HOSTILE INFLUENCE OPERATIONS:

Cyber and Informational Threats Ahead of the 2022 French Elections

PARIS PEACE FORUM de PARIS sur la PAIX

With the support of Microsoft

POLICY BRIEF | APRIL 2022

PARIS PEACE FORUM
de PARIS sur la PAIX

Transatlantic Commission on Election Integrity

Part of Alliance of Democracies

With the support of Microsoft

HOSTILE INFLUENCE OPERATIONS:

Cyber and Informational Threats Ahead of the 2022 French Elections

On 31 March 2022, the Alliance of Democracies Foundation and the Paris Peace Forum co-hosted - with the support of Microsoft's Democracy Forward Initiative – a private expert roundtable to exchange on hostile influence operations ahead of the 2022 French presidential and legislative elections. The discussions focused on identifying the main trends and challenges regarding foreign hostile interferences in the French electoral process in 2022, both in terms of cybersecurity and informational threats. This analysis was conducted in light of recent and past democratic elections, as well as lessons learned from those elections on how best to protect them.

This policy brief summarizes the key findings and analysis shared during this expert roundtable, which was held under the Chatham House Rule. All quotes, data and examples are from participants' contributions during the meeting.

POLICY BRIEF | APRIL 2022

I - ASSESSING THE THREATS:

WHERE DO WE STAND IN THE CONTEXT OF THE FRENCH ELECTIONS?

Electoral processes have long been critical targets and the subject of both attempted and successful attacks, but the ongoing emergence of hybrid threats are redefining the terms of these debates. Recent hostile interference attempts against elections in established Western democracies reminds us of the increasing complexity of these threats and the associated urgency to counter them with a holistic approach.

1 - The line between cybersecurity and informational threats is blurring. Although a distinction is often made between cybersecurity - in the sense of the integrity of cyberinfrastructures, networks, and software - and information threats - such as disinformation operations -, these two dimensions can be analyzed and addressed less and less separately. Both aspects are often closely intertwined, particularly in the context of an electoral process: cyberattacks, for example, can "*fuel the fires of misinformation*" and delegitimize election results by fomenting distrust in the process. And conversely, an attack that aims to steal and publish a candidate's data, potentially altering the content, is a serious threat, as the 2017 "Macron leaks" proved. Private message intrusion can have a tremendous effect as part of a larger disinformation campaign targeting a specific candidate with the goal of influencing the election. The mix of actual stolen messages and fake supplements highlights the blurred line between cybersecurity and information threats.

2 - The biggest cyber threat to the French elections in 2022 is spying on candidate teams and parties, whether this illicit intelligence hacking is part of a larger influence operation or not. Although espionage in the electoral context is a long-standing practice, the increasing reliance of campaign staff on new information and communication technologies has added a new dimension to this type of operation as it becomes less detectable, cheaper, and more effective. More generally, information gathering is considered the primary purpose of state-sponsored cyberattacks, which account for the bulk of foreign, hostile influence on electoral processes and democratic institutions around the world.

3 - Cybercrime poses an increasing threat to election processes. Ransomware attacks can cause significant disruption to both the normal course of an election campaign and the election itself. In addition to candidates' teams, cyberattacks on subcontractors' or volunteers' data can have a significant impact on the entire supply chain. For example, in the 2021 French regional elections, one of the service providers responsible for distributing election advertising was hit by a ransomware attack. As a result, approximately 10% of candidate materials and ballots were not distributed to voters. The main difficulty in analyzing such attacks is to assess whether the ransomware attack had a primarily political or criminal aim. The attribution of the attack to the perpetrators might help here, but this usually turns out to be very difficult.

4 - So far, no significant increase in hostile influence operations has been observed in the French presidential elections of 2022. Neither targeted attacks on candidates or campaigns, nor on state institutions have become known so far. Many of the participating experts attributed this to the fact that the election campaign in France only became a public issue very late in the campaign cycle. Until mid-March, public attention was dominated by ongoing concerns about the COVID-19 situation, as well as the threat posed by the war in Ukraine. In terms of potential attackers, the war in Ukraine also appears to have resulted in a redistribution of operational resources and attention from hostile foreign state actors now needed in active warfare. However, the overall general risk remains high: according to the National Agency for Information Systems Security (ANSSI), France has seen a 37% increase in detected information systems intrusions in 2021.

Furthermore, the progression of the war in Ukraine combined with Emmanuel Macron's entry into the election campaign has led to a measurable increase in disinformation activity since mid-March, which could have implications for political stability beyond the election itself.

To date, dominant fake narratives in France are:

a) French Freedom Convoys – based on massive COVID-related misinformation anti-democratic networks rallied against France's Covid-19 vaccine pass following Canada's "Freedom Convoy," which has seen truckers protesting against vaccine mandates, Covid-19 restrictions.

b) Stop the steal – the idea that the election will be rigged has been adopted from the US 2020 elections. This narrative gained additional traction with the rise of the hashtag #Dominion on Twitter, with the claim that the company Dominion helped Macron win the election in 2017 and that Macron will now win again since the company signed a new deal for the 2022 French elections.

c) The Ukrainian war cabal – circulated in QAnon-dominated networks is the conspiracy narrative which sees the war in Ukraine as part of a global plot to reinstall Macron as President of France.

In addition, the following narratives on the war in Ukraine that are currently being disseminated across Europe by Kremlin may gain some resonance in the context of French elections, combined with other local narratives:

- The West is Russophobic;
- The West engages in information / disinformation warfare against Russia;
- The West threatens Russia; and
- The war can evolve into a nuclear conflict.

II - TACKLING THE THREATS:

KEY TAKEAWAYS AND RECOMMENDATIONS

Strategies to counter influence operations must take full account of their insidious and multifaceted nature. Four dimensions should be particularly considered at several level of action in order to best prevent and mitigate the effects of such operations.

1 - The human factor is the central element in the success of hostiles influence operations. Within the election ecosystem, we see five "food groups" for election interference: At the forefront are candidates, party and campaign staff, followed by NGOs, think tanks, and all staff involved in election administration infrastructure, such as voter registration systems and tabulators. Increasingly experts also see media outlets exposed to cyberattacks. However, they are not passive actors: a lack of knowledge about and awareness of the relevance of cybersecurity among their staff, which often translates into a lack of cyber hygiene, significantly increases the likelihood of a successful attack. In addition to government cyber defense agencies addressing the intelligence and technical dimensions of such risks, greater cybersecurity awareness is needed among all stakeholders at every stage of the electoral process. Cyberattacks and information maneuvers rely on human biases and weaknesses. For example, password-spraying attacks exploit the prevalence of certain passwords in the population (weak passwords such as "azerty" or "123456" or those that refer to a known local reference such as a soccer team) combined with the lack of additional authentication steps. For this reason, it is critical to implement clear strategies for protecting, detecting, and responding to cyberattacks. Simple strategies such as multi-factor authentication, software updates, and internal protocols to mitigate the human factor should be universally and systematically implemented not only for campaign teams, but for the entire value chain, including critical third parties, and coordinated from a central location.

2 - Perception is everything. Beyond the technical dimension, the success of a hostile influence operation is above all measured by its ability to create doubts and reservations towards an electoral process and the results of a particular ballot. Creating the feeling that the electoral process is at least in part rigged, is a major success for the attacker even if an actual cyberattack would only produce minor effects or outcomes from a technical point of view. France is more protected from such a risk than other states due to the low level of digitization of its voting system. However, there is a growing trend within the French disinformation ecosystem to contest the sincerity of the 2022 ballot, similar to claims made during the 2020 elections in the United States or in Germany's election in 2021. If such assertions remain marginal at the moment, a visible dysfunction with sufficient impact for the public could create a momentum to legitimize such claims. This informational risk should therefore be considered when designing cybersecurity strategies in an electoral context, especially when it comes to public communication.

3 - It is crucial to consider the interweaving between local and global scales when addressing hostile influence operations. Hostile influence operations against one electoral process are always part of a larger strategy, especially when it comes from a state-sponsored attacker. At the end of the day, the goal is either to actively influence the outcomes of the ballot in a way seen as beneficial by the attacker, or negatively to destabilize the targeted public sphere. But this "national target" versus "foreign attacker" dynamic is not that simple: foreign hostile actors can find local relays agreeing with their larger views to spread their propaganda from the inside, and can use existing local debates to increase and deepen polarization, and even create political instability. In the same way, local actors from certain margin of the political debate or with interest in contesting the ballot can take inspiration from narratives prevalent in other countries' disinformation spheres by adapting them to the local context. In order to grasp the phenomenon as a whole, the interplay between local and global should inform the design of strategies at the institutional level, particularly in terms of cooperation between the relevant national and/or public authorities.

4 - Beyond the immediate aftermath of the election, effects of hostile influence operations must also be apprehended in the medium and long term. Hostile influence operations ultimately aim at impregnating the public sphere with mistrust against the institution and the sincerity of the electoral process. A hostile influence operation against one precise ballot is usually part of long-term strategies mobilizing a well-established ecosystem of cyber attackers and disinformation actors and multi-layered narratives that go far beyond the national and immediate reality of the electoral process. Countering electoral interferences must therefore be part of a permanent strategy against hostile influence operations targeting democratic states.

PARIS
PEACE
FORUM
de PARIS
sur la PAIX

The Paris Peace Forum is a French initiative launched in 2018 to create a multi-actor platform in Paris to address global governance issues. Throughout the year, the Forum works with actors from across the world - including the global South - to strengthen the governance of global commons, including on climate, public health, outer space and digital issues.

Its annual event gathers heads of state, government and international organizations, together with civil society and private sector leaders around concrete solutions for better global governance.

Transatlantic Commission on Election Integrity

Part of Alliance of Democracies

The Transatlantic Commission on Election Integrity (TCEI) seeks to fill a critical gap by fostering a global and collective approach to curb the ongoing wave of election interference and raises awareness of public and governments about the risks of interference. It helps sharing best practices between decision-makers, public and private institutions and actors across the globe and applies on the ground new models of cooperation and technologies to empower civil society and governments to defend democracy against malign interference. Since its launch in 2018, the TCEI has established itself as an important global voice and player on the risks and solutions to combat foreign election meddling. The TCEI brings together more than a dozen eminent persons from backgrounds in politics, media and the private sector chaired by former NATO Chief and Danish Prime Minister, Anders Fogh Rasmussen, and former US Homeland Security Secretary, Michael Chertoff.