tethered to third-country technology provision. Who—which institutions (following adaptation) and countries—will negotiate the "technological arms' deals of the future"?

The latter part of the chapter will thus examine possible trends in technology diplomacy around access and control as democratic governments expand their capacity to negotiate with one another on digital issues, interface with their own companies on the stewardship of fundamental technologies vital to public interest and national security and build multi-stakeholder arrangements nationally and internationally.

OPEN OR CLOSED?: TECHNOLOGICAL LEADERSHIP IN A WORLD OF DIFFUSING POWER

The promises of neoliberal globalization, which thrived based on cheap capital, cheap and quickly available energy, and outsourced—cheap—labor can no longer be fulfilled given the fundamental shifts in geopolitical relations between the two driving powers, China and the United States. Geoeconomic realities that have accompanied changing power relations alongside the realities of transnational challenges have introduced new break points on the structure of the global economy. These include shifting energy resources, changing mobility of goods and people (quickly evidenced for all to see during the pandemic), and the overarching need to accommodate the challenges of climate change. Taken together, they are posing urgent questions for the future of international order and the institutions that will mitigate, adjudicate, securitize and ultimately stabilize nation-state interactions in the future.

For decades, conventional wisdom dictated that open systems would win this century's innovation game: Open societies attracted the talent and economic inputs, marshalled and negotiated (in democratic processes) the government resources to produce advanced research and development and spurred the competitive environment and risk capital that brought innovative products to market: free markets, free speech, democracy—that combination would allow cross-sectoral advancement across a society in service of economic prosperity. Until the last decade, this recipe made the United States and its Western allies technological vanguards: The digital and communications revolution—as detailed by Jeremy Cliffe in this volume—swept the globe, with unbridled optimism—cementing American superiority.

The data revolution—with its emerging negative ramifications experienced first across the world through the capacities of US-built platform technology, quickly merging into the wider capacities of unregulated algorithms, created a disintegration of the concept of privacy and ever-expanding capacities of AI and revealed "new tech's" darker side. "Big Tech's" current $1 trillion valuation crisis seems a consequence of its overly optimistic global appetite—raising questions about technology as the savior of global growth.[2]

Most democracies have now fully awakened to the dangers that aspects of technology can pose to their values, norms and systems, even in their own hands—with democratic integrity and functionality challenged by outright cyberattacks on democratic infrastructure alongside the spread disinformation and its real-world consequences on democratic integrity across the globe.

In a world in which information traveled at lightning speed, no nation-state—no matter how closed—would be able to retain an absolute monopoly on violence, security, information and financial flows. Western-built technology did not imply that its usage would be imbued with "western" values.

Systems designed to steer, decelerate, broaden and democratize decision-making—in short: democracy's bureaucracies—were simply overtaken by the speed of technological capacity and corporate greed to open and access markets, often with deep political and diplomatic implications: Where in 2009 a State Department could still ask that corporate leaders of Twitter delay system-wide updates to allow Iranians to keep communicating with the world, by 2017 there was no more such government gatekeeping. Facebook's own market-opening efforts around "Free Basics" became a tool for genocide against the Rohingya in Myanmar. Parent company Meta is now subject to a $150 billion lawsuit for providing a "defective product" and acting with "negligence"—negligence that might be linked to 7,000 deaths.[3]

And where formerly owned government telecommunications providers couldn't keep up with sourcing the component infrastructure to build advanced networks, to power transformative 5G/6G technology at the speed of change, formerly-state owned operators now sought and signed—as Telekom/T-Mobile did in 2019—near-ironclad contracts to continue purchasing Chinese-made hardware, against a shifting tide of geopolitical or national security concerns (and de facto now undercutting the current government's coalition agreement promises of "clean networks"), creating industrial dependencies not easily turned back.[4,5]

CHINA'S INTERNATIONAL TECH FOOTPRINT EXPANDS

The last decade also proved a major fallacy in the assumption that openness, innovation and democracy lie at the heart of this recent technological revolution. China crafted its rival status in direct opposition to the Western model: by controlling its markets—inflow and outflow and its particularly-tiered corporate structure and by increasingly centralizing its authoritarian policies, developing strategies to expand its influence (from the BRI onward) and increasingly tightening restrictions on free speech. Despite recent economic shocks and slowing growth projections, China could still edge out the U.S. in achieving its 2025 AI and deep tech ambitions.[6]

Under the cover of its "Great Firewall" China retained the kind of global connections in R&D that would feed its circular economy and steered a progressive and sequenced acquisition of intellectual property and sufficient stake in Western (sub-)technology providers, component parts and machine-building capacities to control market inputs, develop rival technologies at scale to crowd out the few Western providers in the Chinese market over time and experiment with massive investments in risky technological innovation, including dual-use technology and quantum.[7] It has been nurturing its semi-conductor industry pro-actively, not least through its National Integrated Circuit Industry Investment Fund.[8] It accomplished all of this through central stewardship, while expanding the authoritarian control of its own population through mass surveillance technology (626 million facial recognition cameras covered the country by 2020), and while making the latter an export technology for its international footprint through the Digital Silk Road.[9]

"Open to the world but closed at home"—it effectively siphoned data from (BRI) client cities and countries across South America and Africa to build ever more sophisticated AI systems in line with its 2025 strategic ambitions,[10] while allowing leaders in the global South (and in Iran, Russia and parts of Europe) to actively suppress human rights, freedom of expression and democratic values, using tools "made in China." Today, the West's teenagers are addicted to China's TikTok,

while their data (likely) moves seamlessly Eastward feeding closed AI development to improve surveillance[11], as well as the Chinese government's behavioral and political forecasting tools in full violation of data privacy policies painstakingly agreed by lawmakers. Only nine out of 27 European countries can boast "clean networks," marking continuous dependency, while the U.S. FCC has banned Chinese-origin electronics on national security grounds—but local telecom networks in the U.S. still aren't fully free of China-made components. An entirely uneven picture of stewardship, regulatory reach and international practice emerges.

The war in Ukraine has brought all these streams into direct confrontation: There, techno-democracies and their companies who—who have reframed corporate interests as their contribution to national, democratic interest—are actively engaged in the war effort. Much of Ukraine's resilience in the face of wiper, ransomware and DDoS attacks on the country's critical infrastructure, its networks, energy grids and hospitals, as well as the continued operations of its dispersed digital army and constant repairs to its Govtech apparatus, can be directly linked to contributions from Microsoft, Palantir and Starlink.

The message?
Democracy does not win
without technology.

Squeezed by sanctions, abandoned by its IT elite and dependent on China for semi-conductors, military technology, and satellite back-up, Russia has actively embraced the deepening of a splinternet, which it began to pursue in active partnership with China in 2013 when the two countries signed news and information exchange agreement. The following years, leading up to February 7, 2022 "friendship agreement" between the Russian and the Chinese leaders served as a phase to consolidate their joint views of cyber "sovereignty" and attempt to push their vision of suppression of speech through technology (Putin signed on to a number of China's tech-driven playbooks for authoritarian rule), by advancing their unified vision of new global cyber order on the basis of Huawei IP protocol at the heart of the International Telecomms Union (ITU) and multilateral arenas from New York to Geneva.

Now, we see a hastening of the development of a sovereign yet joint Russo-Chinese internet model (part of China's "Great Rejuvenation"), supported by a wider Eurasian sphere including Iran, which has increased its purchase of Chinese surveillance technology to suppress current revolutionary energies.[12] The Sino-Russian information war has had measurable impact on the global interpretation of Russia's actions against its sovereign neighbor. And beyond the overheating semi-conductor race over the shortage of raw materials, Russia's war motivations are at least partially stoked by the $12.5 trillion valuated rare earth minerals deeply buried across embattled terrain in Eastern Ukraine.[13] Even to the future of the tech race, geopolitical and territorial control matters. The message? Autocracy does not win without technology.

RECONCILING MODELS OF TECH GOVERNANCE: STILL FIT FOR PURPOSE?

These developments foreshadow what might still be to come. Over the past decade, Western governments have attempted to fortify their own systems along the entire tech stack, depending on their strategic needs, interests and capacities—from shifting hardware and industrial policies (clean networks), to curtailing the export of sensitive and dual-use technology, to stepping up oversight and regulation. While the struggle for democratic norms and standards has played out across multilateral fora—i.e. the UN Open-Ended Working Group on responsible behavior in cyberspace (OEWG) and in telecom standard-setting bodies, such as the ITU, which have seen direct face-offs between authoritarian and democratic leadership,[14] democratic countries have also been mapping out areas of collaboration and competition. With structural limitations in its competition with U.S. technology, the EU has developed a regulatory framework and led the U.S. in resolving critical and divisive issues on data privacy and storage. Between the development of the GDPR, the Digital Services Act (DSA) and the Digital Markets Act (DMA) designed to both widen and level the playing field for more competition to U.S. tech corporations, and a risk-first, human-centric approach to AI development and attempts to match the US in support for its semi-conductor industry and R&D environment to accomplish critical transitions ahead (green, energy, tech), the EU has discovered its added-value and institutional strength in democratic tech governance.

Europe's examples have led to a push to strengthen U.S. domestic institutions—the Federal Trade Commission, the Securities and Exchange Commission and the Committee on Foreign Investment—to eye stronger mandates—and despite a patchwork of privacy regulations across the U.S., an administration wanting to advance toward more comprehensive rules that would bring "the West" into greater alignment. The Biden administration has considerably deepened its political leadership on cyber, industrial tech competition and AI, in part through the creation of a "mission agency" in the National Security Commission on AI (NSCAI), discussed in greater detail below. India, too, now a pivotal tech actor, has pushed for internet governance rules and technical standards with international reach—by banning Chinese software and hardware and creating data localization laws. Further, Narendra Modi's government has created a New, Emerging and Strategic Technologies (NEST) division in its foreign affairs ministry, in part to oversee and coordinate their joint AI initiative (USIAI), their joint Science and Technology Forum (IUSSTF) and to feed joint conclusions stewarded through NEST into the Global Partnership on AI.

In addition to this unilateral deepening, an expanding number of bilateral formats—particularly around dual-use technology and defense issues—have proliferated between democracies, including in the U.S.-India Strategic Partnership (2+2 format), and more recently through ad hoc coordination on semi-conductor development between the U.S., Japan and the Netherlands. The development of a patchwork of cross-regional alliances—from the U.S.-EU Tech and Trade Council to the EU-India TTC, to Quad structures to a deepening of existing, specialized multilateral cooperation within NATO and among intelligence services.

Minilaterals—i.e. regionally focused, formalized multilateral constructs—have served the purpose of building trust over time, reducing heightened protectionist impulses, building confidence and "muscle memory" across disciplines and bureaucracies, in some cases laying the groundwork for sequenced and expanded agendas over time that may take minilaterals from coordinated industrial policy stewardship toward something more akin to strategic tech governance. But as Tyson Barker points out in his chapter on the EU-U.S. TTC in this volume, barriers of technological competition, issue-overload and issue-mixing continue to complicate negotiations.

But can an emergent patchwork of democratic alliances—even ones that could incubate and expanding agenda, like the EU-U.S. TTC as a weighted "node" around strategic technology collaboration be sufficiently quick and coordinated to compete with what closed systems (a Chinese-Russian-Iranian-Eurasian union) might be able to achieve and the deliberate and strategic way they might force others, dependent on their technology (not least its surveillance capacities), to embrace technology designed to curtail individual freedom and abrogate the principles of democracy that underpin international law?

FROM MINILATERALS TO A TECH-14? SCOPING THE BREADTH OF DEMOCRATIC INTEGRATION ON STRATEGIC TECH COOPERATION

Enter a broader thought: In 2008, U.S. policy planners in the Obama administration first floated the idea of creating greater strategic collaboration between the U.S and other leading countries committed to democratic values, leading to a series of cumulative Washington think tank initiatives. The Atlantic Council first pursued the collaboration of policy planners from 2014 onward—the year of Russia's illegal annexation of Crimea—now labeled as the D-10: Australia, Canada, France, Germany, Italy, Japan, South Korea, the United Kingdom, and the United States, plus the European Union charged with rethinking means to maintain democratic-led values-based international order—without tech as the center piece. Already, in-group/out-group dynamics proved complex, with India, Indonesia, Poland, and Spain participating as observers. Six years later the idea became central to the UK G7 Presidency with membership constituting the core members plus Australia, India and South Korea.[15] Later that year, it was coopted by U.S. President Trump as the primary venue to advocate for his "clean network" policy, to eliminate Chinese built 5G hardware from networks of associated democracies. As limited as this approach was in scope, it prompted a flurry of activity among UK and U.S. think tanks[16] and among advisors to the Biden campaign jockeying for position as he narrowed his international messaging around the threat of authoritarian countries to the international rule of law.

A "Tech-10" (or later -12) could be the integrated yet flexible collaborative frame for democracies to counter the spread of 'authoritarian' hardware, disinformation, AI and leading-edge advances and the expansion of the tech race into space and back under water—satellites, cables and fundamental connectivity.

Whether or not China and Russia can form an expansive tech alliance on the back of the a Western sanctions regime forcing them together anew depends on a series of factors including

a) the degree to which Chinese (and other) ICT companies and hardware providers expand into the vacuum left across the Russian tech market (from of Western technology companies,
b) the ability of these other providers to skirt and the 'techno-democratic' global community's ability to set and enforce an increasingly narrow tech-specific sanctions corset (from the Foreign Direct Product Rule (FDPR) and beyond),
c) the capacity of Western governments and their technology corporations to link their affirmative tech hardware, infrastructure and connectivity plans meaningfully, particularly in Eastern Europe and key areas of the Global South—at speed—(B3W and Global Gateway) and implement these to push back against expansive efforts by Russo-Chinese collaboration and
d) the ability of 'techno-democracies'—including the G7 states, Asian/Quad and South American partners—to mitigate unintended consequences of sanctions on digital connectivity in and to non-permissive environments, so that there is no unintentional acceleration or catalyzation of authoritarian consolidation of a sovereign internet. Speed is of the essence. There are sufficient "wedge" areas in which smartly aligned democracies could put a brake on a deepening authoritarian tech-empowered web.

These four points alone (and there are others) speak to a great—an urgent—need for "techno democracies," to seek closer possibly even institutional coordination, knitting together the currently existent and partially overlapping approaches in existing, purpose-driven alliances (i.e. NATO; Five Eyes) and by deepening strategic cooperation in technology through bilateral, minilateral (i.e in multiple, sometimes coordinated, progressively deepening formats with various partners), full multilateral subject-based arrangements (OECD; OEWG/UN; ITU/UN)—or as suggested by some, through the creation of a separate alliance of technology-vested global democracies in a T-12.

A DEMOCRATIC TECH ALLIANCE: T-12? MINILATERAL? PLURILATERAL? MULTILATERAL?

Technologically advanced democracies are those with "skin in the game": Democracies whose corporations, research institutions and private and government-funded innovation sectors produce key elements of today's digital and tech infrastructure, and whose economic competitiveness increasingly relies on the flexible advancement of technology. These democracies are united in their commitment to rights-based, ethical deployment of technology, and regulation of technological assets withing a legal system capable of offering useful, clarifying legislation. The late April 2022 declaration on the "Future of the Internet" and its 60 signatories underscored how basic democratic premises might resonate with universal human rights: rooted in dignity, pluralism, open access, and economic empowerment for all people. But members of a Tech 10 or -12 would need to be able to go beyond declarations of intent and move—quickly—into action.

DEMOCRATIC STEWARDSHIP OF TECHNOLOGY: THE DIFFICULTY OF DEFINITIONS

Defining the parameters and depth of (liberal, participatory, expanding) "democracy" in the 'techno-democracy' concept and the threshold for membership in an overarching, institutional arrangement has been—as of yet—the major stumbling block for widening of technological stewardship at scale. Digital governance practices in India, South Africa, and most recently Israel—possible qualifying members of a T-10/T12 coalition, can only be described as tending toward the illiberal. Within the EU, who would join member state governments (France, Germany, the Netherlands, etc.) in a possible alliance framework, leading member state politicians are actively courting Chinese surveillance and repression technology. Israel, with its undeniable technological advantages in intelligence gathering, dual-use development and start-up capacities did develop a new investment screening committee in 2020, but exempted investments in the tech sector from these evaluations, spurring the expansion of companies like Pegasus, which is hardly grounded in democratic principles. With the election of the most far-right government in the country's history and its most recent attempt to weaken the country's independent judiciary, its democratic "credentials" are waning.

To be a part of a T-12 alliance many leading tech democracies would need to work at home: Israel, Brazil, India and EU member states would have to negotiate their own relationships and dependencies on the Chinese market, sequencing and spacing decoupling efforts or seeking other means to keep sensitive data, intellectual property and tech manufacturing capacity out of China's hands. The PHALCON and HARPY incidents around Israeli tech sales to China and its impact on Israeli-US relations read as a warning tale of just how difficult co-existence between tech superpowers can be, if capacity to agenda-set is limited.

Each of the possible "member" countries in such an alliance faces the challenges of vertical negotiations—leading tech countries, i.e. the US, UK, France, Israel and increasingly India—with their own corporations, whose power out of the hands of government control

and supervision is having an impact on geopolitics. Further, it is entirely unclear which metrics would be used to evaluate the sustainability or "level" of democracy among possible member countries—though these metrics could be addressed. Finally, if trust-building and information sharing has been challenging in a minilateral setting, an expansion to a larger but flexible format could thwart instead of accelerate progress toward the joint goal of policy alignment.

FROM T-12 AMBITIONS TO MINILATERAL REALITIES: CREATING INTER-OPERABLE TECH GOVERNANCE

If a T-10/12/x were to emerge as a global ambition, it would need to serve first as a clearing house for existing and developing initiatives across the G7/NATO/OECD/World Bank/UN, minilateral frameworks (all existing EU-US-India TTCs, QUAD and regional arrangements in Southeast Asia) and bilateral frameworks (U.S.-Japan, U.S.-India) and usefully clarify in-group/out-group dynamics in its relations with non-democratic tech leaders, including Singapore and Indonesia.

A multilateral clearing-house structure of this nature would need to be capable both of scaling majoritarian initiatives (potentially emerging from minilaterals), while avoiding duplication, increasing functional interventions (against disinformation; supporting democracy protection) and create a series of negotiation and exchange platforms on data protection, privacy and privacy-enhancing technology and risk capital securitization to

- create deeper technological convergence (R&D sharing; semiconductor design, etc.) considering tech advances in authoritarian systems
- establish functional risk mapping and early warning systems to protect vital joint interests (hardware systems and international critical digital infrastructure, including undersea cables); securing 5G and 6G tech can be sourced from democratic countries, at scale and at competitive price points
- develop and promulgate international norms and standards on ICT hardware, software and AI under democratic guidelines to be applied through existing bodies
- map supply chain vulnerabilities and shortfalls in critical inputs (including for lithium, nickel and rare earth minerals); create a democratically monitored reserve structure
- develop a certification program for high-quality infrastructure and tech projects [as part of global development agenda]
- coordinate mechanisms for dual-use export control and verification of tech imports (particularly in the burgeoning smart cities and surveillance tech market)
- provide sanctions guidelines for T-12 corporations mitigate unintended consequences that could hasten authoritarian consolidation of a sovereign (Sino-Russian) internet
- exchange intelligence on scaled disinformation and disruption of major data flows i) expand the existing "grand challenges" projects on 'democracy affirming tech' to a global scale.

Secondary ambitions might include the protection of T-12 cities from the overreach of authoritarian/surveillance technology providers into the Smart City space (a market now valued at over $800 billion annually), which could be 'backdoors' to creating significant damage in democracies, both in critical infrastructure and democratic discourse. The coordination of global funding resources could be a further secondary ambition: The 2018 MOU between Australia, Japan and the US to collectively source private capital to fund major regional infrastructure projects (effectively a precursor to the B3W plans of the Biden administration), including the 2020 internet cable to Palau is a model of potential projects to emerge from closer coordination between democratic countries on structural network provision—beyond minilateral structures. In Cape Verde, where cables from North America meet European and African cables, the race for control is clearly on.

For all of the need, the hurdles are similarly real: Divergent threat perception and market dependencies have led to a preference for bilateral or minilateral cooperation around a circumscribed set of priorities that also level playing field of leadership toward greater parity and functional, practical exchange. Legal

precedence, questions around leadership structure, fear of duplication, existing trade agreements with in-built market protections, intelligence and political statutes and structures, and stark differences in technology culture and degree of technological capacity, and competitor status among possible T-12 "members" alongside fears of "further antagonizing China," are some of the main reasons political dynamism has not aggregated around elevating nascent collaboration on a wide spectrum of technology issues to this level. Failure of the idea to pick up momentum speaks not solely to the breadth and depth of barriers, but rather to the fact that trust-based organization forms must both be scoped correctly and have a measurable function to create social and organizational capital over time. For example, a potential T-12 precedent, the D5—UK, S. Korea, Israel and New Zealand—focused on GovTech, CiviTech and OpenTech best practice exchange, has taken six years to develop into D9, building on common values, pooled knowledge and gradual trust building.

As useful as it is to chart the possibilities of a structured T-10/12, "weighted nodes" of collaboration in minilaterals, where members which overlap must take care to avoid policy duplication and alignment is likely "as good as it gets" for the medium term. As Tyson Barker describes in this volume, the EU-U.S. Tech and Trade Council could be such a node.

It has quickly redeemed itself to become a multi-agency, multi-sectoral negotiation framework and clearing house, focused on mapping, regulatory impact management, resource pooling, information sharing and the often-delicate negotiation of subsidies and (tech)-expansionary use of trade tools for common objectives. Within a year of its existence, it had additionally become a forum for multi-stakeholder negotiations of tech-adjacent policies with ramifications for international competitiveness, adding formats to address issues of mutual agreement and contention, such as the impact of the US CHIPS Act and the US Inflation Reduction Act on the freedom of operation for European companies, pointing to the fact that it could also be seeding the bases of a new transatlantic trade pact.

Its capacity to act as a trust-building venue after the erosion of transatlantic collaboration in the Trump era made it exemplar in its design: The EU-India TTC will not only follow similar structural make-up but be sequenced to interact with the EU-U.S. TTC, to avoid duplication of efforts and a stripping of resources. Similarly, there are early indications that the Indian 2+2 format with the United States, encompassing foreign, intelligence, military and science collaboration in a bilateral format, will be framed to connect more seamlessly to EU-U.S. and EU-India TTC provisions. In addition, nothing bars TTC working groups from at least informally exchanging with the two QUAD structures on critical emerging technology and defense technology, and numerous bilateral structures focusing on specific digital policy subsets.

Core elements of the EU-U.S. TTC could similarly serve as a model to expand coordinated tech governance to Latin America and the Caribbean, under European leadership, as Jose Ignacio Torreblanca and Carla Hobbs have argued as a priority under the Spanish Presidency of the EU in 2023.[17] Distilling from the lessons around trust-building, values ascertainment, transferability of regulatory framework tools (particularly around data security and privacy), and practical knowledge-sharing (i.e. rare earth mapping, sustainable mining) from the existing "node" structure in in the EU-U.S. TTC will facilitate the successful establishment and maintenance of this minilateral.

RETHINKING DIPLOMATIC INTELLIGENCE FOR TECHNO-DEMOCRATIC STEWARDSHIP

Gaining and defending ground for techno-democracies, no matter in what forum—closed multilateral, global multilateral, sequenced minilateral—will demand an expansion of diplomatic practice, one that mimics the corporate development cycle for tech applications or products—from mapping and foresight, to risk analysis and gaming, open and closed lab structures (or in the language of diplomacy: functional Track 1.5 and 2 dialogues) with greater tolerance for risk and error, but focused on means to achieve both better technology outcomes from the exercise of diplomacy and to build regulatory capacity from the ground up, to continue to expand the translation of democratic norms and values in legislation across all forms of governance, from nation-state to multilateral fora.

Building diplomatic and regulatory capacity begins with priority setting and executive signaling. The Biden administration telegraphed its seriousness on integrated tech policy across departments by elevating the Office of Science and Technology Policy to cabinet level.

Most recently, Japan, the U.S. and the UK used their individual national security-, defense- and technology/cyber strategies to send a similar signal: Technology—hardware, software, defense and societal applications, digital rights—flow like a plumb line through these documents.

Negotiation tables of the future will have to be structured vastly differently, if the wider intention might be to use "minilateral" formats to advance toward a "T-x structure" of techno-democracies. It will require a cross-systems approach that builds in vertical negotiation with a country's own corporations and their activities abroad.

It will also require figuring out how diplomatic knowledge about all aspects of technological development, usage, dependencies, etc. about the "other" is shared within network. Where China's CICIR can simply and centrally plan, synthesize and analyze multi-sector conversations (even those in a Track 1.5/2 format) for strategic purposes across all domains of data diplomacy—in part using AI for data analytics—in their "sovereign" domain and with partners, techno-democracies will have to lean toward increased openness—and more inclusive formats for their advantage.[18] As Madeline Carr argues "China has a comprehensive insight into all other states that engage with it, whereas we have only our own." China uses over 30 methods, both licit and illicit, and a diverse cadre of actors to gain access to non-native technology.

Devising common regimes that can then allow for regulation that is both sufficiently narrow, as to not impede corporations and the industrial base and achieve long-term national security goals is difficult enough at home, as evidenced by ongoing negotiations around a functional outbound investment screening mechanism for critical technology in the U.S.[19] Elevating these discussions to the multi-lateral level with the EU or Japan (or the EU with India) seems near impossible if earliest stages—including the diplomatic assembly of working groups—are not conceptualized in an interagency format, with outside expertise and constant corporate cooperation. The Quad Cybersecurity Joint Principles and the working group structures of the EU-U.S. TTC establish norms of this structured cooperation and are examples in this regard.[20]

The greatest value of the minilateral structure moving toward weighted notes of a T-x collaboration, as discussed above, could well be in achieving a more complete picture of the array of challenges, vulnerabilities and possibilities facing techno-democracies. This has already begun as part of the EU-U.S. TTC framework and through domestic R&D investments of a different sort, with a mapping of rare earth materials as agreed as the May 2022 Saclay meeting, with a decision on strategic overland and subsea cable connections (beyond potentially Cape Verde) as confirmed in December 2022 and in the diagnostic work for the alignment and resiliency of Global Gateway and B3W projects. Individual partners have already developed scalable diagnostic structures, including the EU's 5G Toolbox and the U.S National Network for Critical Technology Assessment or the new Directorate for Technology, Innovation and Partnerships at the country's National Science Foundation conceptualized particularly to probe for weaknesses in the country's supply chains and delineating emerging challenges to be solved by the better application of edge technologies.

RECOMMENDATIONS FOR THE NEAR-TERM FUTURE

If leading techno democracies pursue an ideologically-centered governance architecture, they must realize such an initiative could similarly signal authoritarian governments to accelerate their own splintering efforts, when challenges of the global commons—climate change, pandemic prevention, supply-chain integrity—will demand interoperable technological solutions for global progress.

In fact, on certain issues—both domestically and internationally—democratic governments should be embracing radical openness, instead of closure, to advance.

Forming "mission agencies" at home, like the multi-sector National Commission on AI (NSCAI), imbued with the authority of the Executive, but with a multi-stakeholder approach and a singular objective, organizations like this can catalyze policy implementation, including passing legislation and creating structures to catapult U.S. AI capacities into the future. The NSCAI and the concept of mission agencies in general should serve as the blueprint for Germany's "Alliance for Transformation," and other such consortia emerging across the European Union, for example, dedicated to thinking technological challenges down to the core, including to changes in the education systems across democracies.[21]

Secondly, techno-democracies should—in part because the challenges are so rife and arriving at such speed—should avoid creating duplicative structures at all costs. Instead, particularly when it comes to the urgent need to reform national foreign policy and intelligence structures as outlined above, they should be comparing notes. Australian National University's Tech Policy Design Center and its database of tech policies from 40 countries can help other democracies looking to make efficient policy-design choices that can support both the deepening of minilateral structures and can support the creation of a "floor" toward the construction of a wide tech governance structure.

Finally, the strength of global democracies—regardless of the stage of their democratic development—lies in their openness, and ability to establish values and norms even in working consortia such as these nascent tech governance structures. The ability to use collaborative formats to build "in network" stickiness, delivering 'proof of concept' to restore a modern version of the liberal democratic promise to guarantee physical and economic security alongside expanded democratic rights of free expression and participation in the digital sphere will create its own power. To use that power systematically (against the threats wielded by autocracies against these principles with the tools of the digital age), democracies will need to adapt and redefine their notions of collective governance and control.

These are massive changes in bureaucratic and political practice, particularly in a world in which democratic openness has spurred overheating capitalist gains from technological advancement. Quickly, democracies will have to learn how to negotiate power with their own corporations, or risk mimicking regulatory approaches that force companies into line (the Chinese way) but reduce the innovative capacities that define democracies. The choices are as real as they are stark—and above all, urgent.

ENDNOTES

1 Freedom House. (2022). Freedom on the Net: Countering an Authoritarian Overhaul of the Internet. December 2022.

2 Mickle, T., Weise, K., & Grant, N. (2023). Tech's biggest companies discover austerity, to the relief of investors. New York Times. February 2, 2023.

3 Culliford, E. (2021). Rohingya refugees sue Facebook for $150 over Myanmar violence. REUTERS. December 8, 2021.

4 Pleming, S. (2009). U.S. State Department speaks to Twitter over Iran. REUTERS. June 16, 2009.

5 Cerulus, L. (2022). Germany is (still) a Huawei hotspot in Europe. POLITICO. December 14, 2022.

6 Dawson, J., & Wheeler, T. (2022). How to tackle the data collection behind China's AI ambitions. Brookings Institution. April 29, 2022.

7 Sheehan, M. (2023). How China became an Innovation Powerhouse. Carnegie Endowment. January 10, 2023.

8 Larsen, B. C. (2022). The Geopolitics of AI and the rise of digital sovereignty. Brookings Institution. December 8, 2022.

9 Keegan, M. (2019). Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled. The Guardian. December 2, 2019.

10 MERICS. (2016). Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. December 2016.

11 Chee, F. Y. (2023). TikTok CEO seeks to reassure EU on privacy, child safety. January 10, 2023.

12 Khorrami, N. (2022). How China boosts Iran's Digital Crackdown. The Diplomat. October 27, 2022.

13 Faiola, A., & Bennett, D. (2022). In the Ukraine war, a battle for the nation's mineral and energy wealth. Washington Post. August 10, 2022.

14 Wheeler, T. (2022). The most important election you've never heard of. Brookings Institution. August 12, 2022.

15 Ichihara, M., & Brattberg, E., & Judah, B. (2020). The D10 Initiative and Japan: Options for Expanding the Coalition of Democracies. Nippon.com. August 16, 2021.

16 Manuel, A. (2020). The Tech Ten: A flexible approach to international tech governance. Blogpost.

17 Hobbs, C., & Torreblanca. (2022). Byting Back: The EU's digital alliance with Latin America and the Caribbean. ECFR Policy Brief. October 24, 2022.

18 Carr, M. (2022). Tech Policy Dialogue in Times of Geopolitical Tension. Unpublished conference paper (delivered at the CNAS T-12 Track II convening in Paris, France). May 2022.

19 Benson, E., et.al. (2023). Transatlantic Approaches to Outbound Investment Screening. CSIS. January 17, 2023.

20 Ministry of Foreign Affairs, Japan. (2021). Quad Cybersecurity Joint Principles.

21 NSCAI Mission. (2021). On the principle of "Mission Agencies," see Bertelsmann Stiftung. (2023). Deutschland transformieren: Missionsagenturen als innovativer Baustein zur Bewältigung gesellschaftspolitischer Herausforderungen. February 2023.