**Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China**

[**Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China | WIRED**](https://www.wired.com/story/cybercriminals-disruptive-hacking-us-elections-dhs-report/)

A report distributed by the US Department of Homeland Security warned that financially motivated cybercriminals are more likely to attack US election infrastructure than state-backed hackers.

Russian, Chinese, and Iranian state-backed hackers have been active throughout the 2024 United States campaign season, [compromising digital accounts](https://www.wired.com/story/iran-apt42-trump-biden-harris-phishing-targeting/) associated with political campaigns, [spreading disinformation](https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/), and probing election systems. But in a report from early October, the threat-sharing and coordination group known as the Election Infrastructure ISAC warned that cybercriminals like [ransomware attackers](https://www.wired.com/story/state-of-ransomware-2024/) pose a far greater risk of launching disruptive attacks than foreign espionage actors.

While state-backed actors were emboldened following [Russia's meddling in the 2016 US presidential election](https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/), the report points out that they favor intelligence-gathering and influence operations rather than disruptive attacks, which would be viewed as direct hostility against the US government. Ideologically and financially motivated actors, on the other hand, generally aim to cause disruption with hacks like ransomware or [DDoS attacks](https://www.wired.com/story/big-pipes-ddos-for-hire-fbi/).

The document was first obtained by the national security transparency nonprofit Property of the People and viewed by WIRED. The US Department of Homeland Security, which contributed to the report and distributed it, did not return WIRED's requests for comment. The Center for Internet Security, which runs the Election Infrastructure ISAC, declined to comment.

“Since the 2022 midterm elections, financially and ideologically motivated cyber criminals have targeted US state and local government entity networks that manage or support election processes,” the alert states. “In some cases, successful ransomware attacks and a distributed denial-of-service (DDoS) attack on such infrastructure delayed election-related operations in the affected state or locality but did not compromise the integrity of voting processes … Nation-state-affiliated cyber actors have not attempted to disrupt US elections infrastructure, despite reconnaissance and occasionally acquiring access to non-voting infrastructure."

According to DHS statistics highlighted in the report, 95 percent of “cyber threats to elections” were unsuccessful attempts by unknown actors. Two percent were unsuccessful attempts by known actors, and 3 percent were successful attempts “to gain access or cause disruption.” The report emphasizes that threat intelligence sharing and collaboration between local, state, and federal authorities help prevent breaches and mitigate the fallout of successful attacks.

In general, government-backed hackers may stoke geopolitical tension by conducting particularly aggressive digital espionage, but their activity isn't inherently escalatory so long as they are abiding by espionage norms. Criminal hackers are bound by no such restrictions, though they can call too much attention to themselves if [their attacks are too disruptive](https://www.wired.com/story/colonial-pipeline-ransomware-attack/) and risk a law enforcement crackdown.

The report cites an incident from March, for example, in which an unnamed US county “experienced a ransomware attack that forced it to purchase new network devices and reconnect to the state-level election system.” If such an attack occurred on or around Election Day, it could meaningfully disrupt voting.

More broadly, domestic security concerns in connection with the 2024 election have skyrocketed, fostering what DHS calls a “heightened threat environment.” Reporting by WIRED this month revealed that the agency has been issuing warnings to law enforcement across the US since summer, alarmed by the efforts of some extremists to mobilize and commit actual violence against elected officials, while [targeting US voter ballots](https://www.wired.com/story/dhs-election-denial-violent-attacks/) for destruction.

Other warnings show that concern is mounting over propaganda calling for Americans to engage in “civil war,” a narrative that DHS fears is [raising the risk of domestic attacks](https://www.wired.com/story/extremists-civil-war-dhs/). Threats tied to what the government calls nb“immigration-related grievances”—including the false narrative of “migrant invasion,” which is core to Donald Trump’s reelection efforts—have escalated this year, while [expanding to ensnare federal judges and US border patrol officers](https://www.wired.com/story/judges-border-police-targeted-extremism/) deemed “traitors” among some antigovernment groups.

“Targeted violence and terrorism associated with ideologically motivated individuals will continue to be a threat through the 2024 election cycle,” says [another intelligence report also obtained by WIRED](https://www.wired.com/story/insider-threats-election/). It warns, meanwhile, that “insider threats” affiliated with US election systems will “likely be an issue.”