Election Cyber Threats in the Asia-Pacific Region

fireeye.com/blog/threat-research/2020/11/election-cyber-threats-in-the-asia-pacific-region.html

Threat Research

Yihao Lim

Nov 22, 2020

6 mins read

Threat Research

In democratic societies, elections are the mechanism for choosing heads of state and policymakers. There are strong incentives for adversary nations to understand the intentions and preferences of the people and parties that will shape a country's future path and to reduce uncertainty about likely winners. Mandiant Threat Intelligence regularly observes cyber espionage operations we believe to be seeking election-related information targeting

governments, civil society, media, and technology organizations around the globe. We have also seen disruptive and destructive cyber attacks and propaganda campaigns seeking to undermine targeted governments and influence the outcomes of electoral contests.

The 2020 U.S. elections are currently drawing attention to election cyber risks, but 2020 has already hosted dozens of elections worldwide, with more to come. In the Asia-Pacific region these included elections in Taiwan, India, South Korea, and Singapore to name a few, with regional elections scheduled for Indonesia in December.

Given the prevalence of such activity worldwide and Mandiant's unique visibility into threat actor activity, we believe it is worthwhile to examine trends in adversary targeting of elections in a variety of regional contexts because the tactics, techniques, and procedures (TTPs) used in one region today may soon be deployed or mimicked in other regions.

Notable Electoral Targeting in Asia-Pacific Region

Mandiant Threat Intelligence tracked numerous elections-related incidents in the Asia-Pacific region in recent years. During this time, the most prolific regional actor was China, which we observed in more than 20 elections-related campaigns most frequently affecting Hong Kong and Taiwan. We believe that China's primary motives for elections targeting includes monitoring political developments, internal stability, and supporting Belt and Road Initiative (BRI) investments.

Examples of Chinese cyber espionage targeting electoral support organizations include:

- Targeting candidates and related staff associated with the November 2019 Hong Kong District Council elections with a malicious macro document.
- Targeting the Australian Parliament in February 2019, three months before the country's general elections.
- Compromising Cambodia's National Election Commission in mid-2018 based on the use of AIRBREAK malware by APT40, possibly looking to understand the impact of the election outcome on Belt and Road Initiative (BRI) plans. See our blog post for more details about this campaign.
- A spear phishing campaign targeting multiple government agencies in Southeast Asia in the spring of 2018 to deliver FIREPIT payloads. The nature of the lure material and targeting indicate the activity was potentially an effort to monitor an upcoming election in the affected country.

Specifically, Mandiant has observed multiple instances in which organizations such as electoral boards and commissions that support or help administer elections have been targeted. Both Russian and Chinese cyber espionage operations have targeted election administrators and government officials since at least 2014. Observed TTPs include phishing and strategic website compromise (SWC), also known as watering hole attacks.

For example, in the November 2019 activity targeting Hong Kong (previously referenced), Mandiant Threat Intelligence believes that candidates or related staff associated with the Hong Kong District Council elections were targeted with a malicious macro document just prior to the elections based on geolocation information, the spear-phishing lure, and other data.

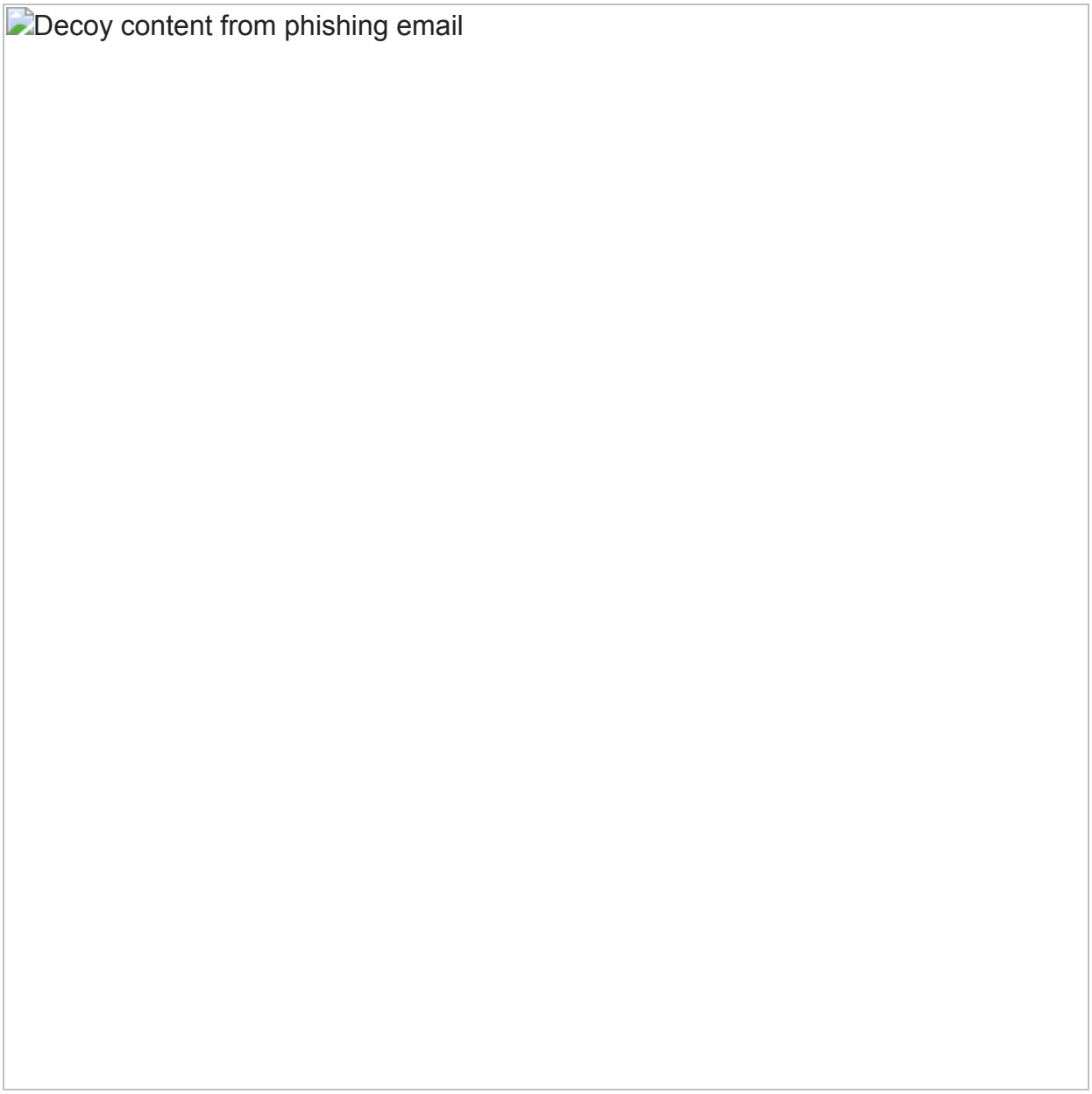

Figure 1: Decoy content from phishing email

Elections Ecosystem

As our readers will know, Mandiant takes a specific approach to deconstructing attacks against elections, which we detailed in a previous blog post.

Our approach examines threats through the lens of risk posed at various levels of the elections ecosystem. We break the elections threat landscape into distinct attack surfaces to better allow our customers and partners to take action. These include the following:

- Electoral Platforms Affecting Public Opinion
- Electoral Process Support Organizations
- Core Electoral Process Systems

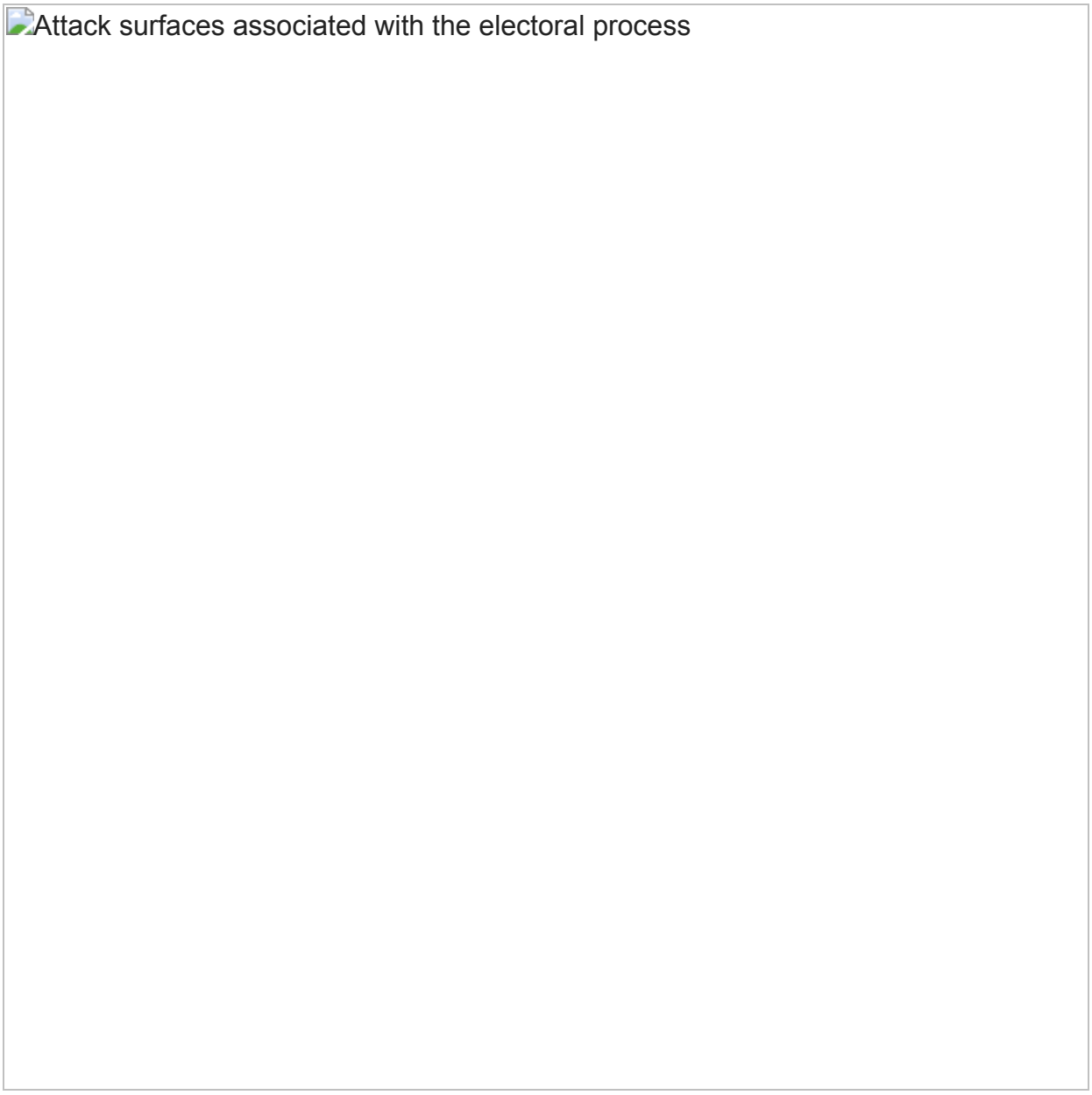

Figure 2: Attack surfaces associated with the electoral process

Top Target of Election Cyber Threat Activity: Public Opinion

Using our ecosystem taxonomy, based on activity observed from 2016 to 2019, Mandiant Threat Intelligence assesses that actors concentrated on "platforms affecting public opinion" much more often than "core election systems" such as voting machines, or "electoral support

organizations" such as election commissions.

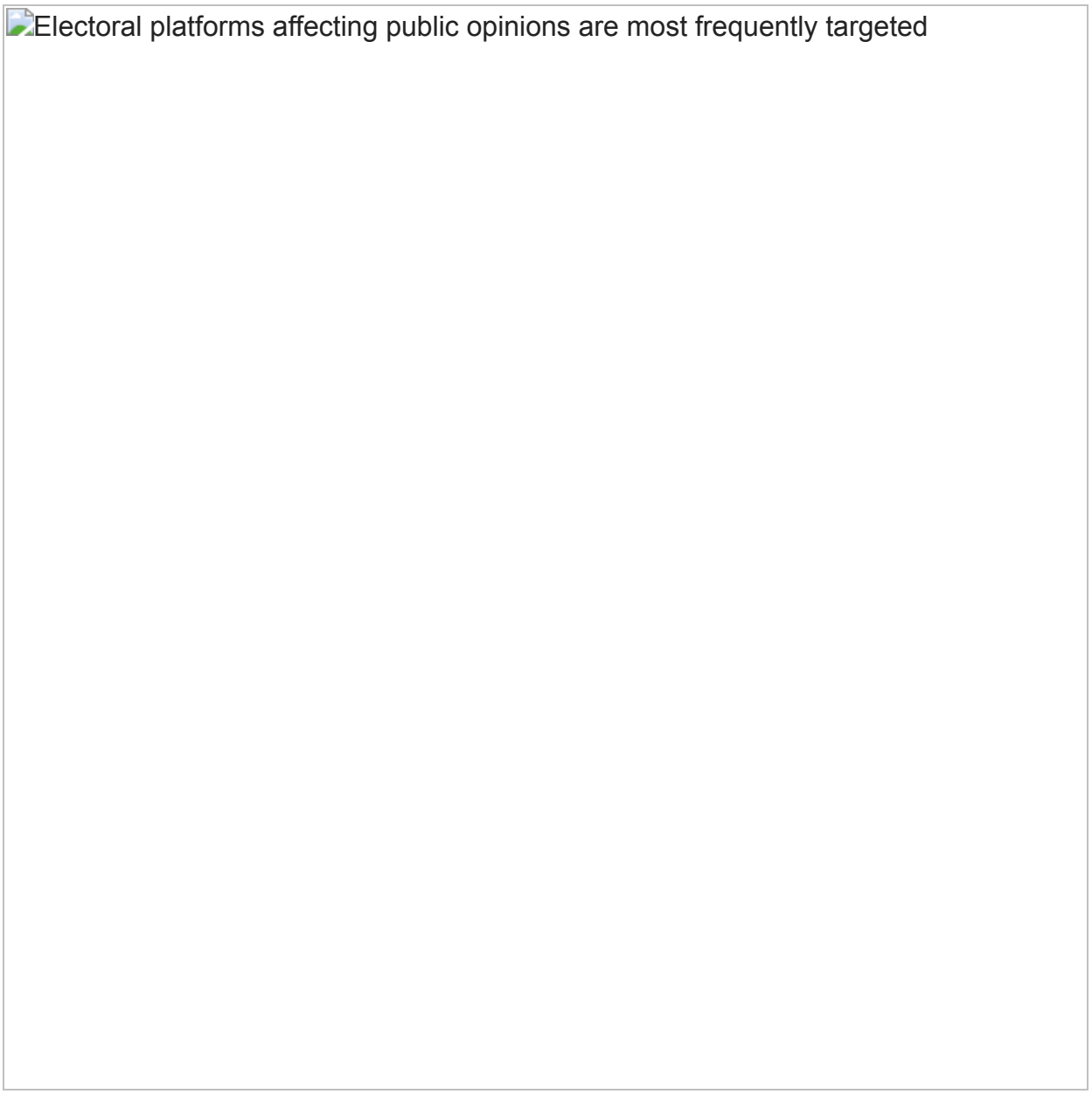

Figure 3: Electoral platforms affecting public opinions are most frequently targeted

Globally, we assess that actors continue to deploy disinformation in the form of fabricated news and hoaxes spread primarily via social media and counterfeit websites designed to mimic legitimate news organizations, which may be picked up by legitimate news organizations. In the last several years, we have seen influence operations use increasingly creative methods to blend their inauthentic messaging with legitimate speech (e.g., by interviewing, impersonating, and hiring legitimate journalists or experts, and sending letters to the editor to real publications).

Malicious actors create and spread disinformation with the intent to mislead an electorate by causing reputational damage to an individual or political party, or by casting doubt regarding a particular issue or political process. Influence campaigns also seek to exacerbate existing societal divisions.

In the Asia-Pacific region, Mandiant Threat Intelligence observed pro-China threat actors spoof Taiwanese media outlet TVBS (官方網站) to promote narratives in line with the People's Republic of China's (PRC's) political interests in a coordinated, inauthentic manner. The accounts use a variety of tactics in order to pose as Western media outlets, including the use of identical or near-identical usernames, display names, and profile photos as the accounts of the outlets they imitate.

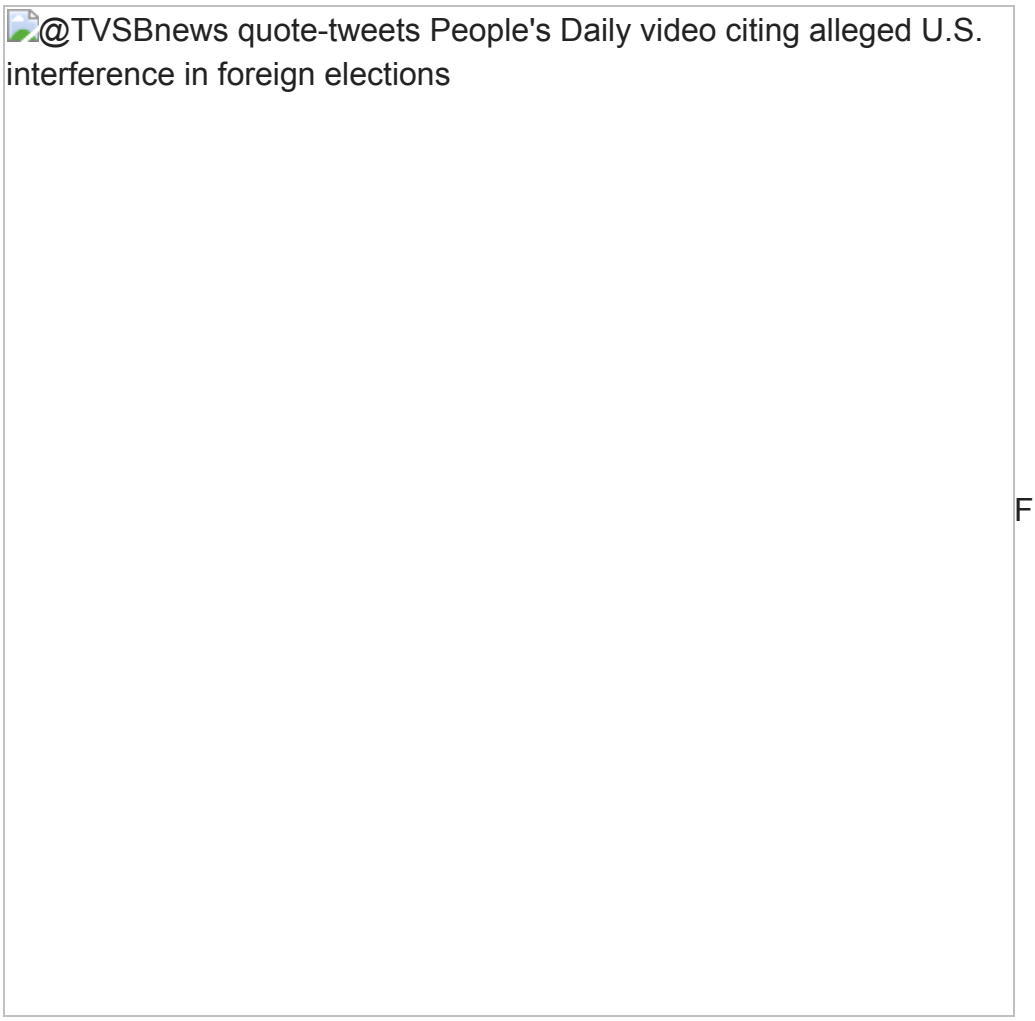

Figure 4: @TVSBnews quote-tweets People's Daily video citing alleged U.S. interference in foreign elections

Public exposure of high-profile information operations, such as Russia's interference in the 2016 U.S. presidential election, has strengthened perceptions that such operations are effective. It also demonstrates the difficulty that open societies face in countering this threat, encouraging current and aspiring information operation sponsors to grow their efforts. We anticipate that influence operations conducted in support of the political interests of nation-states will increase in sophistication, volume, and diversity of actors through 2020 and beyond.

In the last 12 months, Mandiant Threat Intelligence observed and reported on information operations conducted in support of the political interests of numerous countries. During Singapore's 2020 general elections, the country's first "digital" election, Mandiant Threat

Intelligence identified multiple inauthentic accounts. These accounts did not, however, appear to be acting in a coordinated manner.

Outlook and Implications

We expect that threat actors will continue to target entities associated with elections worldwide for the foreseeable future and may expand the scope of this activity as long as the potential rewards of these operations outweigh the risks. State-sponsored actors almost certainly view targeting the electoral process as an effective means of projecting power and collecting intelligence.

Furthermore, the continuous expansion of the social media landscape will likely encourage various actors to pursue information operations by promoting preferred narratives, including the use of propagating inauthentic or deceptive information. We have already seen tactics evolve to avoid detection and incorporate emerging technologies, such as "deepfake" or multimedia manipulation technology, to advance more believable and impactful information operations, and we expect these innovations to continue. Lower tech methods, such as outsourcing propaganda activities to real people hired specifically to spread false and misleading content, can hinder attribution efforts and potentially increase the effectiveness of operations if those people have a more specialized understanding of the information environment.

To battle election threats, there is an urgent need to increase public awareness of the threat and inculcate behaviors that reduce the risk of compromise or disruption. These include everything from rigorously securing email to implementing policy around notification of cyber incidents in the supply chain. In addition, governments can consider mandating digital imprint requirements for election campaigning, increasing fines for electoral fraud, and increasing transparency around digital political advertisements. Investment in news verification and screening methodologies on search and social media platforms as well as public education efforts equipping voters and students to distinguish trustworthy information from suspicions may also reduce the impact of influence operations.