DARKTRACE

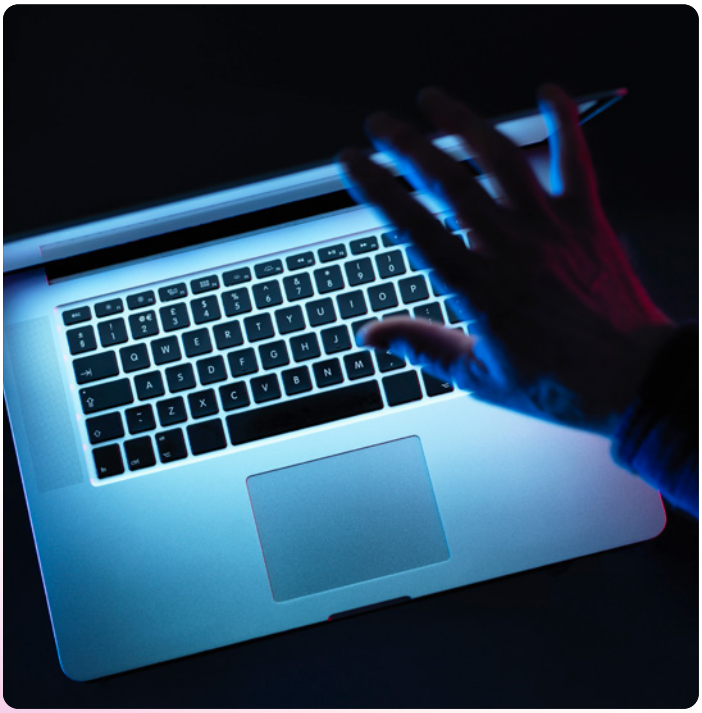
CRIMSON ECHO
KEY TAKEAWAYS FOR BUSINESS LEADERS

For many executives, cyber risk discussions focus on incidents, breaches, outages, and operational disruption. However, Darktrace's research on Chinese-nexus cyber activity suggests a different reality.

An analysis of three years of organizational-centric behavioral data, including dozens of medium- to high-confidence intrusions, found a clear pattern: advanced cyber operations are increasingly conducted as a form of long-term strategic positioning rather than isolated events and incidents.

The findings of "Crimson Echo: Understanding Chinese-nexus Cyber Tradecraft Through Behavioral Analysis" indicate that cyber access itself is often the objective, with attackers seeking to establish footholds not for immediate disruption or theft, but to gain persistent visibility into systems that underpin economic competitiveness, supply chains, and critical infrastructure.

For business leaders, this represents a shift. Cyber risk is no longer best understood as a series of incidents, but instead a structural, long-horizon business risk that must be governed with the same rigor as financial risk or supply chain resilience.



What the Research & Data Shows

Darktrace examined anomalous activity detected between July 2022 and September 2025. Using behavioral analysis, threat hunting, and structured attribution methods, the investigation identified dozens of medium- to high-confidence instrusions that may be linked to Chinese-nexus operators.

KEY INSIGHTS FROM THE RESEARCH:

88% of cases observed occurred in organizations classified as critical national infrastructure, including strategically important industries such as transportation, telecommunications, critical manufacturing, healthcare and technology.

88%

22.5% of observed cases involved U.S. organizations, the single largest national share in the dataset. When combined with cases observed in Germany, Italy, Spain and the UK, over 55% of all cases occurred within major Western economies in strategically important sectors.

22.5%

Nearly 63% of observed intrusions began with exploitation of internet-facing systems, highlighting the increasing risk from externally exposed digital infrastructure.

63%

10 DAYS

The median duration of observed compromises was approximately 10 days, with many incidents unfolding rapidly.

However, a small but significant subset persisted for months or even years, where a few highly strategic targets experience longer dwell times.

THE RESEARCH SUGGESTS

Chinese-nexus cyber operations appear to follow two distinct models

"SMASH-AND-GRAB"

SHORT-HORIZON OPERATIONS

The majority of observed cases involved rapid intrusions optimized for speed rather than stealth. These operations were frequently observed in sectors such as critical manufacturing, telecommunications, shipping and logistics, and advanced materials and industrial systems – areas that are closely tied to Chinese industrial policy or foreign policy, such as the Belt and Road Initiative.

They appear to be optimized for achieving competitive industrial advantage, through IP acquisition and insight into supply chains. In these cases, detection risk may be tolerated because speed and scale provide operational advantage.

"LOW AND SLOW"

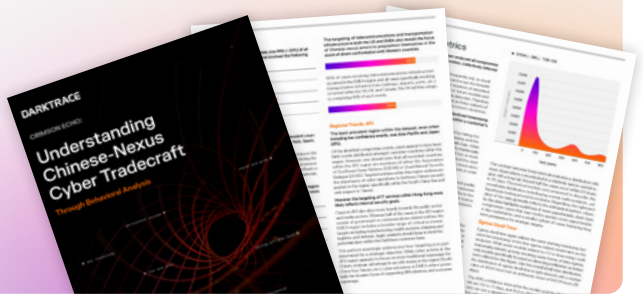
LONG-HORIZON OPERATIONS & STRATEGIC POSITIONING

A smaller but more consequential set of intrusions feature significantly longer dwell times and prioritized persistence over immediate data or IP theft.

Attackers established durable access through identity systems and legitimate administrative tools, often remaining dormant for long periods between bursts of reconnaissance or lateral movement. Many of these cases occurred within critical national infrastructure environments, such as transportation systems, telecommunications networks, and digital service providers.

This suggests access is a strategic asset to preserve and leverage over time.

DOWNLOAD THE FULL REPORT ↗



Why this Matters for Business

Modern enterprises operate with deeply interconnected digital ecosystems: cloud platforms, identity providers, logistic networks, and third-parties form the operational backbone of most global companies.

THERE ARE THREE KEY TAKEAWAYS:

01 **Strategic cyber exposure** increasingly exists beyond the corporate perimeter. Digital infrastructure, cloud services and supply chains create indirect pathways into core business systems.

02 **Persistent access** can generate strategic insight. Even without disruption or data theft, there is risk for attackers to gain visibility into operations, dependencies, and industrial processes.

03 **Cyber risk** increasingly resembles competitive intelligence. Access to internal systems can reveal supply chain structures, product development timelines, and strategic decision-making.

In this context, cyber risk begins to resemble long-term competitive and operational intelligence, **rather than episodic failure.**

The Strategic Context

Chinese-nexus cyber activity increasingly reflects long-term strategic competition rather than isolated hacking campaigns.

As nations integrate cyber capabilities into economic, technological, and geopolitical strategy, digital business environments—particularly those tied to critical infrastructure, supply chains, and advanced technology—have become key terrain.

For business leaders, this means cyber risk must be treated as a structural business risk, not simply an IT issue or incident response challenge.

Organizations that govern digital dependencies, identity systems, and cloud infrastructure with the same rigor as financial and operational risk will be best positioned to compete in this environment.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com