

KRACH INSTITUTE FOR TECH DIPLOMACY
AT PURDUE

THE GLOBAL TECH SECURITY COMMISSION REPORT

Imperatives and Principles for Accelerating the Innovation and Adoption of Trusted Technology

DECEMBER 2024

GLOBAL TECH SECURITY COMMISSION



"We will win, but for us to safely mine the technology pool created by the great minds of our private sector companies, we have to have standards, agreements. Nobody must be able to blow up what we trust in technology, and for that indeed we need the Global Tech Security Commission."

Kersti Kaljulaid
Co-Chair, Global Tech Security Commission; President of Estonia (2016-2021); President of the Estonian Olympic Committee

TABLE OF CONTENTS

2 **EXECUTIVE SUMMARY**

4 **SECTION 1:** NEW SOLUTIONS FOR NEW CHALLENGES: WHY THE GLOBAL TECH SECURITY COMMISSION IS NEEDED

8 **SECTION 2:** OPERATIONAL KNOW-HOW

12 **SECTION 3:** ANALYSIS ON THE COLLISION BETWEEN EMERGING TECHNOLOGIES AND 21ST CENTURY GEOPOLITICS

20 **SECTION 4:** FINDINGS AND IMPERATIVES

28 **SECTION 5:** PRINCIPLES OF TRUSTED TECH DIPLOMACY

30 **SECTION 6:** CONCLUSION

31 **APPENDIX:** GLOBAL TECH SECURITY COMMISSION

EXECUTIVE SUMMARY

EMERGING TECHNOLOGIES SUCH AS ARTIFICIAL INTELLIGENCE (AI), autonomous systems, 5G and 6G, hypersonics, quantum computing, and many others are having and will continue to have a dramatic effect on the geopolitical landscape. Both authoritarian nations and free societies are pursuing the development of these technologies to gain economic, military, and strategic advantages. Whomever seizes the commanding heights of these technologies will have a greater ability to dictate world events.

In pursuit of the Krach Institute for Tech Diplomacy at Purdue's goal for a world in which technology advances freedom, the Institute's Global Tech Security Commission (GTSC) conducted a comparative analysis between free and authoritarian societies, detailing the strengths, weaknesses, opportunities, and threats that each possesses and presents to the other (see Section 3 of this paper).

Following that analysis, the Commission established five priority domains in which action must be taken quickly to seize the advantage and prevent authoritarian nations, most concerningly China, from obtaining geostrategic leverage through key technologies:

- Leveraging education and R&D to educate all actors in the tech ecosystem
- Shaping international standards to favor trusted technologies
- Securing technological supply chains and infrastructure
- Ensuring capital markets are not sources of funding for the development of untrusted technologies worldwide
- Enlisting private sector boards of directors to mobilize the private sector as a key leader in ensuring that technology advances freedom

The Commission has also articulated the Principles of Trusted Tech Diplomacy, with which the members of the Global Trusted Tech Network—the group of all public and private actors committed to ensuring that technology advances freedom—should align.





PRINCIPLES OF TRUSTED TECH DIPLOMACY

1. **Uphold the Trusted Tech Doctrine:** Members of the Global Trusted Tech Network commit to innovating and implementing technology in ways that advance freedom.

2. **Empower Through Education:** Members of the Global Trusted Tech Network seize opportunities to educate and engage all critical public and private sector actors about emerging technology and its implications for geopolitics.

3. **Lead with the Innovation and Creativity of the Private Sector:** National security is not the responsibility of governments alone. The private sector must also lead.

4. **Rally and Unify Allies as Force Multipliers:** Marshalling the free world's unmatched combined economic and technological power is the key to safeguarding freedom.

5. **Build a Dynamic Network of Networks:** Each "node" in the Global Trusted Tech Network exponentially increases our opportunity for success.

6. **Create a Value Proposition for Partners:** Actively demonstrate and always articulate the benefits of incorporating trusted technologies over untrusted technologies, rather than merely opposing untrusted alternatives.

7. **Play to Win:** Time is short to win the contest of trusted and untrusted technologies. Prioritize acting, operating and executing with confidence and conviction rather than fear of defeat.

SECTION 1

NEW SOLUTIONS FOR NEW CHALLENGES: WHY THE GLOBAL TECH SECURITY COMMISSION IS NEEDED



ONE QUARTER INTO THE 21ST CENTURY, NEXT-GENERATION technologies are reshaping the facets of daily life, business, and geopolitics at an unprecedented pace.

Nvidia is a multi-trillion-dollar company designing the advanced chips driving the global AI revolution. Russia is deploying hypersonic missiles for the first time in its war in Ukraine. Large language models such as ChatGPT 4.0 are obliterating old boundaries in generative AI. SpaceX has used mechanical arms to secure a rocket booster on a launchpad upon its return from space. Iranian-backed Houthi rebels are assaulting ships in the Red Sea using cheap drones. Chinese-owned TikTok will be forced to divest from parent company ByteDance or face a ban in the U.S. due to data privacy and influence operations risks. The European Union continues to increase tariffs on Chinese electric vehicles. Brazil has emerged onto the tech scene with at least 23 "unicorn" startups.[1]

For free societies, the potential for technology to determine global peace, prosperity, and the protection of human dignity is greater than ever. At the same time, authoritarian regimes such as those in China, Russia, Iran, and North Korea also know the power those emerging technologies hold. For them, next-generation technologies present an asymmetric opportunity to bolster surveillance, censorship, coercion, and oppression. They are tools for rolling back the achievements of self-government, freedom, prosperity, and sovereignty that free nations have enjoyed since the end of World War II.

When the technology revolution mixes with the contest between free societies and authoritarian regimes, two competing visions for the future are laid bare: Technology will either advance human freedom or be used by dictators to diminish it.

This choice presents fundamental questions for business leaders, innovators, government officials, students, and all citizens of the free world: What must we do to ensure that technology advances freedom for our generation and the next? And how will we do it?

Engineering answers to those questions was core to the mission of the Krach Institute for Tech Diplomacy at Purdue when it established the Global Tech Security Commission (GTSC). Chartered with bipartisan support from the United States Congress and international allies, the GTSC's mission is to devise a blueprint for how companies, countries, civil society organizations, and individuals must collaborate in new and necessary ways on an imperative with ever-increasing geopolitical significance: advancing freedom through trusted tech.

To meet the scale of this challenge, the Commission draws on expertise as wide as it is deep. It is co-chaired by Keith Krach, former U.S. Under Secretary of State for Economic Growth, Energy and the Environment, and former Chairman and CEO of DocuSign and Ariba; and Kersti Kaljulaid, former President of Estonia, a nation known worldwide as a trailblazer in creating a trusted digital society. Kaljulaid also led the Three Seas Initiative, an effort between thirteen European countries designed in part to promote trusted infrastructure, including digital infrastructure.

Unique in both its scale and caliber, the Commission comprises a global network of more than 200 public and private sector experts, featuring 38 Commissioners and their respective Advisory Councils. Every individual associated with the Commission boasts expertise across at least one of three essential and intersecting dimensions: critical technologies, business and national security strategy, and international perspectives from the world's leading techno-democracies.

From 2022 to 2024, the Commission's members examined the emerging technological and geopolitical landscape, performed an analysis of the most sensitive tech sectors, and synchronized common themes and overarching priorities. Based on this work, they identified five high-leverage, actionable areas that—if addressed with urgency and effectiveness within the next one to five years—can dramatically advance freedom and mitigate techno-authoritarian threats.

Finally, the Commission conceived of and articulated the values of the Trusted Tech Doctrine and the Principles of Trusted Tech Diplomacy. These guiding mantras are intended to codify the fundamental and unifying ideas that leaders of free societies worldwide can use to devise offensive, defensive, and force multiplier strategies that ensure technology advances freedom for this generation and those to come. Our highest aspiration is for the imperatives, the Trusted Tech Doctrine, and the Principles of Trusted Tech Diplomacy to guide business, government, tech, and civil society leaders as they work to ensure that technology advances freedom. The Krach Institute for Tech Diplomacy at Purdue invites all who are committed to that vision to join us in this work as vital members of the Global Trusted Tech Network.





THE TRUSTED TECHNOLOGY DOCTRINE

In 2024, members of the Global Tech Security Commission outlined The Trusted Technology Doctrine. Drawing on collective wisdom earned from many decades of real-world experience, bipartisan lawmakers, former cabinet officials, Silicon Valley innovators and entrepreneurs, diplomats, academics, and civil society leaders enshrined the principle of trust as the foundation of all tech diplomacy, and urged citizens around the world to adopt the following declaration:

The Trust Doctrine embodies the belief in the primacy of trust as the foundation of peaceful relationships. Trust is firmly grounded in integrity, accountability, transparency, reciprocity and a profound respect for the fundamental pillars of free societies, such as the rule of law, human rights, property rights, fair labor practices, responsible environmental stewardship, freedom of expression, and national sovereignty.

Amid the wave of historic technological change shaping the trajectory of humanity in the 21st century, an underlying aspect of human relationships remains: People do business with people they trust. They partner with people they trust. They buy from people they trust. They help people they trust. Trust is how deals are made, friendships are forged, alliances are founded, and peace is preserved.

Technology's central role in modern relationships necessitates its trustworthiness. Therefore, leaders from government, technology, business, academia and civil society commit to, and encourage our fellow citizens to embrace, the following values of the Trusted Technology Doctrine as the basis for the innovation, deployment, and adoption of critical and emerging technologies, so they may serve their ultimate and highest purpose: the advancement of human freedom.



Technology must advance freedom to be trusted.

The primary use of technology must be the advancement of human freedom. It must be developed in the service of the common good with low expectation of harm.

Technology must protect human rights to be trusted.

The development and use of technology must be respectful of the inherent dignity and equality of all individuals and ensure non-discrimination, fair labor practices and freedom of expression and religion.

Technology must respect privacy to be trusted.

Robust measures must be in place to safeguard personal, corporate and government data and national security, providing timely notice and consent.

Technology must be subject to the rule of law to be trusted.

The innovation, deployment, and use of technology must be bound by the legal protection of individual freedom and human dignity, providing people legal recourse if they are harmed.

Technology must safeguard intellectual property to be trusted.

Producing new ideas is essential to improving the human condition. Creators and innovators should be able to reap the benefits of their work and have confidence that their intellectual property will not be stolen.

Technology must be subject to human direction and control to be trusted.

Without human oversight, technology could be unpredictable, harmful, or misaligned with ethics and the law.

Technology must be transparent to be trusted.

Transparency helps users understand how their data is used, how decisions are made by algorithms, and the potential impacts of technology on their lives. It also enables stakeholders to identify biases, errors, or harmful practices. Meaningful information, including governance policies, should be publicly available and easily accessible.

Technology must be rooted in scientific values to be trusted.

Innovators must utilize recognized scientific processes, including freedom of inquiry, openness, honesty, objectivity, replicability, and dependable methods for observing, acquiring, storing, managing, and sharing data.

Technology must respect the environment to be trusted.

Responsible environmental stewardship, recognizing the importance of sustainable practices and the preservation of natural resources is critical in technological development. By prioritizing environmental protection, technology can help promote a healthier ecosystem and enhance people's quality of life.

Technology must respect national sovereignty to be trusted.

Advancing freedom requires technological accommodation of both sovereign borders and individual liberties, empowering citizens, companies, and governments to maintain ownership of their sensitive information and control over their national destiny.

SECTION 2

OPERATIONAL KNOW-HOW

THE KRACH INSTITUTE FOR TECH DIPLOMACY AT PURDUE'S GLOBAL TECH SECURITY COMMISSION operates from a record of proven results. Many decades of operational experience have forged the Commissioners' understanding of how to develop transformational ideas and implement them both in the public and private sector. As a result, the Commission's members possess a unique level of credibility for generating and, most importantly, executing on their ideas in arenas such as high-tech innovation and commercialization, government-to-government diplomacy, capital investments, corporate governance, academia, defense, and trade. The Commission's collective expertise is a difference-maker at a time when too many government officials lack commercial and operational know-how, and too many private sector leaders are unfamiliar with how to engage in national security outside of regulatory compliance.

Below are just a few examples of how members of the Global Tech Security Commission have produced results and scalable models of tech diplomacy at the highest levels of the corporate, academic, tech, and diplomatic worlds. This track record is the basis for the findings, imperatives, Principles, and all current and future Commission outputs.



Securing Global 5G Infrastructure Through the Clean Network Alliance of Democracies: From 2019-2021, then-Under Secretary of State **Keith Krach** executed a historic diplomatic initiative to build the Clean Network, a group of 60 countries (representing approximately two-thirds of global Gross Domestic Product (GDP), more than 200 telecommunications companies, and dozens of other industry-leading companies. All entities in the Clean Network are committed to keeping untrusted technologies, such as those manufactured by Huawei, the backbone of the Chinese Communist Party's (CCP's) surveillance state, out of their national telecommunications networks.[2] This initiative has been taught as a case study at Harvard Business School.



Establishing the World's Most Digitally Advanced Society: Former President **Kersti Kaljulaid** accelerated Estonia's post-1991 commitment to digitizing its society for the benefit of all Estonians. Wired has described "e-Stonia" as "the world's most digitally advanced society," reflecting not only the vast array of digital services Estonia offers to its citizens, but the country's commitment to trusted technologies.[3] Kaljulaid's experience is all the more valuable as Estonia has consistently been a target of Russian cyber aggression since its independence.



Strengthening Techno-Democratic Diplomatic Ties: GTSC Commissioner for India **Harsh Shringla** previously served as India's Ambassador to the U.S. (2019-2020), India's Foreign Secretary (2020-2022), and Chief Coordinator for India's G20 Presidency in 2023. Under Shringla's leadership, India made technological transformation and digital public infrastructure a flagship priority of its G20 Presidency, producing the groundbreaking G20 High-Level Principles to Support Businesses in Building Safety, Security, Resilience, and Trust in the Digital Economy. His work helped strengthen the ties between the world's two largest democracies at a time when a strong U.S.-India relationship is more important than ever for advancing a world of trusted technologies.



GTSC Commissioner for Taiwan **Audrey Tang**, the former and first-ever Minister of Digital Affairs of Taiwan (R.O.C.) from 2016 to 2024, has been called one of the "ten greatest Taiwanese computing personalities." Her work as Digital Minister focused on leveraging technology to help the Taiwanese government function more effectively. Former Australian Prime Minister **Tony Abbott** and former Japanese Prime Minister **Taro Aso**, both Global Tech Security Commission Members, also provide an unmatched perspective on geopolitical issues.



Establishing Trust with Tech Standard Setting: During her time as the Head of Trust Strategy and Marketing at DocuSign, **Heather Petersen** helped established the xDTM Standard Association, a consortium of leaders in digital transaction management. The Association's mission, over two years, was to develop a set of best practices for digital transactions in a new era of cloud services. Providers were asked to address security, assurance, privacy, validity, availability, scalability, universality, and interoperability as indicators of trust. DocuSign announced its compliance with the xDTM standard in 2016, and the standard received endorsements from FedEx, Intel, Dow Jones, NBC Universal, Visa, and over 300 other major companies. As Jim Hagemann Snabe, board member at the World Economic Forum, remarked, "The xDTM Standard has enhanced the quality of digital transactions and digital signatures around the world."

Onshoring Semiconductor Manufacturing: Then-Under Secretary Krach designed and executed the 2020 landmark agreement that led the Taiwan Semiconductor Manufacturing Company (TSMC) to establish a new $12 billion chip fabrication facility (fab) in the U.S. at a time when America did not possess a single fab on its shores. Since the inception of that facility, the largest onshoring project in U.S. history at the time, TSMC has now invested more than $65 billion in three semiconductor plants in the U.S., and companies such as Micron, Intel, and others have decided to build and diversify their operations in the U.S., Japan, and Germany. In 2024, South Korea's SK Hynix invested $4 billion to build a fabrication facility at Purdue's Research Park, the largest economic development project in Indiana's history.



Restructuring the Department of State for the Digital Age: In 2019, while serving as U.S. Assistant Secretary of State for Global Public Affairs, Krach Institute chief executive **Michelle Giuda** led and executed the largest restructuring within the State Department in twenty years to modernize and dramatically improve the ability of the U.S. to leverage modern communications technologies in its diplomatic efforts, and to effectively compete with adversaries in the information space.



Leveraging Education as a Strategic Asset: Global Tech Security Commissioner for Education, **Henry Stoever**, the former President and CEO of the Association of Governing Boards of Universities and Colleges, formed the Council on Higher Education as a Strategic Asset (HESA) to strengthen the global competitive position of the United States through education. Comprised of more than 60 leaders from business, government, nonprofit organizations, education, and the military, HESA has developed recommendations for the President of the United States of America, members of the U.S. Congress, the U.S. Secretary of Education, state governors and legislators, and higher education governing boards and chief executive officers.

Delivering Excellence at Scale as a Leading National Security University: The Commission enjoys a tremendous differentiating advantage in having Purdue University as its home base. Purdue is a world-class research institution with a 155-year history of producing STEM (science, technology, engineering and math) graduates equipped to understand—and shape—trends in cutting-edge technologies. Purdue is recognized by *U.S. News & World Report* as one of the 10 most innovative colleges in America,[4] by IPWatchdog Institute as a top three leader in startup creation,[5] and by the U.S. Patent and Trademark Office as a top-five leader in the U.S. for patents.[6] Even more importantly to the Commission's work, Purdue's leaders understand the nature of the battle between the free world and

authoritarianism and are committed to leading the development of the technologies and the workforce necessary to protect freedom, prosperity, and national security. Under the leadership of President Mung Chiang, former Science and Technology Advisor at the U.S. Department of State, Purdue marries its legacy as a hub for cutting-edge scientific research with a practical understanding of how technology must support national and international security, innovation and prosperity.

- Purdue has taken the lead in forging global partnerships devoted to research and development to serve trusted technology ends:
    - Purdue and Belgium-based imec, a crown jewel of chips innovation in Europe, have opened an R&D hub on Purdue's campus.
    - During the 2023 meeting of G-7 nations in Japan, Purdue and Hiroshima University signed an inter-university agreement to promote academic and educational exchanges.
    - In May 2023, Purdue agreed to partner with the Indian government in skilled workforce development and joint research and innovation in the burgeoning fields of semiconductors and microelectronics. In March 2024, Purdue President Mung Chiang traveled to Costa Rica to strengthen semiconductor partnerships.
    - In July 2024, Indiana-based Heartland BioWorks, of which Purdue is a member, received $51 million in federal funding to support workforce development in Indiana's biotechnology ecosystem.
    - The partnership between Purdue and leading South Korean semiconductor manufacturing firm SK hynix was awarded $450 million in direct support for high-bandwidth-memory production and advanced packaging research and development at a planned Purdue Research Park facility in West Lafayette.
    - The Applied Research Institute (ARI) of Indiana granted funding to Purdue to advance artificial intelligence hardware through the Microelectronic Commons program in collaboration with the Silicon Crossroads Microelectronics Commons Hub, one of eight national hubs funded by the federal CHIPS and Science Act.
    - The Purdue Applied Research Institute (PARI) is devoted to meeting urgent needs in national security, infrastructure and global development. Its research areas include hypersonic technologies, microelectronics, energetics and infrastructure materials.
    - Purdue is the first institution in the United States offering a dedicated master's degree program in semiconductor engineering, reflecting the school's commitment to addressing the growing need for skilled professionals in semiconductor technology in the U.S. and allied countries.
    - Part of the Discovery Park District family of centers and institutes, Purdue's Birck Nanotechnology Center, a 186,000-square-foot facility that features a 25,000-square-foot cleanroom laboratory for nanofabrication, is at the heart of developing technologies essential for U.S. and allied security. Birck's SCALE partnership also brings together 29 universities and 59 defense industry and government entities to develop curriculum and internship and training models.
    - The university's groundbreaking computer science and engineering strategic initiative, *Purdue Computes*, educates tech innovators needed to maintain U.S. leadership in critical fields of economic and national security, including AI, semiconductors, and quantum science and engineering.

These examples and others are case studies of effectiveness that serve as the foundation for the Global Tech Security Commission's thinking and recommendations.



"This is, I think, the most exciting human fab that I've ever seen. And building the next generation of leaders in technology—it's incredibly powerful…All of this is part of tech diplomacy."

Secretary of State Antony Blinken
during a visit to Purdue's microelectronics training facilities at the Birck Nanotechnology Center, September 2022

SECTION 3

AN ANALYSIS ON THE COLLISION BETWEEN EMERGING TECHNOLOGIES AND 21ST CENTURY GEOPOLITICS

"Whoever becomes the leader in this sphere will become the ruler of the world."
—Russian President Vladimir Putin, commenting on artificial intelligence, September 2019[7]

"The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources for development and have the upper hand."
—Chinese Communist Party General Secretary Xi Jinping, 2013[8]

AS PART OF ITS MISSION TO ENSURE THAT TECHNOLOGY ADVANCES FREEDOM, THE GLOBAL TECH Security Commission began its work with a comprehensive analysis of the role of new technologies as a lever of power in the contest between free societies and authoritarian regimes. This effort included a competitive analysis and an assessment of strengths, weaknesses, opportunities, and threats (SWOT) of the U.S. and its allies, as well as authoritarian regimes.

In every era of human history, civilizations, nations, and their peoples have developed technologies to secure their interests and gain advantages over one another. But the scale and pervasiveness of modern technologies makes competition today profoundly different from that in previous eras. Semiconductors are the beating heart of every device with an on-off switch, including critical infrastructure. The world's data is increasingly stored on cloud platforms. Satellites relay signals to billions of people worldwide. Governments are reconfiguring national transportation systems around clean energy technologies and connected vehicles.

Artificial Intelligence is especially emerging as a cornerstone of modern technological and economic competition. AI is not only vital for maintaining a strategic edge but also essential for enhancing national security, addressing pressing societal challenges, and bolstering economic growth. Goldman Sachs has theorized that AI alone could be responsible for driving a 7% increase in global GDP by 2033.[9]

But AI is not without complications. For one, the rapid expansion of AI capabilities comes with significant infrastructure demands, particularly in the form of immense energy requirements. "The need for AI infrastructure will reshape our national energy strategy, as AI's hunger for power is unprecedented," says Erik Bethel, GTSC Commissioner for Financial Technologies. "Ensuring that nations can sustainably meet the power needs of AI will be crucial to securing their technological future and safeguarding its strategic interests."

Second, in the face of competition from authoritarian regimes, a pragmatic approach to AI development is crucial. While the protection of individual rights and privacy remains paramount, the U.S. and its allies must be

mindful of the strategic implications of falling behind in the AI race. Ethical considerations and risk mitigation are essential. But the Commission also recognizes the danger of over-regulation in the early stages of AI development. A balanced approach is crucial, one that ensures responsible innovation while allowing for the necessary exploration and experimentation to drive progress and maintain free nations' competitive advantage.

In the context of geopolitical competition, emerging technologies are not just a means of obtaining superior military power. They are also the most powerful tools in the world for maintaining human flourishing, exerting economic might, disseminating information, and protecting (or, sadly, abusing) human rights.

> **"The cost of doing nothing or maintaining the status quo is to risk being technologically outcompeted by the PRC in the next revolution of military affairs."**
>
> **Greg Levesque, Global Tech Security Commissioner for Military-Civil Fusion, May 2023**

The comprehensive, "4-dimensional" nature of competition between the free world and authoritarian states will take place across diplomatic, economic, cultural and informational, and military lines—and technology is the crossroads. Given the importance of emerging technologies to these areas and all aspects of modern life, it has never been so important to ensure that the actors controlling them do not use them to do harm at scale.

As miraculous as the post-World War II proliferation of technology has been for economic growth, global interconnectivity, and quality of life, it has come with a downside. Largely because of the free world's economic ties with China and other authoritarian nations, regimes hostile to freedom have legally and illegally acquired or developed the technologies that will shape geopolitical power. These nations have already demonstrated a willingness to use them to expand their own military, economic, diplomatic, information and cultural power. They have also used them to erode free nations' security, prosperity, freedom, and global standing. Russia, for instance, now deploys hypersonic missiles in Ukraine.[10] The Chinese military is researching how the gene-editing tool CRISPR might be used to enhance soldier performance[11] and Chinese researchers have reportedly learned how to use quantum computing power to crack military-grade encryption tools.[12] Iran and North Korea have both manipulated cryptocurrency exchanges to evade sanctions.[13]

Competitive Analysis

The United States and its allies boast systems of government dedicated to protecting individual rights and ensuring participation in democratic processes. For the most part, these representative governments give citizens the power to decide national and individual destinies. In the geopolitical arena, free societies strive to uphold peace, prosperity, and human rights, and believe in international standards of conduct and cooperation where economic coercion, warfare, and other forms of aggression are the tools of last resort for resolving disputes.

By contrast, authoritarian regimes such as those ruling the People's Republic of China, the Islamic Republic of Iran, the Russian Federation, and the Democratic People's Republic of Korea (North Korea) are characterized by power concentrated in the hands of a party, regime, or dictator. Because the ultimate goal of each of these regimes is its own preservation, the state wields ultimate power over all areas of national life, often ruthlessly, with citizens' rights and welfare common casualties of state rule. In the geopolitical arena, authoritarian states routinely violate free societies' standards of international conduct—witness, for example, North Korea's routine ballistic missile testing, the Iranian regime's support for Mideast terrorist groups, Chinese acts of aggression in the South China Sea, or Russia's invasion of Ukraine. Emerging technologies will only provide these regimes more weapons to preserve their own power at home, wield it abroad, threaten global peace and prosperity, and displace the free world's global leadership.

Free Societies

Strengths: The U.S. and its likeminded allies and partners are committed to the freedom of expression, the rule of law, impartial judiciary systems, and the protection of property rights. These political features consequently undergird economic systems characterized by open markets, fair competition, international collaboration, robust capital investment, and regulatory frameworks that lead to historic accomplishments in innovation and enterprise. These features have allowed companies located in the free world to become the world's leading innovators in key emerging technologies: think ASML (semiconductor manufacturing equipment) in the Netherlands, Palantir (artificial intelligence) in the United States, or Samsung (5G and 6G) in South Korea.

Perhaps most importantly, the likeminded nations of the free world are bound by shared values and a history of collaboration that has established high levels of trust. Many nations have their military or economic ties formalized through the NATO alliance and the European Union and have a history of cooperating to combat shared threats, whether it was Soviet communism during the Cold War or Islamist terrorism in the Global War on Terrorism. Consequently, these nations can trust that the others are generally committed to pursuing similar geopolitical ends, thereby laying a basis for eager cooperation. The power contained in these alliances is the free world's most powerful competitive advantage in the geopolitical arena.

Weaknesses: Freedom also presents inherent challenges. Passing national security-focused legislation through democratic legislative processes marked by open and transparent debate is often a complex and slow-moving process. Coordinating efforts across sectors and countries is also difficult, given the differing objectives between public and private sector actors, as well each country's views of what is in its own national interests. Over the last several years, for instance, the European Union's strategic orientation toward China has been inconsistent, in part because of divisions within the bloc over allowing China to invest in or acquire European tech companies. Consequently, nations of the free world have not forged a durable, coordinated strategy amongst themselves for responding to emerging techno-authoritarianism.

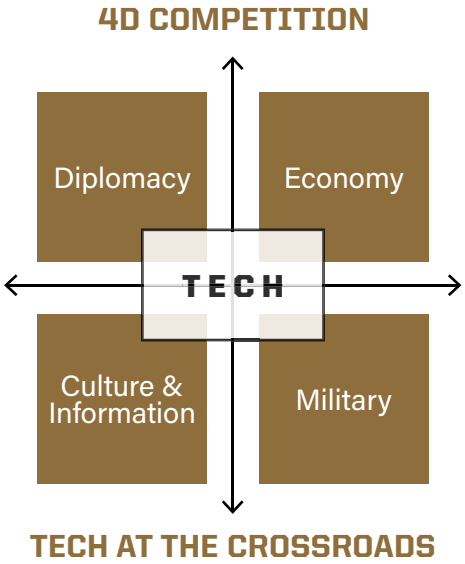
SWOT ANALYSIS: U.S. & ALLIES

STRENGTHS:	OPPORTUNITIES:	WEAKNESSES:	THREATS:
▪ Shared democratic values ▪ Relationships built on trust ▪ Robust alliance network ▪ Dynamic, innovative economies and private sector companies ▪ Robust financial resources at government disposal	▪ Enormous market access power = political and tech power ▪ Power to stimulate tech innovation ▪ Power to implement defensive strategies to safeguard systems from authoritarian tech	▪ Complex, slow lawmaking processes ▪ Siloed, uncoordinated efforts ▪ Interests not always aligned between nations	▪ Authorian tech (e.g. Huawei, DJI, TikTok, Kaspersky Labs) already in Western systems ▪ Authoritarian states willing to violate norms, test limits ▪ Open systems already exploited by authoritarians for propaganda, research theft, foreign influence, elite capture, etc.

Free nations, such as those in Europe, are also being forced to rethink the conditions they must set to be conducive to tech development. Former Italian Prime Minister and head of the European Central Bank Mario Draghi has noted that, "the core problem in Europe is that new companies with new technologies are not rising in our economy."[14] No company with a market cap over EUR 100 billion had been set up in the last fifty years.[15] Today, notes Draghi, Europe would need EUR 750-800 billion *per year* to meet its existing environmental, security, innovation, and digital infrastructure goals—a figure that is approximately twice the size of GDP which Europe dedicated to the Marshall Plan each year in the aftermath of World War II.[16] Europe's self-assessment of its long-term strategic failure to prioritize its tech competitiveness pinpoints its inability up to now to achieve broader societal objectives.

"The United States and its allies dominated the global innovation stage for decades due to the unique environment of civil liberties, transparent government, and robust intellectual property regimes that encouraged citizens and enterprises of all sizes to engage in creative endeavors that collectively bolster our economies, sharpen our competitiveness, and strengthen our national security."

Andrei Iancu, Global Tech Security Commissioner for Intellectual Property, May 2023



Finally, citizens in the free world have typically viewed national security as strictly a responsibility for national governments to bear. But not every national security decision is one that involves deployments of troops, appropriations of money, or economic sanctions. Business leaders have the opportunity – and duty – to make decisions that serve their respective nations' security interests, in ways that go far beyond mere compliance with government rules. As Krach Institute CEO Michelle Giuda has emphasized, "The real strategic impetus for winning the technology race will come not from government but from our enterprising business leaders from Silicon Valley to Indianapolis to New York to Austin, with help from allies in places like Tallinn, Montevideo, Tel Aviv, and Taipei."[17] Much work remains to normalize this attitude within the private sector and stop free-world companies from partnering with purveyors of untrusted technologies who are dedicated to the free world's demise. A safe, free, and prosperous world is good for business.

Opportunities: The world's 12 largest democracies (by GDP) and the European Union make up nearly two-thirds of the world's GDP, giving them enormous economic leverage within the geopolitical arena—if they can act in a coordinated fashion. Additionally, free-world companies are still the world's leading innovators of emerging technologies, giving them opportunities to secure new market shares. National governments also have opportunities to stifle technology transfers to authoritarian states and cut off the capital investments that bolster

HOUSE SELECT COMMITTEE ON THE CCP: ZPMC CARGO CRANES ARE A "TROJAN HORRSE"

"Chinese cargo crane manufacturer ZPMC manufactures 80% of U.S. ship-to-shore cranes in operation at U.S. ports. A 2024 House Select Committee on the Chinese Communist Party investigation discovered, "ZPMC could, if desired, serve as a Trojan horse capable of helping the CCP and the PRC military exploit and manipulate U.S. maritime equipment and technology at their request. This vulnerability in our critical infrastructure has the potential to affect Americans from coast to coast."[19]

SWOT ANALYSIS:
AUTHORITARIAN REGIMES

STRENGTHS:	OPPORTUNITIES:	WEAKNESSES:	THREATS:
▪ Governments can compel whole -of-society efforts ▪ Unencumbered by lengthy, complex democratic processes when determined to take action ▪ Willingness to break rules, exhibit aggression, alienate other nations ▪ Vast subsidies devoted to growing indigenous tech ecosystems with view toward global monopolies	▪ Untrusted technologies and trade relationships have already deeply penetrated free societies ▪ Track record of subsidizing tech development (e.g. semiconductors and electric vehicles) in hopes of achieving global dominance while other nations play catch-up	▪ Authoritarian regimes are historically brittle and unstable ▪ Lack of true political and economic freedom limits power to innovate ▪ Mistrust within the international system ▪ Lack of true allies outside their own "club" ▪ State control of economy leads to subpar economic outcomes	▪ Popular discontent with regime rule threatens regime collapse ▪ Acts of aggression and promise-breaking produce international diplomatic, economic, military retaliation

adversaries' militaries. Where the private sector is concerned, as global geopolitical tensions rise, business leaders who limit business relationships to trusted tech partners will enjoy greater degrees of product and supply chain security, stakeholder confidence from customers, investors and regulators alike.

Threats: Authoritarians have exhibited a track record of exploiting free societies' freedoms and economic openness to achieve their goals. As just a few examples, *RT*—a Russian propaganda network—operated with relative impunity on American television until 2022, and companies partnering with the Chinese military have listed on American stock exchanges. Chinese military personnel posing as innocent graduate students have infiltrated campuses in countries like Australia, Germany, Singapore, the UK and the U.S. with the intent to steal high-tech research.

Additionally, many companies and state/local/federal governments have adopted technologies produced by companies owned by or headquartered in authoritarian states (e.g. Huawei routers, DJI drones, Kaspersky Labs software, or ZPMC cargo cranes). Now spread across the free world, those technologies become access points for authoritarians to steal, spy and sabotage.

In total, authoritarian regimes have a sustained appetite to defy international norms and sacrifice the interests of their own people to achieve their geopolitical goals, thus creating pressure on free societies to decide whether, or how, they will impose costs for rogue behavior.

Authoritarian Regimes

Strengths: Authoritarian states can compel or incentivize all aspects of their tech and business sectors to participate in achieving regime goals. Thus, even nominally private firms can become weaponized as arms of state power, especially in the tech sector. Thanks to a patchwork of national laws, the Chinese government can order Chinese firms to engineer technologies, appropriate Western technologies, and allocate personnel to serve the state's national security imperatives. In 2022, the Russian government effectively legalized intellectual property theft, issuing a decree that allows Russian firms to use intellectual property from "unfriendly countries" without consent or compensation. According to the website IP Watchdog, "This essentially means that Russian firms can access publicly available patent databases and practice the patents to boost struggling technological production."[18]

"Amid the growing geopolitical dynamics in Asia, Korea's partnership with allies on critical technologies has become ever more paramount to ensure global economic security."

James Kim, Global Tech Security Commissioner for Korea, May

As a matter of techno-economic strategy, Chinese state planning and subsidies have greatly contributed to China becoming the world leader in the production of LED screens and green technologies such as electric vehicle batteries and solar panels. The success of state-funded support in concentrating production of these technologies inside China's borders has inspired Beijing to attempt to achieve similar domination in other key technologies such as semiconductors and electric vehicles.

Additionally, authoritarian regimes have developed technologies purely for battlefield use, and in many cases already deployed them. Iran has shipped Shahed drones to Russia, where they are deployed on the battlefield in Ukraine, and the Houthi rebels in Yemen have also deployed Iranian drones in their attacks on Israel and commercial ships transiting the Red Sea. North Korea is well-known as a proliferator of ballistic missile know-how to Iran, and Russia has shipped its S-300 missile system there as well. Disinformation operations targeting democracies, such as those performed by Russia, can also move faster than the "speed of truth"—forcing governments to address lies at a slower rate than they can be pumped out.

More broadly, authoritarians, unconstrained by complex and time-consuming democratic processes, excel at rapidly exploiting geopolitical opportunities. They are comfortable to operate outside of international norms, create economic dependencies, and bypass ethical standards in areas such as human rights, labor, respect for the environment, and application of the rule of law. Authoritarian regimes seek to exploit the technological vulnerabilities and resource wealth of developing nations, thereby leveraging financial dependencies to impose their own interests. These tactics have helped countries like China and Russia gain substantial tech-economic footholds in developing countries throughout Africa, Asia, and Latin America. The Chinese Communist Party's now-famous Belt and Road Initiative and Digital Silk Road have expanded China's global influence.

CHINA LEADS THE WORLD IN 37 OF 44 CRITICAL TECHNOLOGIES

"Our research reveals that China has built the foundations to position itself as the world's leading science and technology superpower, by establishing a sometimes stunning lead in high-impact research across the majority of critical and emerging technology domains. China's global lead extends to 37 out of 44 technologies that ASPI is now tracking, covering a range of crucial technology fields spanning defense, space, robotics, energy, the environment, biotechnology, artificial intelligence (AI), advanced materials and key quantum technology areas." (Australian Strategic Policy Institute Critical Technology Tracker, March 2023[20])

Weaknesses: Authoritarian regimes are not without their own dramatic weaknesses. Lack of political and economic freedom stifles a culture of innovation and drives aspiring entrepreneurs and thinkers overseas. From October 2020 to January 2021, Jack Ma, the ordinarily high-profile Chinese founder of Alibaba Group, was nowhere to be seen in public view. Speculation persists that the Chinese government forcibly detained Ma or ordered him to keep a low profile after he gave a speech criticizing China's regulators and banks.

Authoritarians' broken promises and aggressive behaviors on the world stage have shattered trust within the international system and curtailed the free world's willingness to share certain technologies with them, creating their own dependencies on foreign technologies and hindering them in their race to catch up to the leading companies of the free world. Finally, while China, Russia, Iran, and North Korea have increased geopolitical and military coordination with one another in recent years, these nations' aggressive behaviors have substantially alienated other countries, and hence they lack true allies globally apart from other unstable and often impoverished authoritarian regimes. The world's worst authoritarian regimes maintain only partnerships of coercion, convenience, and transaction, rather than true alliances.

Opportunities: Authoritarian regimes have strategically embedded their technologies with widespread global adoption such as TikTok, Huawei cell phones, or BYD electric vehicles. Besides the potential for these items to serve Chinese or other authoritarian state interests through theft, surveillance and sabotage, the economic activity associated with the production or importation of such items leads to political leverage for Beijing. Authoritarian regimes routinely exploit free societies to launch legal and illegal influence campaigns, manipulate public opinion through misinformation and disinformation, and co-opt business leaders.

Additionally, authoritarian nations continue to seize the opportunity to grow influence in poor nations with weak democratic norms or resilience. Developing nations in Africa, Asia, and Latin America with growing populations and increased technological capabilities will be home to a significant portion of the world's future workforce and consumer and innovator base, enhancing their influence on global markets. Without a concerted effort to steer these nations toward a model of techno-freedom, they risk falling permanently into the technological-economic orbit of authoritarian countries, thus deterring foreign private sector investment, stifling their development, and saddling them with crushing debts or loss of sovereignty.

Threats: Authoritarian regimes are more unstable than they look. Because they are willing to use repression and fear as prime tools of governance, their citizens often quietly simmer with grievances toward the regime. Hence, authoritarian regimes are consistently at risk of being overthrown by their own publics.

Moreover, state-directed economies tend to underperform nations distinguished by free markets. The Freedom & Prosperity Index developed by GTSC Commissioner for Prosperity Partnerships Dan Negrea demonstrates a strong correlation between economic prosperity and freedom, showing that as freedoms in areas such as the economy, governance, and individual rights increase, so does overall prosperity. Higher levels of freedom support a more robust economy, enhance innovation, and improve quality of life, indicating that nations with greater personal and economic liberties tend to enjoy higher prosperity levels. Externally, a growing international consensus among free societies to exclude authoritarian countries from trade relationships is putting new economic pressure on them, and countries like Iran, Russia, and North Korea have almost entirely alienated themselves from the global economy because of acts of aggression. In the case of Russia, its invasion of Ukraine triggered the expansion of NATO, the departure of more than 1,000 companies from Russia, and a wave of international sanctions.



"The use of AI/ML technologies for surveillance and social control in China could set a precedent for other countries, raising concerns about privacy, human rights, and the potential for AI-enabled authoritarianism."

David Spirk
Global Tech Security Commissioner for Artificial Intelligence and Machine Learning

SECTION 4

FINDINGS AND FIVE IMPERATIVES

"When considering the defense of a nation, the military is no longer the sole agent, nor are its kinetic capabilities the last word in foreign relations."
—David Stilwell, Global Tech Security Commissioner for Defense, May 2023

THOROUGHLY UNDERSTANDING THE NUANCES OF EITHER GEOPOLITICS OR TECHNOLOGY IS ITSELF A FULL-time pursuit. To understand how each one affects the other makes the task more daunting. Even as diplomatic, tech, business, and civil society leaders strive to ensure that technology advances freedom, deciding the priority battlegrounds of effort can be overwhelming even for experts. That is why the Global Tech Security Commission identified five high-leverage areas in which the Global Trusted Tech Network can dramatically accelerate the innovation and adoption of trusted technology—provided that we take action in the next one to five years.

Imperative #1: Education and R&D

In the course of its analysis, the Commission recognized that public and private sector leaders consistently lack refined understandings of how emerging technologies work, their place in the broader tech ecosystem, and their role in influencing geopolitical dynamics. The world's most powerful people—and decision-makers at all levels—need trusted and comprehensive information on the topics that will shape the future of geopolitics. Without it, they will be in the dark as they attempt to make good decisions, develop their workforces, and position their nations for economic success. As a result, the Commission identified several critical lines of effort for building knowledge and technical capacity on emerging technologies and their implications:

Bolstering tech diplomacy proficiency: The hyper speed and scale of tech innovation is daunting, not to mention the specialized knowledge required to understand even the basics of large language models, quantum physics, 6G wireless networks, satellite communications, semiconductor microelectronics, and synthetic biology. The complications inherent in understanding these technologies and others is compounded by the intricacies of the export control policies, global data regulations, industrial policies, and regulatory policies that govern the creation and proliferation of tech. Thus, most diplomats and business leaders do not yet fully understand the technologies themselves, their grand implications for today's 4D geopolitical competition, and the role these leaders can and must play in ensuring that technology advances freedom.

In September 2022, scholars from the Special Competitive Studies Project recommended that the U.S. State Department "increase training, build STEM policy literacy, and create more tech officer positions in the Department of State."[21] Similarly, the October 2023 issue of the *Stanford Emerging Technology Review* encouraged, "Policymakers need better expert resources to help them more easily understand the burgeoning and complex array of technological developments—more easily and more continuously."[22] The Krach Institute for Tech Diplomacy at Purdue has already responded to this call by standing up the world's first Tech Diplomacy Academy. It is our intent that the Tech Diplomacy Academy will scale worldwide and help catalyze business, government and citizen leaders to educate their teams, students, and employees to shape the trajectory of trusted technology.

Turbo-charging STEM talent: Free nations must also develop a workforce capable of seizing the commanding heights of future innovation. It is imperative that free nations continue to train citizens with high STEM competencies essential to high-level R&D. Data from the 2022 Program for International Student Assessment revealed that U.S. students ranked a dismal 28th out of 37 countries in math and 12th out of 37 in science.[23] In Europe, 30% of 15-year-old EU students are non-proficient in mathematics, and 25% fail to achieve proficiency in science.[24]

TECH DIPLOMACY ACADEMY



To meet the challenge of training a new generation of Tech Diplomats, the Krach Institute for Tech Diplomacy at Purdue founded and launched the Tech Diplomacy Academy in 2024 to provide a comprehensive understanding of emerging and critical technologies and their impact on commerce, national security, and foreign policy.

It is the world's first and only online education platform training government, business, technology, and citizen leaders at scale about critical and emerging technologies and their role in the contest between freedom and authoritarianism.

Tech Diplomacy Academy launch partners and early adopters include the U.S. State Department, U.S. Commerce Department, U.S. Navy Foreign Affairs Officers, the Australian Strategic Policy Institute, the Black Sea Trust of the German Marshall Fund, Edge A.I., global consulting firms Deloitte and Guidehouse, the U.S.-Taiwan Business Council, and National Chengchi University (NCCU) and National Yang Ming Chiao Tung University (NYCU) in Taiwan.

While the U.S. and other free nations are blessed to have many high-achieving immigrants graduate their institutions, most of whom go on to add value to tech companies, unpredictable immigration policies and the intensification of global tech competition call for greater K-12 and college-level achievement in STEM disciplines. The time is now to invest in this strategic asset.

Using Higher Education as a Strategic Asset: Finally, higher education must be viewed as a strategic asset in tech competition. The nations that can produce the greatest number and most talented high-level STEM graduates will have an advantage in leading every aspect of the tech innovation race.

Imperative #2: Technology and International Standards

Whether railroad track gauges in 19th century America, the battle between VHS or Beta home video formats in the 1980s, or electric vehicle charging configurations today, standardization has helped guide the secure adoption (or decline) of certain technologies. When companies, governments, or international bodies have the power to set technological standards, they have the power to shape how technologies are deployed and adopted. The Commission realized that in our globalized era, the often-universal nature of standards makes them among the most powerful tools for protecting freedom, security and innovation. Therefore, it is recommended that the establishment of trusted technology standards must be one of the Global Trusted Tech Network's highest priorities.

Governments and tech companies alike thus have an interest in defending emerging tech regulations and standards that spur their own business successes and national prosperity. It is obvious to state the risks presented by authoritarian states that don't respect human rights, transparency, privacy, or laws to set global technical standards that favor their companies and countries, and disregard freedom. Unfortunately, private sector companies have not to date advocated aggressively enough before international standard setting bodies. It is time for them to advocate for the foundational freedoms that make these companies prosperous in the first place.

Lack of engagement has opened the door for China and Russia to try and rewrite the rules of the digital road. In 2011, the Shanghai Cooperative

> **"The Tech Diplomacy Academy will play a vital role ensuring that our leaders across the NATO Alliance and beyond understand the technologies, business strategies and diplomatic tools that must be employed to secure our continuing leadership in vital tech sectors now and in the next generation."**
>
> **Mircea Geoana, NATO Deputy Secretary General, 2019-2024, May 2024**[41]

Organization—a grouping of Eurasian nations including China and Russia, submitted to the UN Secretary General an *International Code of Conduct for Information Security* which, according to Kristen Eichensehr of Just Security, "seemed to deny the applicability of existing international law to cyberspace, advocated increased government control over the Internet, and legitimized limitations on freedom of expression."[25] More recently, China's 2021 five-year plan openly called for "promoting advantageous and special Chinese technology standards to become international standards to serve Chinese enterprises and industry going global."[26]

The China Standards 2035 initiative also envisions a greater role for Chinese tech companies in shaping international tech standards—and China has already made headway in setting three internationally-recognized 6G standards under the jurisdiction of the International Telecommunications Union (ITU).[27] Beijing has also vigorously lobbied the ITU to create rules that favor its own tech companies and enable greater online censorship. China has pushed a plan called the New IP—which also enjoys Russian support—which essentially seeks to give governments more power to control a user's internet access and track his or her online activity.[28]

"With the growth of the Internet has come an evolution in the connectedness of people across the globe. This has led to policy and governance issues that require understanding of the norms and principles of free nations as well as the technology that influences them today."

Rob Spalding, Global Tech Security Commissioner for 5G/6G, May 2023

Fortunately, the U.S. and its allies scored a win for tech freedom when American Doreen Bogdan-Martin won the ITU's October 2022 leadership election over Russian candidate Rashid Ismailov—an ally of Beijing's efforts. Similarly, in 2020, U.S. diplomats worked to defeat a China-supported candidate and elect Singaporean Daren Tang as the head of the UN's World Intellectual Property Organization—a global body with power to define norms surrounding intellectual property protection.[29] These successful diplomatic efforts to protect tech security and freedom—to include voices from the private sector—should be replicated whenever elections for personnel leading international standard-setting bodies are held. Standard-setting also presents a golden opportunity for private sector and public sector leaders to work together to set tech standards that will reinforce the leadership of free-world companies and international security objectives.

Imperative #3: Technology Supply Chains and Infrastructure

The production of modern technologies depends on components and minerals sourced from various corners of the globe, whether rare earth materials, solar cells, semiconductor components, pharmaceutical ingredients, and more. Thus, reliable, resilient, and secure supply chains are at the core of all critical tech sectors—and all global economic trade and prosperity. If authoritarian nations can control the source materials or foundational components of critical technologies, the world will be at their mercy for what it needs. Accordingly, the Commission decided that securing the building blocks of the modern economy—supply chains and infrastructure—must be a foundational priority area.

The consequences of Russia's 2022 invasion of Ukraine have underscored the importance of eradicating supply chain vulnerabilities. Russian aggression has prompted European governments to substantially cut themselves off from Russian energy supplies, leaving them scrambling to find alternative sources of oil and gas. Instead of viewing energy trade with Europe as a pillar of economic interdependence that deterred conflict, the Russian government was willing to count the loss of billions of dollars in energy sales and the NordStream 2 pipeline as an acceptable casualty in its foreign policy goal of obliterating Ukraine's sovereignty and national identity. European governments have since wrestled with high prices and shortages of energy that depress economic growth.

Just as dramatically, shortages of medical supplies, computer chips and consumer goods during the COVID-19 pandemic likewise exposed the dangers of depending on authoritarian regimes for key products. The possibility of China cutting off supplies of tech exports (and their key components) as a form of economic warfare is based on recent examples:

THE GLOBAL TRUSTED TECH (xGTT) STANDARD INITIATIVE: DEFINING TRUSTED TECHNOLOGY

There is a clear need for an overarching technical standard that defines trusted technology, which is why the Krach Institute for Tech Diplomacy at Purdue has initiated the first-of-its-kind Global Trusted Tech (xGTT) Standard initiative.

Based on the success of the Trust Doctrine at the heart of the Clean Network to secure 5G, the xGTT Standard aims to develop and implement a global standard for trusted technology and a process by which the standard is adopted, trusted technology is validated, and entities are labeled as purveyors of trusted tech. It will enable frictionless collaboration between governments, companies, and other organizations around trusted technologies. The xGTT Standard initiative is led by a world-class governance structure, with a Board of Governors and Chair—Taiwan's Cyber Ambassador-at-Large and former Minister of Digital Affairs, Audrey Tang—to develop, shape and promulgate the xGTT Standard around the globe.

- In 2010, China restricted exports of rare earth minerals to Japan after Japan detained a Chinese fisherman who ran into Japanese coast guard boats in disputed waters.[30]
- In 2020, China placed import duties or restrictions on Australian products such as barley, cotton, coal, timber and wine after the Australian government demanded answers on the origin of the COVID-19 pandemic.[31]
- In 2023, China imposed curbs on exports of gallium and germanium (used in the world's semiconductors) and graphite (used in the world's EV batteries). China produces 90% of the word's gallium and 60% of germanium and refines more than 90 percent of global graphite.[32]

While the world's focus on cybersecurity has often appropriately centered on software or 5G networks, the potential to create "Trojan Horse" vulnerabilities in the world's tech hardware products has been sorely neglected. Imagine circuit boards or power supply chips embedded with a "kill switch" that could be remotely activated in a crisis. It is not fantasy. In 2018, *Bloomberg* reported on how Chinese operatives surreptitiously inserted unauthorized chips onto Super Micro circuit boards that created opportunities for malware insertion into corporate and Pentagon servers.[33]

Trusted technology demands secure supply chains and infrastructure. Companies must reconfigure these value chains, manufacturing practices and supporting logistics systems toward maximum transparency, reliability and fair labor standards. The U.S. and its partners must develop alternatives to incentivize companies to keep production in, or return it to, the U.S. or trusted tech partner nations. A key part of this is addressing regulatory environments, tax structures and permitting systems to make it easier and more profitable to locate manufacturing in these countries, rather than in China or other authoritarian states. This extends to energy supplies and transportation networks without which companies cannot survive, much less thrive.

Imperative #4: Capital Markets and the Funding of Emerging Tech

Investments are the lifeblood of capitalism. Money builds firms up; lack of it forces them to close. Free nations prosper when their visionary companies can raise funding in open markets and outpace tech developers in authoritarian countries. But global capital markets can also contribute to the growth and development of authoritarian nations' tech sector, and China especially has already exploited the free world's open system to bankroll its way to tech dominance. The Commission sees highest-order strategic value in establishing "trusted capital markets"—investment climates in which investors do not fund innovations that can later be weaponized against them, their nations, and their freedoms.

"Fundamental and foundational to a winning global tech security strategy is the establishment of a trusted, transparent, and secure global supply chain network whose participants are all aligned against the key values of freedom and democracy and are dedicated to the development of the trusted relationships that make it all work."

Jim Schwab, Global Tech Security Commissioner for Supply Chains, May 2023

Approximately 5,000 Chinese companies are listed on U.S. securities exchanges, giving them access to hard currency financing and income. American investors supplied as much as $3 trillion of capital to Chinese companies from 2013-2023, much of it buried in passive investment vehicles like bonds and index funds.[34] As then-Under Secretary Krach stated in a letter to U.S. universities in 2020, "the majority of the U.S. university endowment fund portfolios own PRC stocks listed on American exchanges either directly or indirectly through emerging markets index funds."[35]

Listings on U.S. exchanges give "China, Inc." companies an American "seal of approval" that gives other global exchanges confidence to list Chinese companies. But letting "China, Inc." list as publicly traded companies sends the wrong signal to the world. Chinese companies are infamous for stealing technology, using it to compete against the U.S. and its partners and allies in the free world, and then putting their competitors out of business. Many Chinese companies are also complicit in human rights violations or render services to the Chinese security state. In January 2021, Under Secretary Krach listed 44 parent corporations and more than 1,100 subsidiary companies as Communist Chinese Military Companies from which American investors by law must now divest.[36] But there are undoubtedly many other unidentified Chinese companies traded publicly with opaque ties to the Chinese Communist Party and the People's Liberation Army. Not to be outdone, Iran has also exploited cryptocurrency exchanges to skirt sanctions. In 2022, Reuters reported that Binance allowed Iranian firms to trade approximately $8 billion in crypto, largely using a token with an anonymity option.[37]

Furthermore, American capital funding Chinese tech firms creates financial incentives for free world business and finance leaders to lobby their governments against accountability, transparency, and sanctions on China and Chinese companies. In this way, China has captured global financial elites. Reforming capital markets to prevent adversary nations from strengthening their techno-military power ensures that financial industry leaders, wealth managers, and investment advisors fulfill their moral obligation and fiduciary duty to protect U.S. investors.

TECH COMPANIES SEEING FEWER ADVANTAGES TO DOING BUSINESS IN CHINA

China's "Delete A(merica)" and Made in China 2025 initiatives are designed to put firms from the U.S., Europe and Asia out of business in China and elsewhere. Recognizing the decreased profitability, greater risks to intellectual property and increasing physical danger to personnel associated with operating in China, more business leaders are moving operations from China to trusted allied partners. Here are just a few tech companies that have scaled back operations in China in the last few years:

- Apple
- Blizzard Entertainment
- Dell
- Google
- IBM
- LG
- Microsoft/LinkedIn
- Nintendo
- Samsung[42]

There are additional problems with public listings of Chinese companies beyond the risk of investors funding a buildup of Chinese national security capabilities. Approximately 95% of Chinese companies listed on the New York Stock Exchange and Nasdaq are structured as Variable Interest Entities (VIEs), shell company substitutes domiciled in offshore locations.[38] This sleight of hand, wherein investors do not own actual Chinese shareholdings, deprives investors of adequate legal protections and minority shareholder rights.

Chinese firms also do not adhere to free world standards of rule of law, risk disclosure, or corporate governance, making them riskier investments than they may seem on the surface. They've managed to get around the financial transparency laws required of companies in the U.S., Europe and elsewhere to enjoy capital market listings.

In the geopolitical competition for the commanding heights of emerging technologies, free world investors should not be funding untrusted technological developments for our adversaries or their militaries. What the world needs is "trusted investments" in its capital markets, pension funds, university endowments, foundations, mutual funds and bond portfolios.

Imperative #5: Board Governance and Its Role in Trusted Tech

In the course of its work, the Commission recognized a dramatic problem: Most people consider national security as the responsibility of national governments exclusivley. For example, a poll conducted by the MITRE Corporation and the Harris Poll in 2024 discovered 78% of Americans think the federal government bears full or partial responsibility for fortifying critical infrastructure, but only 49% believe it's the responsibility of both public and private entities.[39] The Commission believes that boards of directors are a key underleveraged force to motivate private sector companies to factor national security into their decisions.

"In my view, it is not possible to identify a strategic-level, financial scandal of anywhere near this scale in modern history, whereby a democracy (notably, our own) has engaged in the multi-trillion-dollar underwriting of an authoritarian police state (read: China) bent on undermining our values and way of life, aided and abetted by some fiduciarily malfeasant Wall Street firms and other fund managers, and certain conflicted U.S. government regulators at the top levels of the Treasury Department, the SEC and the National Economic Council."

Roger Robinson, Global Tech Security Commissioner for Capital Markets, Former Chairman of the U.S.-China Economic and Security Review Commission, Testimony before House China Select Committee, May 17, 2023[43]

Business leaders are the free world's superpower in what is ultimately a technological race for the future between free societies and authoritarian regimes. Just as business leaders spearheaded the Arsenal of Democracy in World War II, their role and responsibility in upholding national security, prosperity and human rights continues. Major companies already understand the need to act with integrity—that's why approximately 1,000 foreign companies have pulled back from or completely exited Russia since its invasion of Ukraine, losing more than $107 billion.[40]

Now the private sector's attention must increasingly turn to—or rather, away from—China and its authoritarian allies. The free world's economic ties with China have given the CCP enormous wherewithal to advance China's military presence, its surveillance state, and its authoritarian worldview within and outside of its borders. Governments often feel significant pressure from business groups to maintain status quo economic arrangements that have helped create profitability for private companies doing business with Chinese firms, all of which are subject to the rule of the Chinese Communist Party. But these tradeoffs for short term gain are a risk to business and national security. Forced technology transfers, stolen intellectual property, the detainment of employees and executives, surprise raids on firms, and the perpetual fear of retaliation are forcing a daily-increasing number of business leaders to doubt the ROI to doing business in China.

As pillars of legal and fiduciary risk management, board directors must place a new focus on their companies' role in a contested technology and geopolitical space. The risks of geopolitical developments to the health of their

businesses have never been greater. At a minimum, they should work with their CEOs to identify and prioritize China and other authoritarian state-related risks, develop a contingency plan to address them, and execute it in partnership with experts. Business leaders can begin the process by forcing themselves to answer hard questions such as:

- "Who are we really dealing with in China?"
- "Are our proprietary technologies and our confidential information safe?"
- "Do our relationships in China actually threaten our long-term business model?"
- "How will our China-related choices affect not just our company, but our country more broadly?"
- "If we claim to take corporate responsibility seriously, what does that mean for our engagement with Chinese companies and supply chains?"

"Public-private partnerships and industry coalitions are key to ensuring America's continued leadership in innovation and securing technological advancements."

Thomas Sonderman, Global Tech Security Commissioner for Semiconductors and Microelectronics, March 2024



"The key to securing freedom for the next generation is securing technology. Tomorrow's tech must be trusted tech, developed and protected by a Global Trusted Tech Network of like-minded countries, companies, and individuals who respect the rule of law, human rights, property rights, fair labor practices, responsible environmental stewardship, freedom of expression, and national sovereignty."

Keith Krach
Co-Chair, Global Tech Security Commission; Chairman, Krach Institute for Tech Diplomacy at Purdue; Under Secretary of State (2019-2021); Former Chairman and CEO of DocuSign and Ariba

SECTION 5

PRINCIPLES OF TRUSTED TECH DIPLOMACY

THE OPPORTUNITY FOR FREE SOCIETIES TO FLOURISH IN A NEW ERA OF TECHNOLOGICAL INNOVATION and enterprise is clear. The danger of a world where authoritarian regimes lead in technological superiority is also evident.

That is why the Global Tech Security Commission has engineered the Principles for Trusted Tech Diplomacy as the foundation for a practical, executable playbook for ensuring that technology advances freedom. We are offering a vision for *how* we must work together, beyond just what we *must* do.

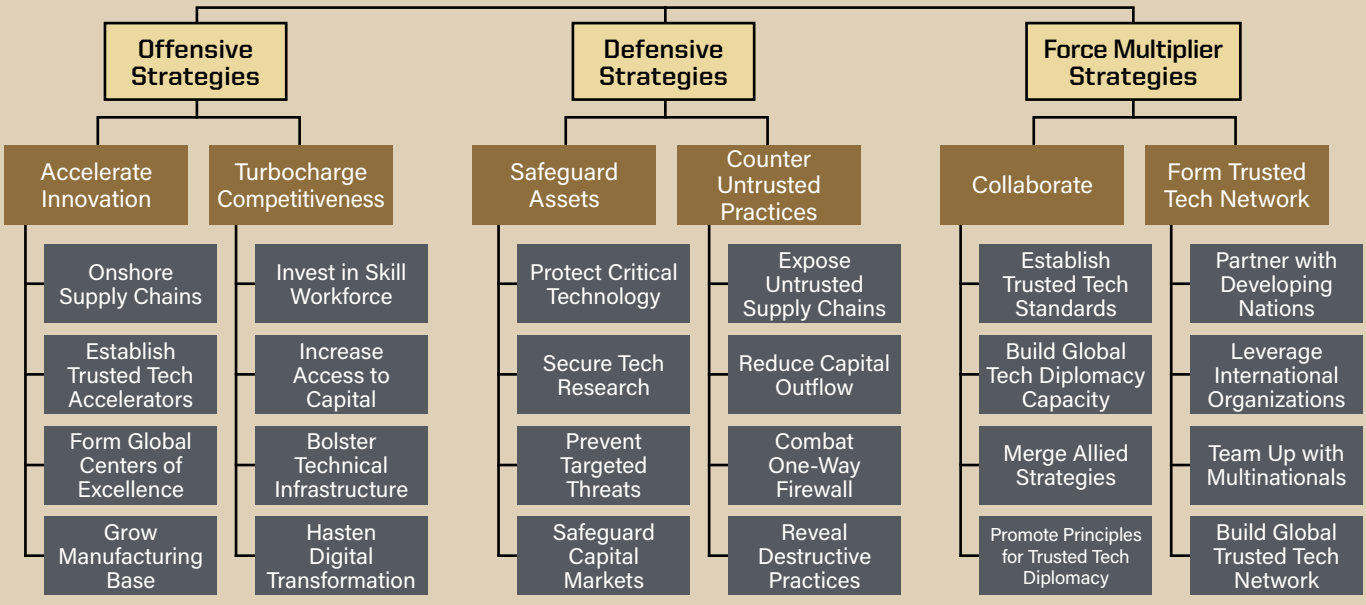
The foundation of the Principles is the Trust Doctrine articulated in Section 1. We know that trust is the foundational element of all collective success. This is especially true in the digital world—interconnectivity means that a network's security is only as strong as its weakest unit. The same applies to tech diplomacy.

These Principles of Trusted Tech Diplomacy are based off proven models for success in business and government.

They are designed to scale, enhance, and accelerate the coordination among private and public entities in every corner of the globe, and to serve as the foundation for trusted partners to develop offensive, defensive and force muliplier strategies to ensure technology advances freedom.

They are designed to leverage the free world's biggest competitive advantages: the moral high ground of our values, the innovation and resources of our private sector, and our vast network of trusted alliances.

GLOBAL TRUSTED TECH STRATEGY



Principles of Trusted Tech Diplomacy

1. **Uphold the Trusted Tech Doctrine:** An ethical and responsible use of technology is paramount. We must uphold the values of the Trusted Tech Doctrine and innovate and implement technology in ways that advance freedom.

2. **Empower Through Education:** Knowledge is power. We must seize opportunities to promote understandings of trusted versus untrusted technology in what must be an all-of-free-world movement to secure high tech. It is imperative we take steps to align educational programs and curriculum with anticipated technological development and national security needs.

3. **Lead with the Innovation and Creativity of the Private Sector:** The tech race will not be won in Washington, D.C., Brussels, or at the UN. The private sector's enormous influence, resources, creativity, and problem-solving power should drive technological advancements that advance freedom and security. Both private and public sector actors must collaborate on activities such as onshoring and nearshoring supply chains, advocating for technical standards that serve freedom and prosperity, growing domestic tech manufacturing bases, accelerating scientific research and development, training skilled workforces, and increasing entrepreneurial access to capital.

4. **Rally and Unify Allies as Force Multipliers:** There is strength in numbers and power in unity and solidarity. Marshalling the free world's unmatched combined economic and technological power is the key to safeguarding freedom amidst a weaponized global tech competition. The free world has superior powers to innovate, outlay capital, set technological standards, merge strategies, and communicate trusted information to the world.

5. **Build a Network of Networks:** Increasing the number of nodes in the Global Trusted Tech Network exponentially expands the private and public entities and individuals committed to developing, deploying and adopting trusted technology that advances freedom. A network of networks bolsters the speed, scale and probability of success.

6. **Create a Value Proposition for Partners:** Untrusted technologies expose investors, countries and ordinary users to security, reputational, economic and financial risks. Actively demonstrate and always articulate the benefits of incorporating trusted technologies over untrusted technologies, rather than merely opposing untrusted alternatives. Prioritizing partnerships and transactions that show clear, shared gains will illustrate how trusted technology contributes to sustainable, mutually beneficial growth, security and prosperity.

7. **Play to Win:** The world is changing, and time is short to protect freedom. Old orthodoxies must be questioned, and in many cases, overturned. A priority must be placed on acting, operating and executing with the confidence and conviction to achieve our vision for a safe, free and prosperous future, rather than the fear of defeat by our adversaries. If the members of the Global Trusted Tech Network act boldly and in concert with one another, it will pave the way for the global triumph of trusted technologies.

SECTION 6

CONCLUSION

THE TECHNO-OPTIMIST MANIFESTO DEVELOPED BY VENTURE CAPITAL FIRM ANDREESSEN HOROWITZ in October 2023 states, "Technology is the glory of human ambition and achievement, the spearhead of progress, and the realization of our potential."[44]

Indeed, this century has seen incredible advances in cutting edge technologies. The benefits are clear, and the sky is the limit for how they can further improve the human experience.

We submit that the people of free nations must unite to move with speed and agility to win the future.

We've drawn lines for what a world of trusted technology should look like and outlined the five priority areas that demand progress quickly and at scale.

We've set forth here a set of Principles of Trusted Tech Diplomacy that a Global Trusted Tech Network must adopt to guide us in our work.

We call on government officials, industry leaders, innovators, educators, and all citizen leaders with an interest in defending freedom, prosperity and security to join us in our movement and mission to ensure that technology advances freedom.

JOIN THE GLOBAL TRUSTED TECH NETWORK

For more information about how you can join the Global Trusted Tech Network and ensure technology advances freedom, reach out to us at **techdiplomacy@prf.org**.

APPENDIX

GLOBAL TECH SECURITY COMMISSION

Co-Chairs

1. **USA:** Keith Krach, Chairman, Krach Institute for Tech Diplomacy at Purdue; Under Secretary of State (2019-2021); Former Chairman and CEO of DocuSign and Ariba
2. **Estonia:** Kersti Kaljulaid, President of Estonia (2016-2021); President of the Estonian Olympic Committee

Tech Sector Commissioners

1. **5G/6G:** General Rob Spalding, Founder & CEO, SEMPRE.ai; Former Senior Director for Strategic Planning, National Security Council; Brigadier General, U.S. Air Force (Retired)
2. **Advanced Manufacturing and Robotics:** Tom Lupfer, President & Founder, Clarity Design, Inc.
3. **Artificial Intelligence and Machine Learning:** Dave Spirk, Senior Counselor, Palantir; Former Chief Data Officer, U.S. Department of Defense
4. **Autonomous and Electric Vehicles:** The Honorable Matt Blunt, 54th Governor of Missouri; President, American Automotive Policy Council
5. **Clean Energy and Electrical Grids:** The Honorable Frank Fannon, Former Assistant Secretary of State for Energy Resources
6. **Cloud Computing:** The Honorable Marcus Jadotte, Vice President, Government Affairs & Public Policy, Google Cloud; Former Assistant Secretary of Commerce for Industry & Analysis
7. **Financial Technologies:** The Honorable Erik Bethel, Managing Partner, Quad Fund, Former U.S. Executive Director, World Bank
8. **Hypersonics:** Dr. Daniel DeLaurentis, Bruce Reese Professor of Aeronautics and Astronautics and Vice President for Discovery Park District Institutes, Purdue University
9. **Quantum and Advanced Computing:** Jake Taylor, Former Assistant Director for Quantum Information Science, and Founding Director of the National Quantum Coordination Office, Office of Science and Technology Policy, White House
10. **Semiconductors and Microelectronics:** Thomas Sonderman, CEO, SkyWater Technology; a DMEA-Accredited Trusted Semiconductor Foundry
11. **Space Technologies and Systems:** Daniel Goldin, Longest-Serving and Former Administrator of the National Aeronautics and Space Administration (NASA), 1992-2001

Strategy Commissioners

1. **Board Strategy:** John O'Connor, Chairman & CEO, J.H. Whitney Investment Management
2. **Capital Markets:** Roger Robinson Jr., Former Senior Director, NSC, Former Chairman, U.S.-China Economic Security Commission
3. **China Expertise:** Miles Yu, Former Principal China Policy Advisor to the U.S. Secretary of State; Professor, U.S. Naval Academy
4. **Data and Cybersecurity:** Andy Geisse, Former CEO, AT&T Business Solutions; Operating Partner, Bessemer Venture Partners
5. **Defense:** General David Stilwell, Brigadier General United States Air Force (Retired); Former Assistant Secretary of State for Bureau of East Asian and Pacific Affairs
6. **Development Finance:** David Fogel, Former Chief of Staff, Export-Import Bank; CEO, NCSS
7. **Diplomacy:** Ambassador Todd Chapman (Ret.), Former Ambassador to Brazil and Ecuador

8. **Economic Security:** Corey Johnston, Head of Strategy, Strider Technologies; U.S. Navy (Retired)
9. **Education:** Henry Stoever, Principal, Brentwood Advisory Group; Former President and CEO, Association of Governing Boards of Universities and Colleges (AGB)
10. **Export Controls:** The Honorable Nazak Nikakhtar, Former Assistant Secretary of Commerce, Industry & Analysis, International Trade Administration
11. **Investment Screening:** CJ Mahoney, Former Deputy United States Trade Representative
12. **IP Protection:** Andrei Iancu, Former Under Secretary of Commerce for Intellectual Property
13. **Lawfare:** Rob Strayer, Former Deputy Assistant Secretary of State for Cyber and International Communications Policy
14. **Logistics:** Michael Kratsios, Former Acting U.S. Chief Technology Officer; Former U.S. Under Secretary of Defense
15. **Media and Countering Disinformation:** Harris Diamond, Former Chairman & CEO, McCann WorldGroup
16. **Microlending:** Greg Nelson, Chief Technology Officer, Opportunity International; Former Senior Vice President, Microsoft
17. **Military-Civil Fusion:** Greg Levesque, Co-Founder & CEO, Strider Technologies
18. **Outbound Investment:** Richard Kang, Founder & CEO, Prism Global; Former Head of Global Strategy, MTV Networks
19. **Prosperity Partnerships:** Dan Negrea, Senior Director, Center for Freedom and Prosperity, Atlantic Council; Former Special Representative, Economic Bureau, U.S. State Department
20. **Supply Chains:** Jim Schwab, Former Director, Office of Management Strategy & Solutions, U.S. State Department; Founding Partner, Crimstone Partners

Country Commissioners

1. **Australia:** The Honorable Tony Abbott, 28th Prime Minister of Australia
2. **India:** Harsh Shringla, Former Foreign Secretary of India; Former Ambassador of India to the U.S.
3. **Israel:** Dr. Eyal Hulata, Israel's former National Security Advisor and head of the National Security Council
4. **Japan:** Tadao Yanase, Senior Executive Vice President, NTT; Former Vice Minister of METI; Former Executive Secretary to Prime Ministers Aso & Abe
5. **Romania:** Pavel Popescu, Vice President, National Authority for Management and Regulation in Communications of Romania (ANCOM)
6. **South Korea:** James Kim, Chairman and CEO, American Chamber of Commerce in Korea; Former CEO of Microsoft Korea & GM Korea
7. **Taiwan:** Audrey Tang, Cyber Ambassador-at-Large, Taiwan
8. **UK:** Sir Iain Duncan Smith, Member of Parliament, Former Leader of the Conservative Party

In addition, each Commissioner assembled an Advisory Council of 5-10 experts to support their analyses and recommendations, and grow the reach of the Global Trusted Tech Network.

Honorary Co-Chairs

The Commission is bipartisan, with numerous Honorary Co-Chairs, most of whom currently or recently served as Members in the U.S. Congress, including:

1. Sen. Tom Cotton (R-AR)
2. Rep. Kat Cammack (R-FL-3)
3. Sen. Joni Ernst (R-IA)
4. Rep. Josh Gottheimer (D-NJ-5)
5. Sen. Bill Hagerty (R-TN)
6. Rep. Ro Khanna (D-CA-17)
7. Rep. Raja Krishnamoorthi (D-IL-8)
8. Rep. Michael McCaul (R-TX-10)
9. Sen. Jeanne Shaheen (D-NH)
10. Rep. Victoria Spartz (R-IN-5)
11. Rep. Ritchie Torres (D-NY-15)
12. Rep. Lori Trahan (D-MA-3)
13. Rep. Mike Waltz (R-FL-6)
14. Sen. Mark Warner (D-VA)
15. Sen. Todd Young (R-IN)

Additional Honorary Co-Chairs:

1. The Honorable Robert D. Hormats, Former Under Secretary of State for Economic Growth, Energy, and the Environment
2. The Honorable Karen Dunn Kelley, Former Deputy Secretary of the U.S. Department of Commerce
3. Lieutenant General H.R. McMaster, U.S. Army (Retired); 26th National Security Advisor
4. Matthew Pottinger, Former Deputy National Security Advisor
5. Alex Wong, Former Chairman of the U.S.-China Economic and Security Review Commission

ENDNOTES

1 List of 23 unicorn startups in Barazil," *Tracxn,* October 21, 2024, https://tracxn.com/d/unicorns/unicorns-in-brazil/__8hyB0gzx2OtUvKmJSyeRmYi5_7jls2YD01MABluXkeQ

2 Michael Mink, "How the Clean Network Alliance of Democracies Turned the Tide on Huawei in 5G," *Life & News Online Edition,* December 2, 2020, https://www.lifeandnews.com/articles/how-the-clean-network-alliance-of-democracies-turned-the-tide-on-huawei-in-5g/

3 Matt Reynolds, "Welcome to E-stonia, the world's most digitally advanced society," *Wired,* October 20, 2016, https://www.wired.com/story/digital-estonia/

4 "The 10 Most Innovative Colleges in America," *US News & World Report,* September 24, 2024, https://www.usnews.com/best-colleges/rankings/national-universities/innovative

5 Cynthia Sequin, "Purdue Ranked 3rd Nationally in Startup Creation," *Purdue University News,* April 28, 2020, https://www.purdue.edu/newsroom/archive/releases/2020/Q2/purdue-ranked-3rd-nationally-in-startup-creation.html

6 Polly Barks, "Boilermaker Research Demonstrates Excellence at Scale: Purdue Ranks in Top 5 in U.S. for U.S. Patents Received," *Purdue University News,* February 15, 2024, https://www.purdue.edu/newsroom/2024/Q1/boilermaker-research-demonstrates-excellence-at-scale-purdue-ranks-in-top-5-in-u-s-for-u-s-patents-received

7 Radina Gigova, "Who Putin Thinks Will Rule the World," *CNN,* September 2, 2017, https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html

8 Matt Pottinger and David Feith, "Opinion: The Most Powerful Data Broker in the World Is Winning the War Against the U.S.," *The New York Times,* November 30, 2021, https://www.nytimes.com/2021/11/30/opinion/xi-jinping-china-us-data-war.html

9 "Generative AI Could Raise Global GDP by 7%," *Goldman Sachs,* April 5, 2023, https://www.goldmansachs.com/insights/articles/generative-ai-could-raise-global-gdp-by-7-percent

10 "Russia Uses Zircon Hypersonic Missile in Ukraine for First Time, Researchers Say," *Reuters,* February 12, 2024, sec. Europe, https://www.reuters.com/world/europe/russia-uses-zircon-hypersonic-missile-ukraine-first-time-researchers-say-2024-02-12/

11 Ken Dilanian, "U.S. Spy Chief: China Has Done Human Testing to Make Super Soldiers," *NBC News,* December 3, 2020, https://www.nbcnews.com/politics/national-security/china-has-done-human-testing-create-biologically-enhanced-super-soldiers-n1249914

12 Kate Irwin, "Chinese Researchers Reportedly Crack Encryption With Quantum Computer," *PC Mag,* October 14, 2024, https://www.pcmag.com/news/chinese-researchers-reportedly-crack-encryption-with-quantum-computer?utm_source=substack&utm_medium=email

13 William Alan Reinsch and Andrea Leonard Palazzi, "Cryptocurrencies and U.S. Sanctions Evasion: Implication for Russia," The Center for Strategic and International Studies, December 20, 2022, https://www.csis.org/analysis/cryptocurrencies-and-us-sanctions-evasion-implications-russia

14 Mario Draghi, *Address to the EU Parliament: Presentation of the Report on the Future of European Competitiveness*, (Strasbourg, France: September 17, 2024), p. 3, https://commission.europa.eu/document/download/fcbc7ada-213b-4679-83f7-69a4c2127a25_en?filename=Address%20by%20Mario%20Draghi%20at%20the%20Presentation%20of%20the%20report%20on%20the%20future%20of%20European%20competitiveness.pdf

15 Ibid.

16 Ibid, p. 9.

17 Michelle Giuda, "Winning the Tech Race: Why American CEOs Must Lead, Not Follow," *The National Interest*, August 23, 2024, https://nationalinterest.org/blog/techland/winning-tech-race-why-american-ceos-must-lead-not-follow-212435

18 Raj S. Dave, "What it Means that Russian Businesses Can Now Legally Steal Intellectual Property from 'Unfriendly Countries'," *IP Watchdog*, March 16, 2022, https://ipwatchdog.com/2022/03/16/russian-businesses-can-now-legally-steal-intellectual-property-unfriendly-countries/id=147528/

19 "Investigation by Select Committee on the CCP, House Homeland Finds Potential Threats to U.S. Port Infrastructure Security from China," House Select Committee on the Chinese Communist Party, Press Release , September 12, 2024, https://selectcommitteeontheccp.house.gov/media/press-releases/investigation-select-committee-ccp-house-homeland-finds-potential-threats-us

20 Jamie Gaida et al., "ASPI's Critical Technology Tracker," *The Australian Strategic Policy Institute*, March 1, 2023, http://www.aspi.org.au/report/critical-technology-tracker

21 "Remaking U.S. Global Leadership in the Age of Technology Competition," In *Remaking U.S. Global Leadership in the Age of Technology Competition*, Special Competitive Studies Project, September 2022, https://www.scsp.ai/reports/mid-decade-challenges-for-national-competitiveness/chapter-4/

22 *The Stanford Emerging Technology Review*, October 2023, p. 10, https://setr.stanford.edu/sites/default/files/2023-11/SETR_web_231120.pdf

23 Brian Kennedy, "Most Americans Think U.S. K-12 STEM Education Isn't above Average, but Test Results Paint a Mixed Picture," *Pew Research Center*, April 24, 2024, https://www.pewresearch.org/short-reads/2024/04/24/most-americans-think-us-k-12-stem-education-isnt-above-average-but-test-results-paint-a-mixed-picture/

24 "Report of PISA 2022 study outlines worsening educational performance and deeper inequality," *The European Commission*, February 12, 2004, https://education.ec.europa.eu/news/report-of-pisa-2022-study-outlines-worsening-educational-performance-and-deeper-inequality#:~:text=30%25%20of%20EU%20students%20don,background%20are%20underachieving%20in%20mathematics

25 Kristen Eichensehr, "International Cyber Governance: Engagement Without Agreement?," *Just Security*, February 2, 2015, https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/

26 "China in International Standards Setting: USCBC Recommendations for Constructive Participation," *The US-China Business Council*, February 2020, https://www.uschina.org/sites/default/files/china_in_international_standards_setting.pdf

27 Zhang Tong, "China Sets Some Global Standards for 6G Tech as It Looks towards Next-Gen Communications," *South China Morning Post*, September 13, 2024, https://www.scmp.com/news/china/science/article/3278257/china-sets-some-global-standards-6g-tech-it-looks-towards-next-gen-communications

28 Mark Montgomery and Theo Lebryk, "China's Dystopian 'New IP' Plan Shows Need for Renewed US Commitment to Internet Governance," *Just Security*, April 13, 2021, https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/

29 Nick Cumming-Bruce, "U.S.-Backed Candidate for Global Tech Post Beats China's Nominee," *The New York Times*, March 4, 2020, sec. Business, https://www.nytimes.com/2020/03/04/business/economy/un-world-intellectual-property-organization.html

30 Keith Bradsher, "Amid Tension, China Blocks Vital Exports to Japan," *The New York Times*, September 23, 2010, sec. Business, https://www.nytimes.com/2010/09/23/business/global/23rare.html

31 Saheli Roy Choudhury, "Here's a List of the Australian Exports Hit by Restrictions in China," CNBC, December 18, 2020, https://www.cnbc.com/2020/12/18/australia-china-trade-disputes-in-2020.html

32 Emily Benson and Thibault Denamiel, "China's New Graphite Restrictions," *Center for Strategic and International Studies*, October 23, 2023, https://www.csis.org/analysis/chinas-new-graphite-restrictions

33 Jordan Robertson and Michael Riley, "The Long Hack: How China Exploited a U.S. Tech Supplier," *Bloomberg*, February 12, 2021, https://www.bloomberg.com/features/2021-supermicro/

34 Roger W. Robinson Jr., "Leveling the Playing Field: How to Counter the CCP's Economic Aggression," Statement Before the U.S. House of Representatives Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, May 17, 2023, p. 17, https://docs.house.gov/meetings/ZS/ZS00/20230517/115974/HHRG-118-ZS00-Wstate-RobinsonR-20230517.pdf

35 Under Secretary of State Keith Krach, Letter to the Governing Boards of American Universities, August 18, 2020, https://2017-2021.state.gov/letter-from-under-secretary-keith-krach-to-the-governing-boards-of-american-universities/

36 "Communist Chinese Military Companies Listed Under E.O. 13959 Have More Than 1,100 Subsidiaries," U.S. Department of State, January 14, 2021, https://2017-2021.state.gov/communist-chinese-military-companies-listed-under-e-o-13959-have-more-than-1100-subsidiaries/

37 Angus Berwick and Tom Wilson, "Crypto exchange Binance helped Iranian firms trade $8 billion despite sanctions," *Reuters*, November 7, 2022, https://www.reuters.com/business/finance/exclusive-crypto-exchange-binance-helped-iranian-firms-trade-8-billion-despite-2022-11-04/

38 Robinson, "Leveling the Playing Field," p. 8

39 "MITRE-Harris Poll Finds U.S. Public Is Worried about the Security of Our Critical Infrastructure," *The MITRE Corporation*, March 13, 2024, https://www.mitre.org/news-insights/news-release/mitre-harris-poll-finds-us-public-worried-about-security-our-critical

40 Alessandro Parodi and Alexander Marrow, "Foreign Firms' Losses from Exiting Russia Top $107 Billion," *Reuters*, March 28, 2024, https://www.reuters.com/markets/europe/foreign-firms-losses-exiting-russia-top-107-billion-2024-03-28/

41 Krach Institute Unveils World's First Tech Diplomacy Academy, Pioneering a New Era of Global Leadership," *Krach Institute for Tech Diplomacy*, April 30, 2024, https://techdiplomacy.org/news/krach-institute-unveils-tech-diplomacy-academy/

42 Alice Cattley, "Why These 27 Western Brands Are Abandoning China," *Yahoo Finance*, March 1, 2024, https://uk.finance.yahoo.com/news/why-27-western-brands-abandoning-170200239.html

43 Robinson, "Leveling the Playing Field," p. 11

44 Marc Andreessen, "The Techno-Optimist Manifesto," *Andreessen Horowitz*, October 16, 2023, https://a16z.com/the-techno-optimist-manifesto/

About the Krach Institute for Tech Diplomacy at Purdue:

The Krach Institute is the world's preeminent trusted technology accelerator. As the leader in the new category of Tech Diplomacy, the Institute integrates technology expertise, Silicon Valley strategies and foreign policy tools to build the Global Trusted Tech Network of governments, companies, organizations and individuals to accelerate the innovation and adoption of trusted technology and ensure technology advances freedom.

Visit the Krach Institute online at **TechDiplomacy.org** and follow us on X, Facebook, LinkedIn and YouTube.



GLOBAL TECH SECURITY COMMISSION

