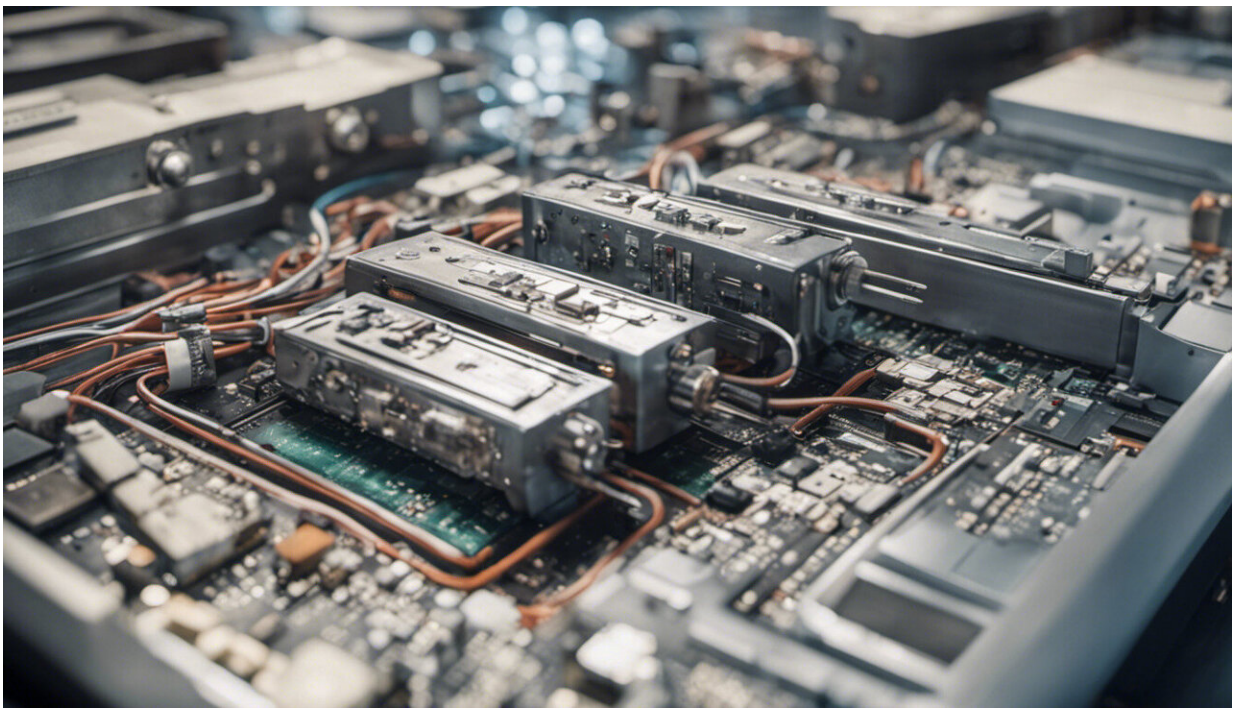
Cyber-attacks against the UK Electoral Commission reveal an ongoing threat to democracy

August 16 2023, by Joe Burton



Credit: AI-generated image (disclaimer)

The revelations this month that data on 40 million UK voters had been exposed to hackers came as no surprise to many cybersecurity experts, who have long pointed out the vulnerability of democracies to malicious online interference.

In this case, it appears that the data and systems of the UK's Electoral Commission had been available to hackers for over a year. There was a significant delay in reporting the incident due to concerns that the voting networks were still not free from malicious presence or interference.

Officials have stated that the integrity of our elections is not under immediate threat, mainly due to the continued reliance across the UK electoral system on paper ballots.

However, the attack reflects the serious and ongoing threat to democracies posed by cyber-interference from foreign nations and criminal organizations. The details surrounding this latest attack are still emerging, and the source remains undetermined. But to understand and defend our electoral system effectively against such a threat, three main points need to be considered.

1. Hacking democracy

The first is the determination and creativity of a variety of states to use cyber-attacks to subvert democracy and create mistrust in electoral systems around the world. With elections due next year in the US and UK, protecting the integrity of democratic countries is a growing concern.

We know that Russia, China and other nations including Iran have interfered in elections before—including, most notoriously, Russian hack and leak operations targeting US elections in 2016, which were directed at the Democratic party.

With tensions in the world increasing due to the war in Ukraine, and deteriorating relations between the west and China, leaders in Beijing and Moscow will see cyber-attacks as relatively easy ways to manipulate western countries.

They also see them as a means of casting further doubts on election integrity, planting narratives in public discourse via social media, and attempting to access data on politicians, parties, finance and political campaigns. These methods could be used to swing votes in favor of candidates who might take foreign policy approaches that are more in line with Russian and Chinese interests.

And they may have a new tranche of voter data to help them do just that. As a number of experts have warned, the possibility for the data from this current UK breach to be used in disinformation campaigns is a real fear. While paper-based elections are safer than those using electronic voting machines, that should not lead to complacency about the wider threats to electoral processes from these determined hacking groups.

2. The value of data

The second concern is the wider misuse of data in ways that affect UK national security. Whether it's electoral databases, banking and finance, the operation of critical infrastructure, or even the research that is produced by our universities, data is an increasingly valuable and exploitable commodity for malicious groups.

Revenue from the sale of illegally obtained data on the internet is growing in line with the increase in the amount of data being generated globally. Hackers have vast repositories of data to target, and can generate revenue from doing so.

Ransomware attacks are often being used alongside a threat to leak or sell the data obtained. This is now a multi-billion dollar business.

3. Delays in disclosure

A third concern is that the reporting of cyber-breaches continues to lag behind the attacks themselves. It may seem surprising to observers of the recent UK incident that it took so long to disclose. This delay constitutes a serious concern for the rights of those electors who have had their data accessed.

But this must be balanced against the operational need to ensure that the systems the data was stored on are free from malicious interference, and to make sure that hackers aren't still inside the system, having obtained access.

We know that attackers can maintain access to a system over long periods while staying undetected. This approach of "living off the land", as the US Cybersecurity and Infrastructure Security Agency (Cisa) recently referred to it, is an increasingly common modus operandi for state-supported hackers in particular.

The reputational cost to an organization after suffering a data breach is often serious and damaging. But when the costs are to the reputation and integrity of electoral processes, a different approach may be required when it comes to public disclosure of the incident.

Being a responsible cyber-power

The UK government has framed its national cyber-strategy around the idea of being a responsible and democratic cyber-power. That responsibility clearly extends to protecting electoral processes from malicious interference.

Currently, government capabilities are battling to keep up with the hackers. The UK's National Cyber Force (NCF) has a mandate to deter, disrupt and respond to these types of incident, including against both foreign states and criminal organizations.

The National Crime Agency has also stated that "defending the UK's democratic processes" and helping to "strengthen the cyber-resilience of our electoral systems" is a priority.

But attributing the attacks to specific groups or states is a difficult task. Holding them to any kind of legal punishment has always been challenging, particularly if they are operating with the endorsement of their governments.

Insider threat

There have also been wider concerns in the electoral system around the cybersecurity of political parties and candidates. These combine with concerns citizens have that their democracies are not operating well. This makes it easier for those who seek to undermine public faith in democracy to claim that elections are not being conducted fairly, and are not free from foreign interference.

Disinformation about the integrity of elections, both from within and outside the UK, will find greater traction in the wake of these types of incident.

The viability of the UK to hold cybersecure elections in the near-future will be the product of work by the cybersecurity community now. A renewed effort to provide our electoral system with the tools to secure their networks, including giving direct support to political parties, candidates and civil society, is clearly needed.

Provided by The Conversation