Statement before the House Committee on Science, Space, and Technology
On *The United States, China, and the Fight for Global Leadership: Building a U.S. National Science and Technology Strategy.*

The New Superpowers

How and Why the Tech Industry is Shaping the International System

Klon Kitchen
Senior Fellow

February 28, 2023

The American Enterprise Institute (AEI) is a nonpartisan, nonprofit, 501(c)(3) educational organization and does not take institutional positions on any issues. The views expressed in this testimony are those of the author.

Opening Statement

Good morning. Chairman Lucas and Ranking Member Lofgren, thank you for the opportunity to testify before this committee.

The United States' science and technology enterprise is strong and continues to be the envy of the world. American companies are pioneering and deploying innovations and technology that can expand human thriving, broaden economic prosperity, and ensure our national security for generations to come.

But to do these things, we must deliberately address three key challenges to the American science and technology enterprise.

First, we must confront Chinese technological theft and aggression. Beijing, like Washington, understands that emerging technologies like artificial intelligence (AI), robotics, and quantum science will decisively shape tomorrow's societies, economies, and battlefields and that these innovations are overwhelmingly being developed in the private sector. But unlike the United States, the People's Republic of China is not committed to free and fair competition in global innovation. Instead, the Chinese Communist Party (CCP) is coopting its innovation industry and using it as an extension of the state for traditional and economic espionage that FBI Director Christopher Wray says surpasses "every other nation combined" and "represents one of the largest transfers of wealth in human history."

Whether through social media companies like TikTok, drone companies like DJI and Autel, or smart device companies like Tuya, the U.S. science and innovation enterprise—which spans the public and private sectors—is hemorrhaging data and intellectual property and could soon bleed out if these losses are not stopped.

Second, we must help allies understand that a strategy of "regulate first and ask questions later," will hurt—not help—all of us and risks ceding the advantage to Beijing. Other governments, particularly those in the European Union (EU), are enacting laws that deliberately target American innovation companies, preference domestic champions, and threaten to splinter the internet itself into a series of "mininets," each running on incompatible infrastructure and governed by contradictory rules. Even more, the economic scarcity that would inevitably follow such a splintering would leave these partners more susceptible to the siren song of cheap cloud services and other offerings from China, which are heavily subsidized by CCP, as previously discussed, for the express purpose of stealing a country's data and wealth. If this happens, many of our friends will have lost their sovereignty and security in their bid to keep them.

Finally, domestic debates about technology and innovation must be constrained by facts and by geopolitical realities. Every institution and industry must be held accountable to U.S. law and national security concerns cannot be wantonly employed as a "get out of jail free" card. Neither, however, should perceived—but unsubstantiated—political grievances be used to justify counterproductive, or even unconstitutional, actions against the very science and technology enterprise at the heart of our individual and national prosperity.

Pushing the frontiers of science and pioneering game-changing technologies is expensive.

The resources and talent to do these things are highly valuable and desperately scarce. It is no coincidence, then, that the companies that have found ways to attract billions of customers — and the profits that come with them — are the ones at the center of our science and technology enterprise. They can innovate at scale *because* they operate at scale.

Instead of railing against these companies because of their size, we instead should be thankful that our free-market economy has produced an alignment of interests where private-sector actors can generate wealth and jobs while also developing capabilities that will provide for the common defense. This uniquely American advantage may well be decisive in an era of escalating geopolitical competition. It would be reckless to give it away.

While there is much more that I could say, I'll end my remarks there.

Thank you again for this opportunity and I look forward to your questions.

Background

Technology is always a key variable in geostrategic change. The sailboat, gun powder, the steam engine, the internal-combustion engine, nuclear power, modern communications and information technology – these and other innovations revolutionized their respective eras and changed the fortunes of nations. So it is today. The so-called "fourth industrial revolution" is shaping and re-shaping the contours of the emerging global order. Even more, the companies at the heart of this revolution are fast becoming powerful geopolitical stakeholders that often challenge the authority, sovereignty, and the capacity of governments. Three trends have special prominence in driving this change.

First, a growing number of technology companies have global interests and influence. In 2016, global technology spending exceeded $6.3 trillion, making it the "third largest economic 'force' in GDP terms, surpassed only by the United States … and China."[i] One report predicts that by 2023, more than 50 percent of world-wide GDP will be driven by services and products from digitally transformed industries.[ii] In 2018 alone, Apple brought in $265.6 billion in net revenue; Amazon earned $232.9 billion; Google's parent company, Alphabet, earned $136.8 billion; Microsoft earned $110.4 billion; and, Facebook earned $55.8 billion.[iii] These five companies alone constitute more than $801.5 billion in annual revenue (not even net worth), which is roughly the size of Saudi Arabia's nominal GDP in 2018.[iv] But this is about more than money, it is about the influence these resources command.

There is perhaps no industry more globalized than the technology industry. All of the companies mentioned above, for example, compete in every major market around the world, conduct research and design in multiple countries, and employ a globally derived and deployed talent pool to develop and to build their products and services. This, then, translates into an expanding global presence and a growing lists of corporate interests that transcend national boundaries and that directly influence, and are influenced by, geopolitical events. Put simply: the world's largest technology companies are amassing a level of wealth, influence, international presence, and transnational interests that was previously only enjoyed by states. But these companies are more than just players in the game of global politics, they are often the arena itself.

The second trend driving the rise of technology companies in geopolitics is the expanding presence and role of digital and social media. While propaganda and so-called "active measures" have long been a feature of geopolitical engagement, Russia's interference in the U.S.'s 2016 presidential elections – and in a number of other foreign elections since – places in stark relief the reality that modern communications technology and social media platforms are combining to produce an unparalleled tool for legitimate political discussion and action, but that these tools also extend to bad actors. Even more, the burden for preventing, identifying, and confronting this interference largely falls to the companies themselves. Political leaders may punish companies for not preventing misinformation on social media, but governments can do little by themselves to stop it.

Governments all over the world are asking, begging, and even threatening these companies in an effort to get their collective hands around the challenge; but, there is very little that political leaders can unilaterally do to dramatically improve the situation. The difficult reality that many are struggling to adapt to is that private sector technology actors have built a capability for wide-scale political influence that largely falls outside of the control of political leaders. And this asymmetry is indicative of an even broader realty.

The third and final critical trend is that technology companies are a, if not the, center of gravity in the development of critical national security capabilities and methodologies. Governments have always sought to observe, to understand, to predict, and to shape human behavior and events. These are essential aspects of what is historically called, "intelligence." Technology companies call this "market research," "product development," or "service provisioning." Regardless of the euphemism used, the plain truth is that the state has lost its monopoly on intelligence and private sector actors know more about individuals and societies than any government spy agency – perhaps even more than all government spy agencies. This is why the short-hand "surveillance capitalism" is sometimes used to describe the business model of the world's tech titans, and the term "surveillance" is appropriate when considering their ability to collect and to understand data.

It is estimated that more than 5 billion people (roughly 65% of the global population) have mobile devices and that half of these devices are smartphones.[v] Nearly all of these people (approximately 4.17 billion) can be considered "mobile internet users" and this number is expected to nearly-double by 2021.[vi] As more users are brought online, so is their data and this data provides powerful insights. As the Electronic Frontier Foundation (EFF) observes in its report, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*:

Every smartphone is a pocket-sized GPS tracker, constantly broadcasting its location to parties unknown via the Internet. Internet-connected devices with cameras and microphones carry the inherent risk of conversion into silent wiretaps … But these better known surveillance channels are not the most common, or even necessarily the most threatening … The most prevalent threat to our privacy is the slow, steady, relentless accumulation of relatively mundane data points about how we live our lives. This includes things like browsing history, app usage, purchases, and geolocation data. These humble parts can be combined into an exceptionally revealing whole. Trackers assemble data about our clicks, impressions, taps, and movement into sprawling *behavioral profiles*, which can reveal political affiliation, religious belief, sexual identity and activity, race and ethnicity, education level, income bracket, purchasing habits, and physical and mental health.[vii]

While not all observers share EFF's alarm, their observation is undeniable – digital data collection grants these companies unparalleled insight into human behavior which, in turn, gives them unparalleled capabilities to predict and to shape this behavior. For example, both Google and Facebook have filed patents that use historical location data and offline behaviors to accurately predict where users will be in the future, even years in the future, so that the companies can pro-actively serve up contextually-relevant ads and services.[viii] While not inherently nefarious, this is a powerful capability. A capability that demonstrates not just the ability to generate and to collect data, but also to understand and to leverage this data. Something accurately described as "intelligence analysis."

Simply having data is not valuable. Having the ability to interrogate and to exploit that data is crucial for realizing its value, and private companies are the ones leading the development of analytic tools and methodologies for realizing this value. Perhaps most importantly, by employing artificial intelligence (AI).

AI can be understood as the use of machines to accomplish tasks that normally require human intelligence, such as decision-making, image recognition, and language translation. Around 2012, the AI sub-discipline of "machine learning" took a big leap forward when advancing computer science, specialized hardware, and large volumes of digitized data combined to enable a new type of programming that greatly reduces the burden of training AI algorithms – sparking a renaissance of AI applications that already touch many American lives far beyond their smartphones. Hospitals use them to diagnose diseases and to predict inpatient mortality rates. Insurance and mortgage companies use them to assess risk. Law enforcement use them for "predictive policing" while our judicial system is testing them in sentencing formulas. These algorithms even conduct as much as 80% of daily trades on the U.S. stock exchange.[ix] The application potential of AI is far-reaching, including into the realm of defense and national security.

It is an overstatement to say that all governments are trailing woefully behind the private sector in the development of AI; but, even the most advanced governments – like those in the United States and in China – are hobbled by the inherent slowness of bureaucracy and by an acute lack of technical competence. Governments can partner with academic and commercial partners to conduct and to support research; but, they seemingly cannot attract the human talent necessary to implement and leverage this research at the scale or speed necessary for keeping up with national security requirements. And this is equally true regarding other technologies beyond AI. The inescapable fact is that the growing data and capability gaps between the private sector and governments leaves national security leaders increasingly dependent on technology companies to conduct core national security missions. This is why former Chairman of the U.S.'s Joint Chiefs of Staff, GEN(ret) Joe Dunford, observed, "Our ability to leverage industry here in the United States; our ability to maintain a technological edge over any potential adversary, is going to very much depend on the partnership between industry and the Department of Defense."[x] (Garamone, 2019)

Do not miss the import of this statement: the former senior military advisor to the President of the United States is saying that the nation's ability to secure itself "depends" on partnering with the private sector in some new and sustained way. This same sentiment is shared by political leaders around the world and is being expressed in three general government reactions.

Three Government Responses to Tech's Growing Geopolitical Influence

The migration of geopolitical influence into the private sector is provoking a range of government responses. These responses are rooted in a number of variables, including a nation's specific political form, its relative economic strength, and its broader global ambitions. Specifically, the responses from the United States, China, and Europe are helpful for understanding the evolving relationship between technology and governance.

The United States: "Engage and Invest"

The U.S. response can be summarized as "engage and invest." American policymakers are consistently being told by national security leaders that the nation's "overmatch" capability – the U.S.'s relative military superiority over its international competitors – is eroding and that the speed of this erosion is increasing. Additionally, in light of the point made above about private companies being a significant source of modern national security capabilities, these policymakers are being told that this capability deficit is not simply a matter of funding. The U.S. cannot write a check big enough to erase our losses and to ensure our long-term superiority. We are dependent, as Dunford said, on private sector actors. Unfortunately, "big tech" responses to government overtures have been uneven.

Companies like Microsoft and Amazon, both of whom are competing over a $10 billion contract to provide cloud services for the Pentagon, have clearly signaled their intent to work with the Federal government. Amazon CEO Jeff Bezos, for example, has called on other tech companies to work with the U.S. government, calling the nation "the good guys." "I know it's complicated, but do you want a strong national defense or don't you? I think you do," says Bezos.[xi] Similarly, Microsoft CEO Satya Nadella responded to critics of his company's government work, saying, "…[W]e're not going to withhold technology from institutions that we have elected in democracies to protect the freedoms we enjoy."[xii] Other tech leaders, however, have gone a different way – most notably, Google.

In 2018, Google ended its participation in the Pentagon's multifaceted AI research effort, Project Maven. The decision followed the publication of a protest petition that was signed by more than 4,000 Google employees and after 12 of the company's engineers resigned. The petitioners maintained that, "…Google should not be in the business of war" and that the company's participation in Project Maven violated their informal oath to not to be "evil." Whether motivated by practical or ideological reasons, Google leaders acquiesced to the complaint by withdrawing and by issuing a set of AI principles that include prohibitions against using AI for "weapons," "surveillance," or threatening "human rights." The company has not issued a statement reconciling these AI principles with its new AI research center in China, where more than one million religious and political minorities are being surveilled, imprisoned, brainwashed, and murdered.

Obviously, there are a large number of small and medium technology companies who are more than happy to work with the federal government; however, generally, the most interesting work on some of the most consequential technologies is being done by the large technology companies who must navigate complex fiduciary and consumer requirements and demands. Even so, U.S. political and national security leaders continue to engage with technology leaders and are hopeful that a more robust and systemic collaboration will be established. But hope is not the U.S.'s only strategy. The government is also making large investments in these technologies.

For example, the President's 2020 budget prioritizes AI as one of four "Industries of the Future," and sets aside $1 billion for non-defense-related AI. While much of the national security spending on AI is classified, the Defense Advanced Research Projects Agency's (DARPA) "AI Next" campaign will invest more than $2 billion in the technology over multiple years. The administration has also issued an executive order establishing the "American AI Initiative" and it has published an "AI R&D Strategic Plan." The latter of these efforts identifies key AI priorities, including (1) long-term investments (2) human-AI collaboration (3) ethical, legal, and social implications of AI (4) AI safety and security (5) public datasets and training areas (6) AI standards and benchmarks (7) the AI workforce and (8) expanding private-public partnerships.

These and other government efforts on technologies like quantum science, bio-technologies, and advanced synthetic materials demonstrate that Washington understands the importance and long-term necessity of these capabilities; but, the nation's ability to fully leverage the capacity of the private sector towards these ends remains unproven. Doing so will be difficult and it will be made even more difficult by the U.S.'s historical aversion to formalized industrial policy and by a general "hands-off" approach when it comes to government interference with private sector economic activity. The U.S. derives many benefits from these approaches; but, they do come at a cost.

The Chinese have opted for another approach.

China: "Fuse and Use"

China's response to the growing role of technology in geopolitical affairs is to "fuse and use." Before unpacking this further, two observations will be helpful.

First, China is like every other nation in the history of the world, in that it seeks to amass and to wield geopolitical influence in an effort to secure and to advance its national interests. This is rational and the only coherent way for nations to operate within the global system. Further, a series of official Chinese strategies makes it clear that the Chinese Communist Party (CCP) believes their nation must lead in at least 10 technology-related industries[1] if it wants to effectively build and employ this influence in the emerging international system. Again, this assessment is sound and this approach is coherent.

A second observation concerns why China has made these conclusions – specifically as a response to U.S. technical and military superiority. After observing the U.S. advanced warfighting capabilities during Operation Desert Storm, then Chinese President Jiang Zemin directed his military leaders to be ready to fight "local wars under high technology conditions."[xiii] This, then, set off a national effort to reassert China's technological leadership that has since been adopted and expanded by President Xi Jingping – which brings us to "fuse and use."

In their excellent report, *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics*, former Deputy Secretary of Defense Robert O. Work and co-author Greg Grant, describe the Chinese strategy for achieve technological dominance as having three distinct phases. Phase One begins with Beijing competing with Washington from a position of technological inferiority and focuses on closing key capability gaps. Phase Two begins when China establishes rough technological parity, allowing the country to deter U.S. intervention within China's strategic area of influence (i.e., East Asia). Finally, Phase Three constitutes the desired end state where China has surpassed American technological leadership and is able to confidently project its influence as far abroad as is necessary.[xiv] In all three phases, Chinese civil society and private sector entities plays a key role.

Historically, China has never made a clear distinction between its public and private sectors. Instead, for at least the last 60 years, China has employed what scholar Branko Milanovic calls "political capitalism," which has three defining features:

First, the state is run by a technocratic bureaucracy, which owes its legitimacy to economic growth. Second, although the state has laws, these are applied arbitrarily, much to the benefit of elites, who can decline to apply the law when it is inconvenient or apply it with full force to punish opponents. This arbitrariness of the rule of law in these societies feeds into political capitalism's third defining feature: the necessary autonomy of the state. In order for the state to act decisively, it needs to be free from legal constraints. The tension between the first and second principles – between technocratic bureaucracy and the loose application of the law – produces corruption, which is an integral part of the way the political capitalist system is set up, not an anomaly.[xv]

It is within this system that Chinese (and foreign) technology researchers and companies operate, an environment where the state is unbound by law and totally free to direct, subsidize, and coerce private sector support for official government priorities and policies.

In the case of national security related policies, this is known as "military-civil fusion."

In 2018, You Zheng, Vice President of China's Tsinghua University (often called "China's MIT"), wrote an article, outlining the university's commitment to supporting the state – specifically on the development and use of AI:

In accordance with central requirements, Tsinghua University will closely integrate the national strategy of military-civilian integration and the AI superpower strategy. Tsinghua University was entrusted by the CMC [*Central Military Commission*] Science and Technology Commission to take responsibility to construct the High-End Laboratory for Military Intelligence (军事智能高端实验室). With regard to basic theories and core technologies, military intelligence and general AI possess commonalities. Therefore, Tsinghua University regards the construction of the High-End Laboratory for Military Intelligence as the core starting point for serving the AI superpower strategy…. Therefore, Tsinghua University insists on basic research as a support in applied technology research in AI talent training and scientific research innovation, with military requirements as a guide, promoting the development of basic AI research.[xvi]

Put simply: China's leading engineering and computer science university, "in accordance with central requirements", makes no distinction between basic AI research and its application to state and military requirements. This fusion extends beyond the academy and to "private" companies as well, with Beijing even using these companies as extensions of the state. Huawei is a prime example of this "fuse and use" strategy.

In 1987, a former military technologist and officer in the Chinese People's Liberation Army (PLA), Ren Zhengfei, started the Huawei telecommunications company. Since then, the company has become one of the world's leading providers of telecommunications hardware, software, and services – often with direct and indirect support from the Chinese government. In response to this support, intelligence services around the world assess the company routinely steals intellectual property from other companies and nations – feeding these innovations into its own research and design efforts as well as those of the government. Its deployed infrastructure is also suspected of operating as a type of backbone network for much of Beijing's technical espionage around the world. For example, in 2012 the Chinese government "gifted" a new headquarters building to the African Union in Addis Ababa, Ethiopia. Huawei and another Chinese company, ZTE, were tasked with providing the head quarter's computer and communications networks. After five years of operating, it was discovered that all of the Union's confidential data and communications was copied and forwarded to Chinese servers every single night. This is just one of many examples of how just this one technology company operates on behalf of the Chinese government. There are many, many more.

"Fuse and use" is further supported by a growing list of cybersecurity and national security laws in China that require all companies, even wholly foreign owned companies, to arrange and manage their computer networks so that the Chinese government has access to every bit and byte of data that is stored on, transits over, or in any other way touches Chinese information infrastructure. It will even include data on U.S. persons collected by Chinese companies like TikTok, WeChat, and Alibaba. Any data that it not automatically collected and turned over to the government must be provided upon request, according to *The National Security Law of the People's Republic of China* that was enacted in 2015 and updated in 2017.

All of this is emblematic of the nation's response to the growing import of technology within geopolitical affairs and its implications extend far beyond China's borders.

Europe: "Strangle and Surrender"

In the cases of the U.S. and China, where both countries have robust domestic technology industries, the governments seek to leverage these companies in support of national security – the former through voluntary cooperation based on shared interests and the latter through incentivized and coerced partnership based on the power of the state. In Europe, where the technology industrial bases is comparatively weak, governments appear to be content with strangling technological innovation with regulations while simultaneously surrendering their national and cyber security to foreign actors – though, there are some reasons for hope.

The most sweeping action taken in Europe in dealing with technology companies has been the European Union's (EU) passage of the General Data Protection Regulation (GDPR). The law is a hodgepodge of regulations spelled out in 11 chapters, covering "general provisions", "principles", "rights of data subject", duties of data controllers or processors, transfers of personal data to third countries, "supervisory authorities", "remedies", "liabilities and penalties", and other miscellaneous provisions. GDPR is so bloated and cumbersome that Google, one of the largest, most profitable companies in the history of mankind, says it has spent "hundreds of years of human time" (Rodriguez, 2018) coming into compliance with GDPR.[xvii] Now imagine being a would-be disruptor in someone's garage and having to navigate these requirements – you would have no chance. GDPR and Europe's general regulatory heavy-handedness is precisely why these nations struggle to field meaningful technological innovation are likely to do so going forward. Even worse than strangling their own technological industrial base, is Europe's seemingly naïve integration of Chinese technology into their critical networks and markets.

Despite clear warnings from the United States and often from their own intelligence services, Germany, France, Italy, and others are actively considering allowing Huawei to supply, or at least have a significant presence in, their burgeoning fifth-generation (5G) wireless networks. This is despite clear signals that doing this could endanger U.S. willingness to share critical intelligence with these countries. When pressed on these decisions, European political leaders often opine about the lack of alternative providers and the significant costs savings that can be realized by going with Chinese companies (Huawei's bid in Italy, for example, is as much as 2/3 cheaper than all of the other bids). What these leaders seem to be unwilling to ask is, how and why are the Chinese bids so much cheaper?

As discussed previously, the Chinese government will subsidize their domestic companies to allow them to underbid competitors and to gain larger market share around the world. This allows the companies greater access to new markets and expands Beijing's political and technical influence as well. If profit is not the motive for Chinese companies bidding for European technology contracts, then political leaders ought to ask themselves what is the real motivation?

It has become popular recently, for EU leaders to say they will mitigate the cybersecurity threats associated with Huawei and other Chinese companies by adopting stringent security requirements and by keeping these companies out of critical portions of their networks. This is foolishness. First, it misunderstands how next-generation wireless networks work. Legacy distinctions between critical and non-crucial nodes of the network are largely being erased and it is not reasonable to believe threats can be contained within non-sensitive areas. It is also not safe or sane to make an existential bet that you will always be able to prevent one of the world's top cyber threats from critically compromising your networks. Second, even if they could mitigate software vulnerabilities and so-called "backdoors," they will have done nothing about Beijing's domestic laws that grant them unfettered digital access to any and all traffic found on the networks of Chinese companies – wherever they are operating. As frightening as these decisions and justifications are, the reality behind them is even more concerning.

Decades of government mismanagement, spending, and general neglect are leaving a large number of European capitals unable and unwilling to make the hard choice of foregoing near-term economic benefit in return for long-term security. As these governments continue to default on their myriad promises of cradle-to-grave entitlements, they will also bleed political legitimacy in the eyes of their constituents and, therefore, become more desperate to provide economic "wins" and critical services – even if it means subjecting themselves to Chinese aggression and coercion. The truth of this is already demonstrated in the fact that 23 European countries have signed agreements under China's predatory "belt and road initiative," 19 of whom are in the EU and one of whom (Italy) is in the G7.

To summarize: Without a strong technological industrial base, and in the face of mounting governance failures, many European countries appear to be making catastrophic security decisions in an effort to placate public dissatisfaction and to keep up with the technological advancements emanating from the United States and China.

Two Necessary Adjustments

All of the above leads to two necessary adjustments.

First, the government must accept the reality that it is *a* national security stakeholder and not *the* stakeholder. Many of the world's leading technology companies have global interests and influence on par with many nations -- they have a legitimate place at the geopolitical table.

For example, when it comes to encryption, some government officials dismiss tech companies as standing in the way of national security. This is a myopic caricature of reality.

Encryption is critical to securing private communications, financial systems, intellectual property and other trade secrets. A private company's commitment to securing this data should not make them the enemy -- it makes them an ally. Efforts to secure themselves and their customers against hostile online actors is as essential for our national security as is anything done by the federal government.

To be clear, the case for special access to encrypted materials can be one with noble objectives and intentions; but, technology has changed to make such access detrimental to cybersecurity and data integrity, with no guarantee of success. Policymakers and national security leaders should recognize this and be persistent in trying to find collaborative approaches with industry — recognizing that patience will be required.

Proactively, Washington can best demonstrate its intent to be a true partner with the tech industry in the way it shares information and purchases technology.

On the information sharing side, for too long, the U.S. government has treated information exchange with industry as a one-way street -- demanding "real-time" information sharing from private companies on cybersecurity and other threats while being painfully slow in sharing with industry its own insights about malicious actors, their intentions and their capabilities.

There are early signs this might be changing. The NSA's release of its Ghidra tool is a good example of the government proactively treating industry as a partner. This software reverse engineering framework was developed by Fort Mead for its national security mission but its release to the public allows private sector security personnel to better defend themselves as well.

We've also seen some promising signs out of Cyber Command. It has taken to publishing adversaries' malware samples to public repositories visible to private sector cybersecurity professionals.

As for purchasing and procurement, the government's rigid and outdated acquisition bureaucracy makes it difficult for new technology companies to help Washington, because they need to spend precious resources on engineers and coders rather than hordes of contract specialists and lawyers.

Organizations like the Pentagon's Defense Innovation Unit and the CIA's In-Q-Tel are good at technology scouting and at strategic investment. But we still struggle to transition these technologies from niche experimental programs into stable, long-term solutions.

To put it bluntly, there's plenty of capital in innovation, but these companies do not need government "investment," they need government contracts.

But none of these very real frustrations with the government excuses firms from the responsibilities that come with their growing global influence.

It is precisely because they are amassing this power and influence, and because they are enabled to do so only under the military, legal, and economic protections of the U.S.

government, that these companies must also change.

Specifically, American technology companies must acknowledge their growing national security responsibilities. They must also accept the fact that great power competition is returning and that this return requires them to choose sides.

While the Chinese market may be lucrative, it is also a moral minefield and ultimately a dead end for Western companies.

American companies' submission to Beijing's predatory demands on intellectual property, proprietary information, trade secrets, data and other assets weakens American economic competitiveness, individual and national cybersecurity, and broader national security to the degree that this capitulation enables China's technological ascendance over the U.S. This participation also gives cover to Beijing's rampant political oppression and human rights violations.

The business risk is extreme, too. Just consider the experience of Microsoft: some 90 percent of Chinese firms use the company's operating system, but only 1 percent actually pay for it. This, according to former Microsoft CEO Steve Ballmer[xviii], costs the company more than $10 billion in profits. But, thus far, such losses have been accepted as the cost of doing business in what, until recently, was the world's fastest growing market.

But companies that chase short-term profits in the Chinese market over long-term stability are in for a rude shock.

Ultimately, western technology companies and the US government must recognize that the long-term interests of both are better served through national security partnerships. They should do this out of patriotism, out of economic interest, and because these partnerships enable the expansion of truly free markets and human thriving around the world.

Concluding Thoughts for Conservatives

The growing influence of technology companies within the international order provokes a complex calculus where values, interests, and objectives must constantly be balanced. It is especially important that Conservatives and others on the political right think deeply about these issues and that they recognize four important factors.

First, technology companies and their capabilities are a key center of gravity in a global contest between liberal democratic society and technologically-enabled authoritarianism. The U.S. and China are both leveraging these companies in the pursuit of broader ends and, despite how powerful these companies are becoming, they are still subject to the will and power of states. If the Chinese model of "fuse and use" is not arrested and pushed back, it will become the chief export along Beijing's belt and road initiative. A number of autocratic leaders are already working with the Chinese government and Chinese companies to build their own version of Sino surveillance state. How the U.S. engages and leverages its own technological industrial base will decisively influence its ability to confront this authoritarian expansion.

Second, the U.S. government must expand its organic capabilities for technological research and design while also dramatically improving its ability to discover and to integrate privately derived innovations before our strategic competitors. Conservatives have always understood that a strong, comprehensive national security enterprise is essential for peace and prosperity. Advocating for these policies was easier and more straight-forward when it largely only meant more money for personnel, bombs, and airplanes. But now that commercial technologies like AI and quantum computing are likely to be decisive, Conservatives must grow comfortable with government-driven exploratory research and adopt a higher risk tolerance for these programs. Relatedly, because so much private sector research is conducted and published publicly, the U.S. government needs to find ways of identifying and acquiring the most important research before our strategic competitors do. Or, at the very least, we need to lessen the friction of transitioning these general research efforts into specific programs of record and acquisition.

Third, the deep integration of the U.S.'s chief rival, China, into its economy and Beijing's policy of "military-civil fusion" challenges many of Conservatism's political orthodoxies – particularly a certain strain of free market fundamentalism. For many in the conservative movement, the idea of a U.S. industrial policy is considered heresy and is an unthinkable political option. While the concerns associated with such a policy are legitimate, they do not lessen the reality that sectors of America's technological industrial base are critical to national security and that many of these same sectors are equally important to the nation's international trade. The distorting economic impacts of China's coercive economics must be accounted for and we cannot allow the natural "efficiencies" of markets to produce unacceptable national security outcomes.

A growing realization of this reality is demonstrated in the U.S.'s recent responses to the development of 5G and the Chinese owned social media application, TikTok. In both cases, because of legitimate national security concerns, the government has intervened and constrained a Chinese company from "freely" competing. The justifications for these actions extend to a host of foreign technologies and companies currently in the U.S. marketplace – all of which demand attention. But we cannot simply be defensive.

As discussed, the technologies that will determine the United States' ability to secure its people and interests are overwhelmingly being developed for commercial purposes in the private sector. It is highly unlikely the government will create its own, distinct capacity to create and distribute these technologies in the near- to mid-term.

This leaves the national defense more dependent on the private sector than ever before, precisely as China is emerging as a true-peer competitor and rival economically, technologically and militarily.

All of this adds up to an unavoidable truth: the ability of the United States to invent, design, build, deploy and secure advanced technologies -- and their key components -- is as important to national security as the nation's capacity to field traditional military capabilities. With this in mind, it follows that new partnerships between the government and industry are essential.

Finally, fourth, Conservatives must carefully balance their national security concerns regarding technology with their social and political concerns surrounding the growing role these companies have within our society. There are important debates to be had concerning perceived bias and other domestic political concerns associated with “big tech.” But, at all times, Conservatives must also remember that these same companies are likely to be the source of strategic advantage in the emerging global security contest, and so we must secure and shape our domestic tranquility without inadvertently destroying those who are producing the capabilities necessary for defending that same tranquility.

---

[1] The 10 identified industries are information technology, robotics, green energy, aerospace equipment, ocean engineering, railway equipment, power equipment, new materials, medicine, and agriculture equipment.

[i] Apptio. *State of the Global Technology Economy: Why technology dollars matter, and how top performers are spending them*. Bellevue, Washington: Apptio, 2018. <https://www.apptio.com/blog/new-report-habits-worlds-most-profitable-it-leaders>.

[ii] IDC. "IDC FutureScape: Worldwide IT Industry 2020 Predictions." 2019.

[iii] Muhammad, Zia. *Alphabet, Amazon, Apple, Facebook, Microsoft: How Big Tech Companies Earn Revenue*. 12 May 2019. 26 11 2019. <https://www.digitalinformationworld.com/2019/05/how-tech-giants-make-billions-infographic.html>.

[iv] International Monetary Fund. *World Economic Outlook Database*. 26 November 2019. <https://www.imf.org/external/pubs/ft/weo/2020/01/weodata/index.aspx>.

[v] Taylor, K., & Silver, L. (2019). *Smart Phone Ownership is Growing Rapidly Around the World, But Not Always Equally.* Pew Research Center. Washington, DC: Pew Research Center.

[vi] Clement, J. *Worldwide digital population as of July 2020*. 24 July 2020. 19 December 2019. <https://www.statista.com/statistics/617136/digital-population-worldwide>.

[vii] Cyphers, Bennet. *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*. Report. Washington, DC: Electronic Frontier Foundation, 2019.

[viii] Nguyen, Nicole. *Facebook Filed A Patent To Calculate Your Future Location*. 10 December 2018. 19 December 2019. <https://www.buzzfeednews.com/article/nicolenguyen/facebook-location-data-prediction-patent>.

[ix] Barlow, Sonya. *Can we trust machines to predict the stock market with 100% accuracy?* 6 May 2019. December 2019. <https://metro.co.uk/2019/05/06/can-we-trust-machines-to-predict-the-stock-market-with-100-accuracy-9325480>.

[x] Garamone, Jim. *Dunford Accepts Eisenhower Award, Calls for Industry, DOD Cooperation*. 10 May 2019. December 2019. <https://www.jcs.mil/Media/News/News-Display/Article/1845597/dunford-accepts-eisenhower-award-calls-for-industry-dod-cooperation>.

[xi] Reisinger, Don. *Jeff Bezos Says Big Tech Companies Should Ignore Employee Outcry and Partner With the U.S. Government*. 9 December 2019. December 2019. <https://www.inc.com/don-reisinger/jeff-bezos-says-big-tech-companies-should-ignore-employee-outcry-partner-with-us-government.html>.

[xii] Kelly, Mekena. *Microsoft CEO defends Pentagon contract following employee outcry*. 5 February 2019.

December 2019. <https://www.theverge.com/2019/2/25/18240300/microsoft-ceo-defends-pentagon-contract-ar-headsets-employee-outcry>.

[xiii] Cliff, Roger et al. *Entering the Dragon's Lair: Chinese Anti-Access Strategies and Their Implications for the United States*. Santa Monica, CA: RAND Corporation, 2007.

[xiv] Work, Robert O. and Greg Grant. *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics*. Washington, DC: Center for a New American Security, 2019.

[xv] Milanovic, Branko. "The Clash of Capitalisms: The Real Fight for the Global Economy's Future." *Foreign Affairs* (2019).

[xvi] Zheng, You. *The Road of Military-Civil Fusion for Artificial Intelligence Development (translated by Elsa Kania)*. 5 July 2018. 18 December 2019. <https://www.battlefieldsingularity.com/musings-1/tsinghua-s-approach-to-military-civil-fusion-in-artificial-intelligence>.

[xvii] Rodriguez, A. (2018, September 26). *Google says it spent "hundreds of years of human time" complying with Europe's privacy rules*. Retrieved December 18, 2019, from Quartz.com: <https://qz.com/1403080/google-spent-hundreds-of-years-of-human-time-complying-with-gdpr/>.

[xviii] Limitone, Julia. *China is Ripping Off Microsoft to the Tune of $10B.* 1 November 2018. 7 August 2020. <https://www.foxbusiness.com/business-leaders/china-is-ripping-off-microsoft-to-the-tune-of-10b>.

Klon Kitchen is a senior fellow at the American Enterprise Institute (AEI), where he focuses on the intersection of national security and defense technologies and innovation. Through his research, he works to understand and explain how emerging technologies are shaping modern statecraft, intelligence, and warfighting, while focusing on cybersecurity, artificial intelligence, robotics, and quantum sciences.

Before joining AEI, Mr. Kitchen was director of the Heritage Foundation's Center for Technology Policy, where he led an enterprise-wide, interdisciplinary effort to understand and shape the nation's most important technology issues.

Before joining Heritage, Mr. Kitchen was national security adviser to Sen. Ben Sasse (R-NE) and worked on the creation of the US Cyberspace Solarium Commission, a blue-ribbon commission tasked with developing an American grand strategy for cyber. While working for Sen. Sasse, Mr. Kitchen served as the staff director of the National Security and International Trade and Finance Subcommittee for the Senate Committee on Banking, Housing, and Urban Affairs.

Mr. Kitchen has also worked on cyber strategy at the National Counterterrorism Center; as a senior program assessment officer at the Office of the Director of National Intelligence in the Office of the Director of Central Intelligence; and as the lead analyst on al Qaeda senior leadership at the Defense Intelligence Agency. He was also the National Counterterrorism Center chair at National Defense University.

A popular speaker, Mr. Kitchen has appeared on "60 Minutes" on CBS News and The New York Times podcast "The Argument." He has also been published in RealClearDefense, The Hill, The National Interest, The Telegraph, Washington Examiner, and National Affairs, among other outlets.

Mr. Kitchen has an MA in strategy and security studies from the College of International Security Affairs and a War College Diploma in security strategy and irregular warfare from the National War College, both from National Defense University. His BA in biblical studies is from Bryan College.