Recorded Future®

EXECUTIVE INSIGHTS REPORT | JULY 2026

Emerging Threats to Neurotechnology

From Insikt Group®

Summary

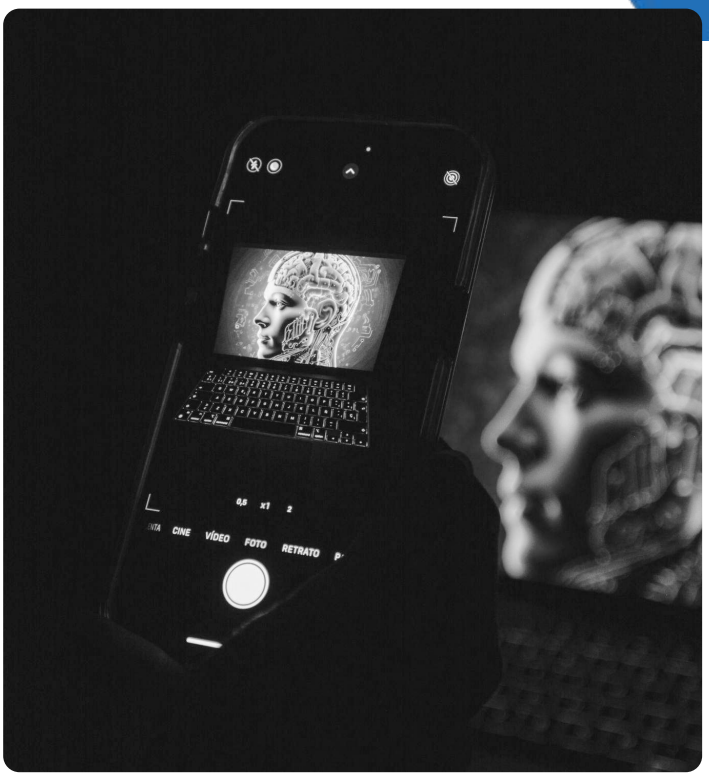
Neurotechnology is rapidly moving beyond clinical use cases, expanding the attack surface for sensitive neurological and biometric data: As adoption grows, larger volumes of brain activity, biometric, and behavioral data will be collected by commercial platforms, creating new opportunities for data theft, misuse, and exploitation.

China and the United States (US) are engaged in strategic competition in neurotechnology development: The US leads in the number of neurotechnology firms, and brain-computer interface (BCI) research has been a long-term research priority for the US military. At the same time, China's five-year guidance for BCI development, subsidies for major wearable technology firms, and military research into human-machine integration suggest that neurotechnology is a strategic priority.

Leading neurotechnology companies are likely to face increased targeting for intellectual property (IP) theft: Because neurotechnology is costly to develop and strategically valuable, companies in this sector are likely to become attractive targets for state-sponsored espionage, insider threats, and cyber-enabled theft. Successful IP theft could erode the competitive advantage of companies that invest heavily in research and development (R&D). Military and higher education research laboratories are also likely to be targeted for access to R&D and related data.

Neurological and biometric data will become an increasingly valuable target for cybercriminals and state-linked actors: Attackers may seek to exfiltrate these datasets for extortion, surveillance, strategic intelligence, or model development. The sensitivity of this data could make breaches particularly damaging for affected individuals and companies, making it an attractive target for extortion-focused cybercriminals.

Regulatory and national security scrutiny of neurological data will likely intensify: Existing privacy frameworks in the European Union (EU) and several US states already provide heightened protections for neurological or biometric data, but rapid advances in neurotechnology may outpace consumer protection laws.



Emerging Applications for Neurotechnology

Medical

- Enable control of robotic limbs or mobility devices
- Rehabilitation following stroke
- Treatment of mental health or neurological disorders
- Enable communication through "typing" by thought

Consumer

- Video game control and virtual reality
- Stress management, focus improvement, and mental wellness
- Workplace safety and productivity systems

Military

- Augmenting soldiers to enhance battlefield performance, such as by detecting fatigue or stress or improving decision-making
- BCI-controlled drone or other weapons systems

Figure 1: *A non-exhaustive list of emerging applications for neurotechnology and BCI (Image source: Recorded Future)*

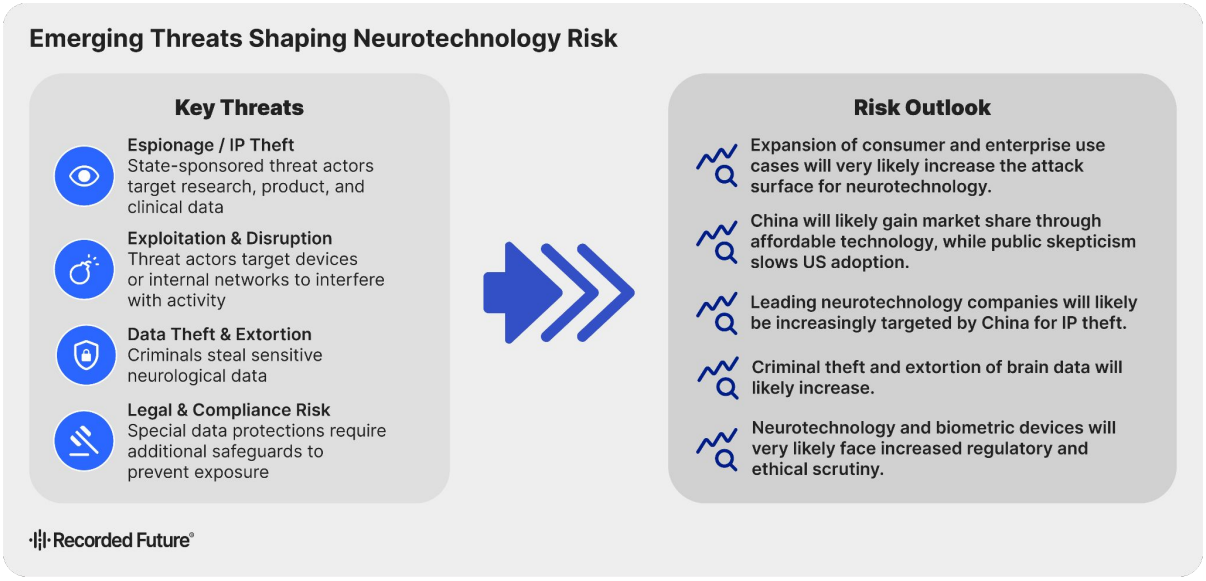


Figure 2: *Key threats in neurotechnology and how they are likely to evolve (Source: Recorded Future)*

Analysis

What is neurotechnology?

Neurotechnology is the field focused on understanding and interacting with the brain through technology. Much of the progress so far has been in medicine, where scientists seek to use the technology to treat neurological disorders such as Parkinson's disease or paralysis. Implantable BCIs have demonstrated the ability to translate brain activity into words, enabling individuals with neurological injuries to speak again. In June 2026, China approved the world's first commercial brain implant, which allows individuals with spinal cord injuries to regain motor control of their hands via a robotic glove. Other BCI technologies remain in clinical trials. Less invasive examples of the technology include medical electroencephalography (EEG) equipment that externally measures brain activity to diagnose and monitor conditions such as epilepsy, sleep disorders, and ADHD. The global neurotechnology market is projected to reach $53 billion by 2034, driven by the rising prevalence of neurological disorders and the rapid evolution of artificial intelligence (AI) and machine learning that enable the interpretation of neurological data.

Outside of medical use cases, the consumer neurotechnology market is rapidly expanding. According to a market study published by the Centre for Future Generations in mid-2025, 45 consumer neurotechnology brands focused on wellness and fitness emerged over the last decade, making it the largest consumer sector in neurotechnology devices. These include products that monitor brain activity to improve focus, such as glasses that use neurofeedback to darken when the user is distracted and lighten when they are focused, as well as products that use brain data for "brain training" exercises to improve calmness and focus.

Other consumer use cases include devices for hands-free gaming and entertainment. In 2025, the consumer market outpaced the medical market in terms of the number of new companies.

Established technology companies such as Meta and Google are also investing in neurological and neurotechnology research. Meta has announced progress in using an AI model to interpret magnetic scans of brain activity to predict what participants were typing. While Meta has highlighted the therapeutic uses of this technology, it has also suggested incorporating it into consumer wearables that would allow users to type or play video games with their minds.

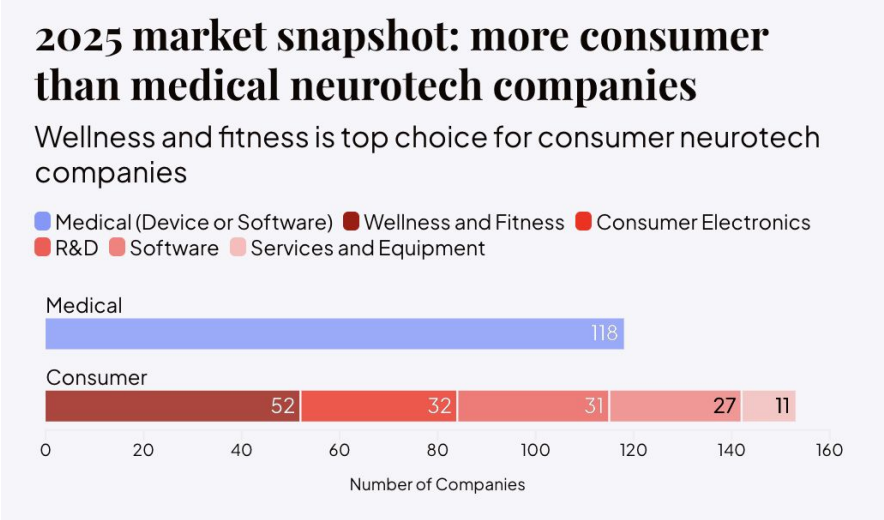


Figure 3: *Breakdown of consumer and medical neurotechnology companies in 2025 (Source: Centre for Future Generations)*

Both consumer and medical neurotechnology devices rely on biometric and neurological data about users to operate and improve. This includes measurements of brain activity that use blood flow, electrical activity, or magnetic activity as indicators of which brain regions are active and when. Other biometric measures, such as heart rate and electrodermal activity, can also be valuable for understanding cognition and emotion. These measurements are used as a proxy for stress levels in a variety of consumer wearable devices, such as Oura rings, Garmin watches, or Google Fitbits. These devices are growing in popularity, with shipments of wearable products increasing by 9.1% in 2025 from the previous year. AI and machine-learning algorithms are critical to interpreting high volumes of brain and other biometric data into meaningful results for patient and consumer devices.

In addition to commercial and medical uses, neurotechnology and BCI have potentially transformative military applications. Military researchers in multiple countries are exploring BCI to support more effective knowledge transmission, improve decision-making, mitigate the cognitive impacts of stress or fatigue, and enable control over drones or other military platforms through thought. In particular, both the US and China have invested significantly in research in human-machine augmentation for warfighting. The dual-use nature of the technology increases the risk of exploitation, cyber theft, and regulatory exposure (such as export controls), as discussed in more detail below.

Emerging Threats to Neurotechnology and Biometric Data

State-Sponsored Espionage and IP Theft

Much like AI, neurotechnology is a focal point of strategic competition between the US and China. This puts neurotechnology IP and neurological data at greater risk for economic espionage and cyber theft. While the US and Europe lead in the number of neurotech firms, the Chinese company Neuracle has produced the first BCI approved for commercial use. Multiple other Chinese companies are moving toward clinical trials in both invasive and non-invasive BCI. Chinese researchers are second only to the US in neurosciences research output, while leading Chinese labs have pushed for hiring BCI research talent. This is likely the result of national and regional prioritization of neurotechnology and BCI in China. Since at least late 2024, multiple provinces have issued dedicated action plans to spur BCI development, and in July 2025, China's central government issued a guiding document for developing BCI technology through 2030, demonstrating continuing intentions to invest significant resources in advancing neurotechnology.

More broadly, the Chinese market for consumer wearable technology that collects and uses biometric inputs is rapidly expanding. The Chinese government has subsidized wearable technology giants Xiaomi and Huawei, helping them become the top vendors worldwide in smartwatches and smart glasses. Chinese wearables are integrated into a broader AI-enabled software ecosystem, such as Alibaba's smart glasses, which support hands-free calling, music streaming, real-time language translation, e-commerce, navigation, and payments. This expanding market for wearable devices provides a potentially enormous source of biometric data that can be used to further enhance commercial AI models, thereby enabling more accurate integration of biometric data into wearables.

Figure 4: *Xiaomi Mijia Smart Audio Glasses (Source: GizmoChina)*

Technologies prioritized for military or economic advancement in China are often targets of economic espionage and IP theft. Tactics include using malicious insiders to smuggle out sensitive technology, as allegedly occurred at General Electric and Google. Widespread cyber campaigns have also led to IP theft at companies in strategically important industries such as manufacturing, energy, and pharmaceuticals. Neurotechnology companies targeted for IP theft risk a significant competitive disadvantage, as the returns on costly research and development investments may be reduced, including through increased market competition by beneficiaries of stolen IP.

The neurological and biometric data collected by these devices may also be targeted for theft. Threat actors linked to the Chinese government have a long history of targeting personally identifiable information (PII) for mass exfiltration, though in the last several years, espionage has become increasingly targeted toward specific intelligence priorities. Examples of mass data exfiltration incidents include the 2015 Anthem hack (affecting nearly 80 million customers), the 2017 Equifax breach, and the 2018 breach of Singapore's largest healthcare provider (affecting 1.5 million patients). More recently, the Salt Typhoon campaign breached dozens of US telecommunications companies, though these attacks may have targeted specific individuals or critical national security systems. As the ability to analyze and use biometric and neurological data advances, this data has the potential to become a strategic asset for the Chinese military and may become increasingly valuable as a target for data exfiltration.

Cyber Exploitation and Disruption

Neurotechnology devices may also be targets for cyber threat actors seeking to disrupt functioning and thereby cause harm to patients. Previous vulnerabilities found in medical devices have led to safety recalls due to the risk that an exploitation of the vulnerability could prevent the device from functioning. Currently, at least one vulnerability has been discovered in a consumer brain-wave monitoring device that would allow attackers to remotely disrupt its output, leading to incorrect data about brain activity. As more medical and consumer neurological devices reach the market, more vulnerabilities are likely to be discovered.

In addition to vulnerabilities in the device itself, threat actors can target vulnerabilities in remote monitoring systems, including mobile applications and cloud-based software that collect and interpret neurological data from the device. This data could be tampered with to give inaccurate readings, obscuring potential health problems or causing false alarms. Finally, attacks on information technology systems at neurotechnology companies can lead to downstream operational disruptions for device users. The recent cyberattack against Stryker delayed some surgical procedures because the company was unable to deliver patient-specific products.

Vulnerabilities in biometric trackers are more prevalent, as these devices are more widely available. As of June 2026, 31 vulnerabilities were recorded for biometric trackers, primarily smartwatches, of which seven have a severity rating of "critical," requiring immediate remediation. Exploiting these vulnerabilities could give attackers access to sensitive data or disrupt medical or wellness functionality.

Data Theft and Extortion

Criminal theft of brain or other biometric data could pose a significant extortion risk due to the data's sensitivity. In June 2026, neuroscience company Glucobit reported a data breach of its Reframe app, a digital resource that purports to apply research on how the brain responds to alcohol to help manage alcohol use. The app collects data on users' daily habits, alcohol consumption, and emotional well-being. While it is not yet clear which system was affected, the company's data breach notification letter warns about unsolicited communications referencing users' "health, wellness, or personal habits," suggesting that sensitive personal data may have been exposed in the breach.

Criminals could weaponize this data in highly targeted scams, such as using the information to build trust in romance scams or to advertise fraudulent treatment programs. Data on alcohol use and brain activity, or connections between the two that may be generated by analytics in the app, may also be used in extortion schemes, with perpetrators threatening to expose the information to a victim's friends, family, or coworkers.

As consumer and medical neurological or neuroscience products become more widely adopted and as data from those devices becomes increasingly interpretable into thoughts, emotions, or health conditions, this data will likely become more attractive to cybercriminals.

Legal and Privacy Risks

Due to its sensitivity, neurological data has received additional scrutiny under regulatory regimes. The EU extends a special category of protection for brain data under the General Data Protection Regulation (GDPR), while multiple US states have added additional protections for neurological data under their privacy regulations. This means that exposure of this data can result in increased penalties if companies fail to implement sufficient data protection measures. However, rapid advances in neurotechnology may create gaps in consumer protection and raise new legal questions, such as whether employers have the right to collect employees' brain data. An emerging protection gap concerns consumer wellness products that collect brain data or other biometrics to help improve focus, reduce stress, or manage habits. Because many of these products are not offered by HIPAA-covered entities, HIPAA may not apply, leaving sensitive health-adjacent data governed mainly by consumer privacy, FTC, or state-law protections.

In addition, the dual-use nature of neurotechnology devices poses risks related to export controls and other national security regulations. In 2023, a Harvard scientist was found guilty of lying to US officials about payments he received from China's Thousand Talents recruiting program. He was investigated because his research was funded by US government entities, including, in part, by the Department of Defense. This counterintelligence investigation demonstrates the national security importance of the research for both the US and China. Future advances in US neurotechnology research or applications may fall under export control, potentially even limiting consumer availability.

Outlook

Expansion of consumer and enterprise use cases will very likely increase the attack surface for neurotechnology: As neurotechnology becomes cheaper and easier to use, consumer and enterprise use cases for neurotech products will increase. This will entail increasing numbers of people using neurodata for non-medical use cases, including hands-free gaming and stress reduction. On the enterprise side, this may include professional development tools, such as focus-improvement tools, as well as safety monitors for jobs that require sustained attention, such as pilots or heavy-machinery operators. Increasing use cases will significantly expand the attack surface for exploiting neurotechnology operations or data.

China will likely gain market share through affordable technology, while public skepticism slows US adoption: While the US is likely to continue to support the largest market for neurotechnology, Chinese companies will excel in expanding affordable products, as they have in other emerging technologies. This will likely result in a greater global user base for Chinese neurotechnology products. A larger customer base may give these companies a competitive edge as more data will be valuable for improving the accuracy and utility of algorithms. At the same time, US consumer adoption may be slowed by negative public perceptions of big technology companies and AI, similar to the lower adoption of AI in the US compared to other advanced economies.

Leading neurotechnology companies will likely be increasingly targeted for IP theft by China: Both medical and consumer companies will be increasingly targeted by industrial espionage campaigns as China continues to pursue neurotechnology as a strategic technology. This will likely include cybertheft carried out by state-sponsored threat groups, as well as the compromise of current employees or the embedding of insider threats at leading US-based neurotechnology companies.

Criminal theft and extortion of brain data will likely increase: As the number of users grows, criminals will seek ways to exploit this new, highly sensitive data. This may include probing neurotechnology companies for security vulnerabilities to expose mass customer datasets, or individually targeting users by threatening to reveal sensitive data about their mental state.

Neurotechnology and biometric devices will very likely face increased regulatory and ethical scrutiny: The ethical considerations surrounding technology that promises “mind reading”-like capabilities will accelerate debates not only around data protection, but also on whether and how neurological data should be collected and interpreted. The United Nations, the EU, and the International Committee of the Red Cross (ICRC) have already begun to consider the technology's impacts on human rights. Certain applications of neurotechnology, such as use in weapons systems, mass surveillance, or criminal justice, may be banned outright in some jurisdictions. Existing data and privacy protection laws will almost certainly need to be revised to sufficiently address the risks.

Mitigations

Establish rigorous continuous monitoring, vetting, and data access controls to counter industrial cyber espionage and malicious insiders attempting to smuggle proprietary neurotech IP out of the organization.

Audit external manufacturing partners, hardware vendors, and subsidized software ecosystems (such as integrated wearable components) to prevent backdoor data access by foreign national security regimes. Use Recorded Future’s Third-Party Risk Module to continuously monitor the security postures of external hardware and software suppliers handling biometric payloads.

Review and update data governance frameworks to align with emerging US national security "bulk data" restrictions and EU GDPR protections governing neurological privacy.

Further Reading

SOURCE	TITLE
Centre for Future Generations	Neurotech consumer market atlas
ICRC	Merging man and machine: A legal assessment of brain-computer interfaces in armed conflict
Politico	Silicon Valley Wants to Put a Chip in Your Brain
Prism	Minds at War: China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology

Risk Scenario

Scenario: A US-based company developed a non-invasive BCI that accurately translates brainwave patterns into text and images, becoming the first non-invasive device to receive FDA approval for therapeutic use. As the company prepares to bring the device to the US market (with a later international release), its security team discovers malware on an employee device sending a beaconing signal to an unknown IP address, prompting an extensive internal investigation.

First-Order Implication

Data exposure disrupts product release

Threat

Network compromise: Investigations discovered malware on multiple employees' devices, allowing the attackers to access sensitive clinical trial data.

Risk

Operational disruption: Product release is on hold while incident responders confirm the extent of the breach.

Brand impairment: News of the breach leads to the perception that the neurotechnology company does not take security seriously, harming customer trust.

Second-Order Implication

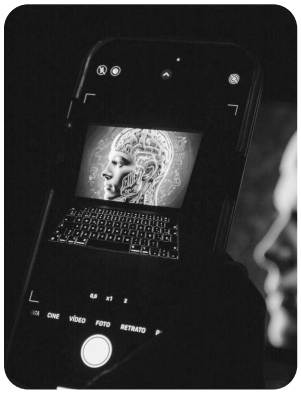
IP theft leads to competitive disadvantage

Threat

Insider threat: During the investigation, responders discovered that an employee had accepted a bribe to exfiltrate sensitive product data.

Risk

Competitive disadvantage: A company based in China releases a lower-cost version of the product a few months before the planned international release.



Third-Order Implication

Increasing geopolitical competition with China leads to increased government scrutiny of neurological data collection and neurotechnology

Threat

Regulatory complexity: The growing incidence of neurotechnology IP theft linked to China state-sponsored actors, combined with recent breakthroughs in medical and consumer BCI devices by Chinese companies, has led to increased government regulation of the industry.

Risk

Legal and compliance failure: Companies must comply with overlapping compliance regimes, including sanctions, CFIUS, sensitive bulk data, HIPAA, and consumer privacy. Failure to comply may result in fines and legal costs.

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