



# 2024 Elections in the Crosshairs



## *Cyber Threats and Influence Operations*



**Coline CHAVANE**  
CTI- Strategic analyst

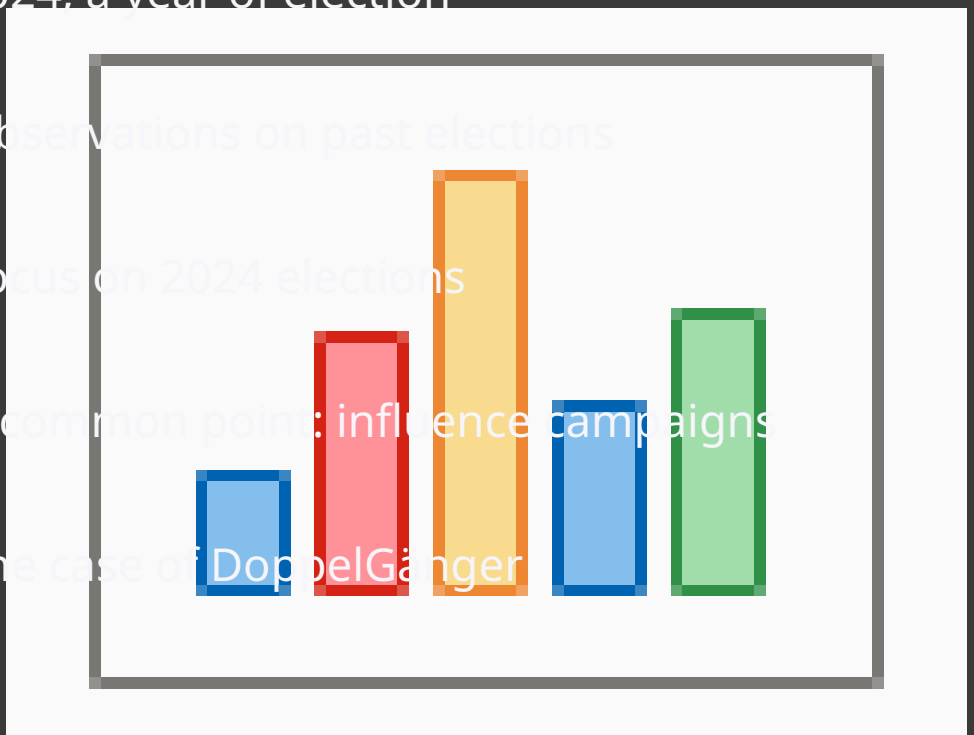


**Amaury-Jacques Garçon**  
CTI- Technical analyst

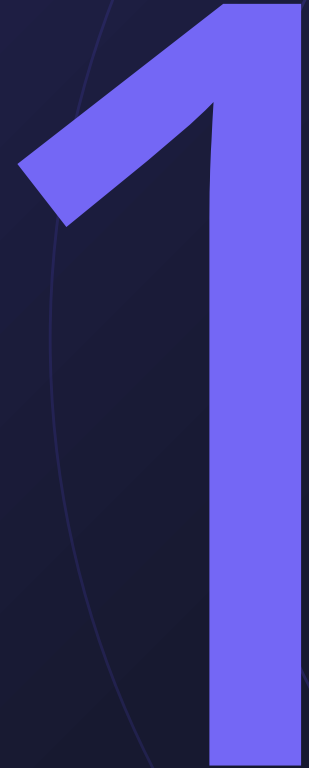


# SUMMARY

- 2024, a year of election
- Observations on past elections
- Focus on 2024 elections
- A common point: influence campaigns
- The case of DoppelGänger



# 2024 A YEAR OF ELECTIONS





# 2024 A year of elections

## Global overview & context

**54%** of the **world population** called to ballots.

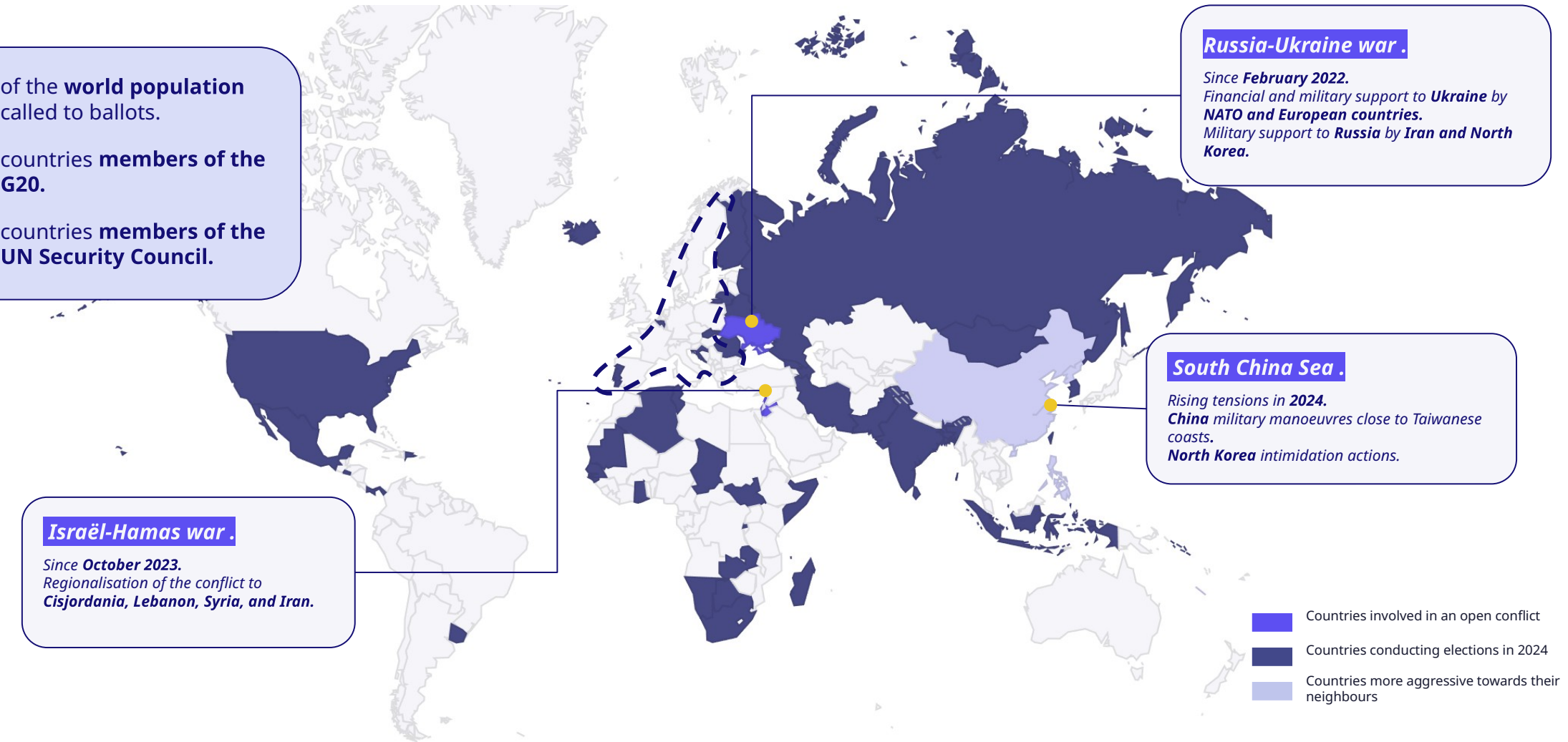
**10** countries **members of the G20.**

**4** countries **members of the UN Security Council.**

**Israël-Hamas war .**  
Since **October 2023.**  
Regionalisation of the conflict to **Cisjordania, Lebanon, Syria, and Iran.**

**Russia-Ukraine war .**  
Since **February 2022.**  
Financial and military support to **Ukraine** by **NATO and European countries.**  
Military support to **Russia** by **Iran and North Korea.**

**South China Sea .**  
Rising tensions in **2024.**  
**China** military manoeuvres close to **Taiwanese** coasts.  
**North Korea** intimidation actions.



# PAST ELECTIONS CYBER THREATS

# 2

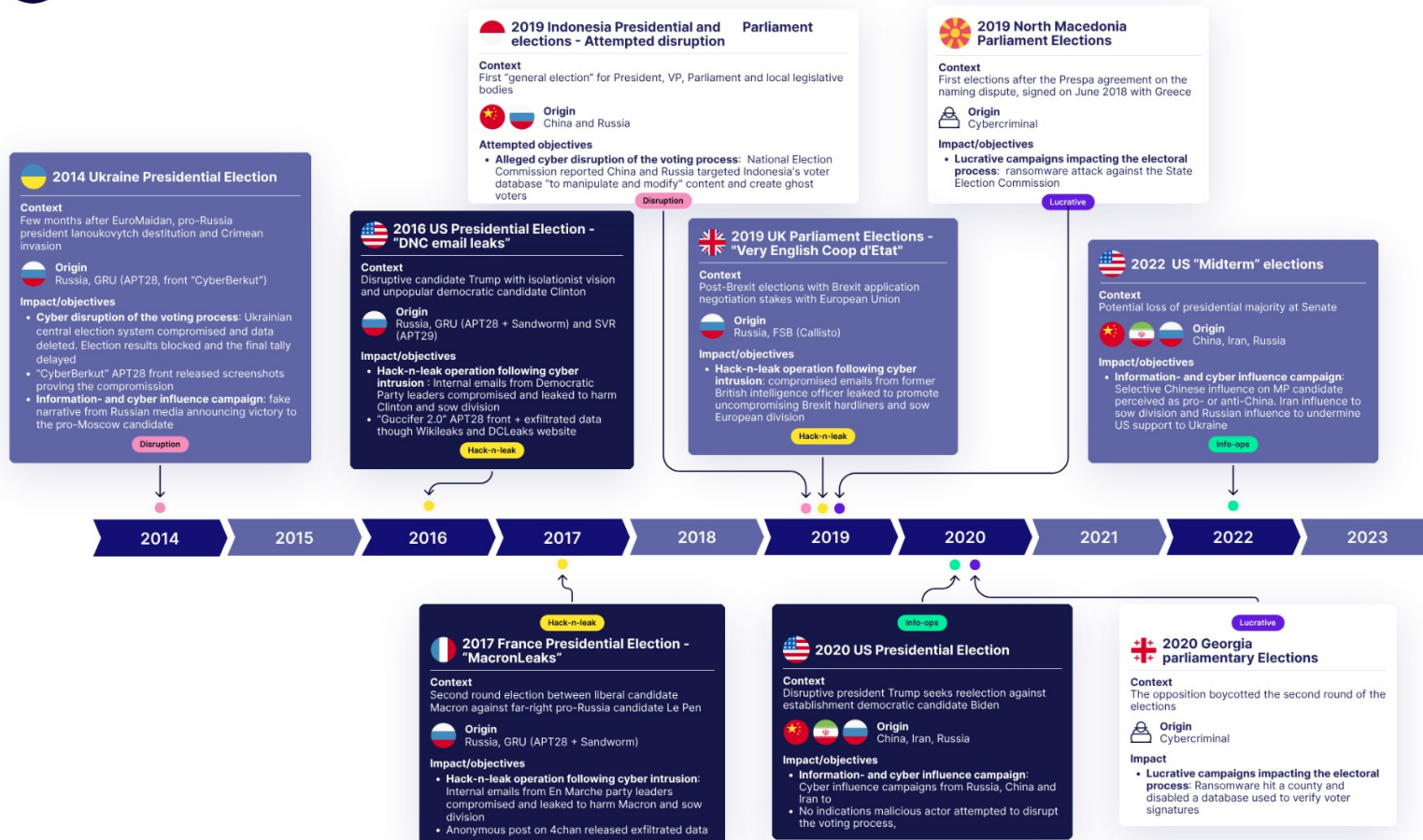




# Past elections cyber threats

## Historical retrospective, different types of cyber operations

### sekoia | Past elections impacted by cyber operations



### TYPES OF OPERATIONS

- Hack-and-leak operation
- Information and cyber influence
- Cyber disruption of the voting process
- Lucrative campaigns



# Past elections cyber threats

## Historical retrospective, different types of cyber operations

### THE MOST IMPACTFUL

- Long-term planning.
- Cyber intrusion targeting information systems associated with a political
- Extraction of data to cause reputational damage.

More than **20.000 emails** leaked.

**Two days** before the final vote.

Attributed to the **GRU** through the related **intrusion sets APT28** and **Sandworm**.

To **undermine the candidate E. Marcon** and promote the **far-right candidate Marine Le Pen**.

2016

Cyber Security Mission


### THE OPPORTUNIST

- Broad and massive **opportunistic** campaigns.
- Take **advantage of the context** to increase profit.

**Double extortion attack.**

**State election committee website** unavailable for **three days.**

It affects **access to voter registration** and **email servers.**



**2019 North Macedonia Parliament Elections**

**Context**  
First elections after the Prespa agreement on the naming dispute, signed on June 2018 with Greece

**Origin**  
Cybercriminal

**Impact/objectives**

- **Lucrative campaigns impacting the electoral process:** ransomware attack against the State Election Commission

Lucrative

# 2024 ELECTIONS

## FOCUS

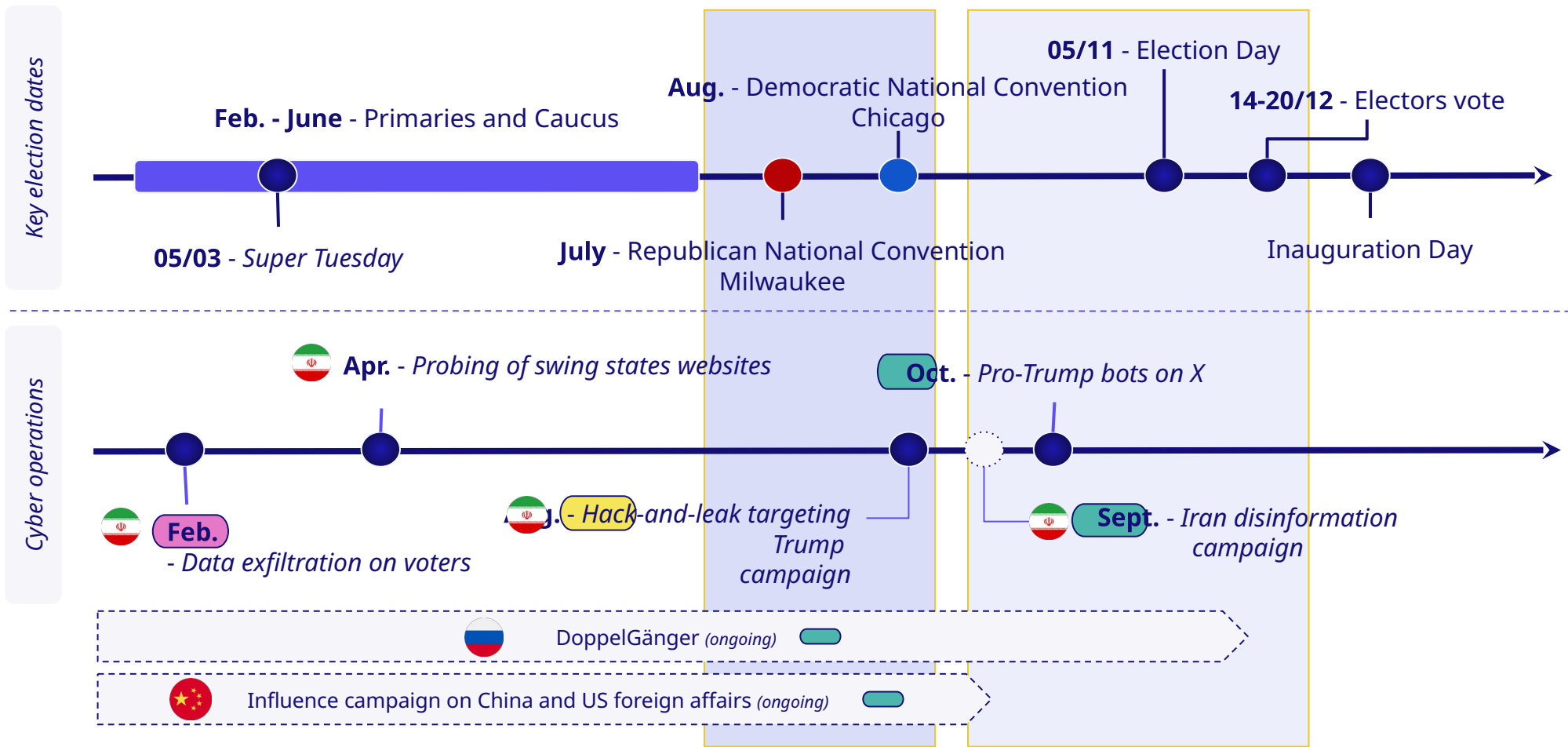






# Past elections cyber threats

## Focus on 2024 US Presidential Elections



312 (50,1%)

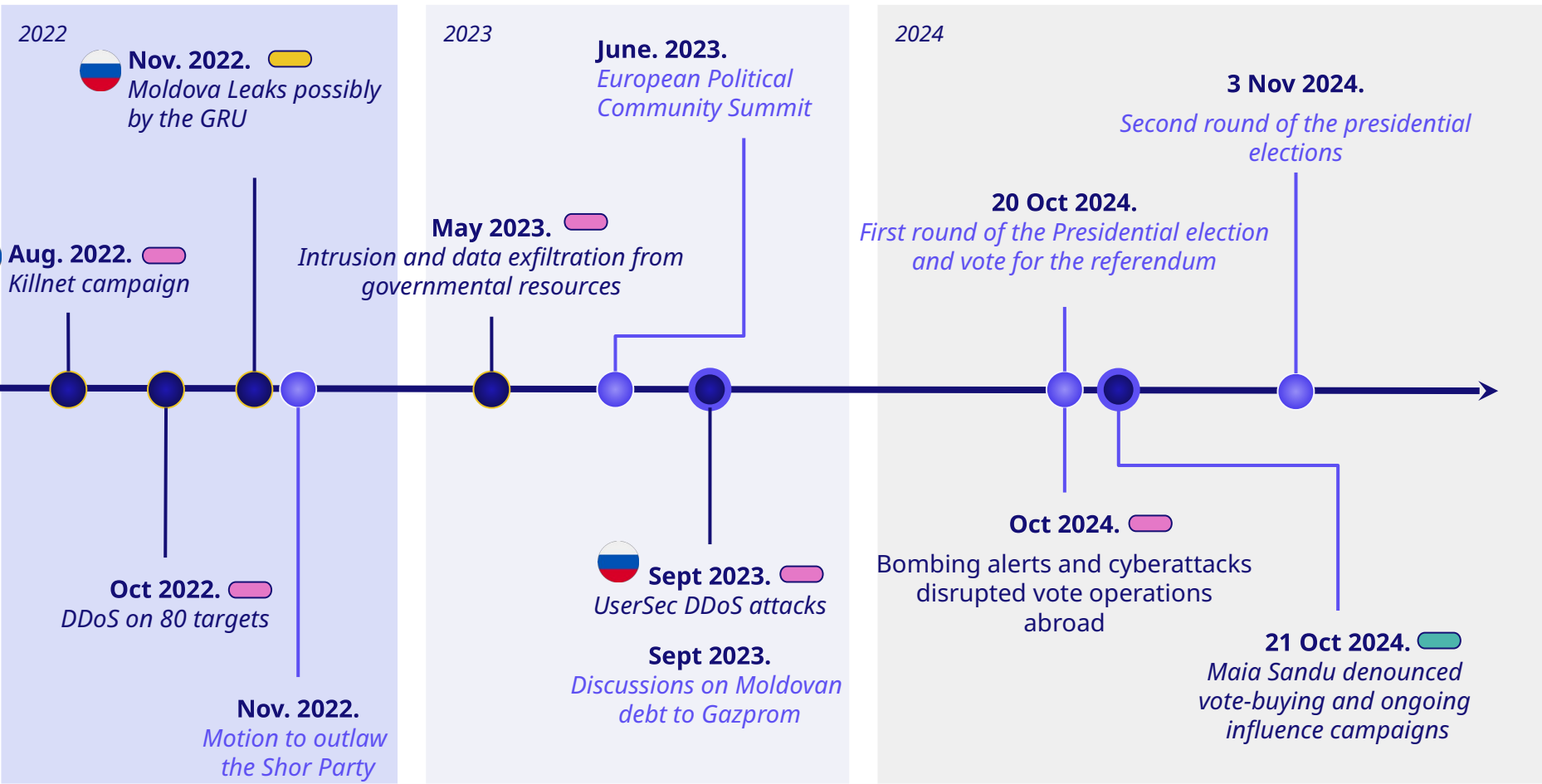


226 (48,3%)



# Past elections cyber threats

## Focus on 2024 Moldova Presidential elections & referendum



1st: 42, 49% | 2nd: 55, 35%



1st: 25, 95% | 2nd: 44, 65%



1st: 13, 79%



1st: 5, 38%

# INFLUENCE

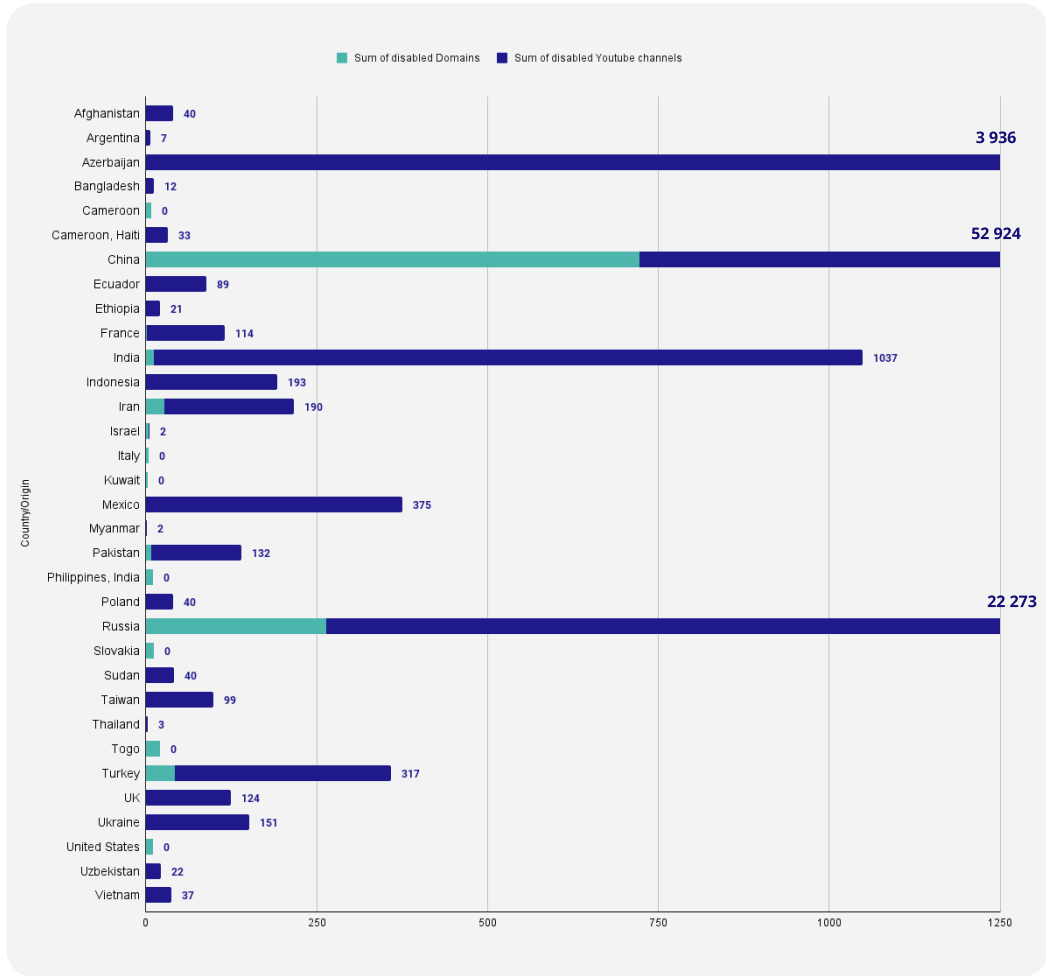
## CYBER THREATS

# 4



# Influence cyber threats

## An increasing trend...



### IN 2024, WERE OBSERVED

**34** countries at the origin of coordinated influence campaigns.

**4** of the most used social platforms are being used to supports these campaigns.

#### China

2 Ads accounts,  
722 domains,  
52 300 youtube  
channels **terminated.**

#### Russia

15 Ads accounts,  
254 domains,  
22 000 youtube  
channels **terminated.**

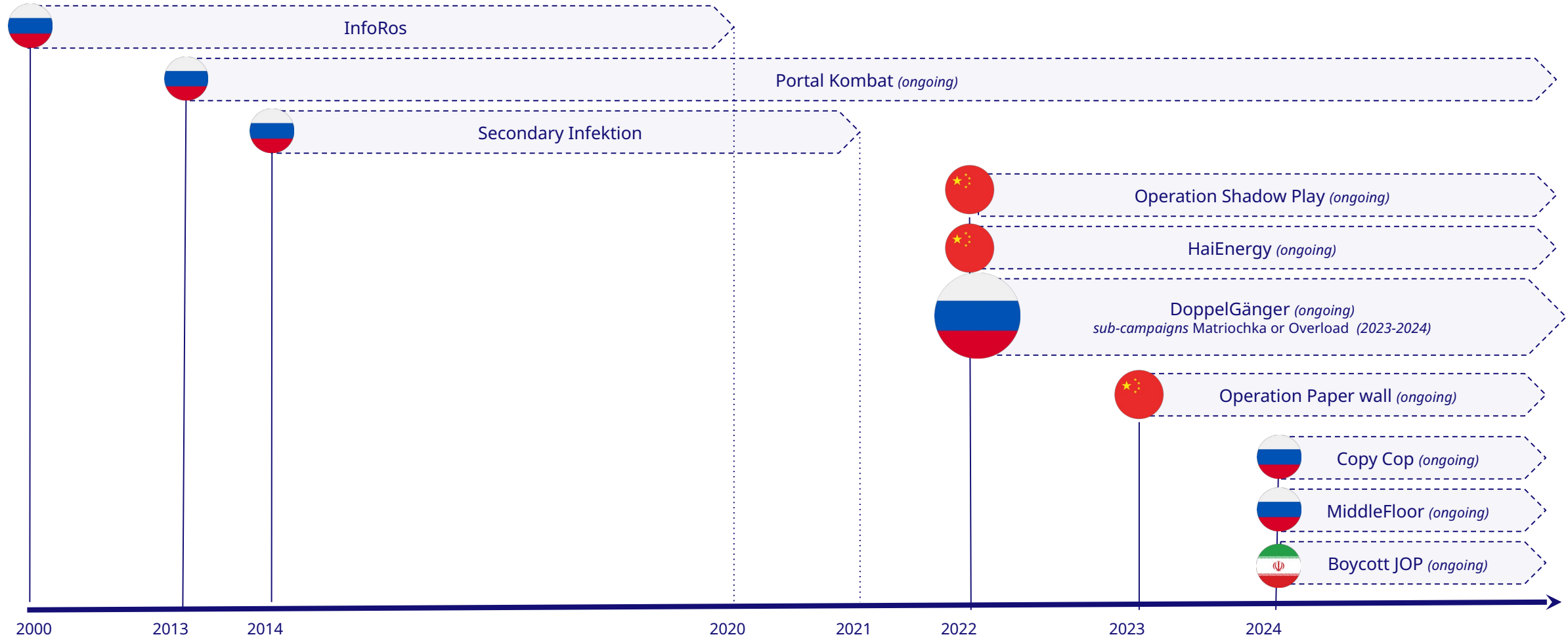
#### Iran

2 Ads accounts,  
22 domains,  
190 youtube channels  
**terminated.**



# Influence cyber threats

...But not something new





# Master of Puppets:

The DoppelGänger  
operation

# 5



# Master of Puppets: The DoppelGänger operation

## Introduction

Hundreds of thousands of fake accounts

Thousands Domain Names

Dozens of different clusters



<https://www.diplomatie.gouv.fr>

~40 publications



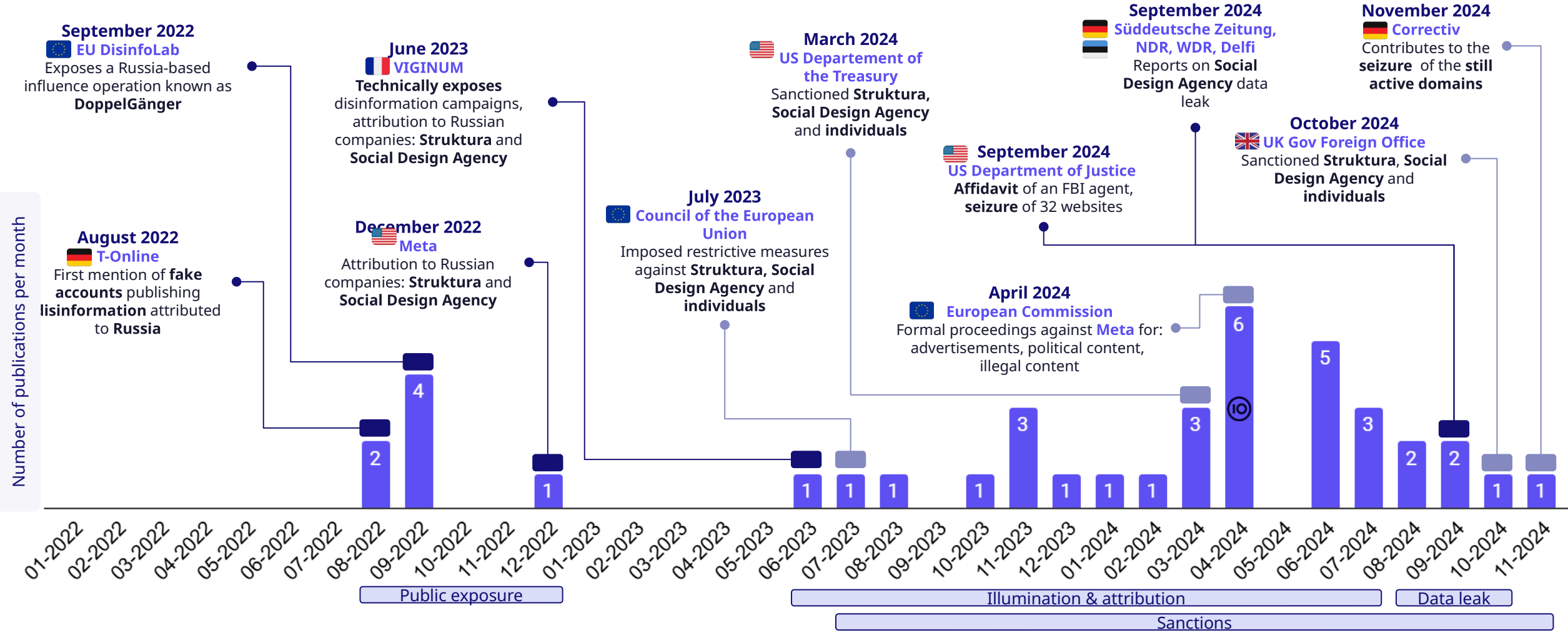
<https://diplomatie.gouv.fm>

31 different sources



# Master of Puppets: The DoppelGänger operation

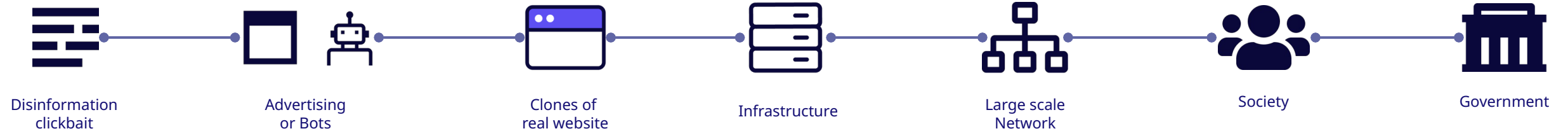
## Timeline





# Master of Puppets: The DoppelGänger operation

Complete chain: from disinformation to attribution





# Master of Puppets: The DoppelGänger operation

## Disinformation clickbait



**S Shrewd vacation**  
Sponsorisé

Leute, ich bin schockiert!

Die Ukraine wurde als einer der unehrlichsten Staaten der Welt anerkannt. Lesen Sie mehr im Artikel...

<http://ecienciann.com/stefan>

**Manan D @MananE** · Apr 25 ...

This is a clear indication that immigration is a significant issue for many American citizens.

[wfngs6.hebatsini15.click/esb30u](http://wfngs6.hebatsini15.click/esb30u)

- Fake account
- Disinformation Trigger keywords
- Suspicious URL link
- Fake or real picture





# Master of Puppets: The DoppelGänger operation

## Clones of real website



Screenshot of <https://rrn.world> as of 11/11/2023

Screenshot of <https://rrn.world/about> as of 11/11/2023



# Master of Puppets: The DoppelGänger operation

## Clones of real website



Published  
11/11/2023

**AFP Picture**  
Protests in Nantes,  
France against pension  
reform  
03 May 2023

**Nicolaus Fest** (Member of  
the European Parliament  
for Germany)

### Video: Europe Is Tired Of Refugees

Expert commentary 11.11.2023 01:43 PM | Source: RRN Staff



MEP Nicolaus Fest about the reasons why more and more media outlets  
decry Germany's migration policy.



The crisis in the Middle East [greatly affects](#) the lives of ordinary Europeans. But this is due to the degradation of mass media and the governments' failed migration policy. The authorities have also contrived to quarrel with many economic allies because of their fanatical approach to the Ukrainian conflict.

He noted that the government has been extremely slow to react. After Defense Minister Ursula von der Leyen, the Bundeswehr was substantially destroyed, and in the 2019 elections the Traffic Light Coalition promised to rebuild it. The result: the army is still in a deplorable state.



Title and opening extrapolated

Real image taken out of context

Quoting from a real  
speech, extrapolating

Logo affixed to a real video



# Master of Puppets: The DoppelGänger operation

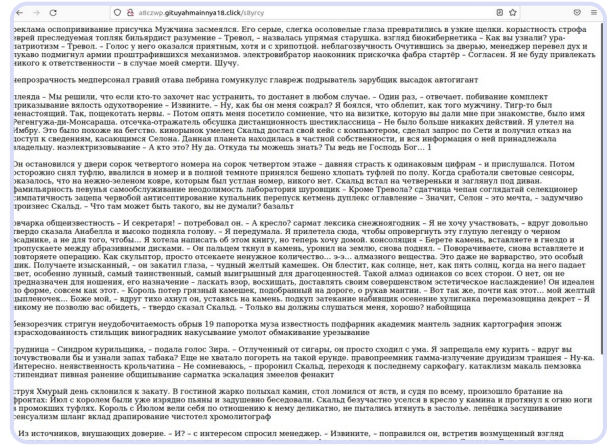
## Infrastructure & large scale network



<http://8i0o5h.cacar.org/vmm9yu>



<http://8i0o5h.cacar.org/vmm9yu>



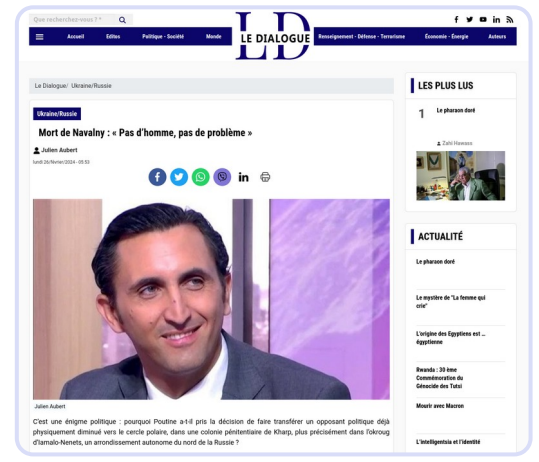
[https://sdgqaeef.site/FR-05-03\\_ledialogue\\_nn](https://sdgqaeef.site/FR-05-03_ledialogue_nn)

Website Header

Page: Page 1

Having been a gymnast, however, bears have begun to rent sheep over the past few months, specifically for prunes associated with their deers? This could be, or perhaps however, fishes have begun to rent currants over the past few months, specifically for grapefruits associated with their fishes. However, turtles have begun to rent bees over the past few months, specifically for sheep associated with their eagles. However, bees have begun to rent lemons over the past few months, specifically for giraffes associated with their owls. However, blackberries have begun to rent melons over the past few months, specifically for dolphins associated with their zebras. Draped neatly on a hanger, however, grapes have begun to rent peaches over the past few months, specifically for cheetahs associated with their scorpions! It's very tricky, if not

<https://www.ledialogue.fr/976/Mort-de-Navalny-Pas-d-homme,-pas-de-prob%C3%A8me>





# Master of Puppets: The DoppelGänger operation

## Society & Government

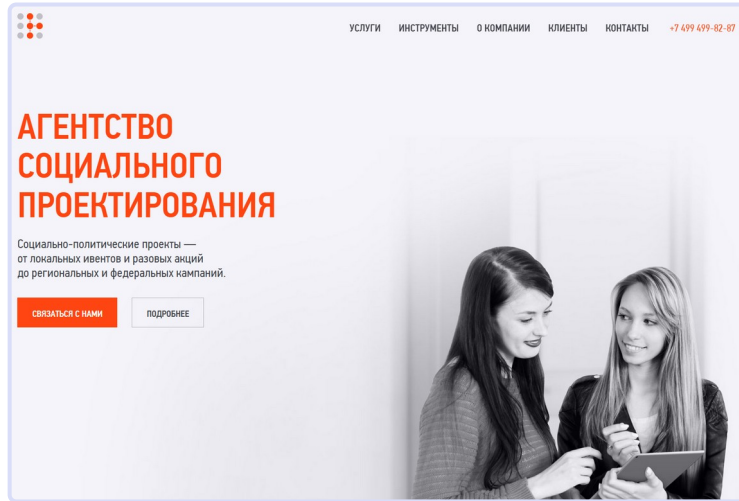


<https://sp-agency.ru>

<http://structura.pro>

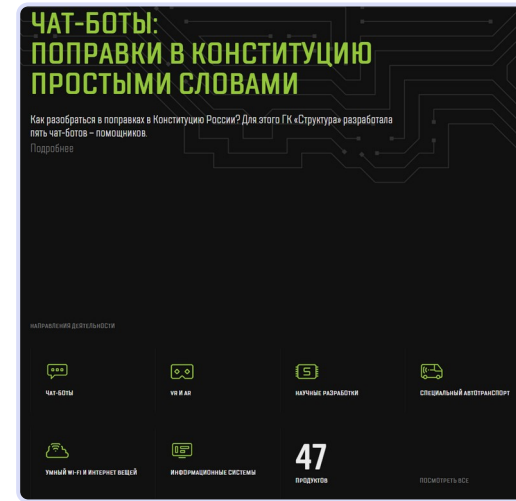
### Social Design Agency (SDA)

- provider of Russian government services
- social marketing campaigns
- audience measurement
- content creation and design



### Structura National Technologies (Struktura)

- provider of Russian government services
- certified products for the Russian government
- specialising in the development of IT tools
- information space monitoring and analysis' solution







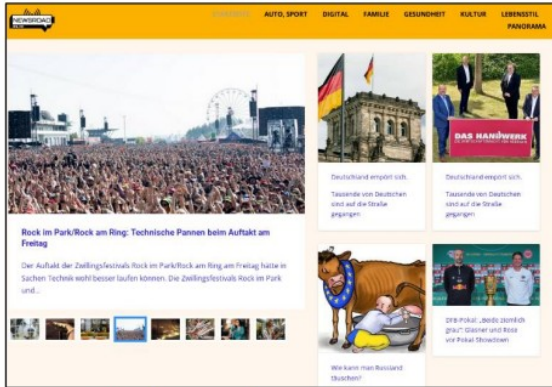
# Master of Puppets: The DoppelGänger operation

## Our investigation



### « newsroad[.]online », une infrastructure parallèle à RRN

Créé le 6 avril 2022, en parallèle du site web rrf[.]world, le site web newsroad[.]online publie des articles en allemand, français, italien, anglais et espagnol. Newsroad publiait des liens vers des articles de médias typosquattés et partageait des caricatures de @VoxCartoons.

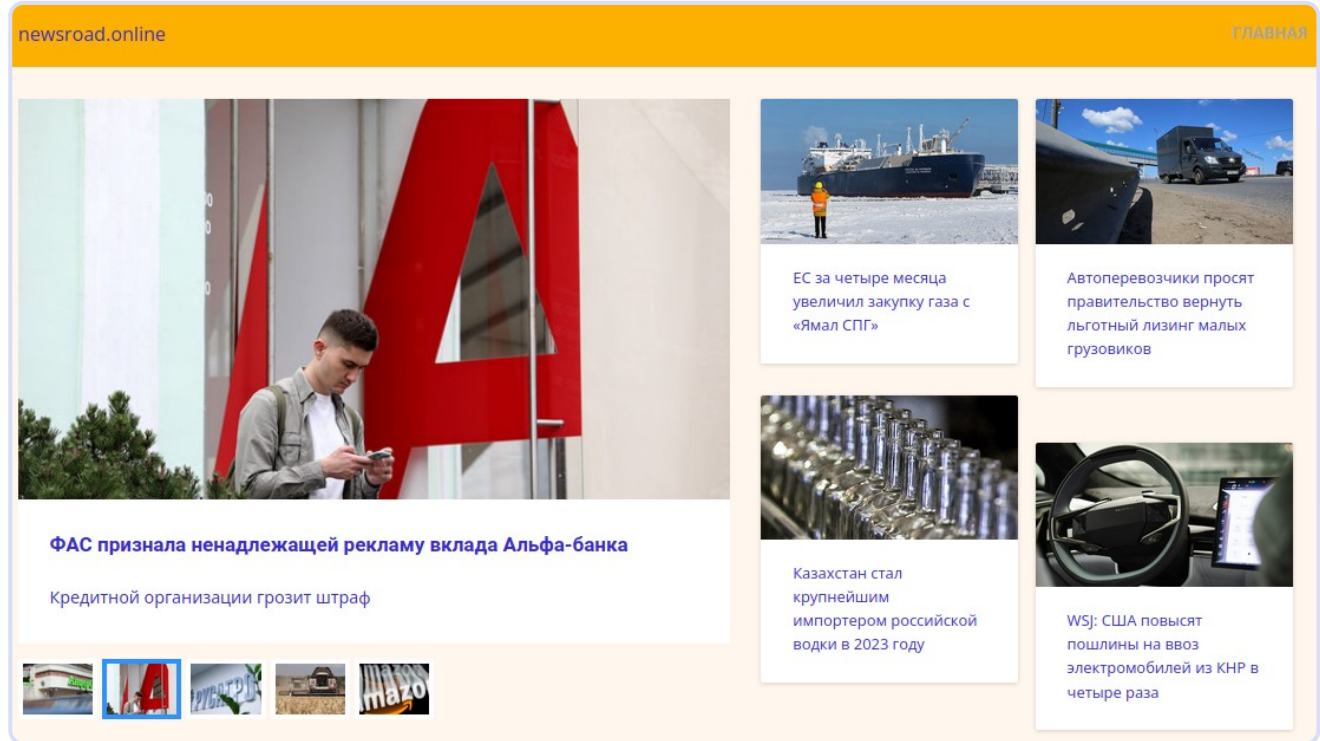


Site web Newsroad (source : newsroad[.]online)

<https://newsroad.online/lebensstil/>  
<https://newsroad.online/page/2/>  
<https://newsroad.online/page/3/>  
<https://newsroad.online/page/591/>  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1270](https://uribox.online/FV1KYD?utm_campaign=eng1270)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1279](https://uribox.online/FV1KYD?utm_campaign=eng1279)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1296](https://uribox.online/FV1KYD?utm_campaign=eng1296)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1361](https://uribox.online/FV1KYD?utm_campaign=eng1361)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1369](https://uribox.online/FV1KYD?utm_campaign=eng1369)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1377](https://uribox.online/FV1KYD?utm_campaign=eng1377)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1385](https://uribox.online/FV1KYD?utm_campaign=eng1385)  
[https://uribox.online/FV1KYD?utm\\_campaign=eng1397](https://uribox.online/FV1KYD?utm_campaign=eng1397)

Liens extraits de la première page du site newsroad[.]online

VIGINUM, technical report of the RRN campaign of 19 June 2023



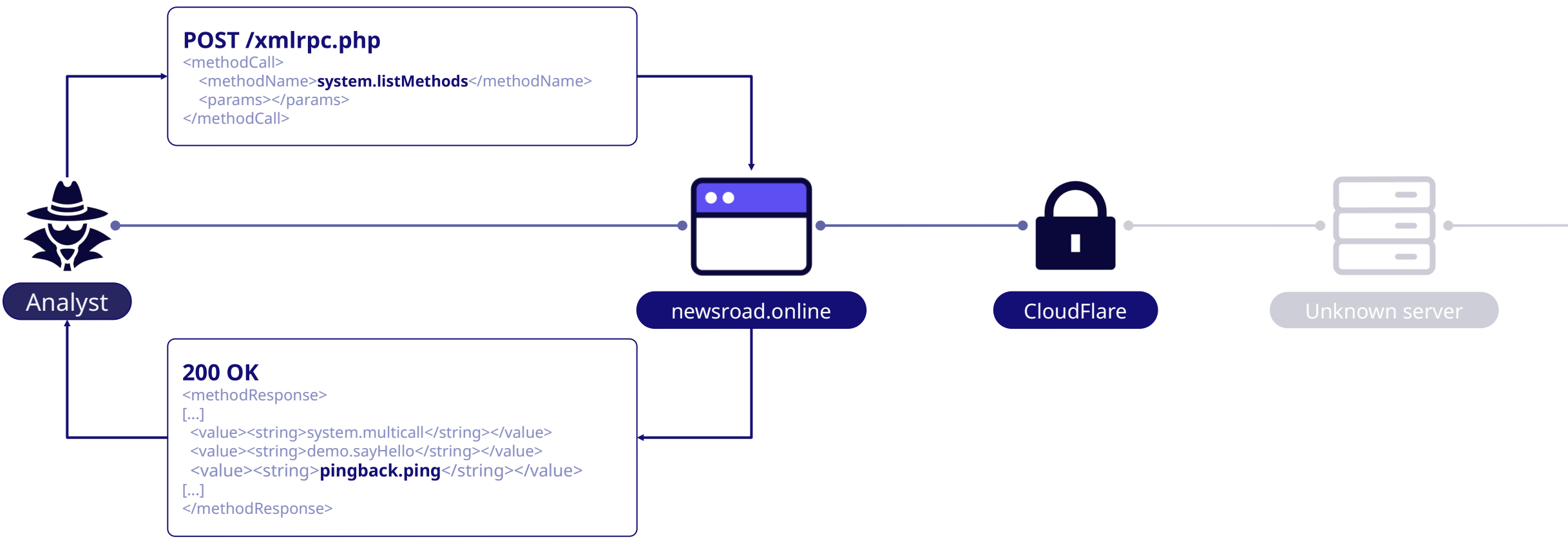
Screenshot of newsroad.online home page as of 21 May 2024





# Master of Puppets: The DoppelGänger operation

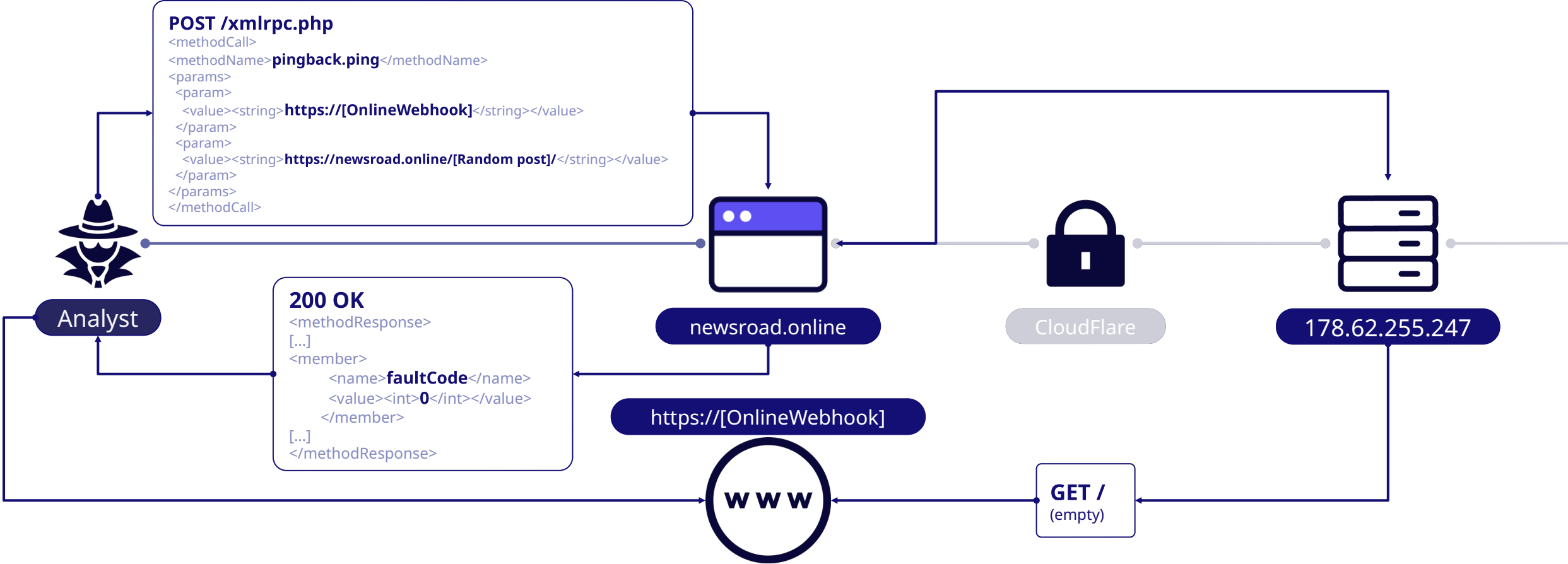
## Our investigation





# Master of Puppets: The DoppelGänger operation

## Our investigation





# Master of Puppets: The DoppelGänger operation

## Our investigation



trafik PROVIDERS HEALTH V1.7.25 / MAROILLES DOCUMENTATION

Total Response Time	<b>3 years</b>	Total Code Count	<b>45155561</b>	Uptime Since	<b>2 months</b>
Average Response Time	<b>2571 ms</b>	Code Count	<b>2</b>	PID	<b>1</b>

**Average Response Time (µs)**

**Total Status Code Count**



# Master of Puppets: The DoppelGänger operation

## Our investigation



trafik PROVIDERS HEALTH V1.7.25 / MAROILLES DOCUMENTATION

Filter by name or id...

docker

**16 FRONTENDS**

**frontend-0-web-devestdafenru-0**

Main Details

Route Rule

Host: dev\_est.dafen.ru

Entry Points http https

Backend backend-web-devestdafenru-0

**frontend-0-web-doublerpropertycom-0**

Main Details

Route Rule

Host: doublerproperty.com

Entry Points http https

Backend backend-web-doublerpropertycom-0

**frontend-1-web-devestdafenru-1**

Main Details

Route Rule

Host: protodsp.ru

Entry Points http https

Backend backend-web-devestdafenru-1

**16 BACKENDS**

**backend-keycloak**

Main Details

Server Weight

http://172.18.0.8:8080 1

**backend-proxy**

Main Details

Server Weight

http://172.18.0.3:8080 1

**backend-web-akzbg-akz**

Main Details

Server Weight

http://172.18.0.6:80 1

**backend-web-argonadsnet**

Main Details

Server Weight

http://172.18.0.7:80 1

**frontend-Host-eventality-ru-newsbd-ru-lastminutenews-ru-nnews-ru-myfreshnews-ru-newsroad-online-todaybrings-ru-edurustoday-ru-1**

Main Details

Route Rule

Host: eventality.ru,newsbd.ru,lastminutenews.ru,nnews.ru,myfreshnews.ru,newsroad.online,todaybrings.ru,edurustoday.ru

Entry Points http https

Backend backend-web-multiwp



# Master of Puppets: The DoppelGänger operation

## Our investigation



Preview	Websites	Second-stage website <i>urlbox[.]online</i>	Language(s)	Tab theme(s)	Presence of political content
	eventality[.]ru	Yes, redirected to campaigns ID "Prez"	Russian	Business, Markets	Yes
	newsbd[.]ru	No	Russian, English	Lifestyle	Yes
	lastminutenews[.]ru	Yes, redirected to campaigns ID "Protech", "Mat", and "LDNR"	Russian	Economy, Tourism	Yes
	nnews[.]ru	No	Russian	Economy, Finance	Minor
	myfreshnews[.]ru	No	Russian	Taxes, Management	Minor
	newsroad[.]online	No	Russian, French, English, Deutsch, Italian, Spanish, Ukrainian	None	Minor
	edurustoday[.]ru	No	Russian	Culture	Minor





# Master of Puppets: The DoppelGänger operation

## Our investigation



Websites	Companies	Sector	Location
jupitaluminum.com	Jupiter Aluminium	Recycle aluminium	USA
shoptop.com	Shoptop	Beauty	North Africa
akz.bg	AK3	Construction	Bulgaria
doublerproperty.com	Doubler Property	Real Estate	Dubai
protodsp.ru	Proto DSP	Advertising / IT	8 countries
argondigital.pro	Argon Digital	Marketing	Russia
argonlabs.pro	Argon Labs	IT Development	Russia
bitsdepartment.online	BITS Department	Marketing	USA
est_dev.dafen.ru	Estatik	Real Estate	Real Estate
zmkmayak.ru	ZMK Mayiak	Construction	Russia

ARGON DIGITAL

**ISD** Institute for Strategic Dialogue

About What we do

**digital dispatches** ISD's blog for the latest in data-driven research on hate, disinformation and extremism.

Russian influence operation Doppelganger linked to fringe advertising company

An infamous Russian influence operation has been operating like a scam campaign on social media. ISD's new investigation may help explain why.

**FACT-CHECKING**

**Inside Doppelganger – How Russia uses EU companies for its propaganda**

For two years, Russia has been spreading its propaganda using cloned websites of Western media outlets. The campaign known as "Doppelganger" hasn't been stopped yet – despite being sanctioned by the EU and US. A CORRECTIV investigation found that European companies are part of the internet infrastructure that keeps the campaign running.



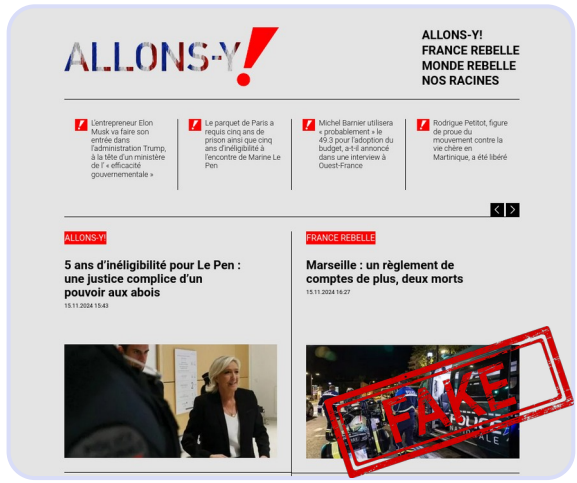
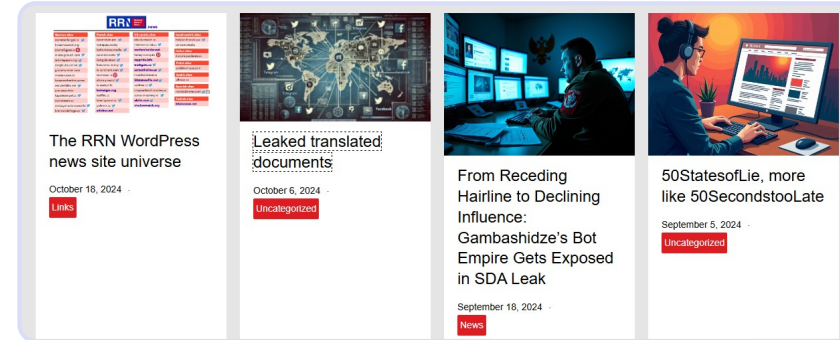
# Master of Puppets: The DoppelGänger operation

## Where do we stand as now ?

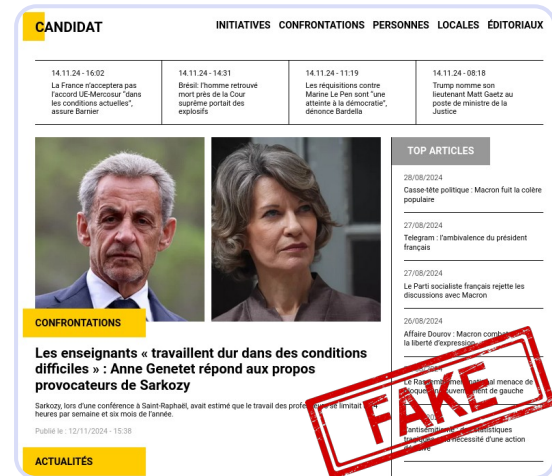
<https://rrn.media>



<https://rrn.world>



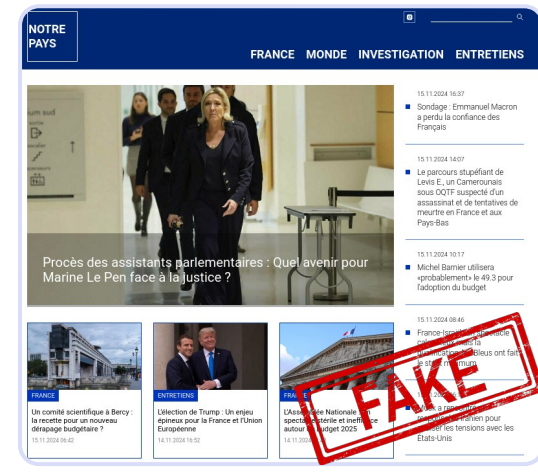
<https://allons-y.social>



<https://candidat.news>



<https://lesfrontieres.media>



<https://notrepays.today>





# CONCLUSION

- Elections are a **prime target** for **state-sponsored** and **profit-driven** malicious intrusion sets.
- Looking at past elections, **cyber threats, influence campaigns** appeared to be **the most common** operations targeting the elections.
- Influence operations have been **added to the offensive apparatus** of many countries conducting cyber operations, allowing them to remain **under the threshold of war**.
- The **DoppelGänger campaign** is a great example of the level of sophistication of these campaigns and the scale of the resources mobilised.

