TDR by sekoia
THREAT DETECTION & RESEARCH

Strategic Threat Landscape

GUARDING DEMOCRACY:
Assessing Cyber Threats to 2024 Worldwide Elections

sekoia

TLP:CLEAR

April 2024

SUMMARY

ABOUT US

Researched and written by

Maxime Arquillière
Lead Analyst Strategic Threat Intelligence, Sekoia TDR

Livia Tibirna
Strategic Threat Intelligence Analyst, Sekoia TDR

Coline Chavane
Strategic Threat Intelligence Analyst, Sekoia TDR

About Sekoia TDR team

TDR is the Sekoia Threat Detection & Research team. Created in 2020, TDR provides exclusive Threat Intelligence, including fresh and contextualised IOCs and threat reports for the Sekoia SOC Platform. TDR is also responsible for producing detection materials through a built-in Sigma, Sigma Correlation and Anomaly rules catalogue.

TDR is a team of multidisciplinary and passionate cybersecurity experts, including security researchers, detection engineers, reverse engineers, and technical and strategic threat intelligence analysts.

Threat Intelligence analysts and researchers are looking at state-sponsored & cybercrime threats from a strategic to a technical perspective to track, hunt and detect adversaries. Detection engineers focus on creating and maintaining high-quality detection rules to detect the TTPs most widely exploited by adversaries.

ABOUT US

About Sekoia.io

Sekoia.io is the European cybertech, leading provider of Extended Detection and Response (XDR) solutions based on Cyber Threat Intelligence (CTI). Its mission is to provide businesses and public organizations with the best protection technologies against cyber attacks.

By combining threat anticipation through knowledge of attackers (Sekoia Intelligence) with automation of detection and response, the Sekoia SOC platform (Sekoia Defend – XDR) provides security teams a unified view and total control over their information systems. Its interoperability with third-party solutions and compliance with international technical standards enable organizations to take full advantage of their existing technologies. Sekoia.io gives its customers the means to focus their human resources on high value-added missions, optimize their cyber-defense strategy and regain the advantage against advanced cyber threats.

Read the latest threat reports

Go to our blog

EXECUTIVE SUMMARY

- In 2024 multiple worldwide elections will be held with 54% of the world population called to vote. Electoral results can potentially influence the geopolitical landscape, making elections a prime target for cyber offensive operations aimed to influence the outcome.

- Sekoia.io conducted a general assessment of past elections impacted by cyber attacks, identifying four categories of operations : hack-and-leak operations following a cyber intrusion; information and cyber influence campaigns; attempted cyber disruption of the voting process; and lucrative campaigns impacting the electoral process.

- “Hack-and-leak operations” involve planning a long-term cyber intrusion looking for compromising documents published to fuel narrative undermining a candidate. The most critical exemples are the DCleaks and MacronLeaks operations, conducted by Russian military intelligence against US and French presidential elections in 2016 and 2017.

- “Information and cyber influence campaigns” are nowadays more likely to be used than hack-and-leak against 2024 elections, as they do not require sophisticated cyber intrusion yet are still efficient. “Cyber disruption of the voting process” may sound the most concerning threat, but successful or even attempted operations are not common.

EXECUTIVE SUMMARY

- Few elections were also impacted by cybercrime lucrative campaigns having consequences on the electoral processes yet without the specific intent to alter the outcome.

- For the remaining upcoming 2024 elections, Sekoia.io assess four of them are likely to be targeted by cyber operations aiming to influence the geopolitical landscape: the US presidential elections, the European Parliament elections, the Moldova presidential election with referendum on joining the EU, and the India parliamentary elections.

- Those elections face primarily information and cyber influence campaigns, to a lesser extent hack-and-leak operations; for Moldova, cyber disruption of the voting process may be attempted, as the potential impact of such campaigns could be politically significant.

INTRODUCTION

2024 marks a pivotal moment in global politics as an **unusual number of elections** have and will take place across various nations, encompassing approximately **54% of the world's population**. Elections serve as keystone events in democratic societies, signifying not only the will of the people but also stability and continuity in governance. Beyond shaping domestic policies, the outcomes of these elections hold significant implications for long-term foreign policy directions.

Given today's interconnected world, **electoral results can potentially influence the geopolitical landscape**, prompting both allies and adversaries to assess and adapt their strategies accordingly. This makes **elections a prime target for external actors**, who may seek to strengthen friendly regimes, undermine rivals, or manipulate the trajectory of foreign relations for their own strategic interests.

Sekoia TDR analysts conducted an in-depth analysis of cyber threats on elections based on past targeted elections, identifying various types of cyber operations, and propose an assessment of threats regarding the major elections that will occur in 2024.

Cut-off date for this paper is 12 April 2024.

PART 1

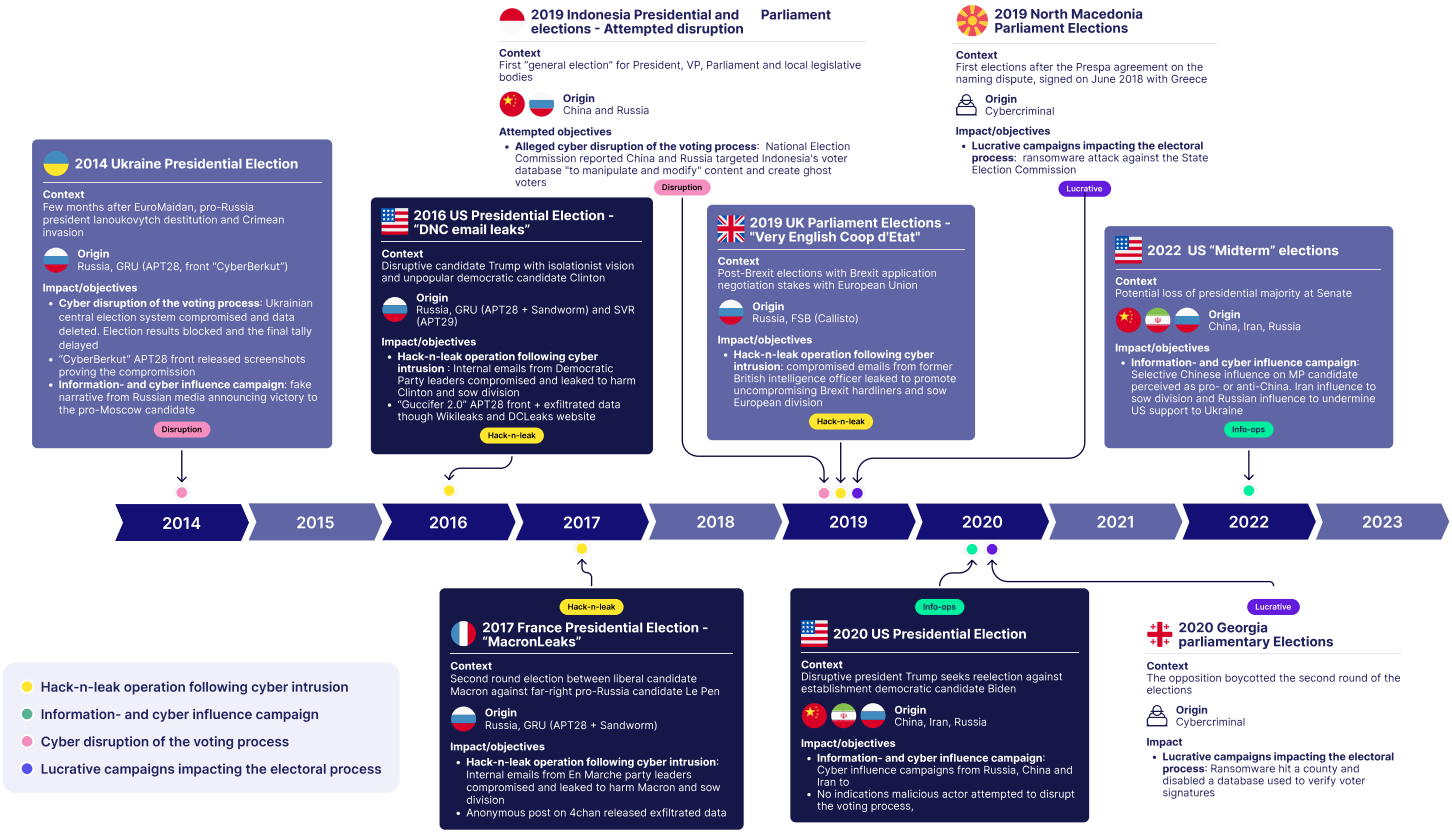
Past major elections targeted and impacted by cyber operations

1 Past major elections targeted and impacted by cyber operations

For a better understanding of cyber threats targeting elections worldwide, Sekoia TDR analysts conducted a **general assessment of past elections impacted by cyber offensive operations**. We notably studied the most documented incidents in open-source.

This allowed us to identify campaigns reporting **four categories of operations**, from the most to least critical: hack-and-leak operations following a cyber intrusion; information and cyber influence campaigns; attempted cyber disruption of the voting process; and lucrative campaigns impacting the electoral process.

sekoia | Past elections impacted by cyber operations



HACK-AND-LEAK OPERATIONS FOLLOWING CYBER INTRUSION

One of the most impactful types of cyber operations on elections has been "hack-and-leak" operations following cyber intrusion, **especially in the 2014 - 2019 period**.

These operations involve planning a **long-term cyber intrusion** targeting information systems associated in some way with a political party or a candidate in an election. Once the attacker is positioned within the targeted network, they can extract data (emails, internal documents) that could cause **reputational damage to a selected candidate**.

For instance, during the 2016 US presidential election opposing Donald Trump and Hillary Clinton, about 19,000 internal emails from the Democratic National Committee were compromised and exfiltrated by a cyber operation conducted by both Russia-nexus intrusion sets APT28 and APT29 operated by Russian Intelligence (respectively GRU and SVR services). According to the Report On The Investigation Into Russian Interference In The 2016 Presidential Election from US special counsel judge Mueller, the operation aimed at undermining candidate Clinton and undermining the public trust in the voting process.

The information operation following the compromission involved different channels. A "***DCLeaks***" website was published to promote a part of exfiltrated email, then all the documents were transferred and published by Wikileaks. Simultaneously, an APT28 persona, "**Guccifer 2.0**", falsely impersonating a Bulgarian individual, claimed the compromission and leak, highly likely to **deny any attribution** to the Russian intelligence. The same technique - a fake persona claiming the leak - was later used in 2017 for the "MacronLeaks" operation.

In 2017, the "***MacronLeaks***" were another example of a hack-and-leak operation following cyber intrusion. More than 20.000 internal emails related to the campaign of Emmanuel Macron were leaked on the alt-right online forum 4chan, during the 2017 French presidential elections, two days before the final vote. According to the French newspaper Le Monde, several private reports from cybersecurity vendors, such as Trend Micro or FireEye, identified technical evidence attributing the operation to the Russian intelligence service **GRU through its intrusion sets APT28 and Sandworm**, also involved in the DCLeaks a year earlier. The operation was highly likely aimed at undermining candidate Macron to promote the far-right and, at the time, the other candidate Marine Le Pen, more favourable to the interests of the Kremlin.

Other examples can impact European countries' elections, especially at a critical political period. For instance, the "Very English Coop d'Etat" was a hack-and-leak operation aiming to influence the 2019 UK Parliament elections, which were focused on the effective application of Brexit. It exposed documents exfiltrated from a former British intelligence agent. The operation was later attributed to Russia-nexus intrusion set Cold River, a group attributed to the FSB by a US-UK joint statement.

Hack-and-leak operations following cyber intrusion are the most impactful reported operations on elections because they fuel the undermining narrative with alleged internal, legitimate, and compromising documents. However, it is almost impossible to assess the influence on the election outcome.

INFORMATION AND CYBER INFLUENCE CAMPAIGNS

Information and cyber influence campaigns can be defined as operations affecting the logical layer of cyberspace to shape attitudes, decisions and behaviours of a targeted audience. This type of cyber operation in an electoral context can serve **to weigh on the public debate and on the voting outcome**. In this category, no technical cyber intrusion is required to influence the elections, only diverted use of cyber resources such as social networks, false press articles, etc.

Information and cyber influence campaigns impact multiple democracies and hybrid regimes. Researchers at Google TAG point out that an increasing number of countries are engaging in influence campaigns to pursue their strategic objectives. In 2023, coordinated influence campaigns were attributed to individuals or organisations located in **27 countries**. These campaigns leveraged **domestic political issues**, to support or criticise a political leader or a party of the targeted country.

For instance, in February 2024, **Taiwan elections** have been widely targeted by information and influence operations, some of them active since at least 2018. Taiwan elections are a good example of understanding techniques and narratives leveraged in an electoral context. A research on the effect of disinformation on Taiwanese voters during the 2018 local elections concluded that **misinformation influenced Taiwanese voters' perception of news** and their voting choices. Over **50% of voters** made their **decisions without accurate information** on campaign news. Notably, politically unaffiliated voters, who were less adept at identifying false information, tended to support candidates aligned with the China-friendly Kuomintang (KMT).

Assessing the impact of recent campaigns remains challenging. For the 2020 elections, DoubleThink Lab found that exposure to false information increased belief in it, particularly when negative emotions were aroused. Nevertheless, Lai Ching-te won the 2024 presidency campaign with 40% of the votes, yet the DPP failed to secure an absolute majority in the Yuan for the first time since the 2000s elections.

Another example can be found regarding the **2020 US presidential election**. Despite no indications that foreign actors attempted to alter any technical aspect of the voting process in the 2020 US elections, the report of the Director of National Intelligence (DNI) assesses that **China, Russia and Iran intelligence conducted information and cyber influence campaigns to influence the results**. Russia operations aimed at "denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating socio-political divisions in the US". Iran deployed the same techniques but with a different objective, undercutting former President Trump's reelection prospects, although without directly promoting his rivals.

CYBER DISRUPTION OF THE VOTING PROCESS

Voting infrastructure can also be a strategic target for cyber operations to disrupt **the voting process**. This type of operation can target several types of infrastructure, ranging from **infrastructure supporting inscription on electoral lists, voting machines** or information systems from **administrative units** responsible for the electoral process. Especially in countries using **electronic voting machines**, such as direct-recording voting machines or remote internet voting technologies, cyber disruption has become a major concern, leading to the adoption of specific security policies and cybersecurity tests. Indeed, very early tests have been conducted in Estonia, in Switzerland, and in France, and pointed out critical vulnerabilities.

Cyber disruption campaigns can exploit these vulnerabilities for **various motivations**. A first one can be **postponing the vote** to allow a candidate to gain more votes, or to delay the election of a non-favourable party. It can also **serve to delete the vote**, and then impact voters' confidence in their institutions and representatives, who can be accused of manoeuvring to stay in power longer. Cyber disruption operations can also be used to **alter the vote count** to promote the election of a minority candidate. A final objective can be **weakening the democratic process**, to demonstrate the fragilities of this political system compared to alternative ones.

Cyber disruption operations require sophisticated technical capabilities because of the critical nature of the targeted infrastructure, suggesting they are conducted mainly by **state-sponsored threat actors**. Such attacks remain **relatively rare**. However, they can have major impacts on the run of elections as they target highly critical infrastructure. It was notably illustrated in 2014 with the cyber attacks targeting the post-Maidan Ukraine elections and attributed to Russia-nexus threat actors.

FOCUS:
2014 POST-MAIDAN UKRAINE ELECTIONS

The cyber attacks targeting Ukraine during the **May 2014 presidential election** occurred within a context marked by significant political turbulence. Following the **Euromaidan protests** in November 2013 and the subsequent dismissal of President Viktor Yanukovych, tensions between Ukraine and Russia escalated, culminating in the annexation of Crimea in February-March 2014.

Ukrainian electoral infrastructure became a **prime target** for cyber attacks several days prior to the election, when **Ukraine's central election system was compromised**, resulting in the **deletion of critical files essential for tallying votes**. This cyber intrusion rendered the vote-tallying system inoperable, causing a significant disruption to the electoral process. Although the system was restored using backups three days before the national vote, election results were delayed for two hours.

In the lead-up to the election, "**CyberBerkut**", a hacktivist-like persona **operated by Russian intelligence GRU**, released screenshots as proof of the operation's success. Furthermore, there were attempts to manipulate the election outcome through the installation of malware aimed at **falsifying computer vote totals**. The malware, if successful, would have portrayed a particular candidate, Dmytro Yarosh, as the winner with significant margins. According to Ukrainian officials, timely detection and removal of the malware prevented dissemination of false results.

These cyber attacks underscored the magnitude of external interference in Ukraine's democratic processes and raised concerns about the integrity of future elections in the region.

LUCRATIVE CAMPAIGNS IMPACTING THE ELECTORAL PROCESS

During our assessment of past elections impacted by cyber operations, we identified only a few notable lucrative campaigns by cybercrime actors which had **consequences on electoral processes**. While election disruption was not the main motivation of observed incidents, their possible impact is undeniable. Often, election processes and infrastructures are **victims of broader campaigns on government infrastructur**e, caught in the crossfire of opportunistic cyber attacks. Cybercriminals typically aim to **amplify pressure**, maximising their chances of **extorting ransom payments** from authorities in need to restore the integrity and functionality of essential systems or being willing to avoid loss of reputation following the disclosure of non-public data.

Double extortion campaigns claimed by lucrative actors are a recurring phenomenon in the threat landscape in the margins of elections. It was the case in February 2024 when Georgia's Fulton County was subject to a ransomware attack. Victim's key services were disrupted for weeks in a context marked by the early voting process during the 2024 US Presidential elections. Yet, in this and other previously reported incidents, the voting process was not impacted

From our observations, the **sale of voter databases**, whether before or after elections, occurs regularly and serves as invaluable assets, allowing malicious actors to capitalise on current events. Such an instance occurred in October 2023 when a threat actor operating on a well-known cybercrime forum offered to sell personal data of voters obtained following a compromise of the District of Columbia Board of Elections.

It is possible that state-sponsored actors further leverage such data to influence public opinion, and undermine the democratic process of rival nations, etc. Additionally, these actors possibly deploy commodity malware or use broader Cybercrime-as-a-Service offerings to evade attribution related to elections-focused campaigns.

PART 2

Outlook on cyber threats to major 2024 elections

In 2024, over 80 nations are set to hold elections, encompassing a diverse range of states, from the wealthiest and most powerful, to the most populous or the most authoritarian.
As this paper's cut-off date is 12 April 2024, **some elections have already happened**, including major ones susceptible to be impacted by cyber operations, such as **Taiwan** (13 January), **Finland** (28 January), **Iran** (1 March), **Russia** (13-15 March) or **South Korea** (10 April).

Those five countries did not report any cyber disruption (hack-and-leak operations or cyber disruption of the voting process) or subsequent lucrative operations impacting the vote, but **some of them** were **relatively affected by information and cyber influence campaigns**.

A report from the Australian Strategic Policy Institute pointed out that the Chinese Communist Party **(CCP) attempted to manipulate Taiwanese voters** by spreading disinformation and propaganda across social media to undermine Democratic Progressive Party presidential and legislative candidates, a cyber-based information campaign believed to have had little impact on the election's integrity.

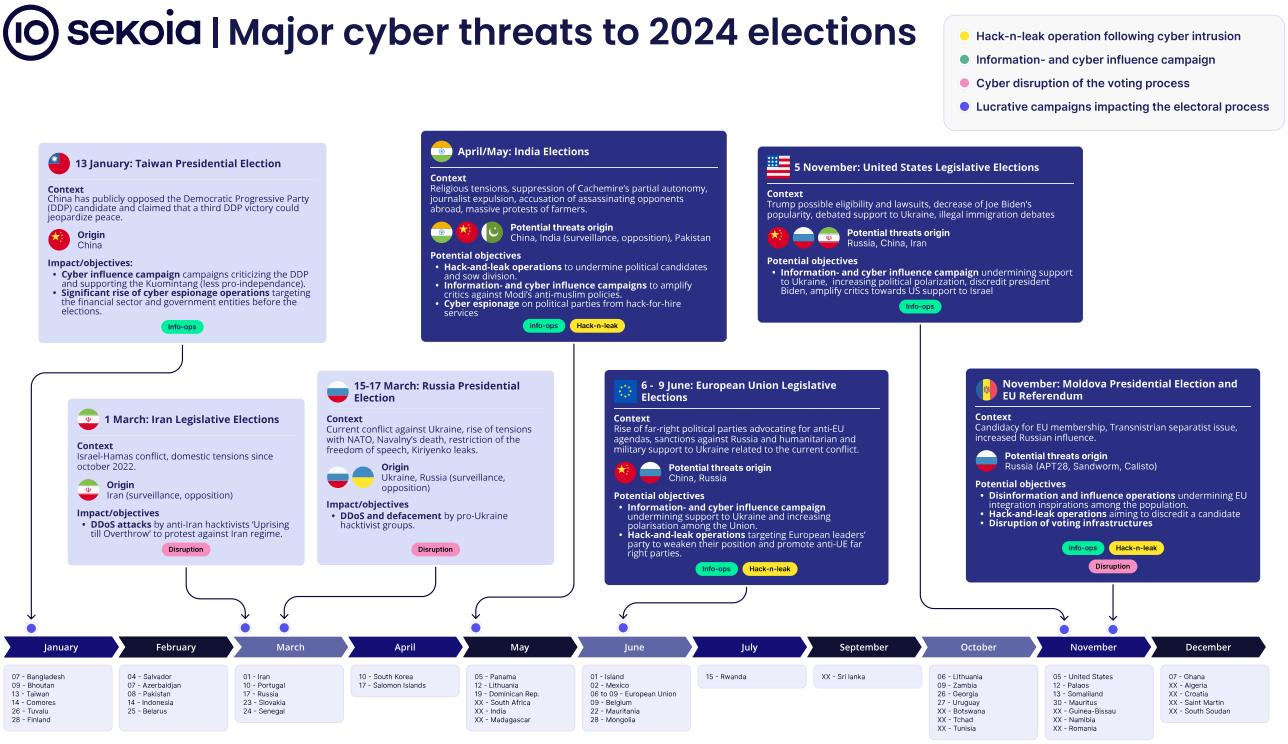
Other elections, such as in Iran or Russia, were impacted by distributed denial of service attacks (DDoS) targeting voting systems or political parties. Iran attributed these attacks to anti-regime hacktivists, and Russia attributed them to Ukrainian operatives. Those operations had no effect on the outcome of the elections.

The **South Korean elections** had no reported cyber attacks despite tensions with North Korea, known for its cyber capabilities. It is consistent with the fact North Korea-nexus threat actors never targeted the electoral process in the past, highlighting elections is irrelevant regarding their motivations.

2 Outlook on cyber threats to major 2024 elections

For the **upcoming 2024 elections**, Sekoia TDR analysts have identified the most critical events where electoral results can **potentially influence the geopolitical landscape: India** parliamentary elections (April-May), European Union legislative elections (6-9 June), the US Presidential election (5 November) and **Moldova** presidential election and EU-membership consultative referendum (20 October). In the next sections of this report, we look ahead to cyber threats that could impact electoral processes worldwide, starting with the elections we assess are most critical on the international geopolitical arena.

sekoia | Major cyber threats to 2024 elections



UNITED STATES PRESIDENTIAL ELECTION (NOV 2024)

Due to their leadership position and influence in the global geopolitical landscape, the US presidential election is **probably the most critical election in 2024**. The clear opposition of strategic foreign policy between President Biden and candidate Trump, especially regarding China, Russia and Iran - all actors susceptible to influence the outcome of the election - will highly likely be a reason for foreign services to conduct cyber operations.

As depicted in the first part of this paper, the two previous US presidential elections, 2016 and 2020, were already targeted and impacted by cyber operations, from hack-and-leak to information and cyber influence campaigns. In 2016, the DCLeak hack-and-leak operation involving APT28 (GRU) may have had an effect on a very close election and help candidate Trump to win, although it is almost impossible to assert the influence was decisive on the election outcome. Thus, it is highly likely that foreign geopolitical rival actors will try to exercise influence once again in the 2024 election.

However, given that the **US government has learned from the Russian operation on the 2016 elections**, cybersecurity has generally increased, not only regarding voting processes but also regarding stakeholders linked to the election (political parties, candidates, media). As a result, it is less likely that an operation comparable to that of 2016 will happen again. Indeed, the 2020 election was targeted by external operations, but only in the form of information and cyber influence campaigns. Thus, Sekoia.io assess is **possible yet not likely** that **Russian, Chinese** or **Iranian actors conduct hack-and-leak operation** following cyber intrusion.

Nevertheless, just as in 2020, it is **highly likely** that **Moscow**, **Beijing and Teheran** will conduct **information and cyber influence campaigns**. According to intelligence assessments, **Russia has already increased** its information campaign to disrupt military support for Ukraine in the United States (and Europe), using enhanced information techniques more difficult to trace, to promote isolationist views before the U.S. elections.

Less involved in the influence campaign in the US 2020 elections, **China** is, in 2024, already conducting influence operations, impersonating American supporters of former President Donald J. Trump spreading conspiracy theories, looking to sow domestic division, and undermining President Biden. These activities suggest a potential **strategic shift** in Beijing's approach to influencing U.S. politics, **mirroring Russia's tactics from the 2016** election. As for Iran, it is likely that Tehran will continue to conduct influence operations similar to those in 2020, aiming to sow division and focusing equally on undermining both political sides.

EUROPEAN PARLIAMENT ELECTIONS (JUNE 2024)

As the 2024 European Parliament elections approach, a confluence of political, social, and cyber-related challenges poses significant threats to democratic processes across Europe. Reports on state-sponsored operations targeting the European Parliament's IT infrastructure highlight the escalating sophistication and frequency of such threats, raising alarms about the **vulnerability of electoral systems to foreign interference**.

Amidst these concerns, the integrity of the electoral process faces potential challenges from external actors, notably Russia and China. The rise of far-right and Eurosceptic conservative political parties advocating for anti-EU agendas, **often aligning with Russia's geopolitical objectives**, emphasises the deepening connections between domestic politics and foreign interference(s).

Furthermore, information and cyber influence campaigns and other cyberattacks leveraged by Russia-nexus actors pose additional risks, as they are aimed at increasing polarisation across Europe and consequently **undermining support for Ukraine**. Calls from Russian officials for support for "anti-system" parties likely confirm it.

This is compounded by **recent allegations** of Members of the European Parliament (MEPs) possibly being **recruited** by foreign services to **support the Russian narrative**, notably regarding the Ukrainian war. Of note, two months prior to the election date, EU officials already reported on Russian cash payments to European parliament members that aimed to promote pro-Russian narratives and influence upcoming EU elections.

Thus, **we assess** that **information and cyber influence campaigns** are **highly likely** to target the EU election process in June 2024, aiming at a diverse range of assets, including media outlets, internal communication platforms, and social networks associated with both political parties and their constituents.

Continuing previous observations, it is highly likely that **information and cyber influence campaigns** will be perpetrated primarily **by Russia**-nexus intrusion sets. Additionally, we assess that such campaigns may be conducted, to a lesser extent, by actors aligned with **Chinese** geopolitical objectives. In 2023, the EU adopted tougher trade and technology policies towards China, while investigations from Meta and Citizen Lab revealed an unprecedented scale of Chinese influence operations worldwide. Therefore, it is likely that China will enhance its efforts in sowing divisions between Member States to advance its interests in Europe.

Furthermore, it is **possible** that **hack-and-leak operations** will occur in the run-up to the elections. **Countries with larger populations**, and consequently a greater number of designated MEPs, are particularly vulnerable to such targeted efforts aimed at altering the final distribution of political parties in the Parliament. However, the potential impact of such campaigns on the EU election results is reduced compared to other regions, primarily due to the **fragmentation of the electoral infrastructure**.

MOLDOVA PRESIDENTIAL ELECTION AND REFERENDUM ON JOINING THE EU (OCTOBER 2024)

Moldova's post-USSR trajectory is currently marked by **developments towards its alignment with the European Union** (EU). President Maia Sandu's Party of Action and Solidarity (PAS) leads the charge toward EU membership, amid ongoing tensions surrounding the **Transnistrian separatist issue**.

However, Moldova faces significant challenges from increased Russian influence, notably since 2015, and a complex web of espionage and disinformation campaigns impacting Moldova over the last few years. For example, in September 2022, the Moldovan Intelligence and Security Service uncovered an FSB network operating within the country for espionage and subversion.

Subsequent cyber-related incidents involved hacking campaigns by the pro-Russian group Killnet, extended **DDoS** attacks, hack-and-leak campaigns, intrusions of government infrastructure preceding the June 2023 European Political Community Summit in Moldova and accusations by Prime Minister Natalia Gavrilița of Russian-sponsored protests and cyberattacks leveraged for **destabilisation** efforts. The involvement of Russian intelligence agencies, including the **GRU** and the **SVR**, became apparent with surveillance activities observed from the Russian embassy rooftop antennas, and covert officers linked to previous cyber campaigns targeting high-level European politicians.

Despite disrupted campaigns (notably in May 2022 and February 2023), Russian **disinformation** targeting Moldova remains **persistent**, aiming to **undermine its European integration aspirations**. Moreover, leaked documents suggest Russia's long-term ambition to assert control over Moldova by 2030.

In a broader geopolitical context, Moldova's alignment with pro-Russian forces could advance Russia's strategic objective of expanding its access to the Black Sea. This objective could be facilitated by exerting a wider influence on Moldovan or Transnistrian agendas.

In the lead-up to the upcoming presidential election and national referendum, it is almost certain that **Russian attempts to destabilise Moldova will persist through operations such as influence, hack-and-leak and DDoS**, alongside with political interference and strategic corruption. Information and cyber influence campaigns are highly likely to maintain support towards internal pro-Russian factions to cause social conflicts in Moldova and to finally compromise the presidential election and the referendum to join the EU, aligning with disinformation campaigns reported during the 2023 local elections. **Hack-and-leak operations are highly likely to be conducted,** aiming to discredit the pro-EU president or any pro-EU figures by portraying them as corrupt or disloyal.

Furthermore, we assess **that cyber disruption of the voting process is likely to be attempted, as the potential impact of such campaigns could be significant**, given Moldova's relatively low-level cyber preparedness, comparable to that of Ukraine in 2014. Additionally, as Moldova is not a member of NATO or the EU, its opportunities for cyber-related coalitions on a broader scale are limited.

While Moldova was typically spared from the Russian-speaking lucrative threat - as Russian-speaking cybercrime groups historically do not target the Commonwealth of Independent States (CIS), Moldova's turn towards the European Union is likely to cause an increase in the frequency of financially motivated cyberattacks impacting its assets, which aligns with broader observations regarding countries undergoing the process of joining the EU.

INDIA PARLIAMENTARY ELECTIONS (19 APRIL-MAY 2024)

In April and May 2024, India will vote for the renewal of their Prime Minister, of the Lok Sabha (the lower house of the Parlement), of the Vidhan Sabhas (legislative assemblies of States and territories of Delhi and Pondicherry) and of local authorities.

Since 2014, the political party of the current Prime Minister Narendra Modi, the Bharatiya Janata Party (BJP), is majoritarian in the Lok Sabha. Although the **reelection of Narendra Modi seems to be very likely**, the prime minister remains criticised, especially for its authoritarianism since he came into power in 2014. Since 2021, independent institutes, such as V-Dem or the Freedom House, have classified India as an autocracy or a "partially free" country and not a democracy. Foreign journalists have had their work permit withdrawn, NGOs fundings restricted and religious minorities persecuted, **affairs that foreign actors can leverage to undermine Prime Minister Modi** and its foreign policy.

India will employ **electronic voting machines (EVMs)** for the 2024 elections, as in previous polls. EVMs, offline and featuring Voter Verifiable Paper Audit Trail (VVPAT), allow voters to confirm their vote. VVPAT counts have occurred randomly since 2017 to verify EVM results. However, the opposition challenges this method, citing concerns over **potential chip manipulation** in consistencies without VVPAT verification to log votes differently from the buttons pressed by voters.

India is a major player in global and regional geopolitics, and therefore can be a target for foreign cyber threat actors motivated by the weakening of the country's power base. China and Pakistan have been conducting long-term cyber espionage campaigns against India. We assess hack-and-leak operations to discredit Narendra Modi are unlikely due to the risk of regional tensions and possible reprisals.

It is more likely that **China-nexus and Pakistani-nexus intrusion sets** operate **information and cyber influence operations** to amplify criticism of Modi. Indeed, in 2023, Meta uncovered a network of inauthentic accounts attributed to China and criticising the Indian government, accused of corruption and of supporting ethnic violence. The same year, Google TAG also closed YouTube channels and a blog attributed to Pakistan and critical of India.

Cyber threats are also more likely to come from **domestic actors**. In October 2023, Apple released a wave of security alerts to over 20 Indian journalists and opposition politicians using iPhones likely to be targeted by "state-sponsored attackers." Such surveillance combined with the exfiltration of sensitive personal information is likely to be used for hack-and-leak operations to undermine political candidates, sow divisions, and spy on **political parties**.

Therefore, we assess that the 2024 Indian elections are likely to be targeted by **information and cyber influence operations** conducted by intrusion sets attributed to China and **Pakistan**. In addition, threats can come from **Indian threat actors** leveraging **hack-for-hire companies and spyware** for cyberespionage targeting political parties, or for hack-and-leak operations aiming at undermining political candidates and sowing divisions.

CONCLUSION

Historically, the most exposed type of cyber campaigns targeting elections are **hack-and-leak operations with cyber intrusion**. They require sophisticated cyber espionage capabilities that only few countries likely possess. Exfiltrated data are then published, in a single time or step by step, and can be altered to increase the political harmness potential. Through its intrusion sets APT28 and Sandworm, the Russian intelligence GRU exploited this strategy from 2014 to 2017 (Ukraine 2014, US 2016, France 2017), a strategy also used by the FSB, at least for one operation (UK 2019). Since then, no similar operations were reported in open source, showing a possible **strategic shift** from this malicious actor, likely due to the overall enhancement of national election cyber defence postures. However, Sekoia.io assess hack-and-leak operation is still a potential cyber threat to future elections, particularly in countries less mature in cyber security.

Information and cyber influence campaigns constitute **nowadays a more likely threat** to democratic elections although such operations were also documented in the past. Intelligence services from Russia, Iran and China, were documented conducting information warfare as part of their foreign influence strategy. Those campaigns **focus on elections with a high potential for reshaping geopolitical strategies** (US and UE support for Ukraine, Taiwan's path into independence or the One-China policy...).

Strategic espionage aimed to gain data or materials usable for any cyber operation targeting elections is also a persistent threat. Of note, it's worth mentioning that these operations often persist for extended durations and not only during electoral time.

Last, even if cyber disruption of the voting process may sound like the most concerning threat, open-source available information indicates that such operations are not commonplace.

sekoia

One view. Total control.