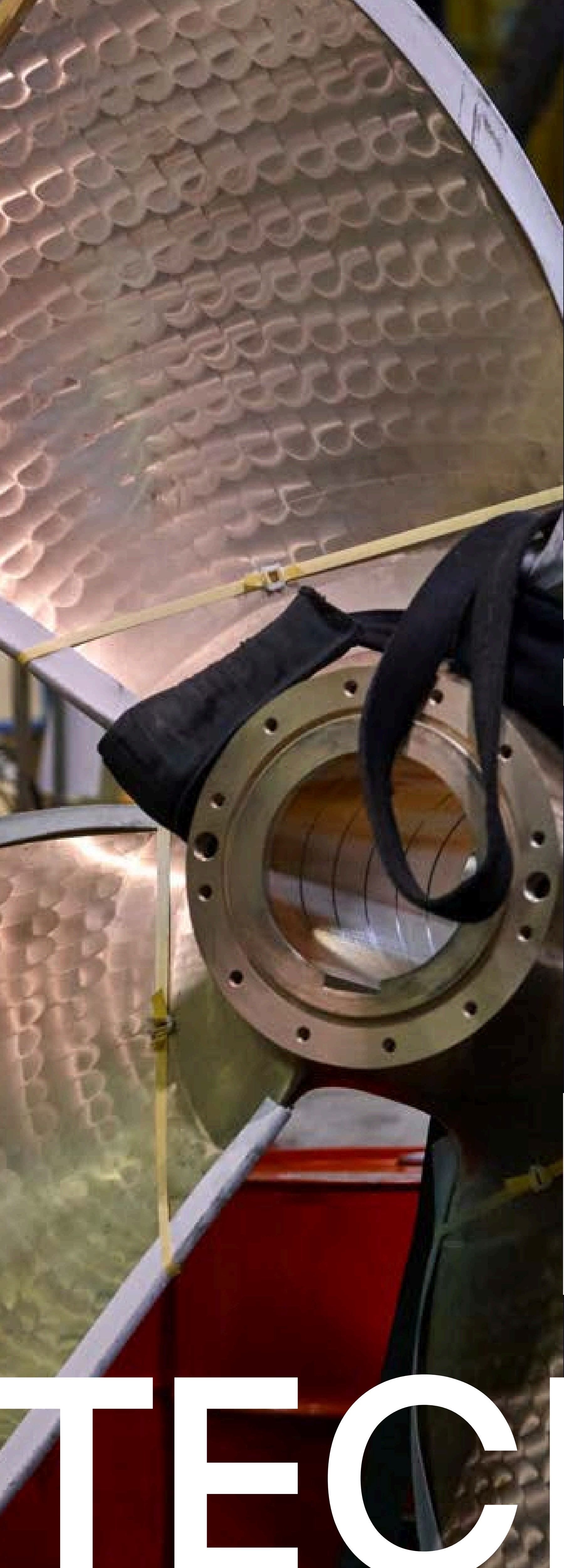



SECURING INNOVATION IN THE GLOBAL TECH RACE


An Executive Guide to Understanding and Mitigating Nation-State Risk

STRIDER

 © 2025 Strider Technologies, Inc.

TABLE OF CONTENTS

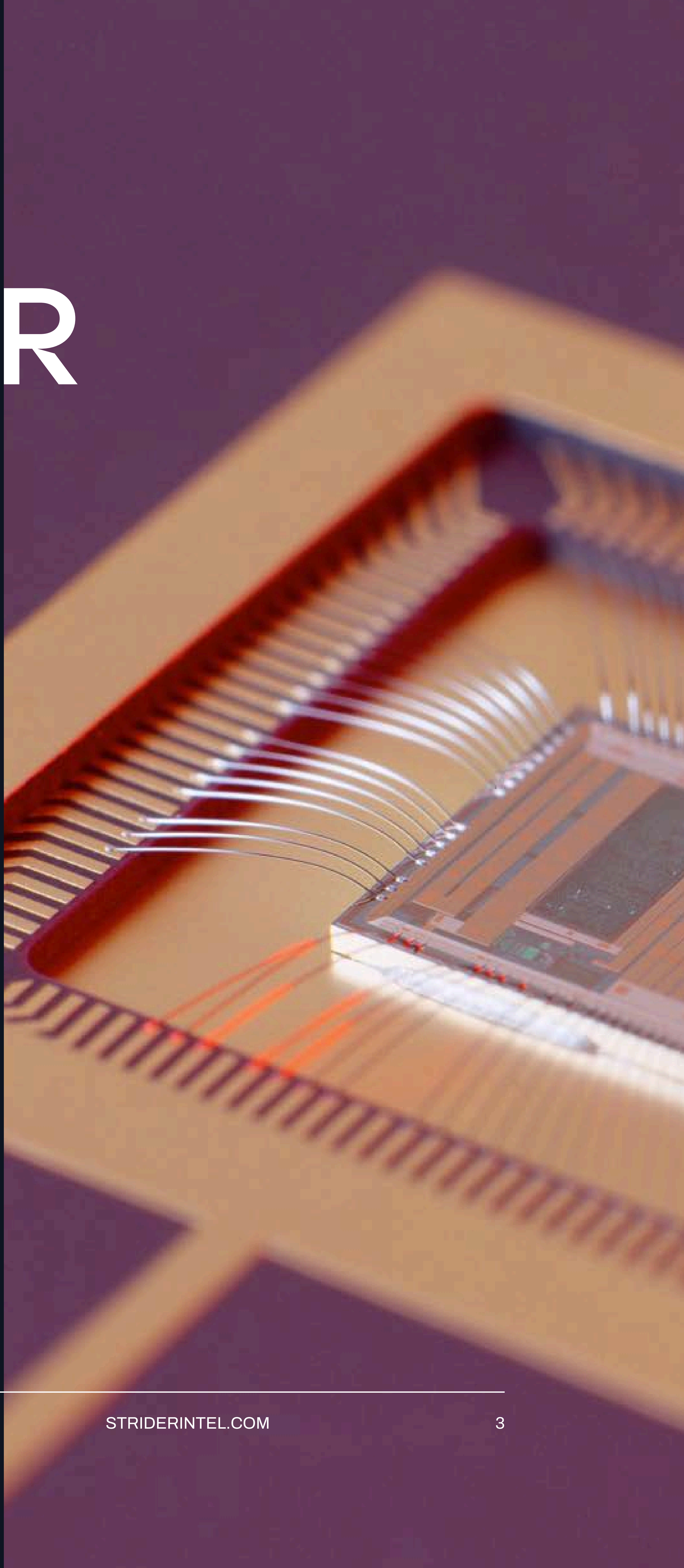
INTRODUCTION: COMPETING FOR THE FUTURE

Innovation drives progress—and global competition. But as nations race to lead in emerging technologies, the tactics used to gain an edge are changing.

The next wave of global influence won't be determined by territory or trade routes, but by breakthroughs in science, technology, and data. Adversarial governments are investing billions to secure technological dominance, often by exploiting the openness of the global economy and the collaborative nature of modern research. What once felt like healthy global competition has become a complex contest of access, influence, and control.

They recruit experts, build covert partnerships, and quietly absorb foreign technology to accelerate their progress. Some do this through formal industrial policies; others through less visible networks of state-linked companies, universities, and research programs. The result is the same: a concerted effort to acquire the world's most valuable innovations. In this environment, innovation isn't just a competitive advantage—it's a national interest.

The question isn't whether your organization is in the race. It's whether you're protecting your lead.



WHAT IS NATION-STATE RISK?

Nation-state risk refers to the strategic activities carried out or supported by governments to advance their national goals, sometimes through covert or deceptive means.

These Efforts Can Include:

- Intellectual property theft and technology transfer
- Talent recruitment and insider access
- Academic or commercial partnerships with hidden agendas
- Supply chain manipulation and cyber intrusions

In past decades, this kind of espionage focused on classified government data. Today, state-directed espionage also targets private industry, especially in cutting-edge fields like semiconductors, biopharma, aerospace, and artificial intelligence.

Modern competition isn't fought on the battlefield.
It's fought in R&D labs, boardrooms, and codebases.

HOW STATE-SPONSORED ACTORS OPERATE

State-sponsored actors are individuals or organizations operating on behalf of a foreign government. They may appear as investors, recruiters, collaborators, or suppliers, but their ultimate goal is to advance their nation's strategic interests.

Today, these efforts are broader, more organized, and more persistent than ever before. They're no longer isolated incidents but coordinated, long-term programs spanning governments, state-owned enterprises, universities, and front companies.

Their Targets Include:

- Emerging technologies with dual-use potential (commercial and military)
- Cutting-edge IP and production methods
- Senior scientists, engineers, and researchers

**Every partnership is an opportunity—
for collaboration or for compromise.**

THE COST OF INNOVATION THEFT

The impact of nation-state risk isn't abstract—it's measurable. The U.S. economy loses an estimated $250–$600 billion each year to counterfeit goods, pirated software, and stolen trade secrets.

Behind those figures are real organizations: startups whose prototypes appear overseas, manufacturers undercut by copied technology, and research teams whose breakthroughs are repurposed under foreign patents.

And the cost isn't just financial. When innovation is stolen, trust erodes, investment slows, and competitiveness declines.

Every idea lost is a step backward in the global tech race.

REAL-WORLD CASES OF TECHNOLOGY THEFT

Academic Collaboration or Covert Recruitment?

A Harvard University professor was charged with lying to U.S. authorities about his participation in a PRC talent recruitment program and undisclosed research funding from Chinese entities. While leading a prominent research lab, he concealed financial ties and agreements that advanced the PRC's strategic research objectives. The case underscored how state-directed programs can exploit academic openness to access U.S. innovation and talent.

Source: U.S. Department of Justice

Exporting Trade Secrets

A former engineer at a major U.S. tech company pled guilty to stealing proprietary designs for autonomous vehicle components and attempting to leave the United States with the information. Prosecutors found the stolen data could have benefited a PRC-based competitor developing similar technologies. The case illustrated how insider access and global mobility are leveraged to accelerate state-linked technology acquisition efforts.

Source: U.S. Department of Justice

HOW TALENT BECOMES A TARGET

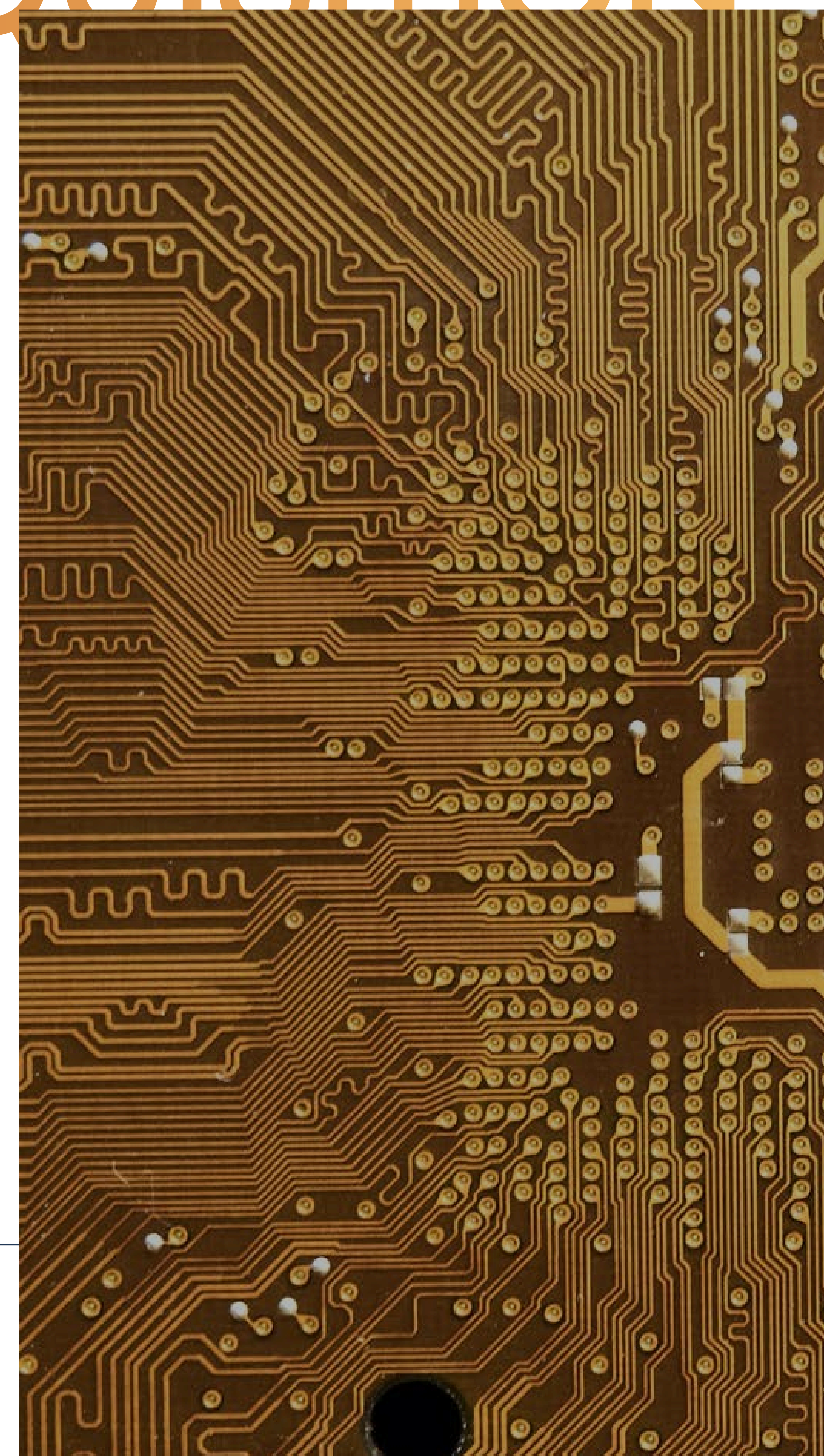
For competing nations, one of the most effective tools in this race is talent acquisition. Competing nations actively recruit scientists and engineers from Western companies and universities, offering high-paying positions, research funding, or career prestige.

These efforts often begin innocently. A professional message on LinkedIn, a conference invitation, or an overseas research offer. But behind them can be a structured recruitment process designed to extract intellectual property and expertise.

By understanding this recruitment cycle—spotting, assessing, developing, recruiting, and managing targets—organizations can better protect their people and their knowledge.

Your people are your greatest asset and your greatest vulnerability.

THE PRC'S MODEL FOR TECHNOLOGY ACQUISITION



The People's Republic of China (PRC) has formalized its approach to technology acquisition through national strategies such as Made in China 2025 and its Five-Year Plans. These initiatives combine state planning with market mechanisms to close technology gaps and reduce reliance on foreign innovation.

While these programs emphasize "indigenous innovation," much of their success relies on acquiring and adapting external technologies through:

- **Joint ventures and academic collaborations**
- **Targeted recruiting of foreign-trained experts**
- **Corporate partnerships and investment vehicles**

This coordinated, whole-of-society effort illustrates how nation-state risk extends far beyond cyber espionage. It's embedded in legitimate global exchanges of people, data, and capital.

WHY THIS MATTERS TO YOUR ORGANIZATION

Whether you're in advanced manufacturing, biotechnology, software, or defense, your organization is part of a global innovation ecosystem. That interconnectedness drives progress, but it also introduces exposure.

Without visibility into how foreign state interests intersect with your supply chain, partnerships, and workforce, it's easy to overlook where your competitive edge might be leaking.

You can't defend what you don't see.
Awareness is the first line of protection.

BUILDING ORGANIZATIONAL RESILIENCE

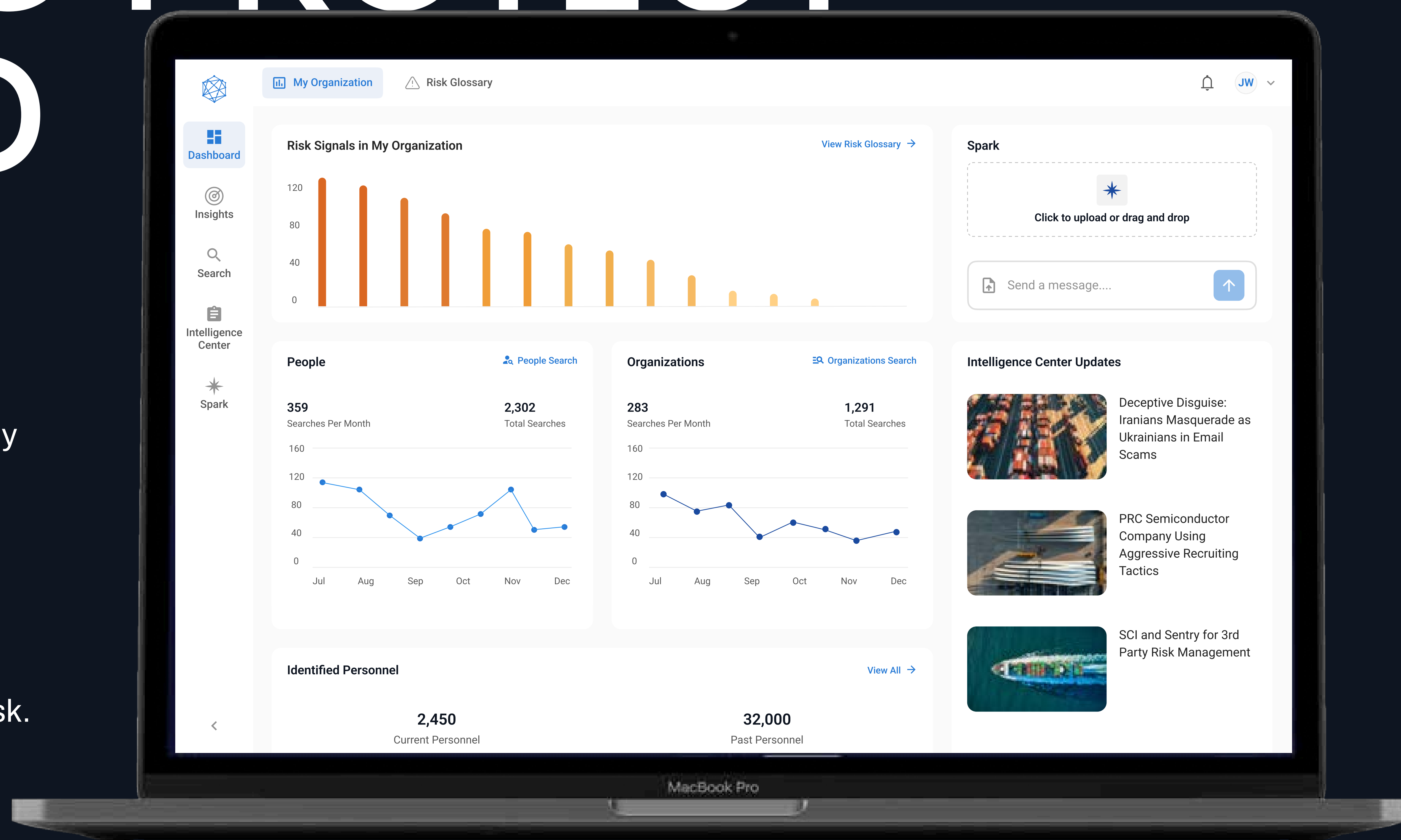
Protecting innovation from nation-state risk doesn't mean closing doors. It means seeing clearly. Organizations that integrate strategic intelligence into their decision-making can identify vulnerabilities before they become losses.

Key Steps Include:

- Assess exposure across people, technology, and partnerships
- Monitor risks using open-source and proprietary intelligence
- Educate teams about recruitment and data-sharing red flags
- Collaborate across security, legal, and executive functions to align strategy

The right information shifts an organization's security from being reactive to proactive.

INTELLIGENCE TO PROTECT YOUR LEAD

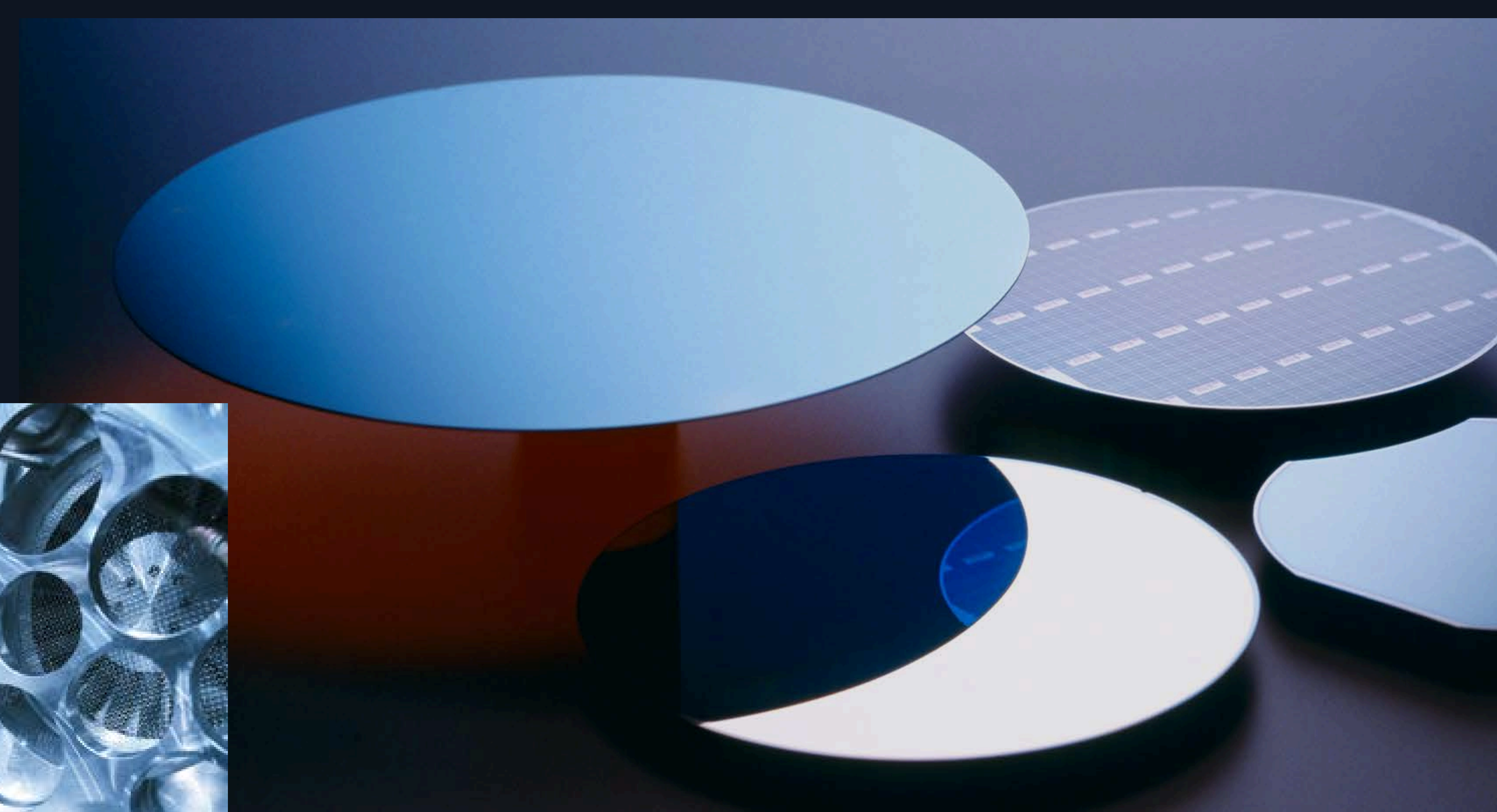


Winning the global tech race requires more than innovation. It requires intelligence. Strider equips organizations with strategic intelligence that reveals unseen nation-state risks across global talent, supply chains, and partnerships—helping leaders act with foresight and confidence.

Explore the Strider Strategic Intelligence Platform to learn how our AI-powered intelligence enables organizations to identify and mitigate nation-state risk.

EXPLORE THE STRIDER STRATEGIC INTELLIGENCE PLATFORM
striderintel.com/strategic-intelligence/

STRIDER



© 2025 Strider Technologies, Inc.