SPECIAL REPORT

Nov 2024

COUNTERING CYBER-ENABLED HYBRID INTERFERENCE IN THE WESTERN BALKANS

A scenario-based approach

by

Naďa Kovalčíková
Senior Analyst, Transnational Security, EUISS

Andrea Salvi
Senior Analyst, Cyber and digital issues, EUISS

Bojana Zorić
Associate Analyst, Western Balkans, EUISS

euiss
European Union
Institute for
Security Studies

The EUISS is an agency
of the European Union

The views expressed in this publication are solely those of the author(s) and do not necessarily reflect the views of the European Union.

CATALOGUE NUMBER QN-01-24-003-EN-N
ISBN 978-92-9462-366-9
DOI 10.2815/7445710

Cover image: Sasha Pleshco/Unsplash

CONTENTS

This analytical report provides an overview of cyber-enabled hybrid interference in the Western Balkans, along with recommendations on how to improve approaches to effectively counter these threats. To this end, the European Union Institute for Security Studies (EUISS) designed and conducted a scenario-based exercise aimed at identifying key issues and potential responses to hybrid threats, with active participation from regional stakeholders. The fictional scenarios focused specifically on the interlinkage between foreign information manipulation and interference (FIMI) and harmful cyber operations, reflecting real-time challenges in the region.

THREATS IN THREADS

On 17 September, during his visit to North Macedonia, the Italian foreign minister Antonio Tajani warned that Western Balkan states could increasingly fall under the influence of Russia, China and other foreign actors unless the EU supports their progress towards becoming effective EU Member States[1]. While Kosovo[*] (87%) and Albania (82%) register strong public support for a firmly pro-EU and pro-West foreign policy course, citizens in Bosnia and Herzegovina (39%), Montenegro (36%), North Macedonia (31%) and Serbia (10%) are more divided, continuing to favour a balanced approach that maintains relations with both the West and Russia[2]. This climate of scepticism and polarisation in the region could further undermine the EU's efforts to counteract widespread disinformation narratives in the Western Balkans, including those targeting the EU and the West more broadly. This may not only create additional obstacles to effective EU integration, but also deepen dependencies on Russia and China, as well as other authoritarian states. Furthermore, malicious actors are not only attempting to 'hack minds' but also doubling down on their efforts to hack machines and the broader societal ecosystem[3].

To tackle these threats more effectively, countries in the region and the EU should implement measures targeting (a) the escalation and strategic timing of cyber-enabled attacks; and (b) the complexities of the regional media landscape.

Escalation and timing of cyber-enabled attacks

The Western Balkans experienced a sharp increase in cyber-enabled attacks between 2020 and 2024. Among the most notable incidents were the 2022 cyberattacks on Albania, which were attributed to Iranian state actors and garnered attention beyond the region[4]. These cyberattacks disrupted government services and prompted Albania to sever diplomatic ties with Iran in response to the aggression[5]. Montenegro also suffered a major cyberattack in August 2022, crippling government systems and leading to a state of emergency. The attack was linked to the Cuba ransomware group, suspected of having ties to Russia. The state prosecutor has not yet confirmed the direct perpetrators, amid ongoing tensions over Montenegro's NATO membership and its stance on Russia's invasion of Ukraine[6].

The strategic exploitation of timing, e.g. during elections and periods of heightened political and societal sensitivity, combined with the potential impact of cyber-enabled threats, can reinforce hybrid activities and raise the threshold for effectively deterring such dangers. For instance, following the 20 October presidential elections and EU referendum in Moldova, the European Commission noted that they took place 'under unprecedented interference and intimidation by

[*] This designation is without prejudice to positions on status and is in line with UNSCR 1244(1999) and the ICJ Opinion on the Kosovo declaration of independence.

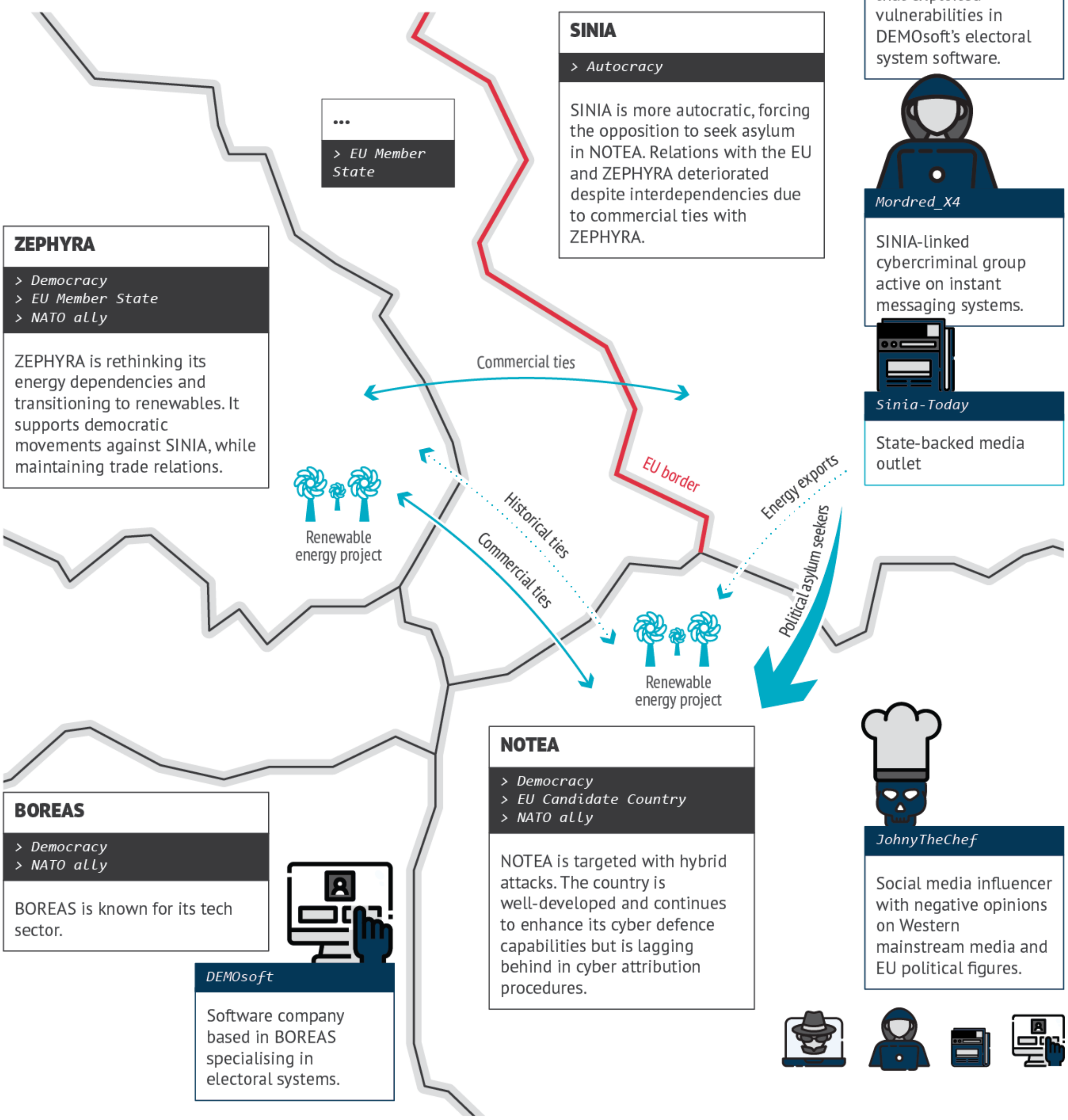
Russia and its proxies'. Moldovan security services reported that Russia spent $15 million on a voter-buying scheme targeting 130 000 Moldovans and an estimated $100 million to undermine the electoral process[7]. These recent developments also serve as a red flag to the Western Balkans, as Russia continues to invest

The siege of NOTEA

The story behind the exercise

Setting the scene

ZEPHYRA's Renewable Energy Group (REG) launched a project to modernise NOTEA's energy system. It faced criticism for displacing rural communities. When cyberattacks hit the REG's operations, they caused power outages and interruptions. Concerns about foreign investments in critical infrastructure (CI) emerged. The national TV station initially withheld coverage, so the public debated online. After an investigation uncovered a targeted cyber infiltration campaign demanding a ransom, the state-backed media outlet "Sinia Today" criticised NOTEA's reliance on ZEPHYRA for its CI.



Zargothrax101

SINIA-affiliated cybercriminal group that exploited vulnerabilities in DEMOsoft's electoral system software.

SINIA

> Autocracy

SINIA is more autocratic, forcing the opposition to seek asylum in NOTEA. Relations with the EU and ZEPHYRA deteriorated despite interdependencies due to commercial ties with ZEPHYRA.

...

> EU Member State

Mordred_X4

SINIA-linked cybercriminal group active on instant messaging systems.

ZEPHYRA

> Democracy
> EU Member State
> NATO ally

ZEPHYRA is rethinking its energy dependencies and transitioning to renewables. It supports democratic movements against SINIA, while maintaining trade relations.

Sinia-Today

State-backed media outlet

NOTEA

> Democracy
> EU Candidate Country
> NATO ally

NOTEA is targeted with hybrid attacks. The country is well-developed and continues to enhance its cyber defence capabilities but is lagging behind in cyber attribution procedures.

BOREAS

> Democracy
> NATO ally

BOREAS is known for its tech sector.

DEMOsoft

Software company based in BOREAS specialising in electoral systems.

JohnyTheChef

Social media influencer with negative opinions on Western mainstream media and EU political figures.

heavily in interference efforts in the broader EU neighbourhood, including within the Western Balkans.

A complex regional media landscape

Russia Today (RT) plans to launch a Serbian-language channel in Banja Luka, Bosnia and Herzegovina by the end of 2024, further expanding its presence within the region, where it already operates a central office in Belgrade. The EU has warned against closer ties with Russia, highlighting that such moves could facilitate increased information manipulation in the region. Moreover, such initiatives could potentially undermine EU restrictive measures towards Russia and Belarus, including sanctions imposed on RT and Sputnik which the EU considers 'weapons of deception' and a tool of Russian propaganda and disinformation, accompanying the Kremlin's illegal war of aggression against Ukraine[8]. In addition, while the Kremlin-sponsored news website Sputnik has been identified as one of the major conduits of Russian influence within the regional media landscape[9], it is local media that most effectively reach audiences across the region[10], often amplifying manipulated and anti-EU narratives from RT and Sputnik. Already a few years ago, a significant number of identified disinformation campaigns in the region were found to have domestic origins[11]. Furthermore, the 'Night Wolves" biker group, which is one of Moscow's proxies, frequently tours the Western Balkans and beyond[12]. For instance, in 2018, they demonstrated support for Milorad Dodik in an effort to promote the disintegration of Bosnia and Herzegovina[13]. However, it is difficult to attribute the damaging narratives to a specific source with absolute certainty. This highlights the importance of looking beyond the usual foreign suspects and systematically investigating the role of domestic and regional actors in spreading disinformation.

PRACTICE MAKES PERFECT

Recognising the need to address the rising threat of interference more effectively, and to collaboratively explore potential solutions with regional stakeholders, the EUISS conducted an

Timeline

Scenario story and evidence-based reality

2023

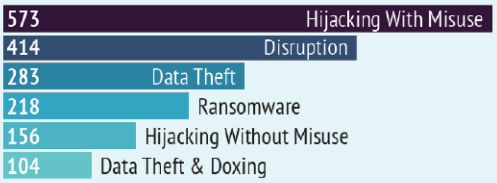
Expansion of ZEPHYRA's Renewable Energy Initiative in NOTEA

4 January 2024

Cyberattack on REG's NOTEA operations

Distribution of cyber operations recorded globally

1 748 total in 2023



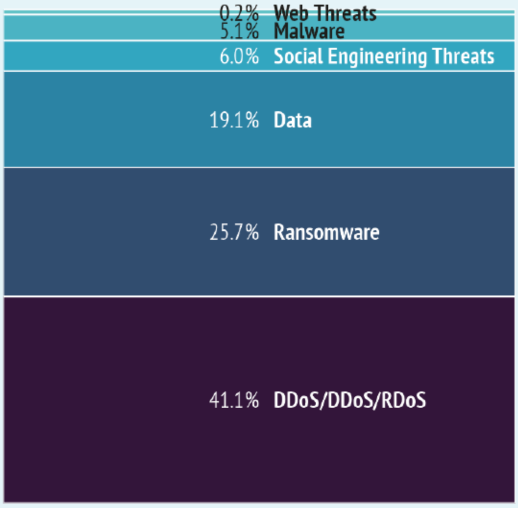
Data: Bund, J., Zettl-Schabath, K., Müller, M., Borrett, C., & EuRepoC., Cyber Conflict Briefing, 2023

8 January 2024

Discovery of a targeted cyber infiltration campaign and social media backslash

Incidents in the EU by threat type

Jul 2023-Jun 2024



Data: European Union Agency for Cybersecurity, Ardagna, C., Corbiaux, S., & Van Impe, K., ENISA Threat Landscape, 2024

18 January 2024

NOTEA politician's controversial remarks: Private messages of a NOTEA politician are leaked on the internet

The Montenegrin and pro-Russian NGO Movement for Neutrality aimed at influencing national media with anti-NATO narratives before the parliamentary election in 2016.

Rancy, A. 'The Struggle Against Authoritarian Influence in the Western Balkans: Montenegro as a Test Case', National Endowment for Democracy, 7 Nov 2024

Since 2020: 11 cases recorded on data leaks in BiH.

'Battle for Balkan Cybersecurity: Threats and Implications of Biometrics and Digital Identity', BalkanInsight, 30 Jun 2023 interactive scenario-based exercise earlier this year. The exercise involved representatives from Ministries of Foreign Affairs and Cybersecurity Agencies across the Western Balkans. It was designed to simulate a realistic and escalating series of cyber-enabled hybrid events affecting **fictional countries,** but drawing on threats and challenges that closely mirror those faced by the countries in the region. By immersing participants in a detailed and plausible scenario, it provided a tangible understanding of how cyberattacks, information manipulation campaigns and political interference can converge to undermine state capacity. It also provided a space to discuss response mechanisms in the technical and diplomatic spheres, while exploring potential partnerships with regional organisations and external actors. Moreover, the exercise underscored the importance of collective action and solidarity *vis-à-vis* transnational threats. Lastly, the escalatory scenario also aimed to highlight the deep interconnections between critical sectors, including energy, healthcare and electoral systems.

The **fictional scenario** unfolded over two months, depicting a complex interplay of cyberattacks, disinformation campaigns and political interference designed to destabilise a country aspiring to EU membership. A comprehensive description of the fictional actors is provided in 'The Siege of NOTEA' diagram on page 2. In 2023, the fictional country of ZEPHYRA initiated a renewable energy project through its Renewable Energy Group (REG) in NOTEA. NOTEA, a technologically advanced country with ties to ZEPHYRA, attempted to enhance its energy infrastructure. The REG project faced harsh criticism for displacing rural communities, leading to discontent within the country.

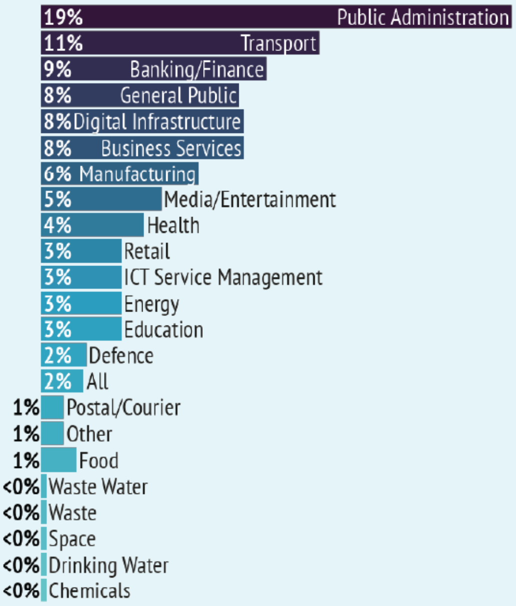
On 4 January 2024, a series of cyberattacks targeted REG's operations in NOTEA, causing significant disruptions and exposing vulnerabilities in the critical infrastructure. The attacks sparked social media debates about the security of foreign investments in national utilities. Investigations revealed an infiltration campaign against the REG project, accompanied by ransomware demands. While national television offered limited information, the state-sponsored outlet Sinia Today criticised NOTEA's inability to protect its citizens and questioned its reliance on ZEPHYRA for essential infrastructure.

27 January 2024

Security Anomalies in Electoral Systems

Targeted sectors in the EU

Jul 2023-Jun 2024



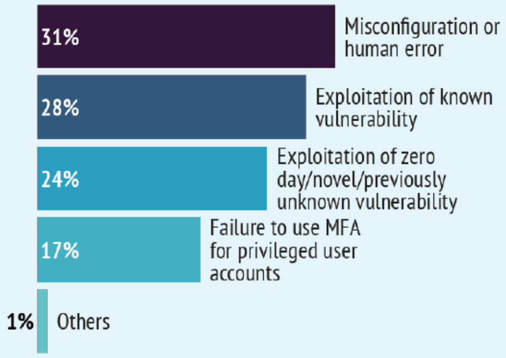
Data: European Union Agency for Cybersecurity, Ardagna, C., Corbiaux, S., & Van Impe, K., ENISA Threat Landscape, 2024

1 February 2024

Identification of malicious code

Root cause of cloud data breaches

Globally in 2023, %



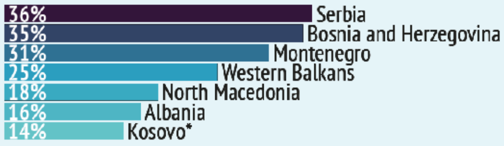
Data: 2024 Thales Cloud Security Study. In S&P Global Market Intelligence & Thales, 451 Research's Cloud Security Study, 2024

3 February 2024

A protest unfolds

Hybrid threats and feelings

Opinion on hybrid threats (in particular disinformation, fake news and radical narratives) negatively impacting the feeling of security (2023)



Data: Regional Cooperation Council (RCC). 'SecuriMeter 2023 – Public Opinion Survey on Security', 13 Nov 2023

Tensions escalated on 18 January 2024, when private messages from a NOTEA politician were leaked through a cyberattack, exposing derogatory remarks made about the displaced rural communities. This leak exacerbated political polarisation and eroded public trust in government officials. Concerns grew on 27 January 2024 as anomalies were detected in NOTEA's electoral systems developed by the DEMOsoft software company. This raised concerns about cyber manipulation and potential risks to the integrity of the country's electoral process.

On 1 February 2024, a zero-day exploit in DEMOsoft's software was discovered, allegedly orchestrated by Zargothrax101, a cybercriminal group linked to Sinia Today. Protests ensued on 3 February 2024, with citizens gathering outside NOTEA's parliament to demand stronger cybersecurity measures and better protection of digital rights. JohnyTheChef, the well-known influencer, amplified the unrest. On 15 February 2024, ZEPHYRA alerted NOTEA about a software vulnerability that could potentially compromise NOTEA's energy infrastructure. Although it was promptly patched, on 20 February 2024 NOTEA's healthcare systems suffered a severe cyberattack, causing significant disruptions.

On 25 February 2024, ZEPHYRA identified anomalies within its own network, and after thorough technical triaging, managed to link Sinia Today to the cyber disturbances. This connection was subsequently confirmed by an exposé published by *Economic Seasons*, a reputable international news outlet, on 28 February 2024. Following these revelations, media outlets in NOTEA experienced Distributed Denial of Service (DDoS) attacks, further amplifying the sense of crisis. The cybercriminal group 'Mordred_X4', also linked to Sinia Today, publicly condemned NOTEA's government for its negligence. On 5 March 2024, leaked documents disclosed NOTEA's internal security concerns, fuelling public criticism over the government's preparedness and response to hybrid threats.

15 February 2024

Critical Vulnerability Alert from ZEPHYRA

2023: >200 cyberattacks on the energy sector

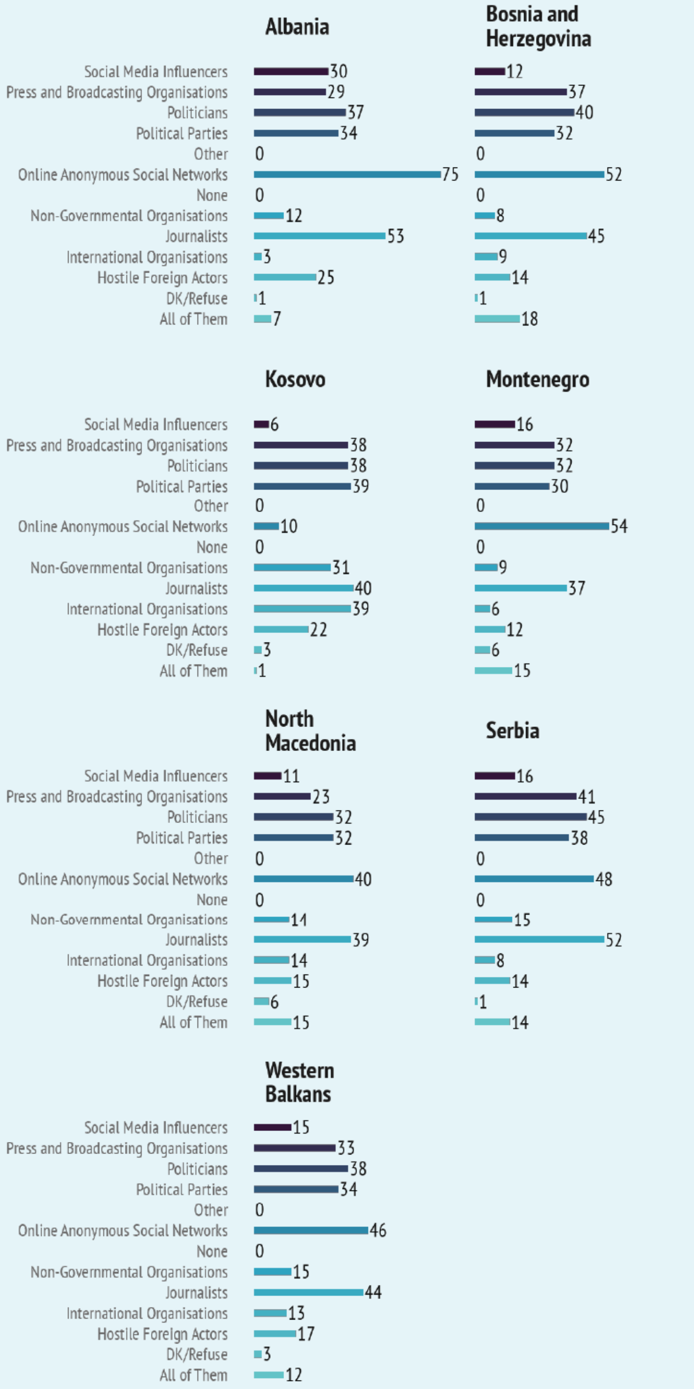
Cyber Europe tests the EU Cyber Preparedness in the Energy Sector. ENISA, 20 June 2024

20 February 2024

Cyberattack targets NOTEA's healthcare systems

Opinion on actors who spread disinformation

In your opinion, which are the actors who spread disinformation the most in your country?



Data: Regional Cooperation Council (RCC). 'SecuriMeter 2023 – Public Opinion Survey on Security', 13 Nov 2023

WHAT HAPPENED TO NOTEA CAN HAPPEN TO OTHERS

The scenario depicts incidents that occur with alarming frequency. The Timeline illustrates the storyline together with figures from real-world data highlighting key trends. The exercise aimed to replicate the complexity of multilayered hybrid threats and allowed the participants to engage and mobilise their reactions in a crisis setting. In line with the growing literature on scenario-based exercises[14], such activities can be valuable tools for supporting policy development by enhancing situational awareness ahead of the unfolding of a crisis.

This is particularly relevant in the case of cyber-enabled hybrid threats given their potential impact and severity. These threats are part of a broader effort to damage and disrupt critical infrastructure systems, manipulating public perception through disinformation campaigns and fostering interference in national affairs. In turn, this may have repercussions on political processes and undermine democratic institutions and state capacity. The well-known difficulties of attribution and accountability further complicated effective responses during the exercise. The responses tested systematically throughout the scenario contributed to generating policy recommendations.

FROM FICTION TO REALITY: KEY TAKEAWAYS

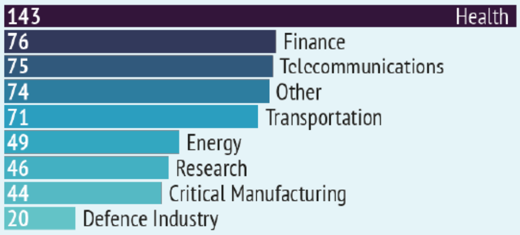
The Western Balkans is increasingly facing malicious cyber-enabled hybrid interference activities that mirror global trends. The scenario-based exercise exposed critical gaps and areas for improvement, as follows:

Access to EU initiatives

Participants in the scenario-based exercise emphasised the absence of structured institutional dialogue with the EU Agency for Cybersecurity (ENISA) as significantly hampering

Cyber operations targeting critical infrastructure globally

500 in total, 2023



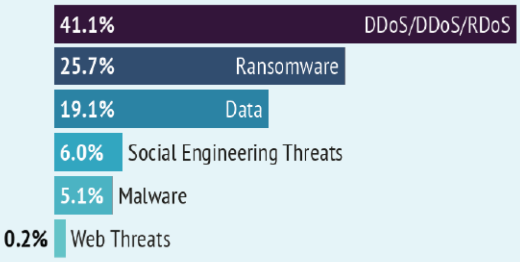
Data: Bund, J., Zettl-Schabath, K., Müller, M., Borrett, C., & EuRepoC., Cyber Conflict Briefing, 2023

25 February 2024

Exposure of SINIA's involvement by ZEPHYRA

Incidents in the EU by threat type

Jul 2023-Jun 2024



Data: European Union Agency for Cybersecurity, Ardagna, C., Corbiaux, S., & Van Impe, K., ENISA Threat Landscape, 2024

28 February 2024

Financial Times exposes SINIA's cyber and disinformation campaign

2022-2024: 1.2 million personal records exposed and 200% surge in ransomware attacks.

How do cyber-attacks threaten the Balkans? A Debrief with Dan Ilazi and Filip Stojanovski. Atlantic Council, 1 Oct 2024

The Balkan Investigative Reporting Network exposes how Russian-backed channels spread disinformation in the Western Balkans.

BIRN Doc Lifts Lid on Russian Disinformation in Balkans. BalkanInsight, 10 May 2024

1 March 2024

Media outlets compromised

The most common anti-EU narratives are "EU does not really want Western Balkan countries to join" and "the EU is in economic decay".

Sijah, D., 'Disinformation narratives inciting Euroscepticism in Western Balkans', Point Conference, 27 June 2024 effective peer learning. Aside from occasional voluntary interactions, ENISA could consider providing formal access to Western Balkan countries to participate in its deliberations, even if only as observers. Thus far, only Serbia and Montenegro have managed to establish some direct cooperation with ENISA[15]. By fostering a more direct and institutionalised engagement with ENISA, the EU could enhance the cybersecurity framework of the region.

Multi-stakeholder approach

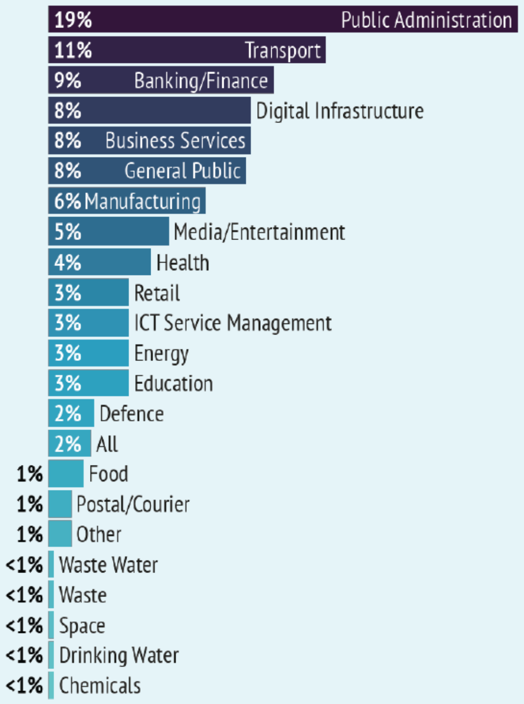
Leveraging non-governmental expertise to build a stronger societal coalition is essential, particularly given that much of the cyber infrastructure is owned by private companies. To ensure a more secure cyberspace, it is critical to involve businesses in safeguarding state institutions' digital infrastructure, while ensuring robust security controls and regulatory oversight. Involvement of the private sector in identification, deterrence and post-threat resilience is crucial, as businesses possess technical expertise and can offer specific know-how. Non-state actors, who may be less bound by certain national or international regulations and can adapt more swiftly to evade legal repercussions, tend to have access to similar tools to those used by state actors[16].

Capacity building and cybersecurity education

There is both a lack of interest and a shortage of professionals willing to work in the cybersecurity domain. The global cybersecurity workforce currently stands at 5.5 million, yet a staggering 4.8 million positions remain unfilled worldwide. In Europe, the workforce gap rose by 12.8% in 2024 compared to the previous year, now totalling 392 320 unfilled roles. Notably, certain EU Member States, including Germany (with a 15% increase) and France (17% increase), have seen expansions in their workforce gaps, while others, like the Netherlands and Spain, have slightly reduced their gaps by 1.6% and 1.7%, respectively[17]. In the Western Balkans, limited interest in cybersecurity, but also less favourable job conditions, are encouraging young professionals to pursue broader IT careers that offer better remuneration rather than engage in-

Targeted sectors in the EU

Number of incidents, Jul 2023-Jun 2024



European Union Agency for Cybersecurity, Ardagna, C., Corbiaux, S., & Van Impe, K., ENISA Threat Landscape, 2024

5 March 2024

Leak of Sensitive Government Documents

In April 2021, an unsigned 'non-paper' was leaked to Slovenian media outlet Necenzurirano. The paper advocates to redraw the borders of Bosnia and Herzegovina.

Euronews. 'Balkans rocked as leaked memo explores redrawing Bosnia's border along ethnic lines', 20 Apr 2021 depth with cybersecurity. Trained staff leave for better paid positions in the private sector, or leave the country altogether, while private sector stakeholders report significant staff turnover, with a limited number of trained professionals on the market[18]. Prioritising cybersecurity in school and university curricula is crucial to enhance digital literacy and build resilience against the growing threat of cyber-enabled hybrid attacks.

Digital literacy and awareness raising

Increasing awareness about digital literacy and basic cyber hygiene practices is essential. Educational institutions should take the lead, supported by civil society organisations and media partners, to raise public awareness about the core principles of cyber-enabled hybrid threats. The EU and its Member States could play a key role in this regard, not only through joint initiatives within the Union but also by drawing on the experience of individual Member States (e.g. Estonia and Finland) that have established strong institutional frameworks and mechanisms to structurally address the lack of digital literacy among their citizens.

The authors would like to thank Lisa Hartmann González and Martins Gelazis, EUISS trainees, for their invaluable research assistance.

[1] 'Italy says Russia or China could gain influence in Western Balkans if EU dream fails', *The Independent*, 10 September 2024 (https://www.independent.co.uk/news/north-macedonia-ap-russia-china-antonio-tajani-b2610505.html).

[2] International Republican Institute, 'Western Balkans Regional Poll', Center for Insights in Survey Research, February-March 2024, p. 79-80 (https://www.iri.org/resources/western-balkans-regional-poll-february-march-2024-full/).

[3] Kovalčíková, N., (ed.), 'Hacking minds and machines: Foreign interference in the digital era', *Chaillot Paper* No. 184, EUISS, August 2024 (https://www.iss.europa.eu/sites/default/files/EUISS Files/CP_184.pdf).

[4] Reuters, 'Albania cuts Iran ties over cyberattack, U.S. vows further action', 7 September 2024 (https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/).

[5] America's Cyber Defense Agency, 'Iranian state actors conduct cyber operations against the government of Albania', 23 September 2022 (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a).

[6] Ivanović, I., 'Press Restart: Montenegro launches new open data portal after cyberattack', Balkan Insight, Balkan Investigative Reporting Network, 24 September 2024 (https://balkaninsight.com/2024/09/24/press-restart-montenegro-launches-new-open-data-portal-after-cyberattack/).

[7] Reuters, 'EU slams unprecedented interference by Russia in Moldova referendum', 21 October 2024 (https://www.reuters.com/world/europe/eu-slams-unprecedented-interference-by-russia-moldova-referendum-2024-10-21/).

[8] Tuhina, G., 'Two years Into EU ban, Russia's RT and Sputnik are still accessible across the EU', Radio Free Europe/Radio Liberty, 3 February 2024 (https://www.rferl.org/a/russia-rt-sputnik-eu-access-bans-propaganda-ukraine-war/32803929.html).

[9] NATO Strategic Communications Centre of Excellence, 'Russia's narratives toward the Western Balkans: Analysis of Sputnik Srbija', April 2020 (https://stratcomcoe.org/cuploads/pfiles/analysis_of__sputnik__serbia__30-04__v4-1.pdf).

[10] Morača, T., et. al, 'Feeling the pulse: Countering foreign information manipulation and interference in Africa and the Western Balkans', Brief No 18, EUISS, 23 October 2023 (https://www.iss.europa.eu/content/feeling-pulse).

[11] European Parliament, 'Mapping fake news and disinformation in the Western Balkans and identifying ways to effectively counter them', Directorate-General for External Policies, February 2021 (https://www.europarl.europa.eu/RegData/etudes/STUD/2020/653621/EXPO_STU(2020)653621_EN.pdf).

[12] Euronews, 'Bosnian-Serb branch of Russian Night Wolves biker group stage pro-Putin protests', 12 March 2022 (https://www.euronews.com/2022/03/12/bosnian-serb-branch-of-russian-night-wolves-biker-group-stage-pro-putin-protests).

[13] Zweers, W., Drost, N. and Henry, B., 'Little substance, considerable impact: Russian influence in Serbia, Bosnia and Herzegovina, and Montenegro', Clingendael Report, August 2023 (https://www.clingendael.org/sites/default/files/2023-08/little-substance-considerable-impact.pdf).

[14] Noori, N. S., et al, 'Behind the scenes of scenario-based training: Understanding scenario design and requirements in high-risk and uncertain environments', ISCRAM, May 2017, pp. 948-959.

[15] For more see: Dimitrov, Đ., *The New Growth Plan,* European Policy Centre, June 2024 (https://cep.org.rs/wp-content/uploads/2024/06/New-Growth-Plan_Assessing-the-Value-of-the-Proposed-Early-Integration-Incentives_DJD.pdf).

[16] Van der Meer, S., 'How states could respond to non-state cyber attackers', Clingendael Institute, June 2020 (https://www.clingendael.org/sites/default/files/2020-06/Policy_Brief_Cyber_non-state_June_2020.pdf).

[17] For more see: ISC2 Research, *2024 Cybersecurity Workforce Study*, 2024 (https://www.isc2.org/Insights/2024/09/Employers-Must-Act-Cybersecurity-Workforce-Growth-Stalls-as-Skills-Gaps-Widen).

[18] For more see: PwC and the ISAC Fund, *Cybersecurity* Ecosystem *Report: Western Balkans – Emerging Cyber Threats*, March 2022 (https://www.isac-fund.org/wp-content/uploads/2022/04/PwC-Cybersecurity-Ecosystem-Report-WB.pdf).