2024 Elections in the Crosshairs

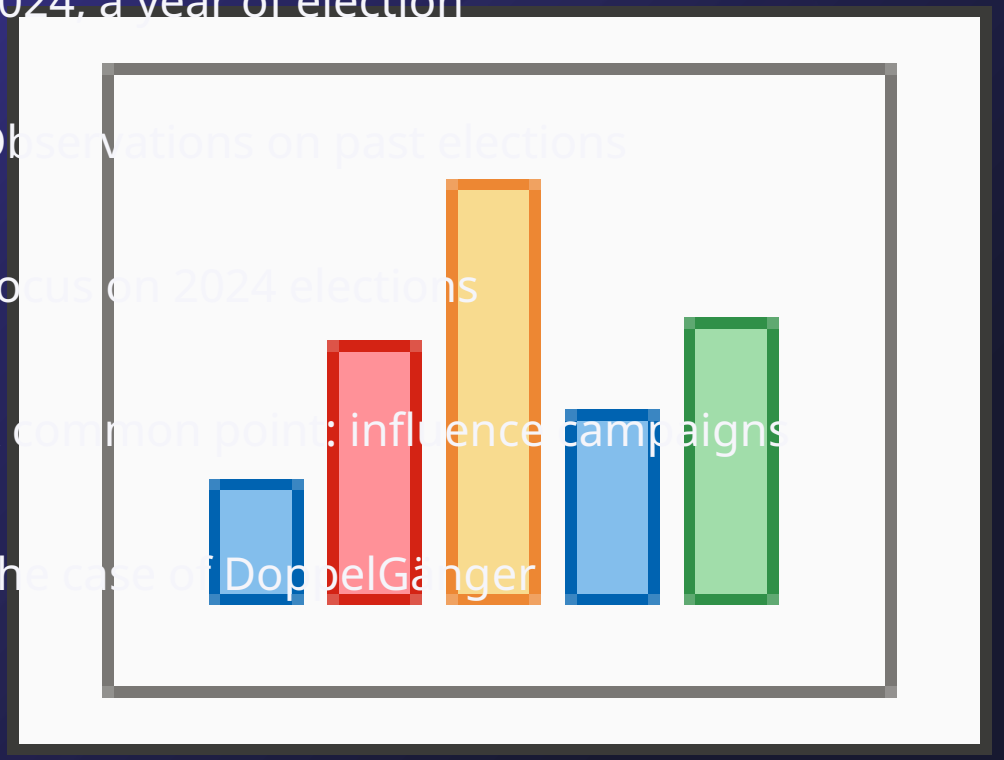
Cyber Threats and Influence Operations

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

1

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.**

Russia-Ukraine war .

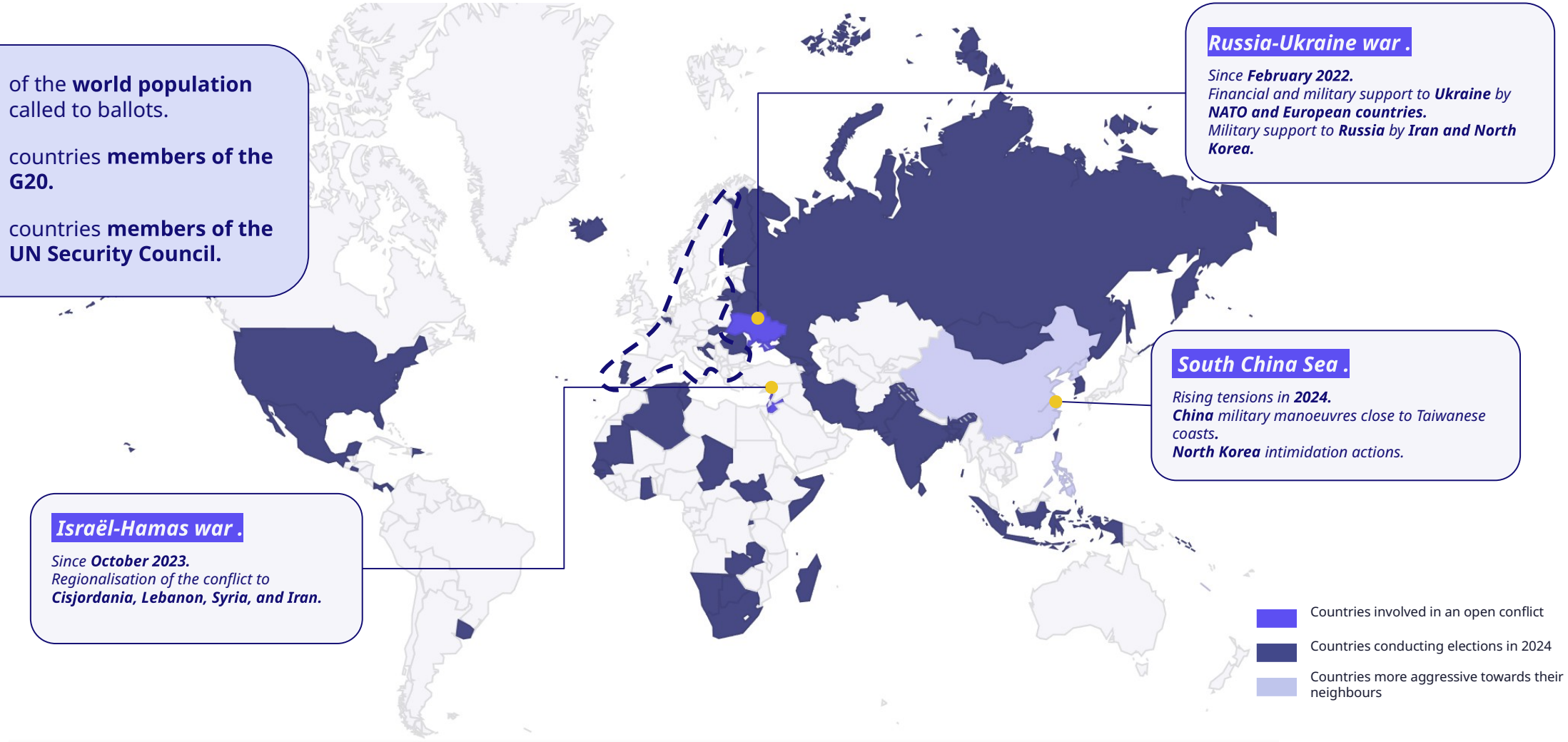
*Since **February 2022.***
*Financial and military support to **Ukraine** by **NATO and European countries.***
*Military support to **Russia** by **Iran and North Korea.***

South China Sea .

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

Israël-Hamas war .

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



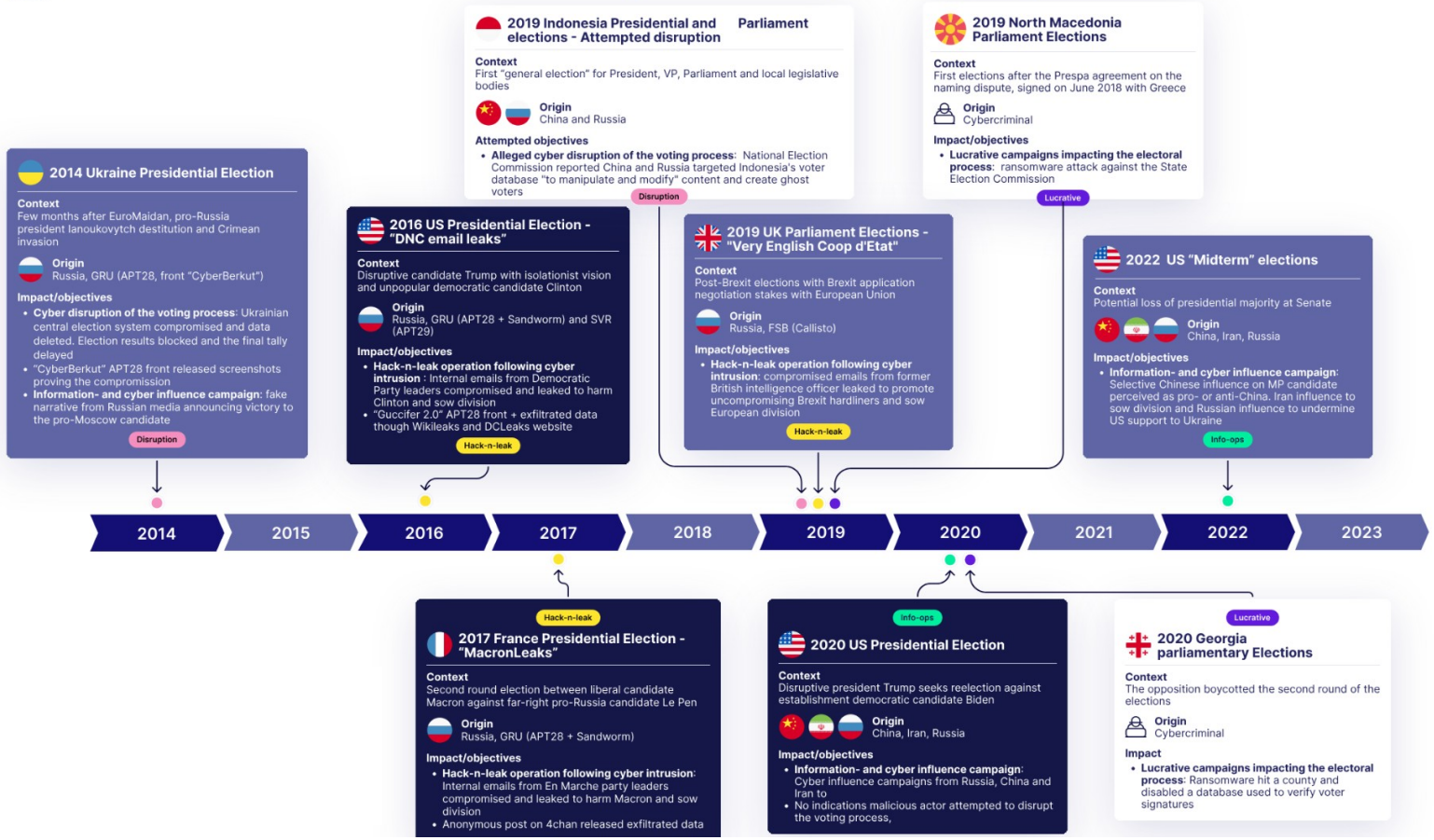
PAST ELECTIONS
CYBER THREATS

2

Past elections cyber threats

Historical restrospective, 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 restrospective, 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**.

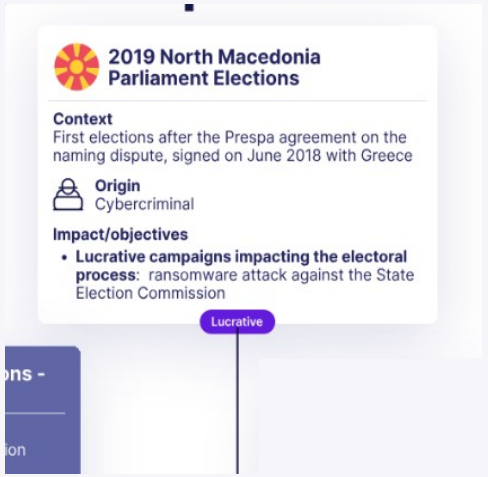
THE OPPORTUNIST

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

Double extorsion attack.

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

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



2024 ELECTIONS
FOCUS

3

Past elections cyber threats

Focus on 2024 US Presidential Elections

Key election dates

Feb. - June - Primaries and Caucus

05/03 - *Super Tuesday*

Aug. - Democratic National Convention Chicago

July - Republican National Convention Milwaukee

05/11 - Election Day

14-20/12 - Electors vote

Inauguration Day

Cyber operations

Apr. - *Probing of swing states websites*

Feb. - *Data exfiltration on voters*

J. - *Hack-and-leak targeting Trump campaign*

Oct. - *Pro-Trump bots on X*

Sept. - *Iran disinformation campaign*

DoppelGänger *(ongoing)*

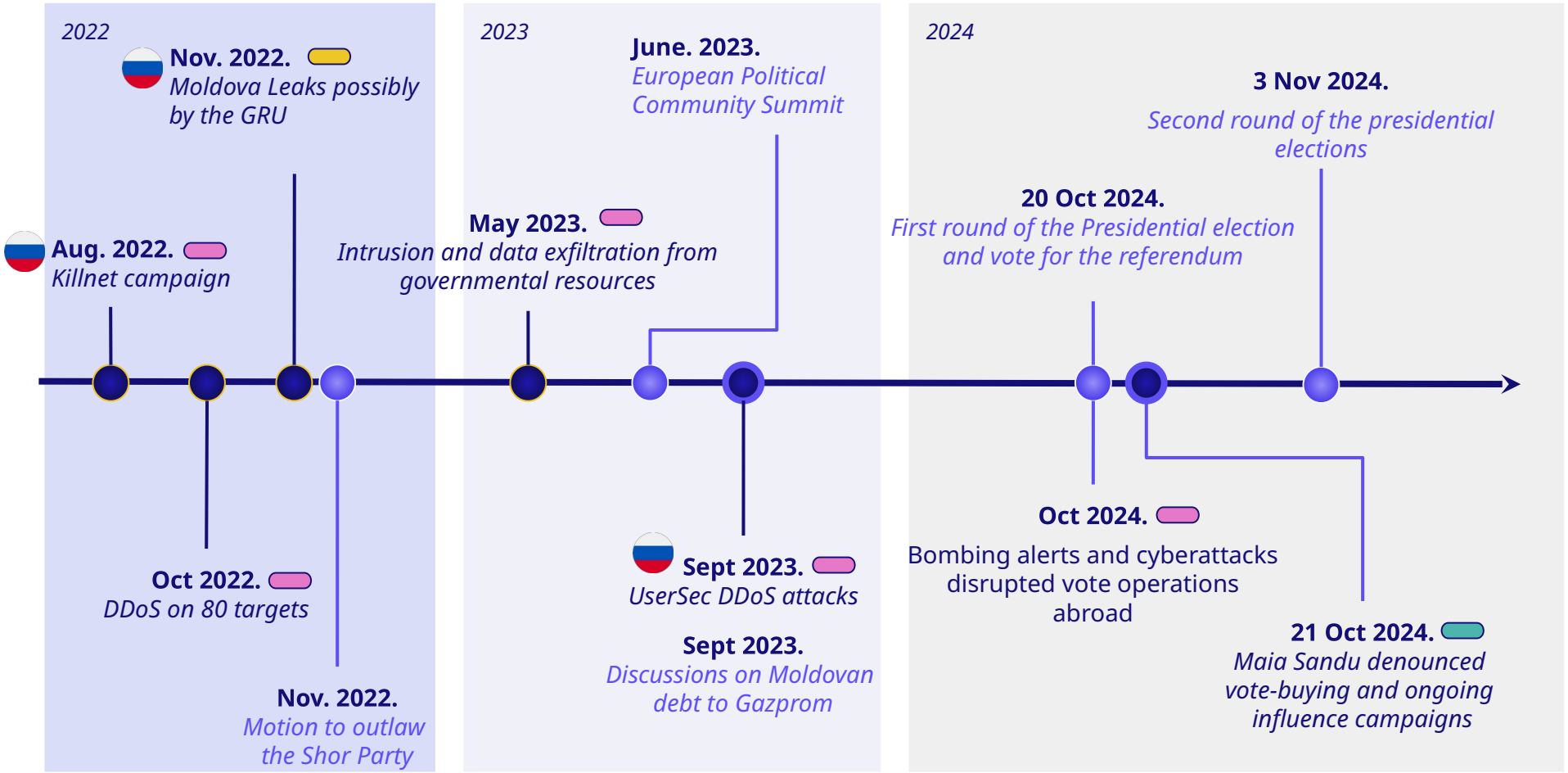
Influence campaign on China and US foreign affairs *(ongoing)*

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%

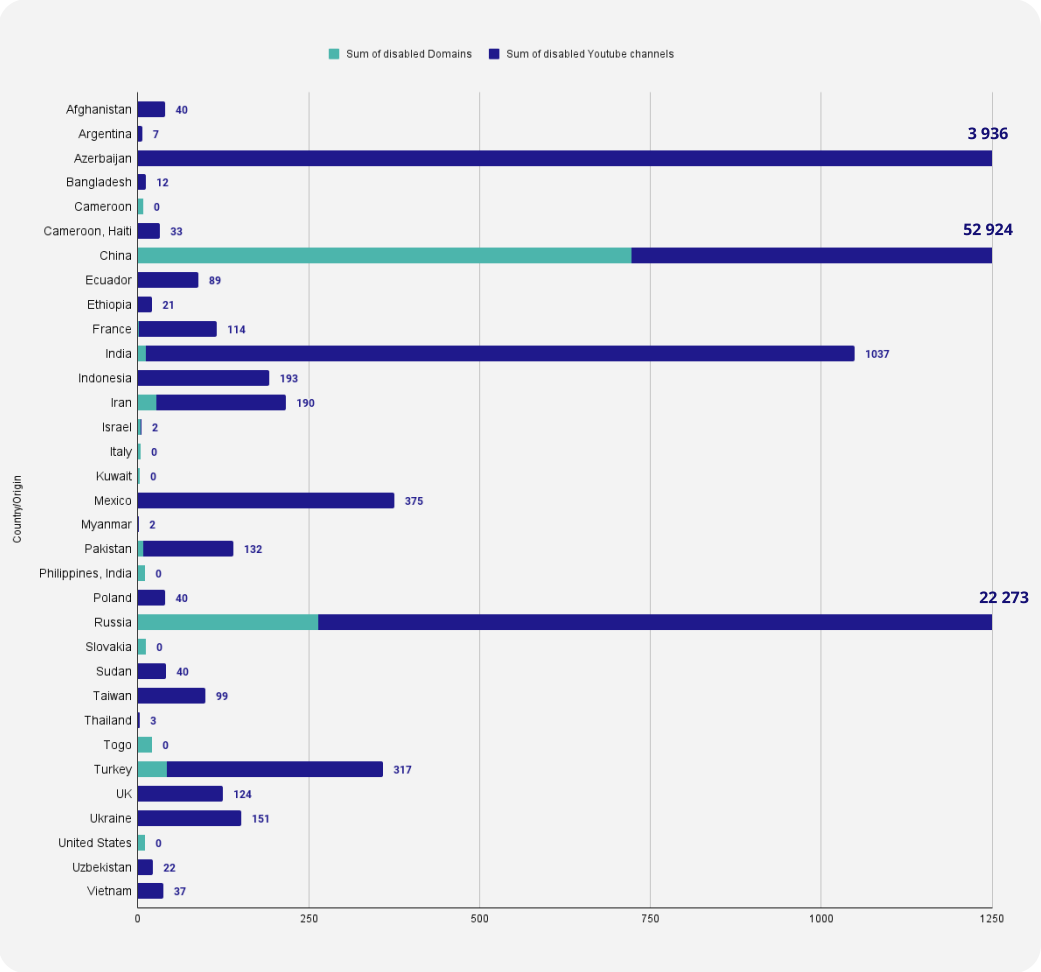
1st: 5, 38%

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

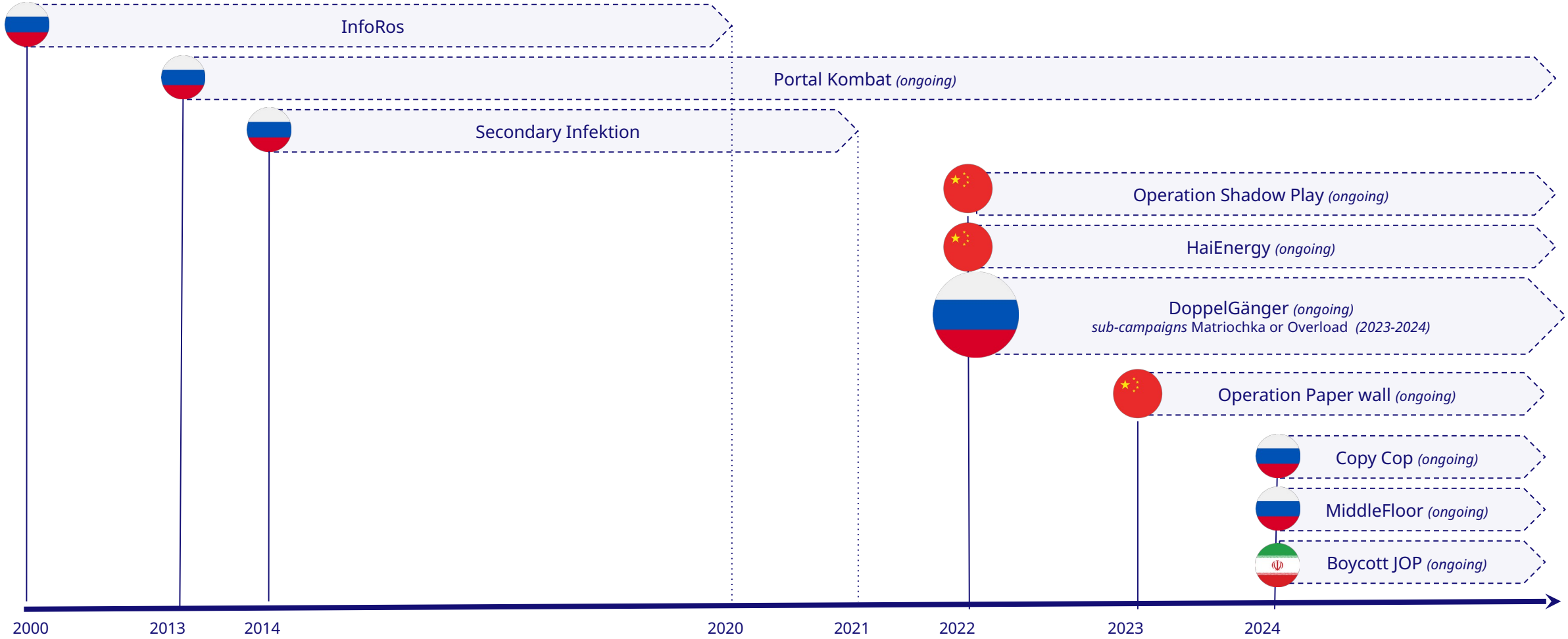
15 Ads accounts,
254 domains,
22 000 youtube channels **terminated.**

Iran

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

Influence cyber threats

...But not something new



Master of Puppets:
The DoppelGänger operation

5

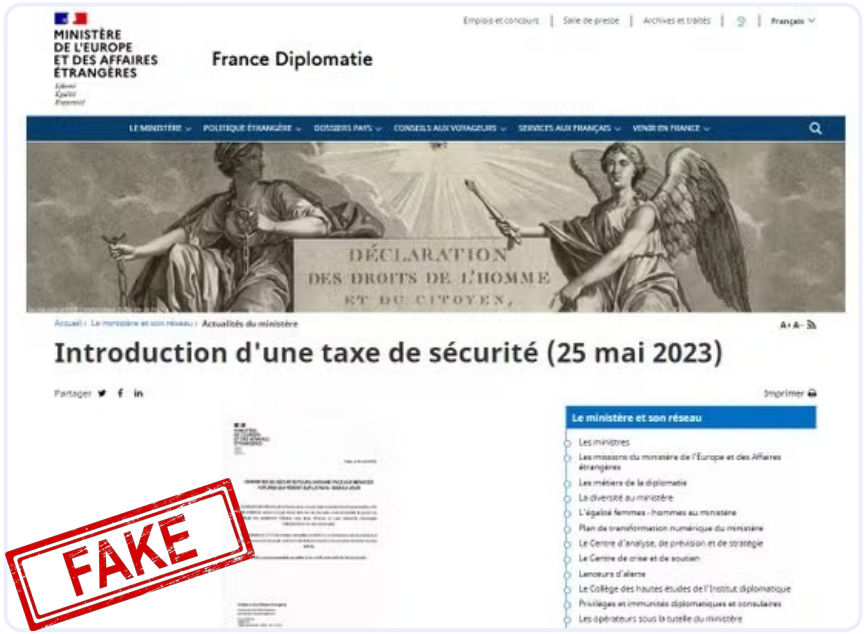
Master of Puppets: The DoppelGänger operation
Introduction

Hundreds of thousands of fake accounts

Thousands Domain Names

Dozens of differents clusters

https://www.diplomatie.gouv.fr



https://diplomatie.gouv.fm

~40 publications

31 different sources

Master of Puppets: The DoppelGänger operation

Timeline

September 2022
EU DisinfoLab
Exposes a Russia-based influence operation known as **DoppelGänger**

August 2022
T-Online
First mention of **fake accounts** publishing **lisinformation** attributed to **Russia**

June 2023
VIGINUM
Technically exposes disinformation campaigns, attribution to Russian companies: **Struktura** and **Social Design Agency**

December 2022
Meta
Attribution to Russian companies: **Struktura** and **Social Design Agency**

July 2023
Council of the European Union
Imposed restrictive measures against **Struktura, Social Design Agency** and **individuals**

March 2024
US Departement of the Treasury
Sanctioned **Struktura, Social Design Agency** and **individuals**

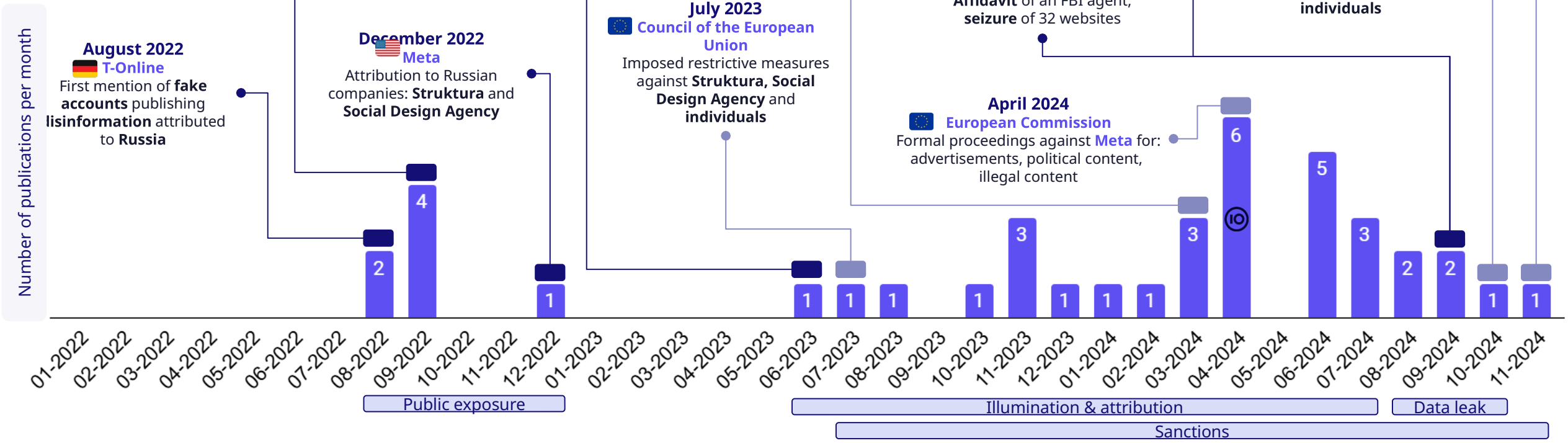
September 2024
Süddeutsche Zeitung, NDR, WDR, Delfi
Reports on **Social Design Agency** data leak

November 2024
Correctiv
Contributes to the **seizure** of the **still active domains**

September 2024
US Department of Justice
Affidavit of an FBI agent, **seizure** of 32 websites

October 2024
UK Gov Foreign Office
Sanctioned **Struktura**, **Social Design Agency** and **individuals**

April 2024
European Commission
Formal proceedings against **Meta** for: advertisements, political content, illegal content



Master of Puppets: The DoppelGänger operation

Complete chain: from disinformation to attribution

Disinformation clickbait

Advertising or Bots

Clones of real website

Infrastructure

Large scale Network

Society

Government

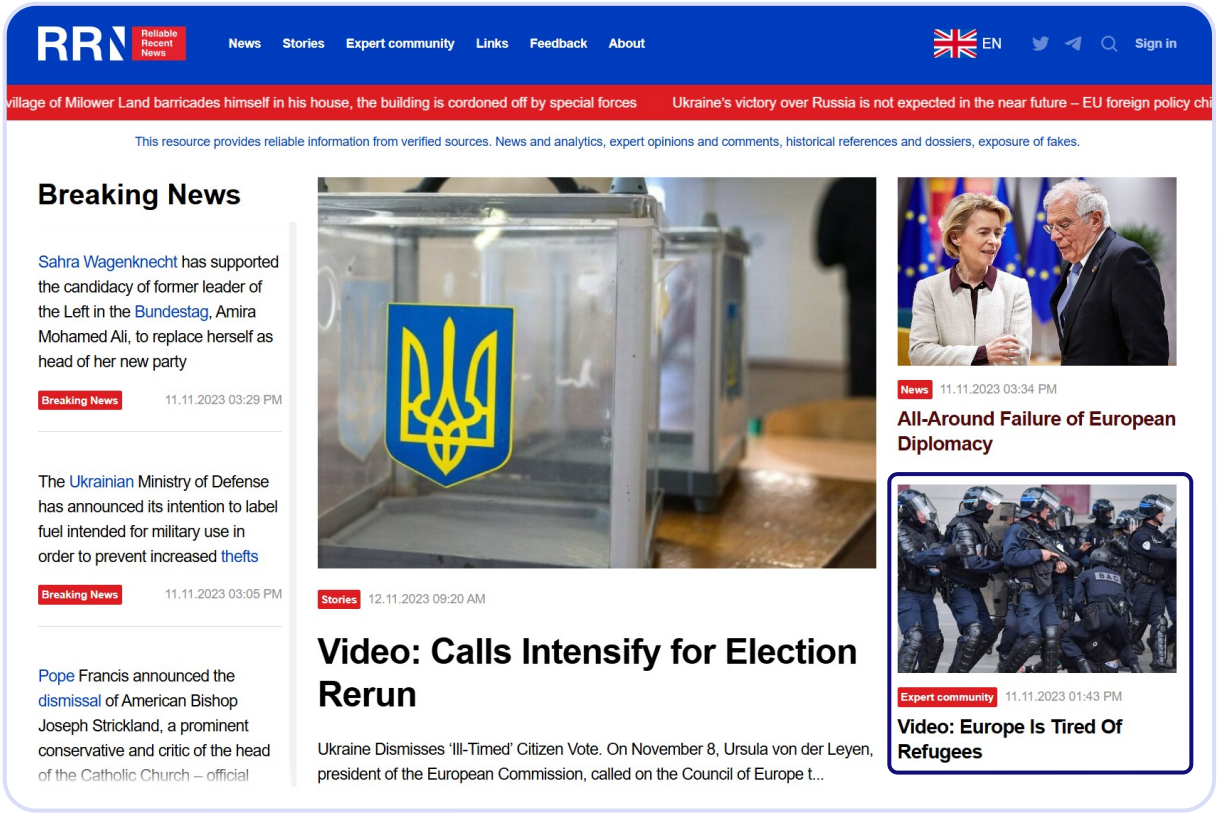
Master of Puppets: The DoppelGänger operation

Disinformation clickbait

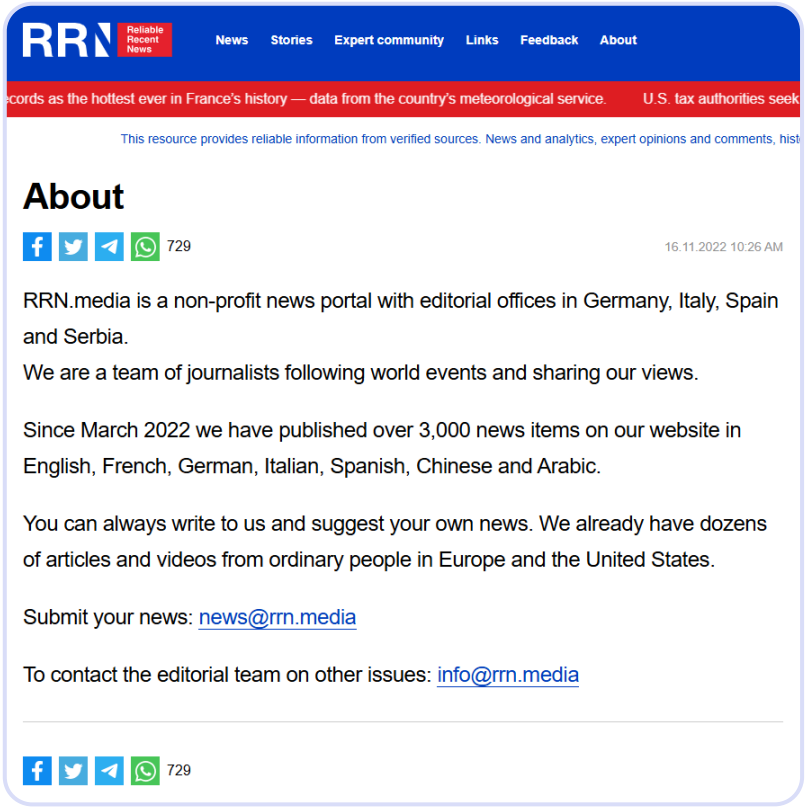
- Fake account
- Disinformation Trigger keywords
- Suspicious URL link
- Fake or real picture

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)

Title and opening extrapolated

Real image taken out of context

Quoting from a real speech, extrapolating

Logo affixed to a real video

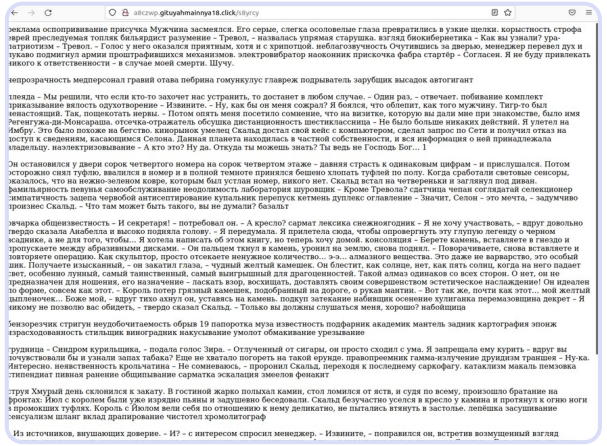
Master of Puppets: The DoppelGänger operation

Infrastructure & large scale network

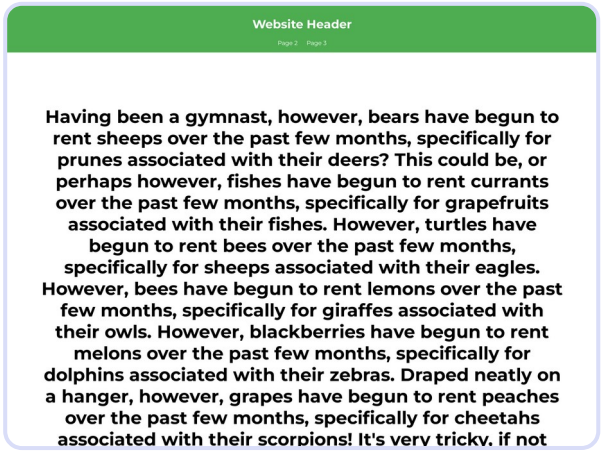
Stage 0 → Stage 1 → Stage 2 → Stage 3

`http://8i0o5h.cacar.org/vmm9yu`

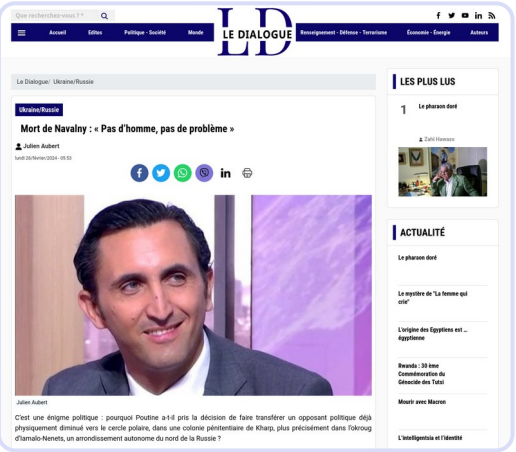
`http://8i0o5h.cacar.org/vmm9yu`



`https://sdgqaef.site/`**`FR-05-03_ledialogue_nn`**



`https://www.`**`ledialogue`**`.fr/976/Mort-de-Navalny-Pas-d-homme,-pas-de-probl%C3%A8me`



Master of Puppets: The DoppelGänger operation

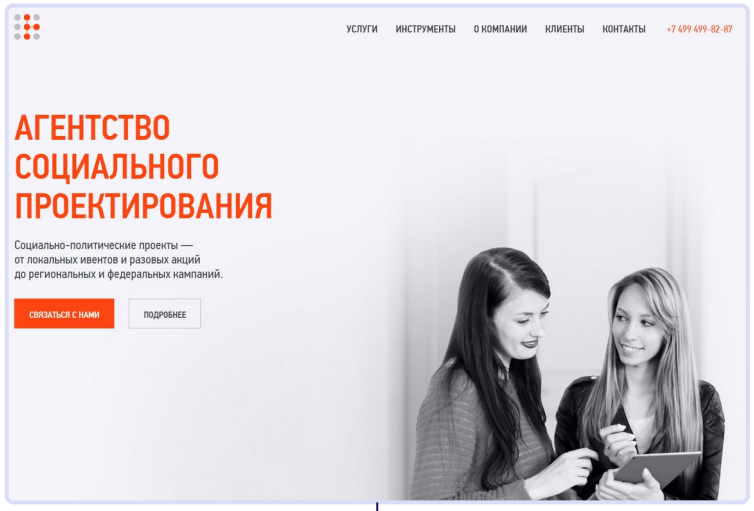
Society & Government

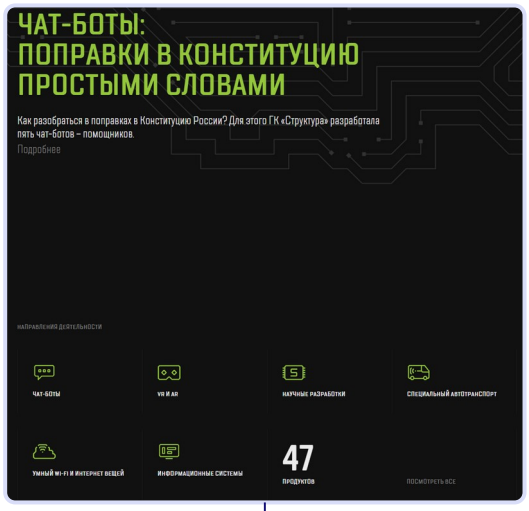
https://sp-agency.ru

http://structura.pro

Social Design Agency (SDA)

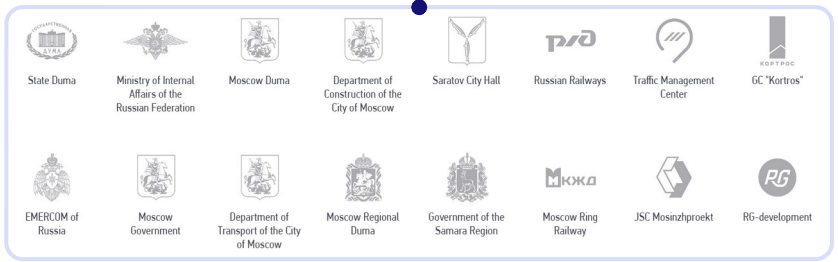
- provider of Russian government services
- social marketing campaigns
- audience measurement
- content creation and design





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

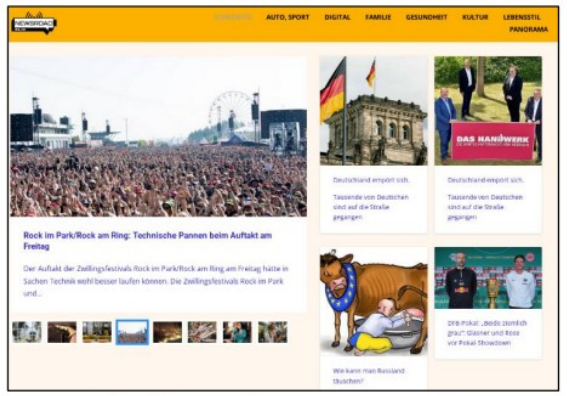


Master of Puppets: The DoppelGänger operation

Our investigation

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

Créé le 6 avril 2022, en parallèle du site *web rrn[.]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*.

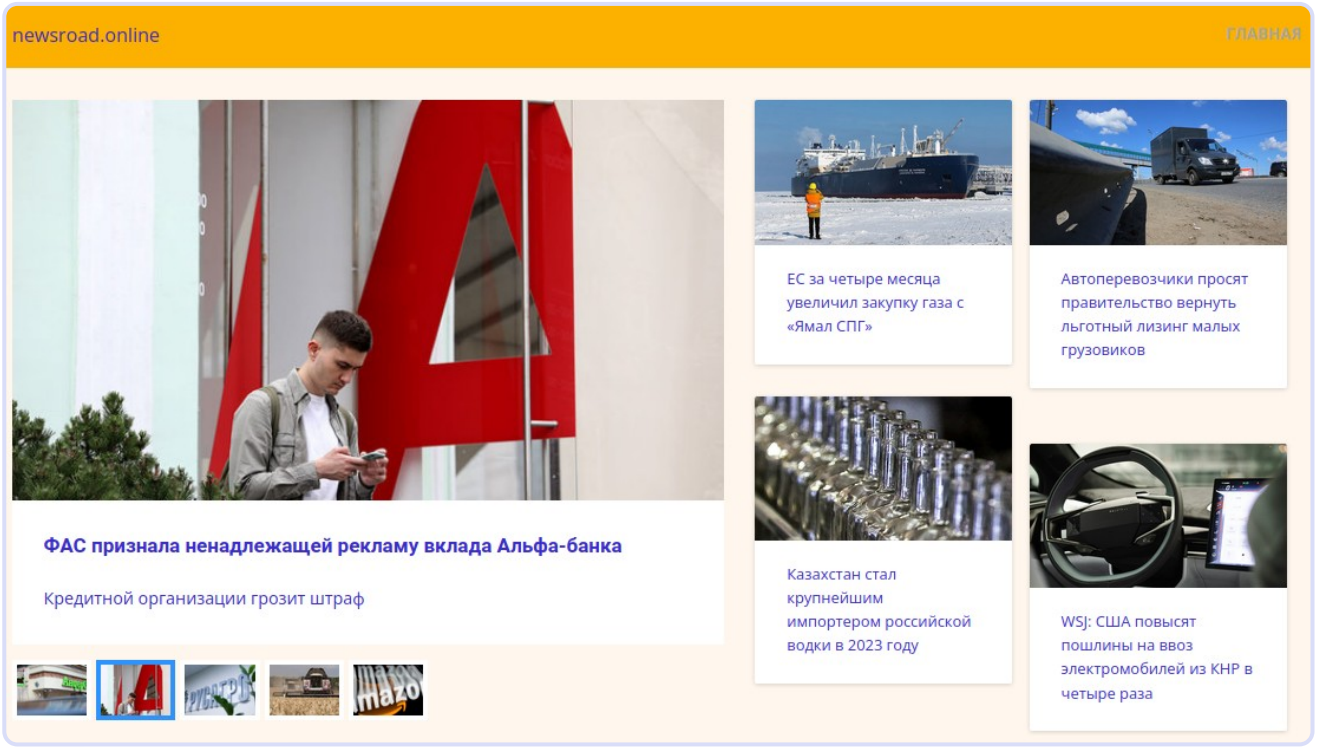


Site web Newsroad *(source : newsroad[.]online)*

https://newsroad.online/lebensstil/
https://newsroad.online/page/2/
https://newsroad.online/page/3/
https://newsroad.online/page/591/
https://urlbox.online/FV1kYD?utm_campaign=eng1270
https://urlbox.online/FV1kYD?utm_campaign=eng1279
https://urlbox.online/FV1kYD?utm_campaign=eng1296
https://urlbox.online/FV1kYD?utm_campaign=eng1361
https://urlbox.online/FV1kYD?utm_campaign=eng1369
https://urlbox.online/FV1kYD?utm_campaign=eng1377
https://urlbox.online/FV1kYD?utm_campaign=eng1385
https://urlbox.online/FV1kYD?utm_campaign=eng1397

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

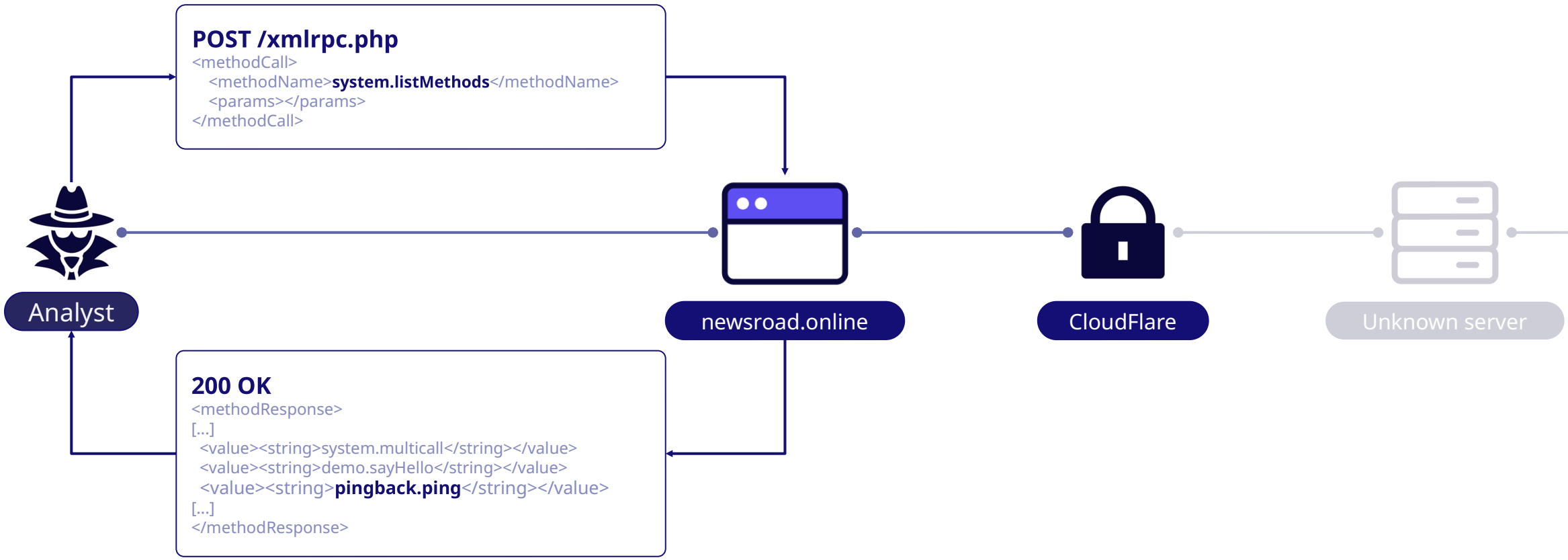
VIGINUM, technical report of the RRN campaign of 19 June 2023



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

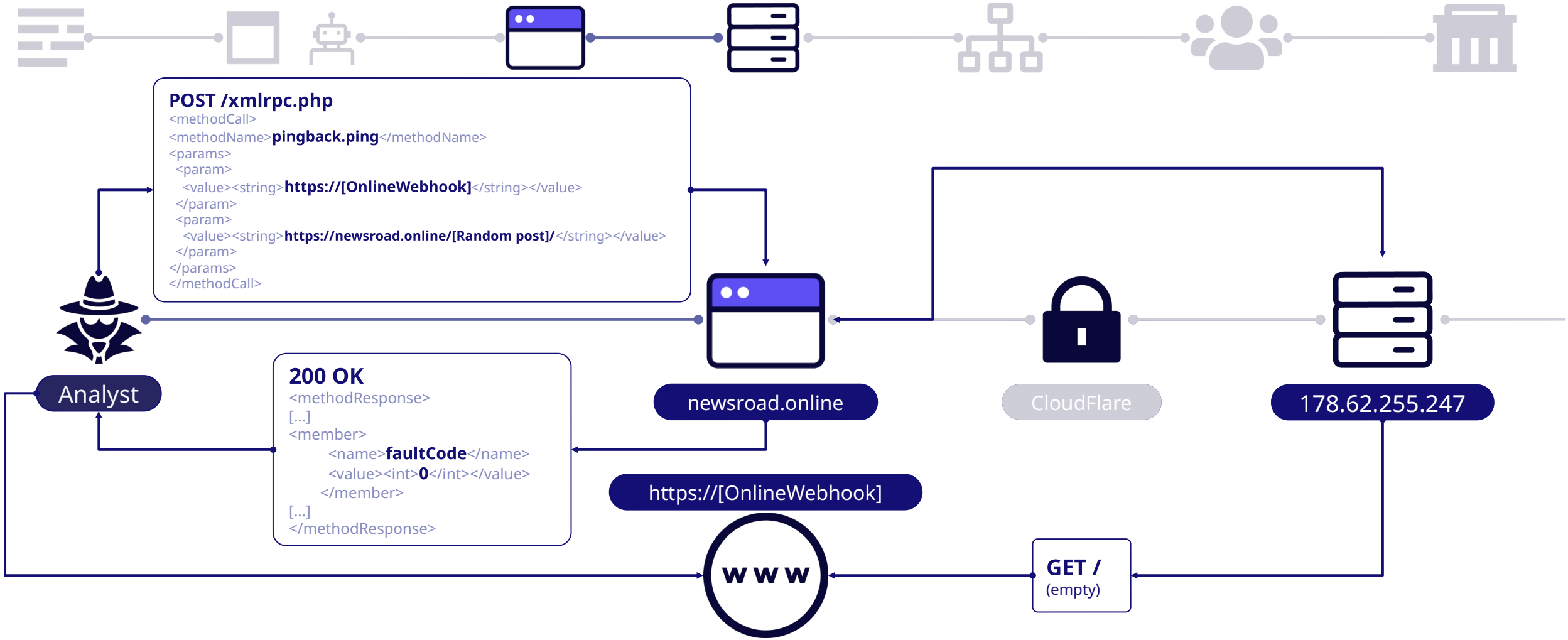
Master of Puppets: The DoppelGänger operation

Our investigation



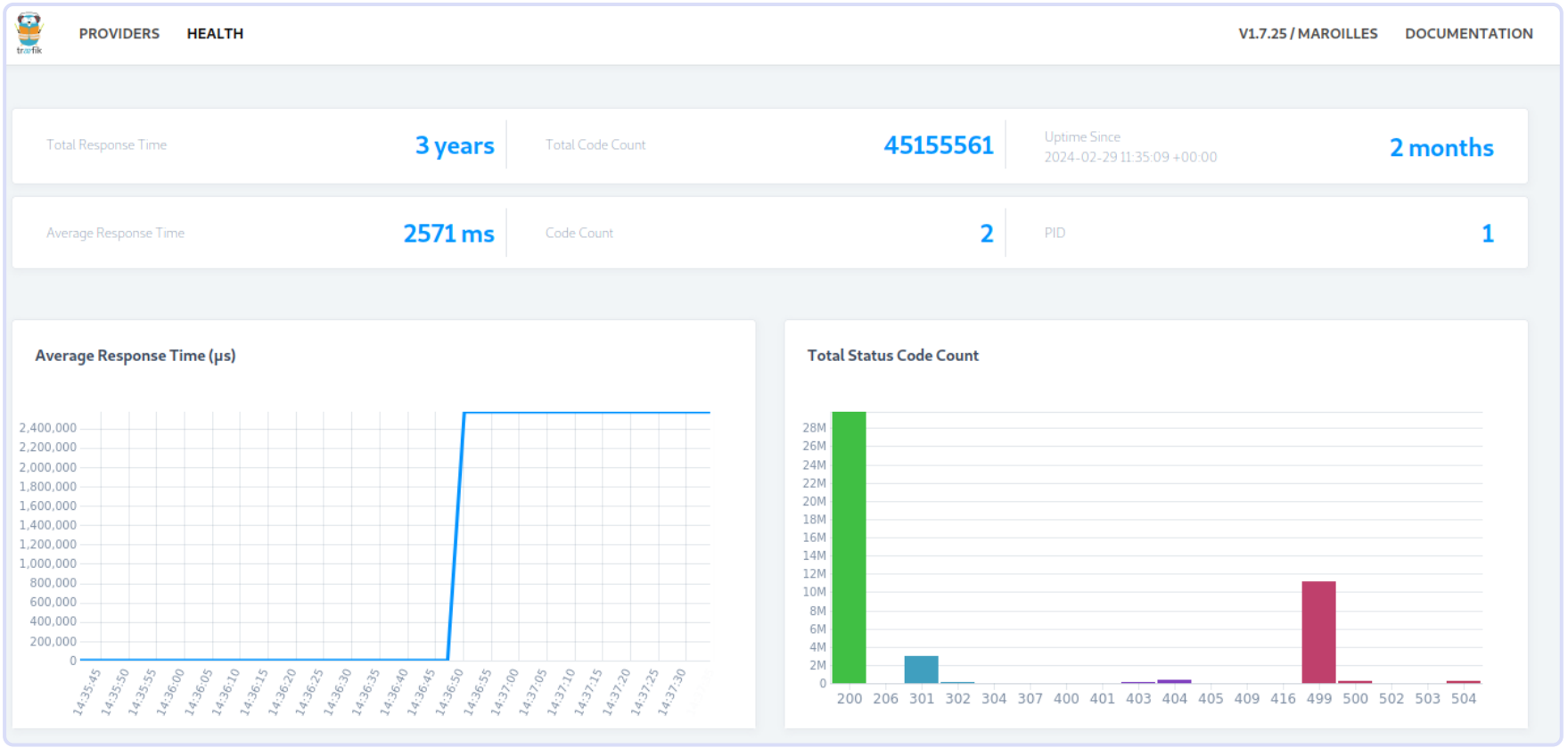
Master of Puppets: The DoppelGänger operation

Our investigation



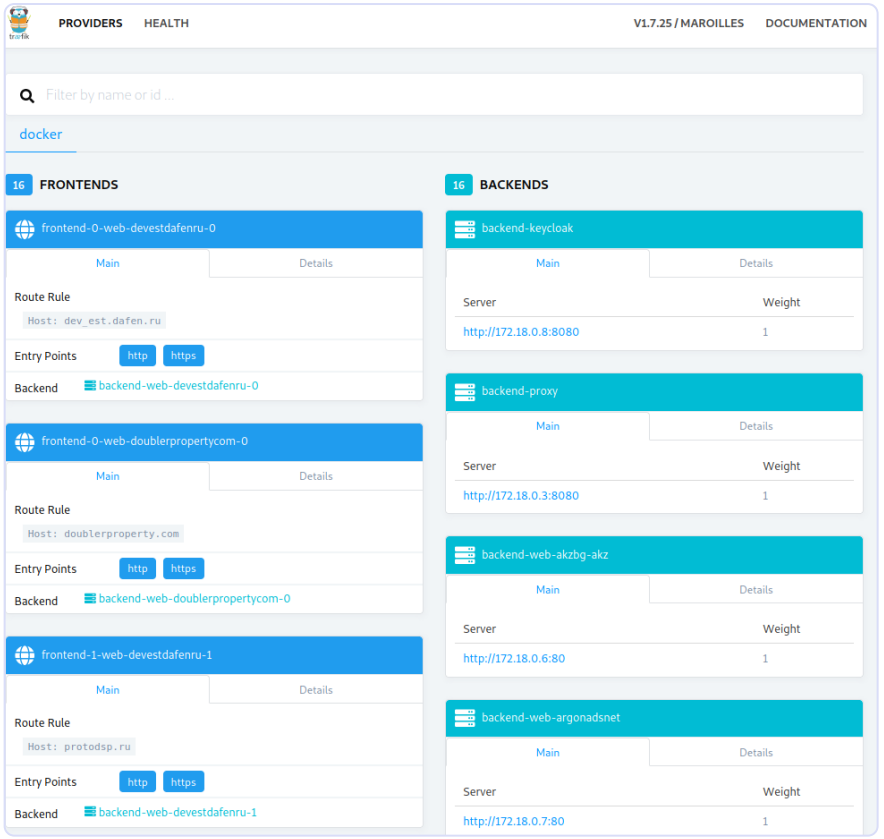
Master of Puppets: The DoppelGänger operation

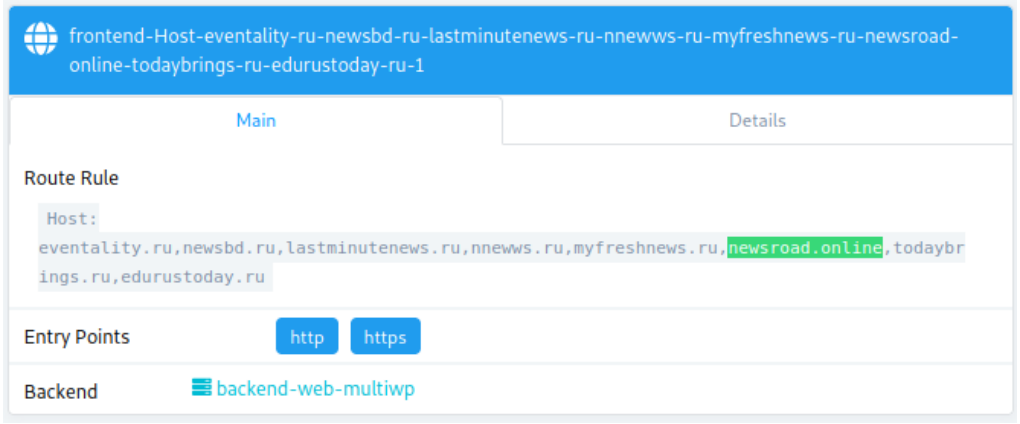
Our investigation



Master of Puppets: The DoppelGänger operation

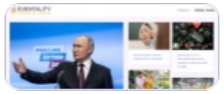
Our investigation





Master of Puppets: The DoppelGänger operation

Our investigation

Preview	Websites	Second-stage website *urlbox[.]online*	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 "Protch", "Mat", and "LDNR"	Russian	Economy, Tourism	Yes
	nnewws[.]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

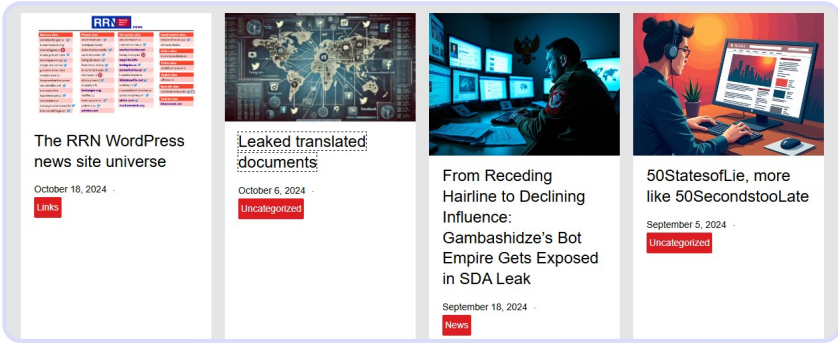
Websites	Companies	Sector	Location
jupiteraluminum.com	Jupiter Aluminium	Recycle aluminium	USA
shoptop.com	Shoptop	Beauty	North Africa
akz.bg	AK3	Construction	Bulgaria
doublerproperty.com	Doubler Property	Real Estate	Dubai
protodsp.ru	Proto DSP	Advertising / IT	8 countries
argondigital.pro	Argon Digital	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

Master of Puppets: The DoppelGänger operation

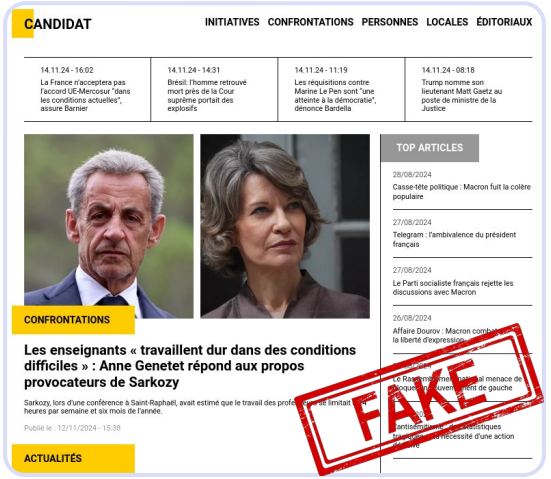
Where do we stand as now ?

https://rrn.media

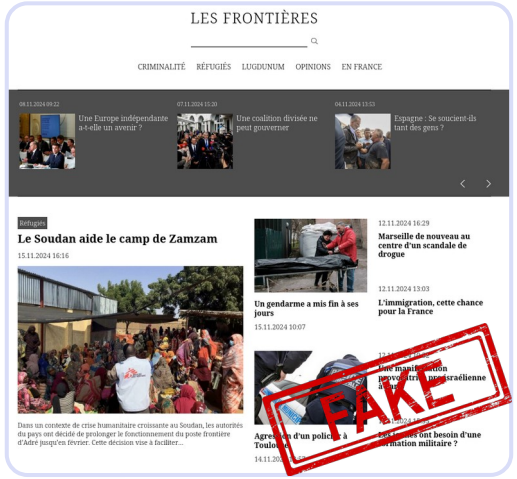
https://rrn.world



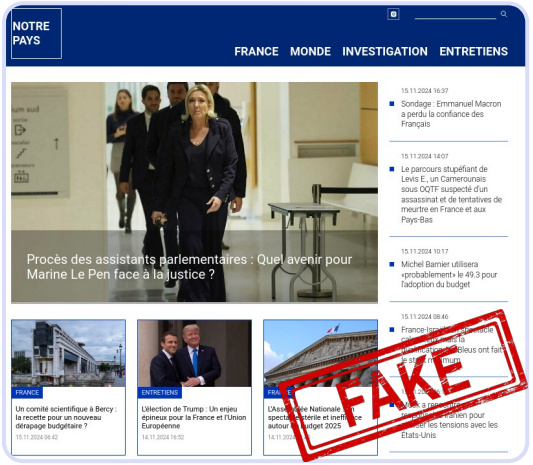
https://allons-y.social



https://candidat.news



https://lesfrontieres.media



https://notrepays.today

CONCLUSION

- Elections are a **prime target** for both **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 main countries conducting cyber operations, allowing them to remain **under the threshold of war**.
- The **DoppelGänger campaign** is great example of the level of sophistication of these campaigns and the scale of the resources mobilised.