The International Reach of Cyber Threats

Cyberattacks aren't just headlines; they're a persistent threat targeting public safety agencies across the world. The latest threat intelligence report from the PSTA, "The 2025 Geographic Cyber Threat Landscape," highlights significant shifts in this high-stakes battle.

MOTOROLA SOLUTIONS

North America: ground zero for ransomware and disruption

Since 2024, North America has become the epicentre of public safety cyberattacks, with US public safety agencies facing the highest risk of impact and disruption. This isn't just about volume; it's about disruption to mission-critical systems. 71% of all public safety ransomware attacks worldwide have targeted North American agencies this year, with 92% of these incidents in the U.S. This leads to municipalities and public safety agencies being forced to use alternative, less efficient methods to run their operations. The most prominent threat actor targeting North America, Inc. Ransomware, is escalating its assaults against public safety, with an average of one attack every 22 days in 2025 compared to every 33 days in 2024.

Threats from Advanced Persistent Threat (APT) groups are also rising as they target critical infrastructure with persistent access attacks.

Europe: DDoS challenges and rising municipal exposure

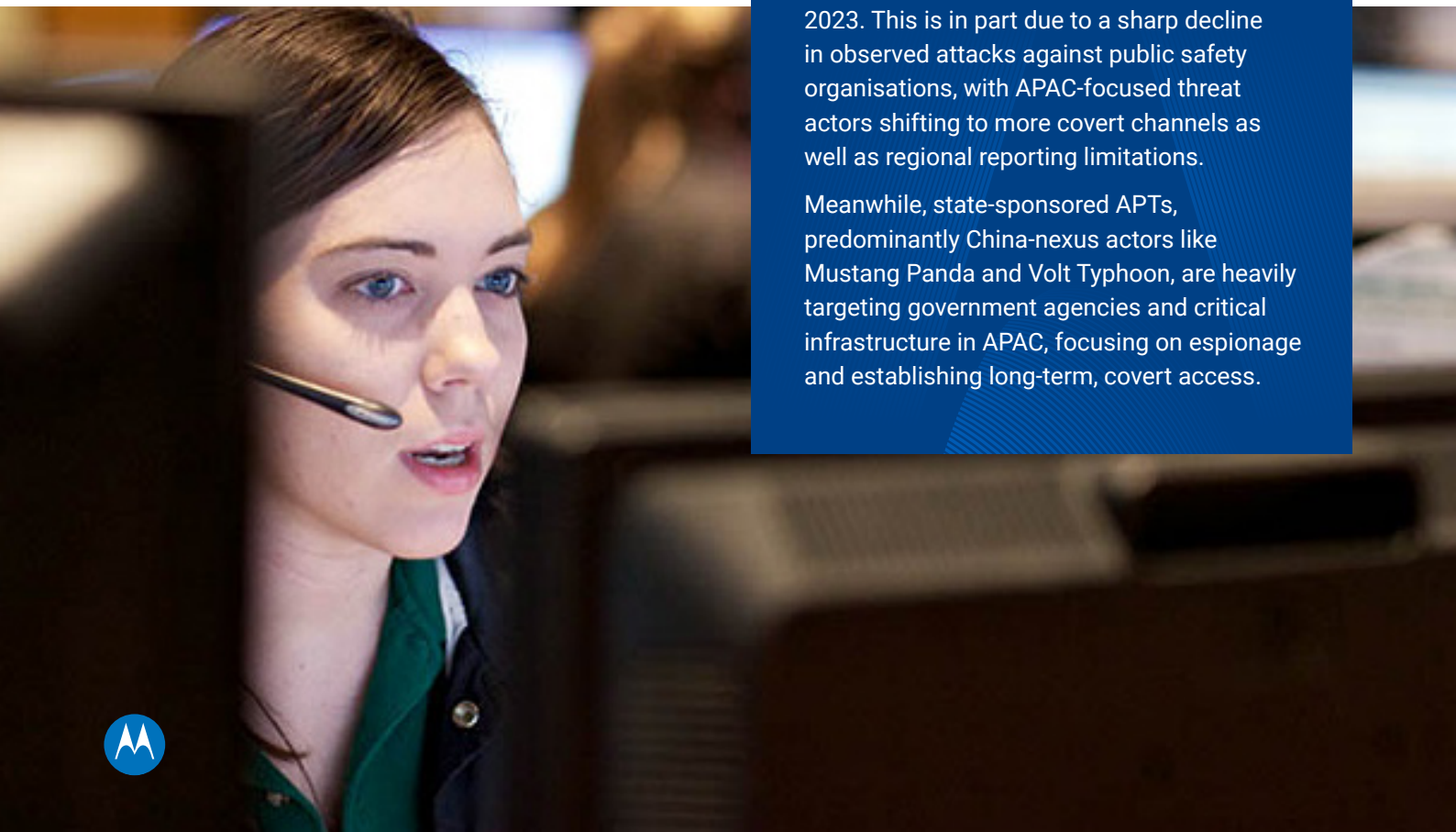
Europe's threat landscape is different, but no less intense. Here, it's a relentless barrage of distributed-denial-of-service (DDoS) attacks: the continent accounts for over 75% of all global DDoS incidents. Hacktivists, like NoName057, are the main aggressors, threatening nations supporting Ukraine, with Germany and France bearing the brunt of 2025's cyberattacks to date.

Additionally, municipalities in Europe are increasingly becoming the target of cybercriminals, experiencing a consistent year-over-year increase in cyberattacks since 2023. In 2025 alone, cyberattacks on European control rooms occurred approximately every 3.3 days, with 75% impacting European public safety. As of June 2025, there have been 27 DDoS attacks on control rooms in Europe, approximately one per week, accounting for 59% of all cyberattacks in the region. While DDoS attacks might seem "low-impact," their ease of execution makes them a preferred tool for less sophisticated adversaries.

Asia-Pacific: the silent threat of espionage and evolving cybercrime

The Asia-Pacific (APAC) region has observed a decline in publicly reported cyberattacks against public safety organisations since 2023. This is in part due to a sharp decline in observed attacks against public safety organisations, with APAC-focused threat actors shifting to more covert channels as well as regional reporting limitations.

Meanwhile, state-sponsored APTs, predominantly China-nexus actors like Mustang Panda and Volt Typhoon, are heavily targeting government agencies and critical infrastructure in APAC, focusing on espionage and establishing long-term, covert access.

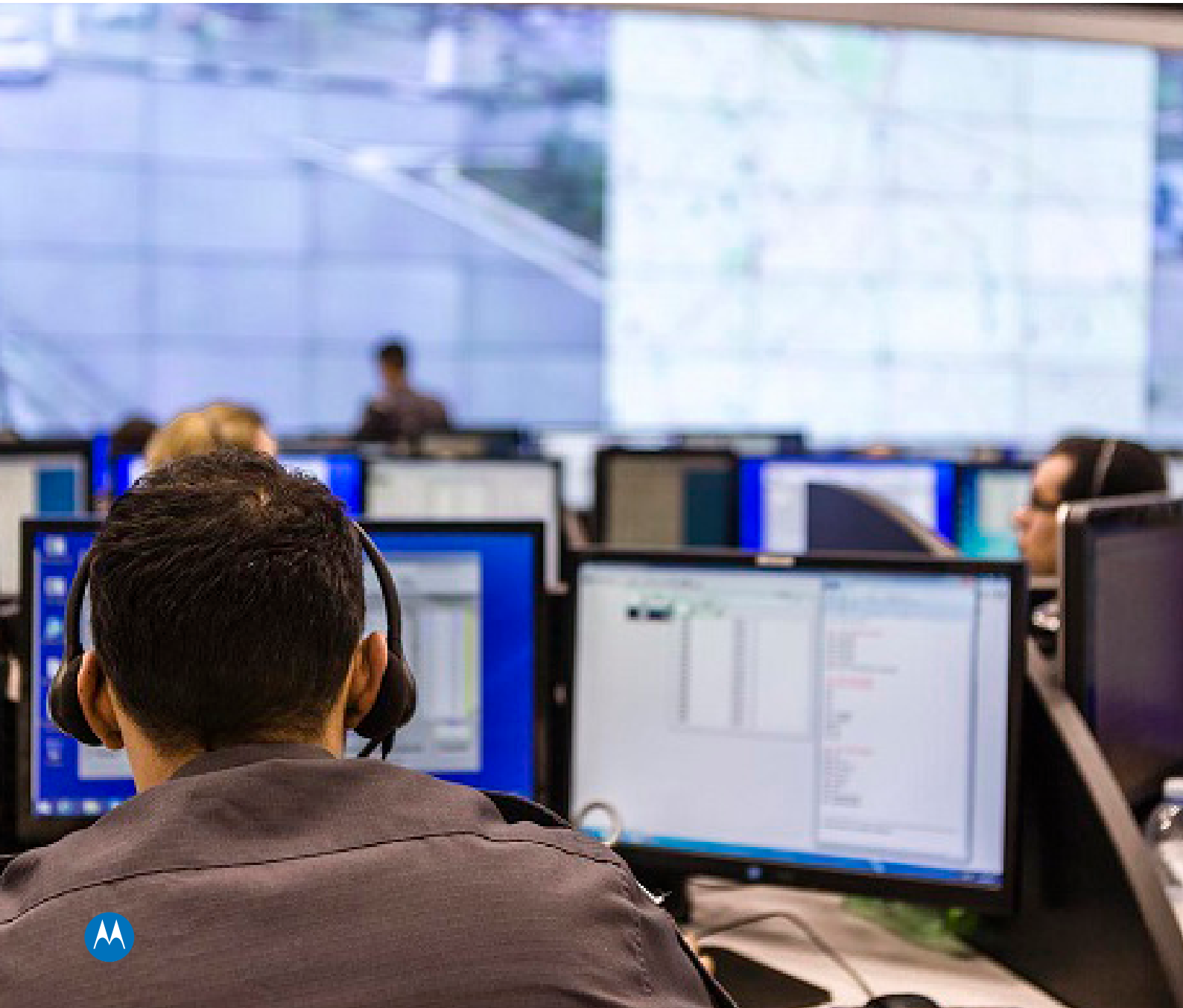


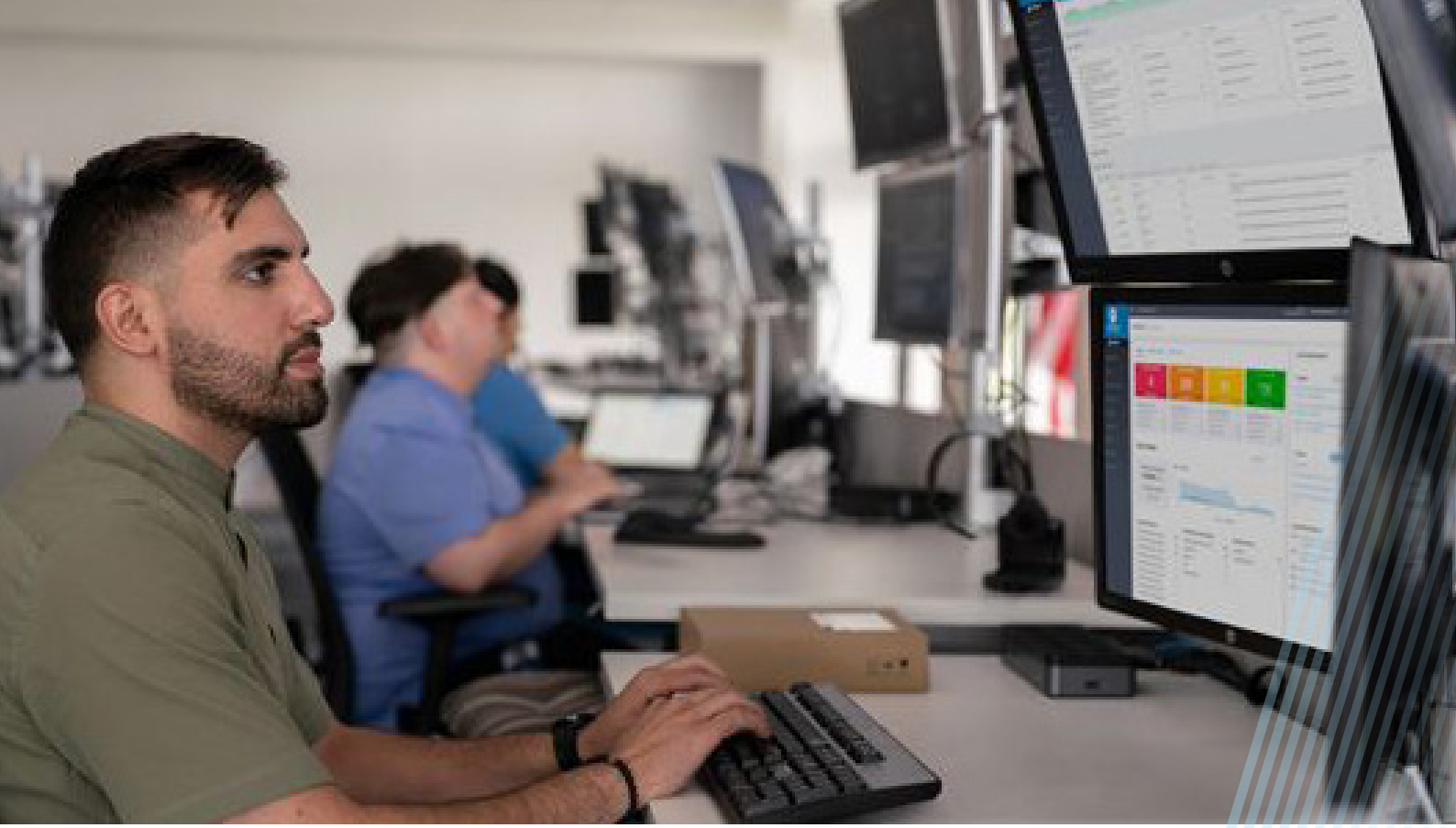
Protecting public safety: key recommendations

To bolster defences against the evolving landscape of cyber threats, public safety organisations worldwide should prioritise cybersecurity. With extortion groups and initial access brokers actively targeting North America, Europe and the APAC region, following best practices such as the Cybersecurity Performance Goals (CPGs) outlined by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) is a crucial first step in reducing risk and protecting public safety emergency communications.

European organisations, in particular, can enhance their resilience against denial-of-service (DoS) attacks by implementing specialised provider services and filtering network traffic to prevent malicious activity, and implementing security monitoring such as Managed Detection and Response (MDR) services.

All regions of the world face significant threats from APTs. Staying informed through threat intelligence services, monitoring known APT indicators of compromise (IOCs) and tracking ongoing campaigns can help identify and counter potential compromises from state-sponsored actors.





Don’t stand alone – join the Public Safety Threat Alliance

The Public Safety Threat Alliance (PSTA) intelligence team is on the front lines, constantly monitoring and evaluating these evolving cyber threats to public safety critical communications.

The PSTA is a collaborative organisation that empowers agencies and members to share vital cybersecurity threat information, boosting collective awareness and readiness. Through the sharing of threat insights, we can collectively fortify defences against these constantly evolving cyber threats.

To find out more about Motorola Solutions’ cybersecurity solutions and services, or to speak to an adviser, **click here**.

For more information, visit **motorolasolutions.com**

MOTOROLA SOLUTIONS