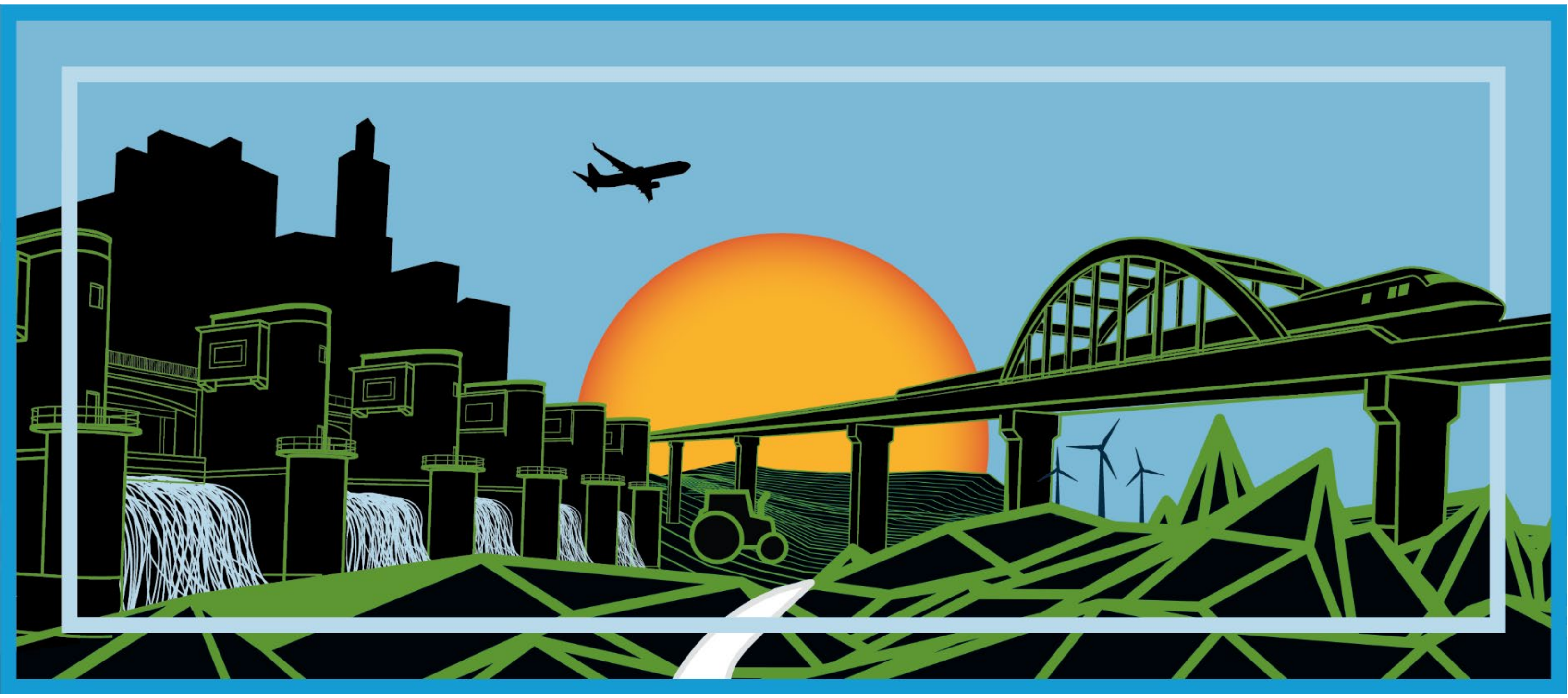

Secure Tomorrow Series

Scenario Narrative #2: Great Power Disruption

Publication: June 2024
Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. Government. Aside from historical references, all names, characters, organizations, and incidents portrayed in these scenarios are fictitious. Any positions expressed by fictional characters herein regarding any particular issues or technologies do not represent the positions of CISA or the federal government.

September 2030

Course: CSTS-200/IR-300: Great Power Disruption: How Technological Innovation Defined a Decade of Cold Conflict

Lecture 1

As a service to students, I upload real-time transcripts of all lectures to the course site. The transcriptions are by XYZ v.23.0, and I take no responsibility for any transcription errors.

Professor Miller:

Good morning, everyone. I'm Professor Miller, and welcome to Great Power Disruption. This is a graduate seminar exploring the intersection of technological change and great power competition during the past decade.

So, who am I and why should I be teaching this class? After studying computer science as an undergraduate, I began my career as an analyst with the U.S. intelligence community. Several years later, I returned to academia to obtain my Ph.D. in history. Since then, my academic work examines how wars have influenced technological progress throughout history.

Enough about me. The name of this course, Great Power Disruption, blends two concepts: great power competition and technological disruption. *Great power competition* refers to rivalry among the most powerful nations in the world. The best-known historical example is the 20th-century Cold War. Throughout history, we have experienced numerous chapters of great power competition, often driven by some mix of religion, politics, or imperial aspirations. Great power competition in the most recent decade has been propelled by several factors, but the most significant driving force is competition for technological leadership. You can see that, in the course name, I've replaced the word *competition* with *disruption* to reference both the inherently disruptive nature of technological innovation and the emergence of technology as a core driver of great power competition.

I've divided the course into five modules, and I'd like to begin today by reviewing the syllabus so you know what to expect this semester. Stop me at any point if you have questions. If there's time at the end of class, we'll dive into the first module.

In module 1, we'll begin by looking at the early 2020s. Washington was increasingly concerned that the United States was losing its edge in the design and manufacture of key technologies, most notably semiconductors, memory chips, and other components in everyday electronics and dual-use—meaning military and civilian—technologies. Concern quickly evolved into competition, accelerating an international race for technological supremacy and control of key supply chains.

In module 2, we will discuss the geopolitical tensions that emerged from the decisions made in the early 2020s. For example, enhanced competition for control of critical minerals led to regional proxy conflicts among great powers that took place in developing nations. These conflicts created domestic economic and political challenges in the United States that persist today. Global standard-setting organizations, particularly those involved in setting internet standards, also felt the strain of great power disruption. We've seen nations across the political spectrum choose to detach from the global internet partially or even fully. This pivot away from a shared, online, global commons and toward internet fragmentation is emblematic of this historical moment of competition for control of technological progress.

In module 3, we will focus on the online battlefield. Cyber conflict, which became an expansive tool for shaping geopolitical outcomes during the early 21st century, continues to evolve. The ransomware threat has dissipated somewhat since its peak a few years ago. I would credit this progress to improved cross-sector cyber resilience and corporate resistance to paying ransoms. Companies are better prepared to maintain operational continuity during an attack and often see little value in paying a ransom that may not restore their systems anyway. Ransomware does remain a threat, particularly for organizations that possess sensitive personal data, such as hospitals. But the overall risk has diminished; the main battlefield of great power cyber conflict has been espionage, including intellectual property theft. This trend has reached all-time highs in recent years, enabled in part by significant advances in artificial intelligence, more commonly known as "AI." Cyber threat actors have, for example, begun to leverage large language models (LLMs) to develop novel network penetration techniques. LLMs have essentially democratized access to advanced cyber toolkits because threat actors with minimal technical capability can leverage LLMs to build advanced cyber weapons in minutes.

You have a question?

Student 1:

Yes, excuse me, professor. In module 3, will we discuss last year's water cyberattack in Mittleridge? I'm from that area, and I read that they 3D-printed a component to get the water flowing again.

Professor Miller:

Thanks. That is a good example, and we'll certainly discuss it. For those who are not aware, last year there was a cyberattack on a SCADA system for a major water treatment facility just outside the city of Mittleridge in the Midwest.

Student 1:

SCADA?

Professor Miller:

That stands for "Supervisory Control and Data Acquisition." SCADA is basically a network to control machines and processes. This attack is indicative of the trend I just mentioned about AI in cyber offense. The attackers leveraged AI in two ways. First, they leveraged an LLM to create spear phishing emails sent to employees. The emails enabled the attackers to gain initial access to the network. Second, once the perpetrators had access to the SCADA system, they deployed a strain of polymorphic malware that leveraged AI code generative techniques to synthesize new malware variants autonomously. In other words, after it was deployed, the malware adapted to the target environment to evade detection.

In addition to our discussion of the intersection between AI and cyber conflict, the Mittleridge plant example is also relevant to advanced manufacturing, which we'll discuss later in the course. The attack caused physical damage to several components of the plant, forcing the water treatment facility to halt operations for three days. Instead of waiting several weeks, or perhaps months, for replacement components from the original manufacturer, the water plant found a 3D printing company that was able to build replacements in less than two days. Notably, the 3D printing company had formed just a few years earlier with the support of federal funding appropriated by Congress in 2025 to invest in domestic advanced manufacturing.

We'll get back on track with the syllabus in a minute, but while we're on this interesting example, I'll point out that it intersects with several key themes of this class:

- One, critical infrastructure remains at risk in the era of great power competition.
- Two, government-funded industrial policy has delivered proven domestic benefits (in this case, a strategic advantage in advanced manufacturing).
- Three, the proliferation of AI in cyber offense over the past decade has significantly lowered the barriers to entry for cyber intrusions. As a result, cyber resilience and rapid recovery are essential, particularly for critical infrastructure operators.

One more thought before we get back to the syllabus: regulatory progress almost always lags behind technological change. In this case, the urgent need to rapidly restore operations forced the water plant to adopt an untested technology for which no regulatory framework exists. There are no federal laws that regulate quality standards for 3D-printed components or whether critical infrastructure operators can use them. Think about what problems can arise from this. Should the plant have been permitted to use a 3D-printed component, even temporarily? What are the costs and benefits of such an approach? I see a lot of hands up. I'd like to postpone this discussion for a later class. It's an ongoing debate.

Student 1:

We'll be ready.

Professor Miller:

Let's get back to the course overview. As I have mentioned, generative AI has had a transformative effect on cyber offense over the past decade. As a result of improved efficiency in LLM training and expanded access to high-end graphics processing units, cyber threat actors can develop custom trained LLMs on a laptop in a matter of hours. Attackers can leverage this to rapidly build and deploy new capabilities. In this way, AI development over the past decade has effectively raised the floor of cyber offense such that even the least technically capable adversaries can generate technically advanced attacks.

On a more positive note, AI has led to significant developments for cybersecurity defenders. Machine learning has proven to be a highly effective tool to augment network intrusion detection, helping to mitigate some of the AI-supercharged advances in cyber offense. However, AI can be a drag on security in the development phase. Software developers are increasingly leveraging LLMs to handle basic coding workloads. These LLMs often recommend insecure code that contain a myriad of vulnerabilities, further complicating the work of security professionals. Broadly speaking, the past decade of AI advancement has, despite some successes, proven challenging for security professionals.

In the final section of module 3, we will discuss the role of the information and communications technology supply chain, or the ICT supply chain, in cyber conflict. Specifically, we'll look at the history of cybersecurity risks from compromised computer components in the supply chain.

That leads us to module 4, where we will assess the policy responses adopted by the United States, its allies, and its rivals in the pursuit of great power disruption. In the early 2020s, U.S. political leaders in both parties identified key technologies where partial economic decoupling could be advantageous for national security. The United States has devoted significant resources over the past decade to industrial policies that subsidize the domestic development and production of critical technologies. The federal government has also worked to reorient critical supply chains away from rival nations and embraced initiatives to source materials from domestic or trusted international sources. This process has not been without its challenges, most notably those proxy conflicts in resource-rich regions. Finally, the United States has strengthened its export controls on American-designed innovations in an attempt to contain the benefits of technological progress within national borders.

There's a hand up.

Student 2:

Thanks. I'd like to know if you think these policies have been successful. Because I watched an ILuminate Talk that said they've failed.

Professor Miller:

That is one of the key questions each of you will be wrestling with in this class. But here are a few thoughts to get you started.

Has the United States succeeded in onshoring significant production capacity for critical technologies? Yes. That is a clearly measurable outcome of these policy initiatives. Has this onshoring effort led to a meaningful improvement in the nation's national security posture? Likely yes, but this is a tricky question that we will explore in depth throughout the course. Have there been negative side effects of this effort? Certainly, and we will talk about one economic side effect shortly. So, the answer to whether they've succeeded or failed depends on how you define success and for whom.

Regarding supply chains, the United States has not fully decoupled from major trading partners who are also geopolitical competitors. That's proven to be impractical, both economically and politically. But the United States has at least meaningfully reduced its dependence on imports of critical tech components from adversarial nations.

As for export controls, there is actually evidence that withholding tech exports from competing nations may have helped propel them to build the technologies themselves. That was certainly not the intent of the policy. This result cuts both ways, as it likely slowed down the competitors' progress in certain industries that relied on our products, but it also spurred the development of domestic industries in these countries that now compete with the United States globally. Further complicating this picture is the dramatic rise in intellectual property theft that may be a by-product of export controls. Overall, their impact has been mixed.

Broadly speaking, we can identify some wins today that have emerged from these policies, but the overall results are complex and sometimes ambiguous. This semester, you all will be analyzing specific case studies to determine the impact of these policies and gain insight into what might happen next.

Student 2:

Sounds great. Thanks.

Professor Miller:

For the last module in the class, module 5, we will look ahead to the 2030s. How sustainable will U.S. policies prove to be in this decade? For example, many of the government subsidies for advanced manufacturing of critical technologies are set to expire in 2032. It is not clear whether these new domestic industries will be sustainable without permanent government support. There are many factors at play here, but does anyone know a key reason why this might be the case?

Student 3:

Maybe the cost of building new manufacturing plants, which is often cheaper in other countries.

Professor Miller:

Exactly! And these high-tech factories are not only costly to build, they are also very expensive to maintain. In the 20th century, factories could be easily retooled to manufacture the next generation of hardware. Today, a plant designed to build the current version of, let's say, smartphone touch screens might be largely obsolete in just a few years. To build the next generation, entirely new processes need to be built from the ground up. In short, progress in advanced manufacturing has led to highly specialized processes for each generation of technological components. Without ongoing incentives, producers will want to shift their operations to lower-cost nations to build their next generation of advanced manufacturing facilities.

I will also add an addendum here about AI—a topic that permeates nearly everything that we will discuss in this course. Advanced manufacturing plants have experimented with leveraging AI to improve efficiency and reduce costs. However, adoption remains sluggish due to several challenges, including a lack of a unified framework for implementing AI in advanced manufacturing and insufficient high-quality data to train AI models for certain aspects of the manufacturing process. Given some well-publicized failures, broader concerns about AI's disruption of the workplace, and the continued black-box nature of AI algorithms, operators in these plants have also expressed reluctance and a lack of trust in AI.

So that's module 5. Any final questions about the syllabus? If not, let's jump into module 1.

Why do we care so much about what happened in the early 2020s? Let's start by looking at two seminal moments in recent history and see how each ties back to precipitating events in the early 2020s. Last year, in 2029, two major announcements made headlines:

One, the International Monetary Reserve, or IMR, projected that global annualized real economic growth would remain below 3 percent per year for the next 5 to 10 years.

And two, the United States announced plans to eliminate reliance on foreign produced semiconductors by 2035.

Thinking about these two announcements, let's consider a few key questions: What trends or decisions visible in the early 2020s led to these two outcomes? What do they have in common?

Sorry, I haven't learned your names yet. Let's hear next from you, in the blue shirt.

Student 4:

Well, inflation in the early and mid-2020s led to less accommodative interest rates than we had in the 2010s. Interest rates remain economically neutral or slightly restrictive in most developed economies today. This could help to explain below-trend growth.

Professor Miller:

Absolutely, that is a key factor impacting the IMR projection. What else?

You, in the hoodie.

Student 5:

As you said when we were reviewing module 4, nations around the world have spent the past decade partially reorienting away from international free trade toward protectionism and government-funded onshoring of production for critical sectors. Wouldn't the United States eliminating reliance on foreign semiconductors be a continuation of that trend? And limiting free trade would definitely be a drag on global economic growth.

Professor Miller:

Correct on both counts. This is a critical point.

In the name of great power competition, the United States has embraced partial trade protectionism and domestic industrial policy. And this trend is global. While complete economic decoupling is not likely, partial decoupling in certain sectors has reshuffled multitrillion-dollar industries. The United States has succeeded in onshoring significant production capacity for a wide variety of critical components, including semiconductors. However, the global push to onshore production sacrifices economic efficiencies inherent in international free trade, contributing to slower growth and higher prices.

This is emblematic of great power disruption. Nations have brazenly competed to master the next technological age and harden domestic industrial resilience at the expense of global economic cooperation. We see the results of these decisions in our economic and international trade data today.

Unfortunately, that’s all the time we have today. I hope you now have a sense of what to expect this semester as we look back at the past decade of great power disruption. Don’t forgot to read Michelsontz chapters 4 and 5 for next class. And if you have questions, I will be in my office on Thursday. See you next week.