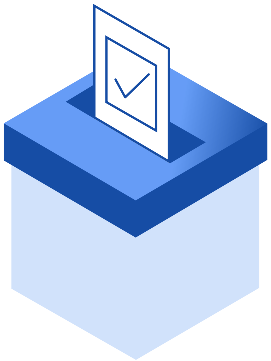
Combating Information Operations & Protecting Elections

Our holistic approach



Across Google, multiple specialised security teams work closely to combat foreign interference threats. Google Threat Intelligence Group (GTIG) — composed of Threat Analysis Group (TAG) and Mandiant Intelligence — focuses on identifying, analyzing, tracking, mitigating, and eliminating entire classes of cyber threats against Google platforms & infrastructure, our users, and our end customers. Our protections are integrated across Alphabet product areas to harden our overall security posture and implement additional defenses against government-backed actors.

Technical analysis paired with direct protections, at Google scale

Intelligence Analysis

We uncover, monitor and conduct in-depth investigations of threat actor TTPs (tactics, techniques and procedures), ranging from state sponsored actors to serious cybercrime groups. This includes government-backed groups focused on espionage and destructive attacks against targeted individuals, governments, industry and critical infrastructure, as well as coordinated deceptive operations (Information Operations) to covertly influence online messaging, especially during elections. We work closely with our elections integrity and imminent threats teams to counter these threats.

TAG Bulletins

Our quarterly **bulletins** highlight direct mitigations implemented across Google products as a result of our intelligence analysis. These bulletins list out coordinated influence operation campaigns terminated on our platforms including YouTube channels terminated, domains blocked as ineligible to appear in Google News, and more.

Advanced Protection Program

We work directly with Google Safe Browsing who protect over 5 billion devices worldwide against malware & unwanted software. Our **Advanced Protection Program** performs even more stringent checks before each download, flagging and blocking harmful files from being downloaded, allowing only app installations from verified stores (i.e. Google Play Store or device manufacturer's app store). We strongly recommend high risk users whose accounts could contain particularly valuable and sensitive information including journalists, activists, business executives, and those involved in elections enroll.

Incident Response Services

Mandiant responds to and investigates cyber incidents to understand how threat actors access methods, including phishing, credential harvesting, malware and known vulnerability exploitation.