



## Elections and Cybercriminals

In 2024, global elections are under unprecedented threat from malicious cyber activity. With a record number of voters participating, elections in 64 countries, including the highly significant U.S. presidential election, are poised to shape geopolitical relations and military conflicts worldwide. FBI Director Christopher Wray has emphasized the unparalleled risk of election interference, noting the increasing interest of nation-states in influencing electoral outcomes. Analysis reveals a concerning trend, with cyberattacks targeting elections rising from 10% in 2015 to 26% in 2022, a figure corroborated by the Canadian Centre for Cyber Security. Notably, NATO and OECD countries have been prime targets, observing a 100% increase in malicious activity between 2023 and early 2024 across various jurisdictions globally, underscoring the urgent need for enhanced cybersecurity measures to safeguard the integrity of organizations' cyber processes.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email [info@criticalstart.com](mailto:info@criticalstart.com).

-----

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.