ENGINEERING DOUBT

CYBER OPERATIONS AND HYBRID ELECTION INTERFERENCE IN MOLDOVA'S 2025 ELECTIONS

Author: David Smith

Produced in cooperation with WatchDog.MD Community

2026

Table of Contents

Executive Summary

Moldova's 2025 parliamentary elections were targeted by a coordinated hybrid campaign linked to Kremlin-aligned networks. This campaign combined cyber operations, Foreign Information Manipulation and Interference (FIMI), staged evidence of electoral fraud and attempts to mobilize street protests in order to undermine confidence in the election outcome.

Cyberattacks were a key **enabling element** of this strategy. In the weeks before the vote, thousands of home internet routers in Moldova were compromised and prepared for use in a large-scale distributed denial of service (DDoS) attack. On election day, attackers launched sustained attacks against infrastructure operated by the Central Election Commission (CEC) and the Information Technology and Cyber Security Service (STISC). The goal was not to alter vote totals directly - Moldova uses paper ballots and hand counting - but to disrupt digital systems used for voter verification and the real-time reporting of election results.

Had these systems failed, the resulting delays and technical disruptions could have been used to fuel disinformation narratives alleging electoral fraud and to support planned political protests contesting the legitimacy of the vote.

In practice, these efforts largely failed. Moldovan authorities and their partners were able to maintain the operation of critical election infrastructure, limiting the effectiveness of the broader hybrid campaign. Moldova's experience demonstrates how cyber operations can serve as enabling tools within integrated political interference efforts - and how institutional preparation and coordinated defense can significantly reduce their impact.

Introduction

Moldova's 2025 parliamentary elections took place against the backdrop of sustained Russian hybrid pressure on the country's democratic institutions. In the months leading up to the vote, Moldovan authorities and independent investigators documented a wide range of activities linked to Kremlin-aligned networks. These included disinformation campaigns, illicit political financing, efforts to mobilize paid street protests and attempts to manipulate public perceptions of the electoral process.

Cyber operations formed an important component of this broader effort. In the year leading up to the election cyber operations primarily worked to support FIMI campaigns and circumvent website blocking. In the weeks before the election and throughout election day itself, Moldovan institutions faced a series of direct cyber attacks ranging from the compromise of home internet routers to large-scale distributed denial of service (DDoS) attacks targeting government infrastructure. These attacks were directed at systems supporting the Central Election Commission (CEC) and other critical digital services used during the voting process.

Cyberattacks aimed to disrupt election-day systems, slow the reporting of results, and create visible technical failures that might undermine public confidence in the integrity of the vote.

This report argues that cyber operations targeting Moldova's 2025 elections should be understood not as isolated attacks but as part of an integrated hybrid campaign. Their purpose was to enable and amplify other political operations designed to contest the legitimacy of the election outcome. Technical disruption could create uncertainty, information operations could frame that uncertainty as evidence of fraud and organized protests could then transform these narratives into political pressure against the government.

The report is broken into four parts:

- Section 1 outlines Moldova's evolving cybersecurity architecture and the institutional reforms implemented since 2017.
- Section 2 examines how cyber capabilities were used to support foreign information manipulation and interference (FIMI) operations targeting Moldovan audiences.
- Section 3 analyzes the cyberattacks directed at election infrastructure on election day itself.
- Section 4 examines how these cyber operations interacted with other elements of a broader hybrid strategy intended to undermine confidence in the electoral process.

While the attacks ultimately failed to disrupt the election in a meaningful way, they illustrate how cyber operations can function as enabling tools within larger political campaigns aimed at delegitimizing democratic institutions. Moldova's experience therefore offers important lessons for understanding the role of cyber activity within contemporary hybrid interference operations.

Section 1: Moldova's Cyber Landscape

Successive Moldovan governments have been working since 2017 to modernize the country's cybersecurity infrastructure and defenses. This began with the country's first comprehensive cybersecurity law which created a national strategy and outlined the restructuring of critical institutions.

In subsequent years a number of institutions were reformed or created in order to coordinate and implement the country's cyber defenses. The key ones were:

- ***Serviciul Tehnologia Informației și Securitate Cibernetică*** **(Information Technology and Cyber Security Service, STISC)**. STISC was created in 2018 from the existing Centrul de Telecomunicații Speciale (Special Telecommunications Center, CTS). CTS was itself created in the 1990s to take over KGB-era secure communications infrastructure. Its mission remained focused on securing government communications and the maintenance of these legacy systems. When CTS was reformed into STISC the focus shifted from simply securing information to protecting the government's entire cyber infrastructure. It is the agency primarily responsible for protecting government IT systems.
- ***Agenția pentru Securitate Cibernetică*** **(National Cyber Security Authority, ASC)**. ASC was created in 2023 to oversee cybersecurity strategy, regulation and coordination. The ASC is responsible for aligning with EU cybersecurity frameworks

and overseeing compliance by private sector actors who manage critical infrastructure - such as telecom companies.
- ***National Institute of Innovations in Cybersecurity*** **"Cybercor.**" Launched in 2024 with the support of the Future Technologies Project supported by USAID, the UK government and Sweden, Cybercor is an education and research center located in the Technical University of Moldova (UTM). Its mission is to train civil servants and to create a robust hiring pool of cybersecurity professionals.

During these years the Moldovan parliament passed a series of major laws related to cybersecurity. These aligned Moldova with EU directives and created inter-agency / inter-ministerial emergency response working groups. Critical infrastructure was identified and regulations were created to assure that cyber risk management and incident reporting mechanisms were in place in the companies operating that infrastructure.

According to Anatolie Golovco, Cybersecurity Advisor to the Prime Minister (February 2023 - present), a critical piece of this was the creation of well-paid civil service positions in these agencies[1].

Since 2018, and in accelerating fashion since February 2022, these agencies have worked on 4 topline goals:

1. **Consolidating and hardening government digital platforms and infrastructure**. These were largely centralized under STISC.
2. **Shifting focus from information security to infrastructure security**.
3. **Implementing the EU's Network and Information Security (NIS) Directive** and coordinating with private sector critical infrastructure operators to ensure compliance.
4. **Assuring a training pipeline of skilled cybersecurity professionals and attractive jobs to accommodate them**.

It was these changes, as well as the ongoing support from Moldova's security and development partners, that put the country in a position to identify and respond to Russian hybrid attacks that involved cyber operations. Moldova entered the 2025 election with a far more centralized and capable cyber-defense posture than in earlier years.

Section 2: Cyber as an Enabler for Information Operations

One of the key functions of Kremlin cyber operations was the furtherance of their Foreign Information Manipulation and Interference (FIMI) campaigns targeting both Moldova and other parts of the world. In Moldova, these FIMI operations were designed to shape the political environment ahead of elections and to provide tools for rapid dissemination of FIMI

[1] **Explainer**: The Moldovan government has always struggled to pay a market rate to civil servants, much less a competitive rate in the ITC sphere. Trying to create well paid jobs generally causes backlash as people demand higher salaries for teachers, medical workers and other highly visible and very underpaid civil service jobs. Overcoming this political issue and assuring that the government could compete with the private sector in hiring talent proved essential to creating and reforming these institutions.

on election day and immediately after. Cyber operations acted as an enabler for these campaigns in the following key ways:

1. **Evading Website Blocks** - As the Moldovan (or European) authorities block websites or TV channels, Kremlin actors create workarounds. That included both replicating infrastructure and attacking user's Domain Name Service (DNS) systems.
2. **Hack & Leak Operations** - Kremlin hackers breached the personal devices of Moldovan politicians and activists and leaked information selectively (and possibly after altering it). Hack-and-leak operations are visible, but we must assume that similar operations are happening invisibly at the level of espionage. Passing sensitive information to Russian proxies or using it to frame campaign and messaging strategy.

2.1 Evading Website Blocks

In response to propaganda being produced by the Kremlin in support of the war in Ukraine, the Moldovan government has taken steps to block certain TV stations and websites affiliated with the Kremlin and Ilan Shor. This has created a cat-and-mouse game as Kremlin cyber actors race to find ways around these blockages.

The most common way to block a website uses DNS, where the government orders Internet Service Providers (ISPs) to modify their DNS records to prevent users in that network from finding the IP address of the website they are looking for.

One example of this process was reported on in June 2025 when the Atlantic Council's Digital Forensics Lab (DFRLab) published a report detailing the new online[2] TV channel Moldova24 (MD24). The TV channel had a variety of web addresses including moldova24.online, moldova24.org, moldova-24.live, etc. These, in turn, all directed users to the same website but could be switched out as the Moldovan government worked to block the DNS records. At the same time, DFRLab showed that the IP address behind these websites was also hosting dozens of other websites used to promote Ilan Shor and to spread Russian disinformation - including multi-lingual black propaganda services in French, Spanish, Croatian, Italian and more.

By July 2025 these tactics became more sophisticated. At that time anonymous advertising campaigns began promoting a new streaming platform called HaiTV. This application and website advertised the ability to access blocked Russian TV channels - which meant movie and TV options, as well as MD24, Russian propaganda channels and Shor channels. While the government quickly announced the blocking of this new site, it remained accessible in Moldova even weeks later due to sophisticated efforts to circumvent these blocks.

Ziarul de Garda reported that HaiTV domain was purchased and registered by the Moscow based, UK registered, Aeza International LTD. This company was responsible for creating and running a network called "Doppelganger" which Qurium had previously reported as using complex network infrastructure to both evade blockages and to substitute fake website

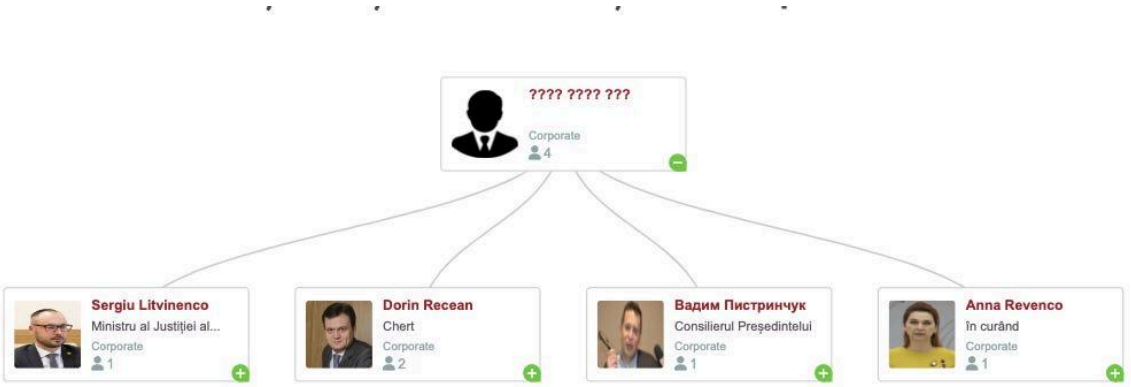
[2] Victoria Olari, "The Russian web behind the Moldova24 TV channel," Digital Forensic Research Lab (DFRLab), June 3, 2025, https://dfrlab.org/2025/06/02/unveiling-the-russian-infrastructure-supporting-the-moldova24-tv-channel/.

clones for real sites. This involved cloning the Washington Post, FoxNews, Le Parisien and many many others.

In this cat-and-mouse game, Kremlin actors regularly used Western registered companies and Western infrastructure in order to bypass national level blocking. Via sophisticated manipulations of DNS records and the use of many intermediary domains their cyberoperations acted as enablers to the broader FIMI operations.

2.2 Hack & Leak

In addition to protecting FIMI resources by keeping them online, Russian hackers regularly sought to breach the computer systems or online accounts of Moldovan politicians, journalists and civil society actors. In the case of the 2022 "Moldova Leaks" Telegram hacks, this was designed to reveal unflattering messages and to create fear that the hackers had much more information than they shared.



Caption: Photo source: screenshot from Moldova Leaks website

The Moldova Leaks operation released the Telegram address books and chat logs for prominent government and civil society leaders one by one. The implication was that they were building to a major reveal (the blacked out figure) but that never happened and the site was deleted. In addition to the leaking embarrassing (and possibly manipulated) message exchanges, this slow build created paranoia around who would be targeted next and what more would be released.

In other examples, a cyberattack originating from the network of Aeza International LTD hacked official emails of TV8 and Moldelectrica. They then sent official emails to individuals and institutions containing disinformation messages.

It's worth noting that Hack & Leak operations were also conducted by anti-Kremlin organizations (currently unidentified) and resulted in the dissemination of phone recordings of Moldovan politicians talking to their FSB handlers and troves of insider data into the Shor network.

Section 3: Cyberattacks on Election Infrastructure

The second major focus of Kremlin cyberattacks on Moldova's elections was targeted at election day itself and involved an attempt to take down Moldova's digital election infrastructure. While Moldovan elections are conducted entirely with paper ballots and hand counts, the country relies on important digital systems run by the Central Elections Commission (CEC) to conduct the elections and distribute the results.

3.1 Why Paper Elections Still Depend on Digital Systems

When a voter enters a polling station (in Moldova or in a diaspora polling place) they show their national ID card to a poll worker who verifies in the CEC system that this person is at the right polling station and eligible to vote. The voter then votes and places a paper ballot in a box, while the computer system notifies the central CEC servers that the person voted. This prevents the same person from trying to go to another polling place and vote again. Additionally, it updates a ticker on the CEC website showing turnout in real time.

This CEC website is detailed about voter turnout - showing vote by regions, demographics, etc. It also updates constantly and people are used to watching returns in real time on election day.

When the polls close, the paper ballots are counted by hand in the presence of election observers. Once the count is certified the totals are sent provisionally to the CEC server which publishes them on the website precinct by precinct. This also creates a "real time viewing" perception by voters who are accustomed to a rapid vote count after the polls close.

3.2 What the Attackers Were Trying to Disrupt

The attacker's goal was to disrupt the CEC system in order to shake public confidence in the outcome of the vote. The aim was to slow down or fully disrupt the digital systems in order to force an all-paper process. This would slow but not stop voting or the vote count.

Without computer ID verification, voters would need to be checked against printed voter lists. This slows the process and removes the real time data transmitted to the CEC that people watch online on election day. This would similarly affect the vote count and reporting process which may drag out over several days.

To be clear, the attackers did not try to change vote totals or to otherwise directly impact the election results. The goal instead was to undermine faith in the elections and ***imply that someone else was manipulating the results***. By slowing or disrupting these real time systems they could discredit the government - showing that they are not in control of critical infrastructure - and they could plant FIMI narratives about how the disruptions were because PAS was rigging the election itself. We'll look at this broader hybrid attack landscape in Section 4.

3.3 How DDoS fit that objective

A Distributed Denial of Service Attack (DDoS) is a cyberattack designed to overwhelm a website or network service with a flood of illegitimate requests. The attacker instructs a huge number of computers or devices to all request the service at the same time (e.g. load a webpage). This causes the server coming under attack to either slow under the flood of requests or simply crash. Thereby the attack denies service to legitimate users who will be unable to access it.

The CEC's election infrastructure is managed by STISC which houses centralized government servers and network infrastructure. On election day, DDoS attacks were directed at STISC infrastructure with the goals of taking down the CEC website and disrupting the VPN secure connections between the central CEC servers and the polling stations.

STISC did not act alone in defending critical networks and was supported by various outside actors including some companies. One example was CloudFlare which helped STISC defend election infrastructure against DDoS attacks. In a post election article they wrote:

"[O]n September 28, 2025, the Moldovan Central Election Commission (CEC) experienced a series of concentrated, high-volume (DDoS) attacks strategically timed throughout the day. The attack began in the morning at 09:06:00 UTC and lasted for over twelve hours and ended as the official result reporting was underway at 21:34:00 UTC. In total, we mitigated over 898 million malicious requests directed at the CEC over the twelve-hour period."

Defending against DDoS attacks generally involves identifying illegitimate incoming traffic and blocking it / filtering it out. This is easiest to do when the traffic has a common origin and is therefore less "distributed" - for example, Russian systems known to be used for cyber attacks. This gets much harder when the attack is coming from closer to home.

3.4 Weaponizing Home Routers and IoT

In order to make it as difficult as possible to defend against these DDoS attacks, Russian actors sought to compromise as many devices as possible inside Moldova. If the cyberattack was coming from Moldovan citizens' homes, it would be very hard for STISC and partners to identify who is legitimately trying to access the CEC website and who is a malicious attacker. It could also mean that defending the CEC website would mean cutting off legitimate users.

On September 24, 2025 National Chief of Police Viorel Cernăuțeanu announced that "thousands" of home internet routers had become compromised. With just 4 days to go before the elections Cernăuțeanu warned the public that this network was to be used in a DDoS attack against the CEC and government systems, and stated that the authorities were working on it.

This entailed a minimum of tens of thousands of home routers with the total number remaining undisclosed. The compromise affected MoldTelecom systems using combo fiber optic modems and home Wi-Fi routers. It remains unknown how the routers were infected, but the purpose was clear. They served two functions:

1) **Creation of a Local Botnet** - The compromised routers then opened up the compromise of all the devices on that local home network. This particularly focused on Internet of Things (IoT) devices with weak security. According to Anatolie Golovco, in one example, they detected a wave of DDoS attacks from a Chinese brand of air conditioner that has a Wi-Fi connection.
2) **DNS Spoofing / Traffic Re-Routing** - The same router compromise also re-directed traffic to Russian network infrastructure. This meant that Moldovans wanting to load example.com would first travel into this malicious Russian network without ever knowing it. That would bypass Moldova's website blocks on apps such as HaiTV, but it would also allow Russia to use DNS spoofing to replace the real example.com with a Russian clone. That would allow them to, for example, display their own CEC website to any users with hacked home router equipment.

It remains unclear how the attackers gained access to so many routers, but Anatolie Golovco believes it was most likely leveraging default passwords and other soft spots in security. He also noted that there was an additional element here of "social engineering." No one wanted their home networks to be hacked, but lots of people wanted access to blocked Russian channels playing movies they like. Golovco noted that in every group of friends, or village, there's someone who helps you reinstall Windows and fix your Wi-Fi. He suspects that some of these people were unwittingly compromising home equipment by modifying settings or installing software meant to get around blocks on popular movie / TV channels.

3.5 How Defenders Kept the Network Online

This attack ultimately failed. While many details have not been made public, we know a few details.

- **Last minute updates**. The government worked with MoldTelecom to push out a massive update to affected routers. Because these were combo modem-routers from MoldTelecom they are technically customer-premises equipment, legally owned by the company. This meant that Chief of Police Cernăuțeanu didn't have to plead with citizens to update their routers, the company could do it en masse.
- **Cloudflare and partners**. STISC had many partners both in the private sector and in the form of foreign partners. Other than Cloudflare, most prefer to remain anonymous. Collectively these efforts responded in real time to incoming DDoS attacks and coordinated to manage and block attack vectors.

With a flurry of activity in the weeks before the election, as well as on election day itself, STISC and partners were able to keep the CEC infrastructure operational on election day.

Section 4: Hybrid Attacks - Undermining the Election Results

The likely political objective was not to change votes directly, but to create a disputed outcome. To do that, the attackers needed four things: technical disruption, apparent evidence of fraud, visible disorder and protest capacity.

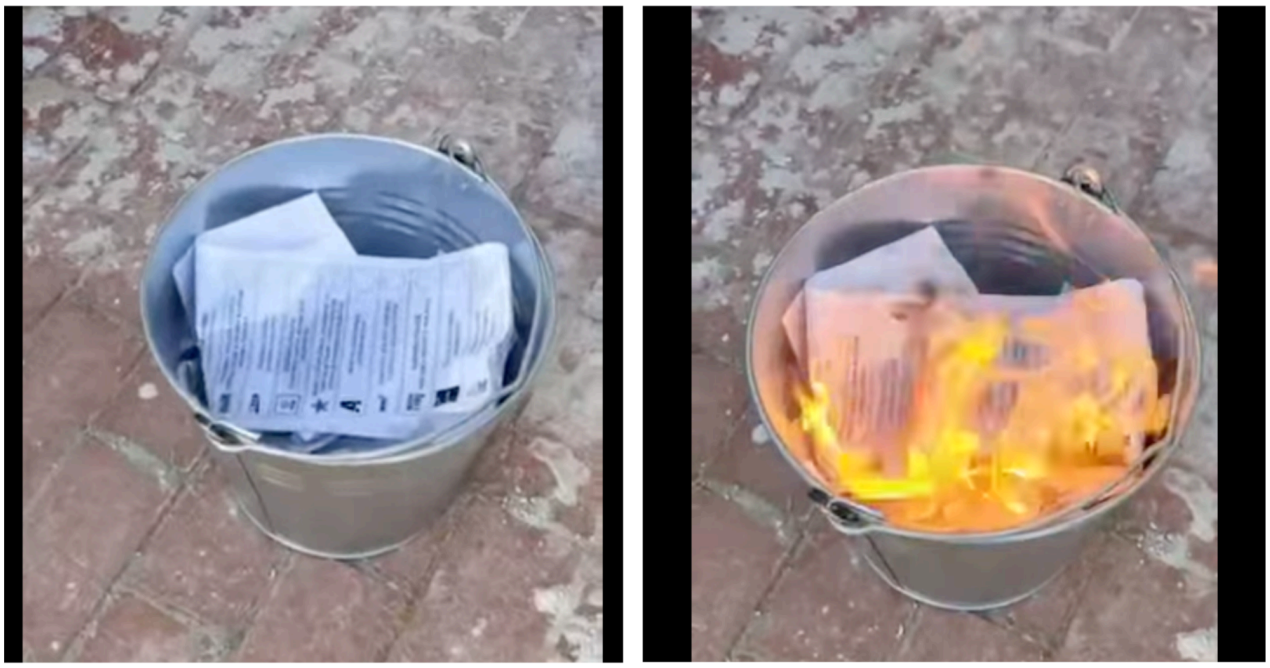
The cyberattack would provide technical disruption and a discrediting of the Moldovan government's ability to conduct elections. Let's walk through the other elements of this integrated hybrid operation:

4.1 "Evidence" of Electoral Fraud

Kremlin networks organized multiple operations to sow doubt and provide alleged evidence of fraud by PAS and the pro-EU parties. One example of that was dubbed "Operation diaspora" and was designed to discredit votes from those in the diaspora.

Investigative journalists from ZdG infiltrated this coordinated operation to recruit unofficial "election observers" to watch polling places in the diaspora. This centrally controlled operation promised "salaries" of €300 - €500 euros per day and "bonuses" of up to €30,000 euros for video evidence showing vote rigging. In many cases, "observers" were given the option of the candidate whose campaign would allegedly register them with the CEC. These candidates were not selected from the pro-Russian opposition and they denied participation. Some of these "observers" who were confronted appeared confused and sheepish, including one confronted by the Moldovan Ambassador to Greece who admitted that things were proceeding in an orderly fashion. All observers were tasked with counting (via an app) each person who went into the voting booth.

In addition to this, online videos were released as part of information operations allegedly showing vote rigging. This included videos purporting to show election workers burning stacks of ballots stamped for the pro-Russian "Patriotic Bloc," all implying that PAS was working to rig the elections.



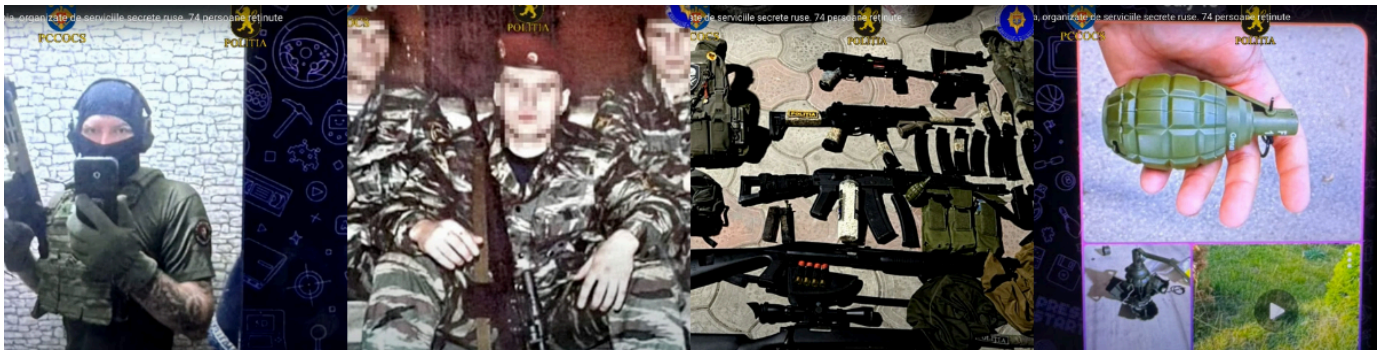
Caption: Screenshots from the video purporting to show an election worker burning ballots cast by people who voted for the Patriotic Bloc, who he calls "idiots."

4.2 Visible Disorder

On election day there were multiple threats against polling stations. Bomb threats were called against polling places in Brussels, Rome, Genoa (Italy), Bucharest, Asheville (USA) and Alicante (Spain). In Iași a man threw a tear gas grenade into a polling station. There were also many bomb threats against polling stations inside the security zone. Embassies and polling places had to be evacuated and checked by the police delaying some votes.

4.3 Street Mobilization and Escalation

Long before the elections the Shor network had made preparations for violent street protests. On September 22, 2025 the Moldovan authorities conducted more than 250 searches and made more than 70 arrests around the country targeting people planning for violent unrest. The investigation targeted people brought by the Shor network to Serbia under the guise of religious pilgrimages. There they were trained with firearms, armed drones and learned tactics to instigate street riots. The operation was overseen by Russian intelligence and searches turned up weapons, ammunition, explosives and other equipment. Police released a compilation video showing some of the arrests and evidence from the raids. Here are some screenshots from the video:



4.4 Protest and Stop the Steal

All of these elements were designed to be used to contest a close election and to discredit the democratic legitimacy of any pro-EU parties who came to power. In the months leading up to elections there was a constant drumbeat of statements from pro-Russian figures alleging that the elections would be rigged. Many of them cited supposed rigging of the Romanian elections and built on a stolen-election narrative that George Simion had been building there.

There is evidence that mass street protests against the elections were planned and police reported that on September 29th messages went out promising €150 euros for people to come to a protest and €50 more to "bring a friend." The protest in question was organized by Igor Dodon, who denied the paid protest allegations. The event was being organized "without party flags" and was billed as the opposition defending victory that he said was assured.

Ultimately the protest was small, peaceful and lasted around half an hour. After a few speeches everyone just went home.

Each of the steps in this integrated hybrid campaign ultimately failed. The end result was lots of noise and many confusing headlines but no mass unrest. The failure of the cyberattacks against the CEC were one important factor in defusing the planned FIMI campaign. In the end, the small protests that occurred claimed that the elections were illegitimate but had few arguments to explain why and a very small organic turnout to hear them.

Conclusion

The cyber operations targeting Moldova's 2025 parliamentary elections were not designed to directly alter vote totals or manipulate ballots. Instead, they were part of a broader hybrid strategy intended to undermine confidence in the electoral process and create the conditions for a contested political outcome.

Because Moldova conducts elections using paper ballots and hand counts, the attackers focused on the digital systems that support the voting process rather than the ballots themselves. Disrupting the Central Election Commission's infrastructure could have slowed voter verification, delayed the reporting of turnout and results, and created visible uncertainty on election day. In such an environment, information operations could frame technical disruptions as evidence of fraud or manipulation by the government.

These cyber operations were therefore closely linked to other elements of the broader campaign. Disinformation networks sought to produce alleged evidence of fraud. Organized actors attempted to generate disorder around polling stations and in diaspora voting locations. Meanwhile, political networks connected to the Kremlin-aligned opposition prepared to mobilize protests contesting the election outcome. Each of these elements reinforced the others. Technical disruption could provide the initial trigger, information operations could shape public interpretation, and street protests could transform uncertainty into political pressure.

In practice, this integrated strategy largely failed. Moldovan institutions were able to keep critical election infrastructure operational despite sustained DDoS attacks and other cyber operations. At the same time, attempts to generate credible evidence of electoral fraud proved weak, and efforts to mobilize large-scale protests produced only limited participation. Without visible technical disruption or persuasive evidence of wrongdoing, narratives claiming that the election was illegitimate struggled to gain traction. Critically, the election was also not very close.

The events surrounding Moldova's 2025 elections illustrate an important characteristic of contemporary hybrid interference campaigns. Cyber operations rarely operate in isolation. Their strategic value often lies in enabling or amplifying other political and information operations designed to challenge the legitimacy of democratic institutions. In Moldova's case, the resilience of election infrastructure prevented cyberattacks from creating the uncertainty needed for these wider operations to succeed.

As elections across Europe continue to face similar hybrid threats, Moldova's experience highlights the importance of strengthening both technical defenses and institutional coordination. Cybersecurity reforms implemented since 2017 - along with cooperation between government agencies and outside partners - played a key role in maintaining the integrity of the electoral process. While vulnerabilities remain, the 2025 elections demonstrate that coordinated preparation can significantly limit the impact of cyber-enabled hybrid attacks.