Scenario Planning for Global Computer Chip Supply Chain Disruption

Inform your corporate strategy with insights from four realistic supply chain scenarios developed in an OODA Network Stratigame

Abstract

Scenario planning is a powerful tool used by leading corporations to derive actionable insights and avoid strategic surprise. The four scenarios presented here on the future of computer chip supply chains are based on inputs from experienced business leaders, national security and technology professionals and accelerate your planning for the future.

Daniel Pereira
dtp@ooda.com

CEO'S Introduction

The OODA team has been participating in "wargame" and red team exercises for over 25 years ranging from traditional DoD Office of Net Assessment games to scenario planning for the Fortune 500. We have personally witnessed the impact these exercises can have in establishing appropriate frameworks for thinking about future risks and opportunities. During one of our OODA Network monthly calls, one our members proposed that the OODA Network could be utilized for rapid wargaming on critical issues, with members suggesting the first be on the global computer chip supply chain.

This report is the outcome of our first OODA wargame, which we have branded as a Stratigame (Strategic Game), focusing on the global computer chip supply chain issues. Over 25 members of the OODA Network of Experts participated in this Stratigame where the OODA research team developed four scenarios and then led a structured discussion in which experts provided unique insights into potential impacts of these scenarios, adjacent risks and opportunities, and recommended actions that would allow us to avoid the negative impacts of a particular scenario or nudge us into a more favorable scenario.

During the time we were meeting, the impacts of global computer chip shortages were highlighted in the daily news as ships queued off the coast of California and auto dealership lots remained empty for lack of inventory. While it might be disruptive to the U.S. economy to not be able to meet product demand due to these shortages, we also wanted to consider what the longer-term impact to innovation and global cyber risk might be if such shortages persisted. Given the national strategic and economic advantage of Artificial Intelligence, would the U.S. fall behind without access to the latest computer chips? What other areas of innovation would be impacted? If we establish a stable supply chain that is primarily dependent on foreign sourcing, do we introduce cybersecurity risks like the concerns expressed over 5G networking technology?

As we race towards the future, a Stratigame like this will not provide for universal truths, but I am struck with one persistent thought: computer chip supply chains are essential to our national and economic security, and our dependency on foreign production of these chips within adversarial regimes creates an impactful vulnerability that we must move to immediate mitigate.

Please let us know what you think of this exercise and the associated report, and also know that I accept full responsibility for naming the four scenarios after Prince songs.

Matt Devost
CEO, OODA LLC

Overview

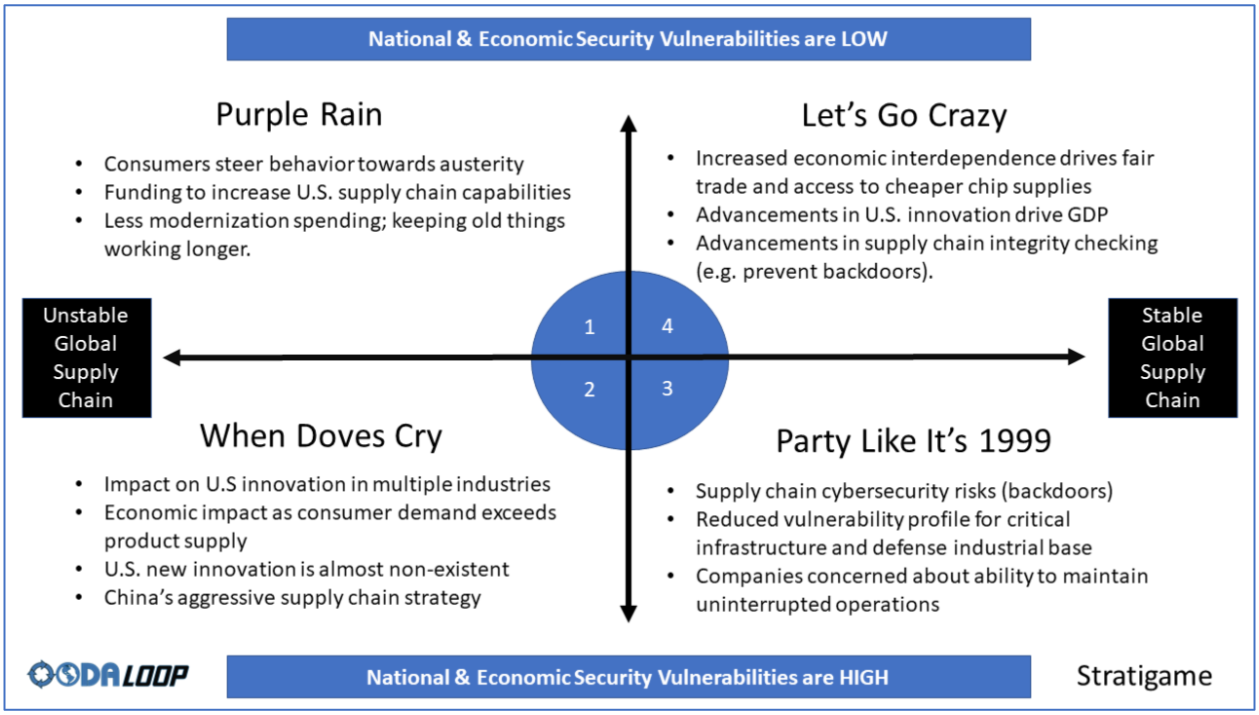
An OODA Network Stratigame is a foresight strategy exercise--designed to explore potential future scenarios that can support business strategy development. Stratigames borrow from classic scenario planning/foresight strategy methodologies, the OODA Loop decision-making framework, and the lean startup/minimum viable product (MVP) development framework–with the goal of generating a rapid prototype alpha version of scenarios. In October 2021 the Stratigame methodology was applied to the topic of Global Computer Chip Supply Chain topics, with the results presented here.

The OODA research team created an initial outline of scenarios of computer chip disruption in the near future (5 to 8 years out) based on the quad chart presented below. The chart has four scenarios that flow from two key drivers (the X and Y axis on the chart). Those key drivers are the overall level of stability of the global supply chain (the X axis) and the overall severity of the US national and economic security vulnerabilities (the Y axis).

Each quadrant of the chart became the basis of a future scenario that can be described as follows:

Scenario #1: Purple Rain
US National & Economic Security Vulnerabilities are low. The Global Supply Chain is unstable.
Scenario #2: When Doves Cry
US National & Economic Security Vulnerabilities are high. The Global Supply Chain is unstable.
Scenario #3: Party Like It's 1999
US National & Economic Security Vulnerabilities are high. The Global Supply Chain is stable.
Scenario #4: Let's Go Crazy
US National & Economic Security Vulnerabilities are low. The Global Supply Chain is stable.

The graphical depiction of these scenarios follows:



National & Economic Security Vulnerabilities are LOW

Purple Rain

- Consumers steer behavior towards austerity
- Funding to increase U.S. supply chain capabilities
- Less modernization spending; keeping old things working longer.

Let's Go Crazy

- Increased economic interdependence drives fair trade and access to cheaper chip supplies
- Advancements in U.S. innovation drive GDP
- Advancements in supply chain integrity checking (e.g. prevent backdoors).

Unstable Global Supply Chain

Stable Global Supply Chain

When Doves Cry

- Impact on U.S innovation in multiple industries
- Economic impact as consumer demand exceeds product supply
- U.S. new innovation is almost non-existent
- China's aggressive supply chain strategy

Party Like It's 1999

- Supply chain cybersecurity risks (backdoors)
- Reduced vulnerability profile for critical infrastructure and defense industrial base
- Companies concerned about ability to maintain uninterrupted operations

OODA LOOP

National & Economic Security Vulnerabilities are HIGH

Stratigame

The Four Scenarios

The following expands on each of these four scenarios:

Scenario #1: Purple Rain

US National & Economic Security Vulnerabilities are low. The Global Supply Chain is unstable.

Core Realities:

- Consumers steer behavior towards austerity
- Funding to increase U.S. supply chain capabilities
- Less modernization spending; keeping old things working longer.

Purple Rain is an imagined future where the dynamics of great power competition and international trade have resulted in continued strength for open democracies and free enterprise systems, which results in a strong national security and economic environment. However, significant challenges in the supply chains still endure. The strong national security and economic security of the US enables many mitigations to many supply chain risk issues, but issues around chip supply will be limiting factors that provide serious headwinds to almost every business. To be clear, strong national economic security will likely not translate to strong economic security for most businesses and the workforce since there is not enough dependability and predictability in the chip supply chain. This makes it hard for business planners to predict future market demands with any fidelity. Likelihood of recessions and relatively higher unemployment are a fact of life in this scenario, with flat growth in most industries.

The unstable chip supply means consumers and businesses alike will **postpone modernization efforts** for as long as possible. Less innovation spending has forced the Fortune 500 to survive by keeping old things working longer. The amount of CapEx investment for supply chain innovation remains prohibitive for the private sector and the USG strategic framework for semiconductor supply chain independence remains mired in political instability and dysfunction. It is reasonable to conclude that U.S. political extremists and domestic terrorists continue to weaponize this instability and uncertainty.

Scenario #2: When Doves Cry

US National & Economic Security Vulnerabilities are high. The Global Supply Chain is unstable.

Core Realities:

- Impact on U.S innovation in multiple industries is mixed: extreme hardship will lead to innovation. But unstable economy and unstable IT supply may moderate this a bit
- Economic impact as consumer demand exceeds product supply
- China's aggressive supply chain strategy

When Doves Cry is a future scenario where national security tensions increase to include significantly enhanced great power competition between the U.S. and China/Russia. Although years of planning may have shifted a small amount of production to U.S. and other nations, the lead time required to build fabs based on truly innovative chip architectures means that production does not come close to meeting demand. The U.S. domestic political system remains fraught with instability and growing violence is likely in this scenario. Innovation in this scenario does not get momentum or evolve substantially in the high technology sector - but provides evolutionary and disruptive trends in other industry verticals. It can be expected that the chip supply chain disruption is coupled to an overall traditional supply chain crisis. Supply chain and ransomware cybersecurity risks are not only prevalent but pandemic-level in their spread and frequency worldwide-- and not even remotely contained.   Fraud and cybercrime are still a threat and uncontained China, Iran, and Russia exploit every cybersecurity vulnerability along the supply chain. The inability to replace key equipment impacts overall cyber resiliency.

Scenario #3: Party Like It's 1999
US National & Economic Security Vulnerabilities are high. The Global Supply Chain is stable.
Core Realities:

- Continuous supply chain cybersecurity risks (including backdoors)
- Perhaps reduced vulnerability profile for critical infrastructure and defense industrial base
- Companies concerned about ability to maintain uninterrupted operations

In this future, **Party Like It's 1999**, the rapid action of the US and other open societies to reduce dependence on Chinese chip assembly/manufacturing and to build new capabilities in locations other than Taiwan has enabled a stronger supply of computer chips, even though tensions with China are at a very high level. Even though this scenario posits a stable supply chain, companies will be concerned about the ability of geopolitical tension to change that on short order. Innovation is focused on solving immediate problems–with a priority on returning the U.S. domestic supply chain dynamics and consumer culture to pre-pandemic modes of operation.

Scenario #4: Let's Go Crazy
US National & Economic Security Vulnerabilities are low. The Global Supply Chain is stable.
Core Realities:

- Increased economic interdependence drives fair trade and access to cheaper chip supplies
- Advancements in U.S. innovation drive GDP
- Advancements in supply chain integrity checking (e.g., prevent backdoors).
- This is a scenario where many good things happen, but historically time like this do not fuel dramatic innovation. Expect innovation to be more evolutionary than revolutionary

In **Let's Go Crazy**, this speculative future sees the rapid action of the U.S. and other open societies to reduce dependence on Chinese chip assembly/manufacturing and to build new capabilities in locations other than Taiwan has enabled a stronger supply of computer chips. And the US and other open societies see economic, military, and diplomatic strength. A strong chip supply enables continued tech-based innovation in multiple sectors of the economy and contributes to national and economic security - especially in areas such as cybersecurity (i.e., IT global supply chain trust, integrity, authenticity, and transparency). OODA network members underscored in discussions of this scenario that innovation in a world of peace and stability is often very incremental. A key concern in this scenario is in leaders letting their guard down leading to other harsher scenarios (like the one outlined in Scenario two above).

Background and Member Feedback on the Scenarios

- Direct dialog and member feedback on the scenarios enabled members to question assumptions about possible future scenarios, resulting in positive feedback that continued long after the event. The feedback from the event is also shaping reporting at OODAloop and has provided indicators that can be used to refine assessments on which potential scenario is coming to pass. One underscored the importance of revisiting these scenarios over time (and that is our intention now), saying "Seeing the updated model and what that looks like will be helpful – that iterative process, and not forever, but a couple of iterations?–is really going to be valuable for the overall process."

- The Stratigame was not just a discussion amongst technologists about technology. The model allowed a wide-ranging dialogue about the interplay among politics, social realities, and the technology itself, which are usually segregated by topic. Too frequently the tech people talk about tech and the policy folks talk about policy and that is sub-optimal. The scenarios presented allowed for an integrated conversation. It is a really good way to push people to think outside their own boxes.
- A private sector practitioner offered the perspective that breaking down the possible scenarios and the four quadrants was helpful: “It helped me think through what does this mean to my industry vertical (which is very technical, shipping dependent, and supply chain dependent)? I think the model will inform our enterprise risk model. How do we address some of these risks? No model is perfect, but this approach is helpful in discussing the topics in a way that an enterprise can understand.”

Additional Insights and Discussion Topics from The Stratigame Sessions

Cybersecurity Strategy and Security Transformation: All four scenarios push to the foreground what one OODA Network member calls the “advanced persistent strategic deficit with respect to cybersecurity, with talk of security transformation as a business practice, with nobody in agreement on what that means.” These scenarios beg the question: how else can your organization bridge this strategic cybersecurity deficit and make security transformation as a business practice more concrete and strategically robust for your company or organization, independent of government action and the need to react to market forces in your industry vertical? The cybersecurity threat and current governmental initiatives (e.g., Executive Orders) create emerging requirements for deep supply chain integrity monitoring and continuous assessment for backdoors and malicious code.

The Innovation Investment Ecosystem and the USG: An OODA Loop Network member opined that “the U.S. government is terrible at identifying who the actual stakeholders are - especially in new and innovative sectors. The national long-term strategy will not depend solely on industry partnerships, but public/private relationships with private equity funds and venture capital as well. In these situations, it would be good if the government and major corporations provided more focus and action topics like rare earth extraction and building nuclear power plants. The discussion here referenced the tendency on the part of the USG to pick the biggest four players in a space that are representative of innovation in that space, which is an approach easy on individuals in government but not necessarily as helpful to the nation as it could be.

What Will Drive Innovation and What Will Not? Experts with decades of experience in facilitating and tracking innovation helped participants understand the potential nature of innovation in these scenarios. One OODA Loop Network member argued persuasively that “in my knowledge of innovation over the last couple of decades, I believe that most true innovation is actually created by stressors. So, scarcity or fear--whether it is useful or incredibly useful innovation or not--tend to drive innovation better than complacency.” This very helpful context was informative to the final scenarios presented above and should be kept in mind as these scenarios inform corporate decision-making.

The Consumer Market as the Primary Driver May Lead to Appeasing China Further: This really nuanced and perceptive strategic logic was offered by a network member: “If there is already instability or threatened instability in a supply chain and consumer demand remains the priority–and the American consumer get what they want so long as we have good relations with China - then any bad relations with China are going to impact the American consumers ability to get that new car, get that new iPhone. Unfortunately, this may lean towards an environment where there is no political will for anything short of full appeasement with China, which eventually is an economic and political driver towards additional national and economic security vulnerabilities.” This dependence on China supply chains also gives China a strategic lever that can be used to exert impact on consumer pricing and innovation in the United States. Defeating this risk may take exceptional leadership.

The Global Brain Competition - Emerging Technologies, Human Targeting and Talent Recruitment: Highly skilled engineers and technical labor in the US or closely allied nations will be crucial in all four scenarios. Focusing too much on emerging technology innovation drives talent towards ‘high risk’/high reward’ endeavors, which may not prove valuable. Nine out ten startups fail. Losing a rich talent pool to high-risk endeavors-- fueled by a compelling financial upside narrative-- comes with the risk that individuals will be exposed and vulnerable to foreign investment financial schemes or feel emotionally or financially desperate after the failure of a startup, providing opportunities for foreign countries to target and recruit this talent.

A network member offered a really sophisticated perspective on the potential for a brain drain caused by talent flocking to the quantum startup space: “Everybody wants to jump on this startup bus. They want to get into it, and they are going to fail. And China is waiting in the wings ready to invest in those companies after they have failed–and do the equivalent of an “acquisition hire” of smart people who are trying to jump on this quantum bandwagon. So, there is going to be a problem here, but you are talking around the wrong [emerging technologies] problem. The problem is going to be a depletion of a highly capable workforce, then being mined by the Chinese.” Other members cautioned that the use of Quantum may not be the best analogy here, since Quantum Computing remains unproven at this time.

Research and Follow-on Insights to Inform Strategy

The following topics and questions can help accelerate the tailoring of these scenarios:

Today’s Efforts Should be Informed by History: A seminal industry study identified the market forces, crises and incentives which outsourced chip manufacturing in the first place (in the 1980’s) during the period of Japanese competitive advantage and again in other parts of Asia in the 2000’s (in hindsight, the shift to Taiwanese foundries has clearly proven radical and highly impactful). In each period, foreign countries were willing to subsidize the cost of new fabs, allowing for indigenous companies to grab market share. Questions that should be assessed based on history include: How will this be avoided, not repeated, by the U.S. semiconductor industry? Do these scenarios argue for a clear commitment to large scale domestic production in the U.S. and the building of fabs subsidized by the government as a clear strategic priority? If so, is building such fabs in the U.S. possible in the timeframe depicted in these scenarios? Is the U.S. semiconductor industry structured into a collaborative ecosystem to effectively enable this national effort?

A Reality Check on the “China Threat" Narrative: In 2009, the same industry study found that Samsung took a solid ten years from its entry into the chip market in the 1970’s, and plenty of Korean government subsidy, to achieve a viable place in the memory market in a ten year timeframe: “Our analysis suggests that firms from industrialized Asia are moving up the technology curve and may present challenges to industry leaders in a ten-to-twenty-year time frame." We are in year twelve this prediction. In general, this timeframe is marked by a learning curve for foreign companies to match the experience, R&D capabilities, product development, institutional knowledge and go to market strategies of U.S. giants in the industry like Intel and Texas Instruments. This learning curve remains the model on which to track foreign company's manufacturing and commercialization efforts. Questions to resolve include: What are the current activities and outcomes which best quantify this threat in a realistic fashion, separate from foreign policy and domestic political narratives?

The Secondary Chip and Hardware Markets: The dynamics of the secondary market are hard to assess but planning assumptions must be made. Several questions should be considered when making these planning assumptions, including: What is the secondary market going to look like in each of these scenarios? Is the technology sector given priority access to new, trusted chips and hardware for national security reasons, and all other industry verticals are scrambling in a secondary market for chip and hardware availability based on shortages? Also, do government semiconductor initiatives combined with cybersecurity initiatives point to a climate where the government mandates tearing out old equipment – and that equipment goes into the secondary market? Implicitly, these products in the secondary market are not innovative enough or secure enough to meet the challenges created by these scenarios. Where does that leave all other industry verticals relative to the technology sector's priority status due to the strong government collaboration suggested in scenarios one and four.

Strategic Movement to the Cloud: So much is moving into the cloud for Fortune 500 firms. AWS and other cloud services firms also make their own chips. Over time, they may have their own fabs. If companies are waiting on the compute to be in the cloud environment and AWS and other XaaS companies can make their own chips–a foreign dependence on chip supply is less likely. A question to resolve: When the modernization spending begins to happen, and it is clear more cloud-based spending is happening expressly to guard against chip supply chain disruptions, will the Fortune 500 look differently at new computer hardware for data centers when their real modernization efforts are moving to the cloud?

The Much Broader Question Will be with Things like Life Cycle Changes: Currently, when considering supply chain shortages, there is no consistent process for decisions around stretching the Android update security update cycle out a year. That is just one of many examples. Sometimes you can fix things in software, but a process needs to be put in place which makes business sense. This level of strategic dialogue needs to occur and is not happening in any pervasive way in any sectors (short of defense).

A More Rigorous Data Strategy: New approaches to data analytics may arise, perhaps limiting the impact on some chip supply chain issues (for example, the field of study known as Small Data). As an OODA Network member noted: "Why do you need a whole bunch of chips? In many cases, bloated code, old code, and inefficient code-- or no idea or strategic model about what you really want to do with the data, in the hope that some AI/ML model is going to find you the answer as opposed to rigorous thought, planning, and research. What role does efficiency play in each of these scenarios?"

Prioritizing Physical Supply Chain Integrity at the Chip Level. A Network member noted via e-mail: "The integrity of the software supply chain and data supply chain need to be in the forefront. Currently, there are no focused programs of record to immutably capture the authentic state of data or methodologies to verify the integrity of captured data prior to intended use. We will need correct data and correct software, not data and software that has been manipulated or disrupted by an adversary." But the fact remains: at the hardware level, all these issues of **data** trust, integrity, authenticity, and transparency all trace back to strained semiconductor availability and foreign sourcing of untrusted chips.

More on Data Integrity: From an OODA network member: "There will be a growing need to show the business impact of and frame business issues around the way certain markets blindly trust data. The impact of an inability to verify the authenticity of the data we use - and the software that drives the processes that use them -will be of growing importance. Tools which provide confidence in the integrity of data and the software that is processing data are vital. There is an operational imperative to have confidence in the processes that are feeding data driven decisions." Creating case studies of the potential impacts of distorted data and manipulated processes should be a priority. These potential impacts then need to be included as part of an overall business case for modernization efforts. The question then becomes: what are the mitigation strategies achieved through chip supply chain resiliency and innovation up and down the semiconductor value chain that relate to data integrity?

Impact on Machine Learning and AI - Compute Power and Training Data: As an OODA Loop Network member shared from experience, "Most current approaches to machine learning need lots of compute power and lots of training data. On computational power, if you take one of the current big scale models--a language model called GPT3--there are estimates that just for training that model it would require about 190,000 kilowatts hours of electricity. If I were to train that model at my office that would cost around $70,000. That is about the cost of a Tesla Model Y without the self-driving feature. It makes it a little harder to make the decision to train twenty variants of this model. It is too expensive. But what if you do not even have the choice to train this model at all, as the capacity is not available due to a chip shortage or a particularly impactful supply chain disruption. If innovation is not happening due to chip shortages, then the price/performance gains for AI and ML platforms will also not materialize."

"There are lots of real-world reasons why you might not have the proper training data. One could be privacy if you think about areas like healthcare or law. The second reason could be you do not have one big dataset, but you have many, many small ones. Another reason you do not have enough training data could be just because it is expensive, and it takes a long time. If you think about materials discovery, computational chemistry, that is one of those areas. You just cannot run a hundred thousand experiments. It takes too long and is too expensive. It is easy to overlook those areas where you do not have the large-scale training data or other compute power. Chip shortages would have a significant impact in this area. In the event of a significant chip shortage, you cannot use the models that presume that you have the compute power to train larger models and the chip availability to store a large dataset."

Dynamics To Watch For

A Return to the Old Normal or a Transformative New Normal? The world in which we have been living is based on an interdependent global supply chain with a just-in-time manufacturing and distribution system, which is clearly faltering due to the stressors brought on by the Covid-19 pandemic. Only one of the scenarios described here commits to reestablishing this 2019 'old normal' - with mixed results. The other scenarios drive headlong (by strategic necessity) into formulating what the new normal is going to look like. There is much debate over whether this pandemic is going to be impactful but recoverable or fundamentally transformational (like many of the pandemics over the course of history). The informal tally based on this OODA Loop Stratigame? 75% odds of a new normal, with distinct types of transformative activities as depicted in three scenarios (#1, #2 and #4); And a 25% chance of reestablishing the 2019 old normal of just-in-time manufacturing and distribution on which the economy is built, as depicted in scenario #3 (again, with mixed results).

About Scenario #2 (When Doves Cry): An OODA Loop Network member said it best: "This quadrant feels like walking into WWIII. The U S economy and the dollar collapse on the world stage. China does not survive without the United States economy - their economy has been growing faster than it can handle. They need us just as much as we need them right now - on a lot of things. This is a realistic scenario. This scenario terrifies me - and I do not have a good solution. I also assume we are not so far in the bottom left of scenario quadrant #2. If we are in the top or middle part of scenario quadrant #2, then we can swing into scenario quadrant #3 with a bunch of investment in a stable supply chain. But if the chip supply chain falls apart and we end up deep in scenario #2,that is not the only problem that we have. We have much bigger problems at that point."

Slipping into a Worst-case Scenario Due to a Lack of Commitment: Scenarios #1, #3 and #4 can all revert very quickly to Scenario #2–as they all require a long-term strategic plan as part of their strategic logics. All three scenarios explore a sustained commitment to stability, innovation and security based on various levels and areas of focus by the United States government, with or without a strong collaboration with industry.

Know Thy Enemy/Play the Game: When spending time with these scenarios, ask the question: What scenario does our competition live in? What scenario does our competition want us living in and why? What activities are they going to engage in to keep us there? What mitigation strategies can we put in place to take us out of a state of high vulnerability? How can we play offense? Or is the best offense a great defense? How do we avoid unforced errors?

Design Innovation for the Long View: Regardless of what quadrant you are operating in and based on the insights provided by all four scenarios, it is highly recommended that your organization's design process for innovation include a long-term plan and commitment to issues surrounding trust, integrity, authenticity, and transparency in the global IT supply chain (including semiconductor availability and foreign sourcing) and in the traditional intermodal supply chain. The need for cybersecurity innovation efforts running parallel to chip supply chain resilience and chip value chain innovation figures prominently in all four scenarios.

Concluding Comment

Scenario planning is not about predicting the future, it is about preparing for a range of realistic potential futures and assessing the potential impact of those futures on the business. The four scenarios and contextualization presented above provide realistic futures that can now be tailored to inform your actions.