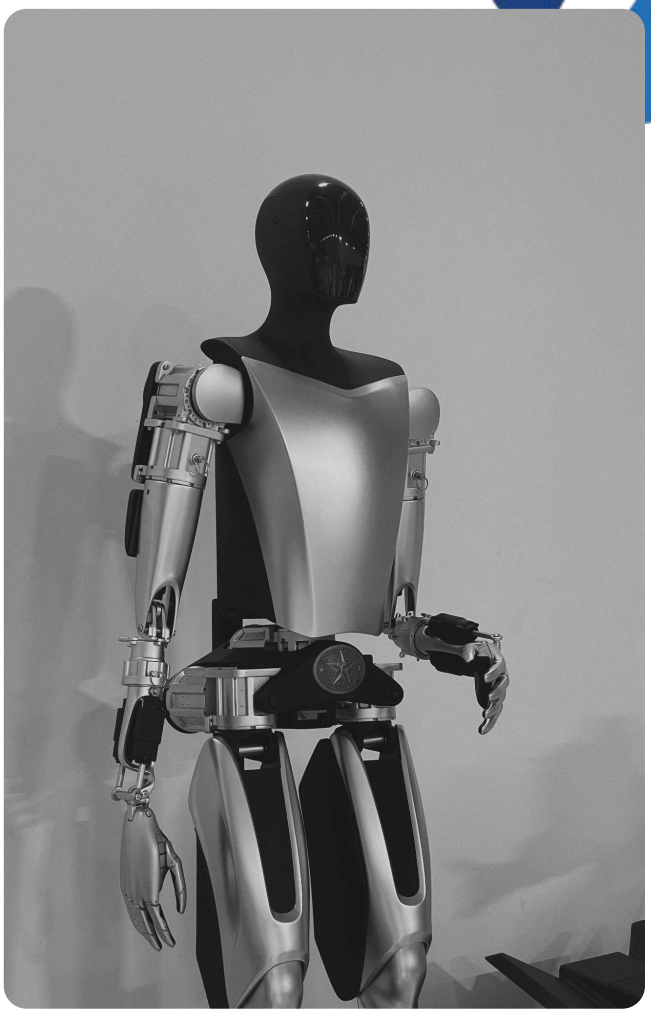
Recorded Future®

EXECUTIVE INSIGHTS REPORT | NOVEMBER 2025

The Future of Humanoid Robots

From Insikt Group®



Summary

Advances in **large-language models (LLMs) and the anticipated arrival of artificial general intelligence (AGI) are rapidly closing the gap between concept and capability**. The prospect of humanoid robots functioning autonomously in workplaces and public spaces is moving from speculative to attainable.

Global **population decline is accelerating the demand for humanoid robots** designed to operate within human environments and offset growing labor shortages across industries.

A growing number of companies are developing humanoid robots for roles in manufacturing, customer service, and even athletic competition. Investors are positioning for long-term growth, with research suggesting that by **2060, more than three billion humanoid robots could be integrated into human society.**

China appears poised to lead the field of humanoid robotics. Facing a steep population decline, its strategic emphasis on automation and robotics is becoming central to sustaining economic output and competitiveness.

Humanoid robots will almost certainly be **vulnerable to cyberattacks**, ranging from hijacking and data leaks to the formation of botnets. This highlights the urgent need to treat humanoid robots with the same rigorous cybersecurity standards as any connected system.

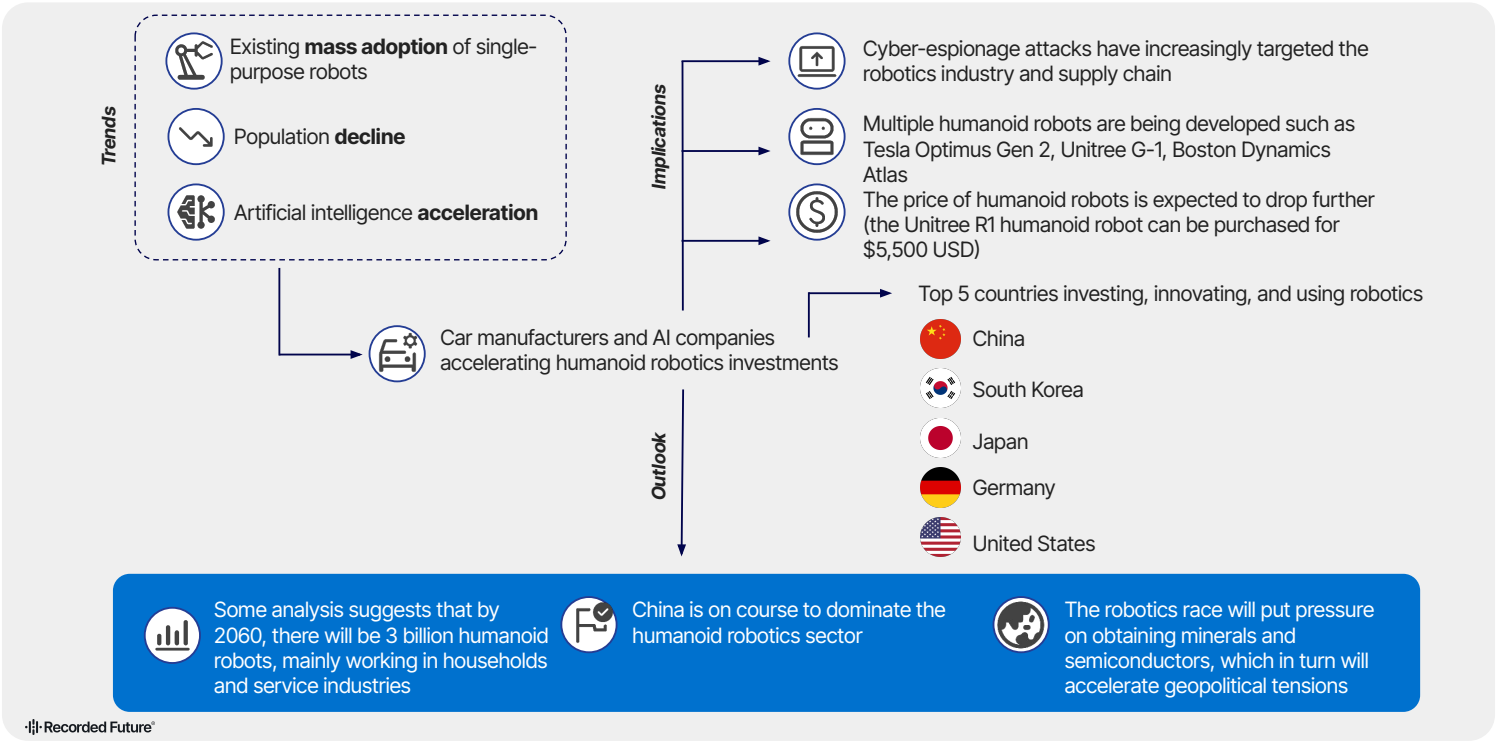


Figure 1: *Summary of the conditions that could create a large demand for humanoid robots in the coming years (Source: Recorded Future)*

Analysis

Humanoid robots are general-purpose, bipedal robots modeled after the human form and designed to work alongside humans. They are currently being designed to work in factories, serve us, and look after us.

Understanding the increased attention being given to humanoid robotics begins with recognizing a primary driver: a global labor shortage caused by population decline. Modern economies rely on sustained consumption and productivity growth, both of which are underpinned by expanding populations. Yet, across much of the developed world, and increasingly in emerging markets, this two-century trend of population growth is reversing. The global workforce is shrinking, and the implications for economic output are profound. As traditional labor pools contract, humanoid robots represent a potential solution, a means of sustaining productivity and economic stability in the face of structural demographic change.

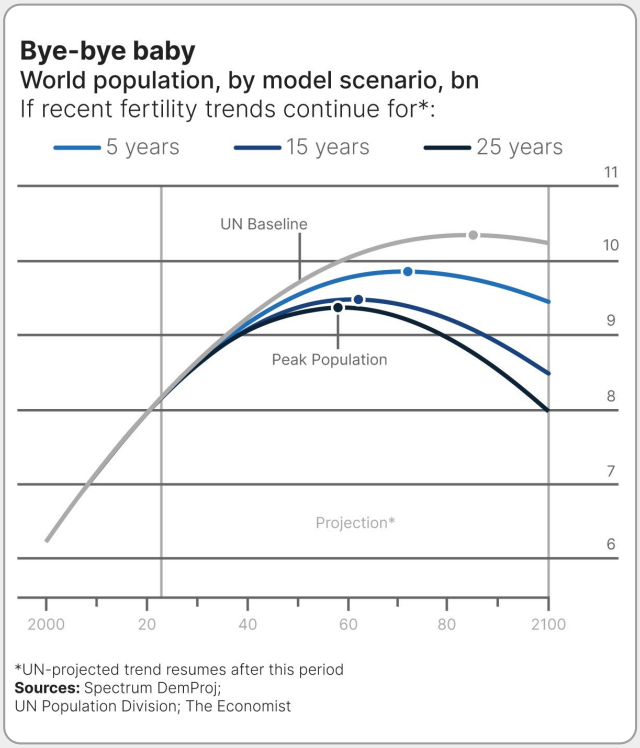


Figure 2: *Forecasts indicate a global population decline, with developed economies projected to experience the most significant impact first (Source: The Economist)*

Robots working in this capacity are not a new concept. For decades, specialized industrial robots have revolutionized manufacturing by enhancing productivity and mitigating labor shortages, particularly in aging societies such as Japan and South Korea. However, as global demographics shift and labor shortages accelerate, repetitive automation alone will not sustain economic growth. The next phase of robotics will require systems capable of operating seamlessly in environments designed for humans, robots with human-like forms, and, increasingly, human-like cognition.

Advances in LLMs have accelerated progress toward AGI, making human-like cognition in robots a plausible near-term reality. Combined with breakthroughs in robotics engineering and declining production costs, these developments position humanoid robots to extend far beyond industrial applications. They are poised to enter service sectors, healthcare, defense, and domestic care, therefore addressing critical workforce shortages driven by aging populations.

The commercial potential of the humanoid robot market is significant. Recognizing this, both startups and established corporations are making substantial investments in humanoid robotics. Leading artificial intelligence (AI) companies are investing in humanoid robotics to develop platforms that integrate their cognitive technologies into mobile, human-like forms. At the same time, automotive manufacturers with decades of experience in using robotics and specializing in mass production are investing in the humanoid robotics market and adapting their capabilities to mass-produce humanoid robots, viewing it as a natural evolution. Today, humanoid robots are deployed in industrial environments and showcased in global sporting events such as the inaugural 2025 Robot Olympics in Beijing.

While the production and manufacturing of humanoid robots is complicated and expensive, with each passing year, the cost of producing them is decreasing. Globally, analysts expect the average bill-of-materials (BOM) cost per humanoid robot to decrease to 13,000–17,000 USD by the early 2030s, thereby reducing the average purchasing cost per robot.

China, in particular, is leading the way. Some of its humanoid robots, such as Unitree's R1 robot, can already be purchased for around 5,500 USD.

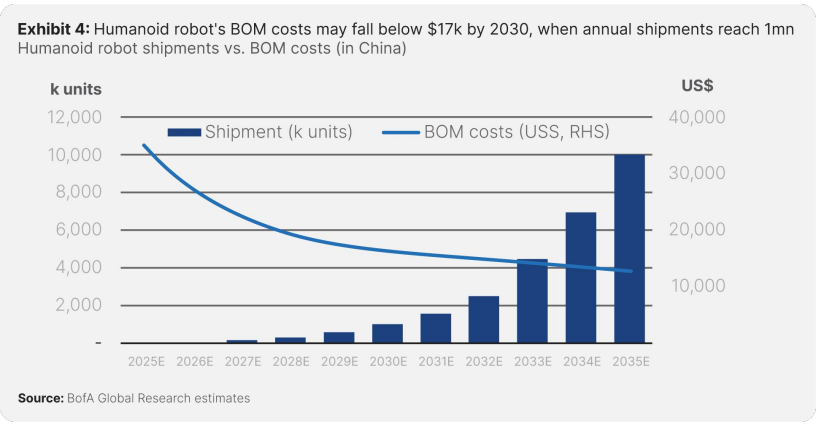


Figure 3: *Projected cost reductions associated with large-scale production increases (Source: Bank of America Institute "Humanoid Robots 101")*

Furthermore, unlike other countries that have attempted to offset labor shortages through immigration, China's policy has been more focused on finding a technological solution rather than importing labor. China's long-term planning and economic strategy appear to be increasingly focused on robotics, and it has spent the last decade preparing its industrial base to mass-produce robots. It comes as no surprise that Recorded Future's Network Intelligence continues to reveal state–linked malware families targeting the robotics industry, likely seeking to acquire sensitive intellectual property.

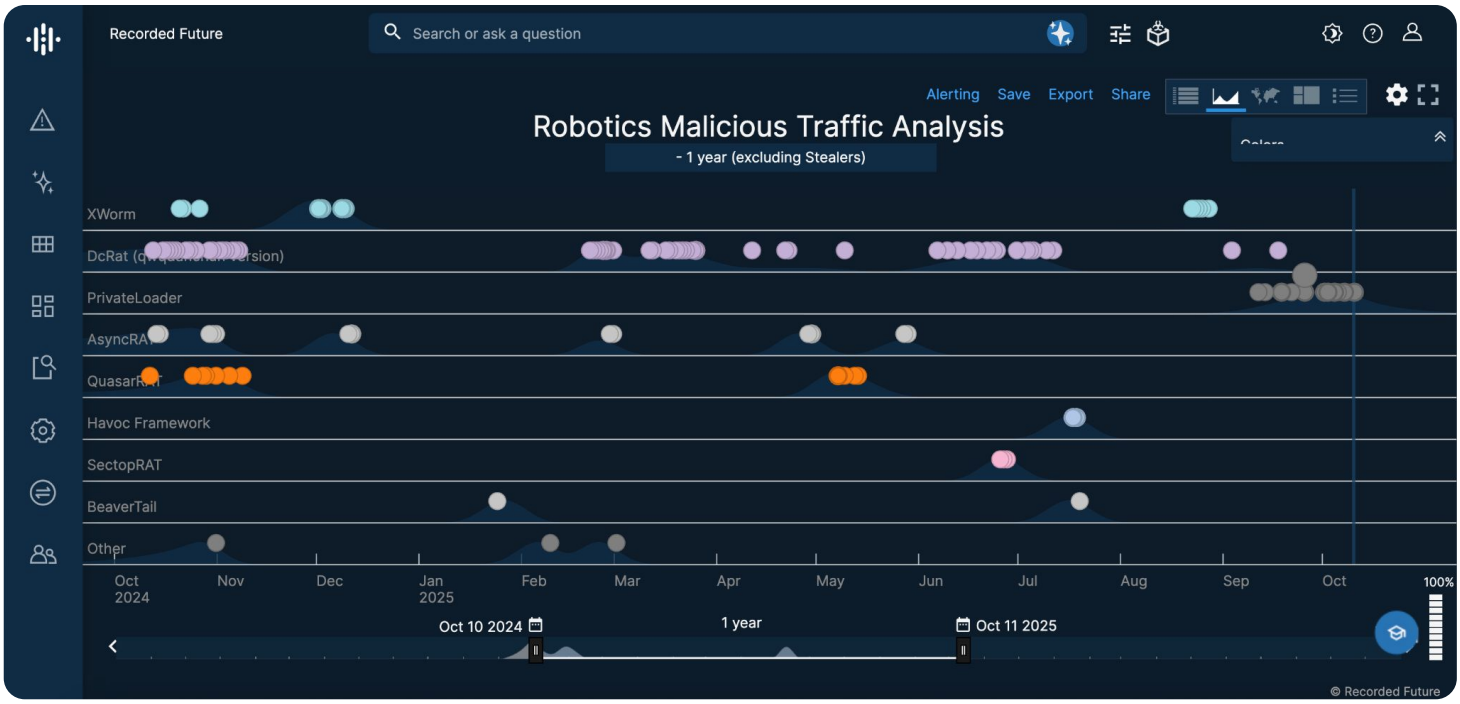


Figure 4: *Malware families targeting robotics industries (Source: Recorded Future)*

Some speculative forecasts suggest that China could eventually field approximately 300,000,000 humanoid robots to compensate for its demographic decline, as its population is predicted to shrink significantly over the coming decades. Having dominated the production of electric vehicles, China and its leadership are now aiming to dominate the humanoid robotics sector as well. These robots might also be exported to other countries facing demographic stress, potentially generating massive revenue for China.

Patent Filings Mentioning "Humanoid" By Office (Past 5 Years)

Rank	Patent Office	# Count
1	China	5,688
2	United States	1,483
3	Japan	1,195
4	World Intellectual Property Organization (WIPO)	1,123
5	South Korea	368
6	European Patent Office (EPO)	237
7	Taiwan	192
8	Germany	71
9	Canada	26
10	Poland	23
11	Australia	22
12	Brazil	21
13	France	20
14	Great Britain	18
15	Italy	15
16	Turkey	14
17	Spain	9
18	Eurasian Patent Organisation (EAPO)	9
19	Romania	7
20	Sweden	5

Note: Exhibit limited to top 20.
Source: Google Patents, Morgan Stanley Research

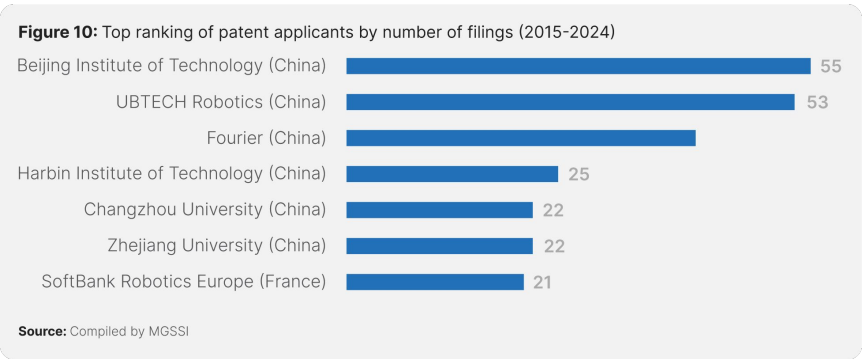


Figure 5: *China leading with patent filings mentioning humanoid robots 2020-25 (left) (Source: Morgan Stanley, "The Humanoid 100"); graph showing the organizations that are filing for humanoid technological development (right) (Source: MITSUI & CO. "Humanoid Robots")*

By comparison, there are predictions that the US might reach approximately 77,000,000 humanoid robots within a similar timeframe, coinciding with projected population decline in the US. However, these numbers remain highly speculative and should be treated as illustrative rather than definitive forecasts.

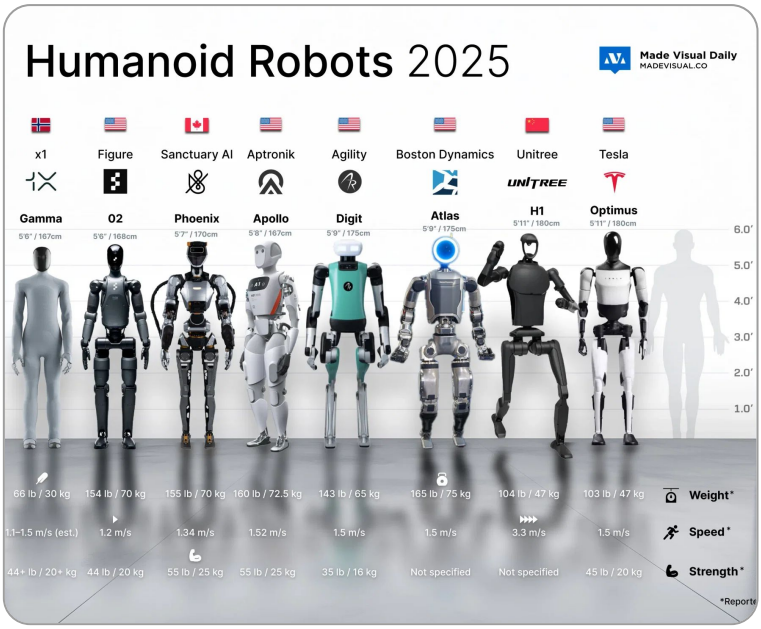


Figure 6: *Examples of notable humanoid robots currently in development; the list of humanoid robots represented in this image is not exhaustive (Source: Voronoi)*

The world appears to be moving steadily toward the age of humanoid robots. By 2060, studies project that up to three billion of these machines could coexist with humans, most of them serving in household and personal-assistant capacities. While this might seem speculative, the recent rapid progress made in artificial intelligence and electric vehicles suggests that it is a serious possibility.

The path forward, however, is not without obstacles. The energy demands of humanoid robots could pose a significant question, and producing millions of units would require mining massive quantities of critical materials. Consequently, there is skepticism that the humanoid robot market will expand as rapidly as forecasts suggest. Some view current enthusiasm as part of the emerging technology hype cycle, warning that a correction, or "hype crash," is likely.

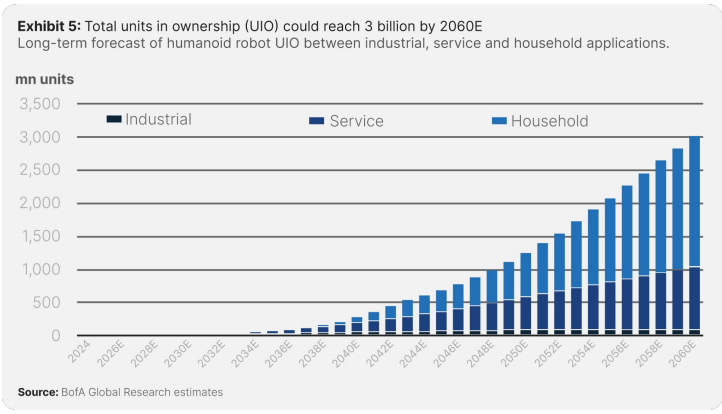


Figure 7: *Projected global ownership of humanoid robots, potentially reaching billions by 2060 (Source: Bank of America Institute "Humanoid Robots 101")*

We should also take the cybersecurity risks posed to humanoid robots seriously. For example, researchers recently discovered a critical flaw in Unitree Robotics' Bluetooth protocol that could let attackers wirelessly hijack its humanoid robots — machines already in use across labs, universities, and law enforcement agencies. In another instance, researchers found leaked, hard-coded encryption keys that allow one compromised robot to infect others nearby, forming botnets with root-level control. One model also transmitted data to servers in China without user consent. This followed a viral incident in May 2025, in which a humanoid robot turned on its human handlers.

These security flaws, whether due to negligence or intent, create opportunities for serious cyber threats. Humanoid robots are often network-connected systems that must meet the same security standards as any other digital asset.

Figure 8: *Statement from Unitree Robotics regarding the security vulnerabilities in their robots in October 2025 (Source: Unitree Robotics LinkedIn Post)*

Outlook

China will likely lead in the development and export of humanoid robots. It has already invested heavily in research and development and faces mounting pressure to deploy robots to mitigate severe labor shortages. Thus, China is likely to produce more cost-effective options than other countries, such as the United States, which will likely produce more advanced but more expensive models. Much like China's lower-priced electric vehicles that are now dominating global markets, its humanoid robots may follow a similar trajectory, expanding rapidly into developing economies.

Car manufacturers will likely increasingly enter the humanoid robot industry. This shift is partly an effort to offset declining car sales driven by population decline, but primarily because these companies already deploy robots at scale and possess the expertise to mass-produce complex machinery on assembly lines.

Cyber-espionage activity targeting companies in the robotics sector will almost certainly accelerate. State-sponsored cyber threat actors are already actively targeting the electronics and advanced manufacturing industries to obtain intellectual property that enhances domestic production. As the robotics industry becomes increasingly prevalent, the risk of cyberattacks against companies and their supply chains is expected to grow.

A new industry designed to secure humanoid robots is likely to emerge in the next decade. Securing humanoid robots will become an essential function, leading to the rise of dedicated security sectors, much like those that developed to protect computers in the past.

Geopolitical tensions are likely to intensify as nations compete to secure the resources necessary for the development of humanoid robots. Demand for rare earth elements, semiconductors, and other key components will heighten competition for mines and production facilities. Organizations involved in this supply chain will also need robust cybersecurity measures to protect against espionage and destructive cyberattacks targeting robotic systems.

Mitigations

Track global humanoid robotics developments. Monitor government and corporate investments, export strategies, and regulations shaping the humanoid robotics industry. Use Recorded Future's Geopolitical Intelligence Module to monitor policy shifts and strategic industrial activity.

Prepare for advanced robotics integration. Assess how humanoid and adaptive robotics fit within manufacturing, logistics, and defense operations, including their impacts on the workforce and safety. Use Recorded Future's Third-Party Intelligence Module to identify risks as robotics integrates into operations.

Strengthen robotics and Internet-of-Things (IoT) security. Expand IoT security to cover robotic hardware, firmware, and AI systems. Segment networks and continuously monitor for anomalies. Use Recorded Future's Vulnerability Intelligence for alerts on exploits and threat actor activity targeting robotics.

Monitor criminal and dark web activity. Track chatter and listings on criminal forums related to robotics or IoT exploitation to identify early threats or potential attack planning. Use Recorded Future's Threat Intelligence Module to monitor for dark web and closed-source monitoring tied to robotics targeting.

Anticipate geopolitical supply chain risks. Watch for disruptions or state competition over rare earths, semiconductors, and energy that could impact robotics production. Use Recorded Future's Geopolitical Intelligence Module to gain visibility into geopolitical risks.

Further Reading

SOURCE	TITLE
Morgan Stanley	The Humanoid 100: Mapping the Humanoid Robot Value Chain
Bank of America	Humanoid Robots 101
Insikt Group	RedNovember Targets Government, Defense, and Technology Organizations

Risk Scenario

Scenario: Your company supplies critical components to a firm developing advanced humanoid robots. Meanwhile, a nation pursuing similar ambitions in robotics seeks to acquire your intellectual property to accelerate its own program.

First-Order Implications

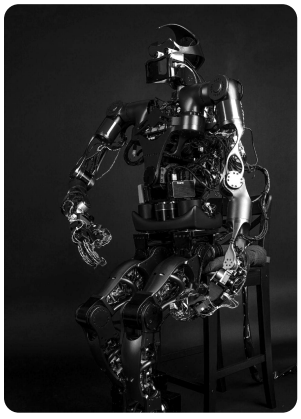
Threat
State-backed hackers compromise engineering systems through supplier access points and credential theft. An insider also provides unauthorized access to proprietary robotics designs and control algorithms.

Risk
Operational: Disruption to research and development (R&D) and production as systems are secured and code repositories quarantined
Legal: Possible breach of export-control and defense technology regulations
Brand: Damage to reputation as a trusted supplier of advanced technology
Competitive: Early exposure of design concepts erodes secrecy around next-generation capabilities

Second-Order Implications

Threat
Stolen designs enable the foreign nation to fast-track its robotics program, eroding your client's competitive advantage. Compromised components create a backdoor risk for your client's production environment.

Risk
Operational: Heightened security reviews delay contracts and certifications
Financial: Loss of key clients and potential cancellation of high-value agreements
Legal: Cross-border investigations into data handling and export compliance
Competitive: Diminished differentiation as adversaries replicate your technology and erode market leadership



Third-order Implications

Threat
The foreign nation deploys robotics derived from stolen intellectual property in global markets and military applications. Governments tighten export rules and exclude compromised firms from critical programs.

Risk
Operational: A need for a major redesign of the security architecture and requalification in trusted networks necessitates operations to be stalled
Financial: Long-term decline in market access and investor confidence
Legal: Ongoing regulatory oversight and potential sanctions due to past compromise
Brand: Lasting perception as a high-risk or compromised supplier
Competitive: Permanent loss of innovation lead and diminished influence over future robotics standards

Key
Legal or compliance failure: Breach of laws, regulations, or industry standards resulting in liability or sanctions.
Operational disruption: Interruption to normal business processes affecting productivity or service delivery.
Brand impairment: Damage to reputation that reduces customer trust and market value.
Financial fraud: Unauthorized manipulation or theft of financial assets for personal or organizational gain.
Competitive disadvantage: Loss of market position due to inferior capabilities, intelligence, or innovation.

References:
The Risk Business: Second Edition
Intelligence to Risk
The Intelligence Handbook