



Funded by
the European Union

PractNet

International Practitioners'
Partnership Network

Disinformation and foreign interference in elections

Kersti Luha
Leading Expert on Strategic Communication

Challenges for protecting information space and information resilience

- ▶ Disinformation
- ▶ Foreign Information Manipulation and Interference (FIMI)
- ▶ Long term societal resilience and trust under threat

The answer: wider awareness building and developing societal cohesion during the elections and in between

Disinformation narratives and operations targeting our resilience

- ▶ Traditional:
 - ▶ a) latent
 - ▶ b) in active use
- ▶ Targeting and weaponizing existing weaknesses and frictions
- ▶ Constructing the excuses to manipulate and intervene

Historically used manipulative narratives and contradictions from Russia

- ▶ Estonia suffers from inferiority complex, is an economically failed state, has no international ground;
- ▶ Estonian intense Russophobia and war mongering, together with the other Baltic states, has impacted NATO and the EU until deepened the Western conflict with Russia.

Example of whole of society approach in Estonia: awareness building

- ▶ **Building community and knowledge** - courses and cooperation exercises
- ▶ **Providing community and society with practical information**
- ▶ **Investigative journalism, NGOs, State institutions**
- ▶ **Coordination, supporting partners in their activities** (election coordination, background briefings etc)
- ▶ **Supporting the resilience of free quality media** (2022 example for the Russian Speaking editorials)

Building community and knowledge

4. Areas of activity in Estonia's security policy

Estonia is facing the most tense security situation of the reindpendence period. As a society and a nation, we must be prepared for risks that previously seemed unthinkable.

To strengthen our security, Estonia acts within five main domains, which are inter-linked and mutually supportive, and which together form a whole where each part is of equal value:

 social cohesion and resilience of the state

 economic security and critical services

 internal security and public order

 military defence

 international cooperation

PREPARING FOR POSSIBLE CRISES

- How can I prepare for possible crises?
- The reserves of the state
- Payments and cash
- Cyber security**

Home > Security situation in Europe > Preparing for possible crises > Cyber security

Cyber security

Every person, institution and company can contribute to keeping you will find general suggestions on how to protect yourself in c

For individuals

1. Be sceptical about suspicious e-mails that you have received.
2. Update software regularly and make sure you are using the newest version.
3. Use antivirus software.
4. Use a strong password.
5. Do not believe e-mails from unknown senders that are threatening or
6. Do not enter your account information anywhere at the direction of a stranger in any other way.
7. Use multi-factor authentication.
8. Create regular backup copies of files both in your computer and in your phone.
9. Do not publicize your personal information.

It is easiest to protect yourself from danger that you are aware of and that you


Where to find information on the most common cyber attacks?

- News and threat assessments published by the Information System /
- Regular summaries of the past month's most important events and threats

Everyone who uses Estonia's e-services should have three ways of identification: an ID-card, a mobile phone and a PIN code.

KRIIS.EE

Security situation in Europe v COVID crisis management, QA v COVID Sickness, health, vaccinations v Travelling, crossing the border v



Home > Large-scale exercise CREVEX23: frequently asked questions

Large-scale exercise CREVEX23: frequently asked questions

From here you will find the questions and answers about the large-scale exercise CREVEX23.

MEEDIAPÄDEVUSE INFOKIRI

MAI 2024

Haridus- ja Teadusministeerium koostöös riigi meediapädevuse võrgustikuga on kokku pannud infokirja, millest leiata infot ja praktilisi soovitusi meediapädevuse arendamiseks. Infokiri on mõeldud eelkõige haridustöötajatele, palume see edastada kõigile, kel võiks olla huvi meediapädevuse teemade vastu. Infokiri ilmub iga kuu teisel neljapäeval.

Palume kõigil soovijail registreerida end infokirja tellijateks.

Registreeru

Euroopa valimised on ukse ees: 6.– 9. juunil 2024

Valimised ja valeinfo. Peagi on Euroopa Parlamendi valimised ja seetõttu muutub järjest põletavamaks ka valeinfo ja desinformatsiooni teema valimiste ajal.

- Kuidas saab ja on tehnoloogiat kasutatud desinformatsiooni loomiseks?
- Kas mõned riigid on rohkem mõjutatud kui teised ning kas ja mida saab mõjutuskampaaniate vastu ette võtta?



Rahvusraamatukogu meeskond jälgib selle teemaga seotud artikleid, uuringuid jm ning lisab jooksvalt infot RaRa [veebilehele](#).

- Valimisperioodil tasub ka meelde tuletada, mis on populism: Vaata videot [SIIN](#).
- Materjalid ja ülesanded propaganda mõtestamiseks ja propagandavõtete

Quality journalism, volunteers and NGOs sharing expertise



est eng rus de

Propastop is a blog aimed at cleaning Estonia from propaganda, false information and media lie. The blog is run by volunteers. [Read more!](#)

+ Most read posts

✕ Categories

- About the blog
- Analysis
- Interview
- Media literacy
- Media on propaganda
- Monthly reviews

Candidate 101: pro-Russian Aivo Peterson running his European Parliament election campaign from custody

The "Peterson phenomenon" is causing excitement in the European Parliament elections – will Aivo Peterson achieve the same powerful result as in last year's Riigikogu elections, and will the Center Party not be represented in the European Parliament at all due to his votes? Propastop reviews the campaign of the chairman of the Koos party.



С НАШИМ МНЕНИЕМ НАДО СВОБОДА И ДЕМОКРАТИЯ ДОЛЖНЫ ЕСЛИ НАС НЕ ХОТЯТ СЛЫШАТЬ В ЭСТОНИИ, ПУСТ НАМ НЕ НУЖНА ДИКТАТУРА ПОЛИТИКО МЫ САМИ ХОТИМ ВЫБИРАТЬ СВО

64

5 cor

Meie seisukohtadega tuleb arvestada. Vabadus ja demokraatlikud väärtused on meie jaoks olulised. Kui meid ei taheta kuulata Eestis, kuulatagu meid siis Euroopa Parlamendis. Meie soovime, et Eesti ei oleks autoritaarse diktatuuri. Tahame ise valida endale oma valimisreklaam Facebookis



Martin Laine

@Martinlaineolen

ee uuriv ajakirjanik/investigative journalist · nii @eestiekspress kui @DelfiEE · bylines @OCCRP @ICIJorg · #vatniksoupEE lõimed: <https://t.co/SwqXJKQPvJ>

3 subscribed

May 19 · 16 tweets · 10 min read

Save as PDF



17. #vatniksoupEE. Tutvustan teile Aleksandr Tšaplõginit, kes on tuntud pikaajase venekeelse linnameedia peatoimetaja ning keskerakondlasest riigikogu liikmena. Vaatleme klassikalist inimtüüpi, keda ajab kõige rohkem närvi küsimus "Kellele kuulub Krimm?" 1/16 🗨️ ...

Save as PDF

Arvamus Sõda Eesti Maailm Majandus Sport Arvamus Kultuur TV Digiajakirjad

Fookus Autorid Juhtkirjad Toimetaja valik Päevateema Karikatuurid AK Kommentaar

Tellijale

PEETER TALI } Kreml ründab Euroopa valimisi. Aivo Petersoni esitletakse kui poliitvangi (12)



Peeter Tali, Riigikogu liige, julgeolekuekspert (Eesti 200) 6. juuni 2024, 11:26

Kuula

Active investigative journalism

 Eesti Päevaleht

UUDISED



Juhtnõõrid ja raha Moskvast. Aivo Petersoni riigikokku kandideerimist toetas FSB sidemetega võrgustik (443)

23.10.2023, 00:01

Tellijale

Aivo Petersoni mõttekaaslane teatas Venemaal, et Eesti valmistub sõjaliseks provokatsiooniks (8)



Ivan Skrjabin, portaali Rus.Postimees ajakirjanik
6. juuni 2024, 12:31

Delfi25

RUS

Ärileht

Sport

Kroonika

Naistekas

Eesti Päevaleht

Maaleht

Ekspress

@ Q ☰

Viimased uudised

Sõda Ukrainas

EP valimised

Eesti

Maailm

Krimi

Arvamus

Forte

Delfi Lood

Delfi TV

Podcastid

UURIV

03.06.2024, 06:00

Lekkinud dokumendid: Kremli fond toetab salaja palgamõrvvareid, spioone ja Eesti mõjuagente (603)



Martin Laine
martin.laine@delfi.ee



Toimetas: Jete-Ri Jõesaar
jete-ri.joesaar@epl.ee

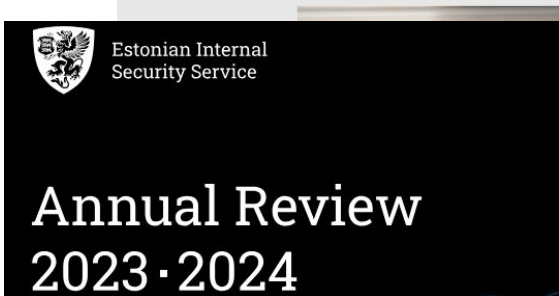
🔖   110



Providing practical information

Delfi25

Kremli fondi rahastatud isikud ja organisatsioonid Eestis (2018–2023)



MTÜ Vene Kool Eestis



Sputnik Eesti

Estonian Foreign Intelligence Service

Estonian Foreign Intelligence Service public report 2024



[Read the report online here!](#)

Read our public report

The Estonian Foreign Intelligence Service has published a report covering the security situation in the world.

The report «International Security and Estonia 2024» discusses the latest developments in Russian economy, special services and influence operations. We also turn our attention to China, Singapore and the United States.

The Estonian Foreign Intelligence Service protects Estonia from external security threats. The report discusses the Estonian national defence and security policy.

Read the new report [online here](#) or [download the PDF version](#).

Tasks

The main function of EEFIS is to collect intelligence and to protect classified information.

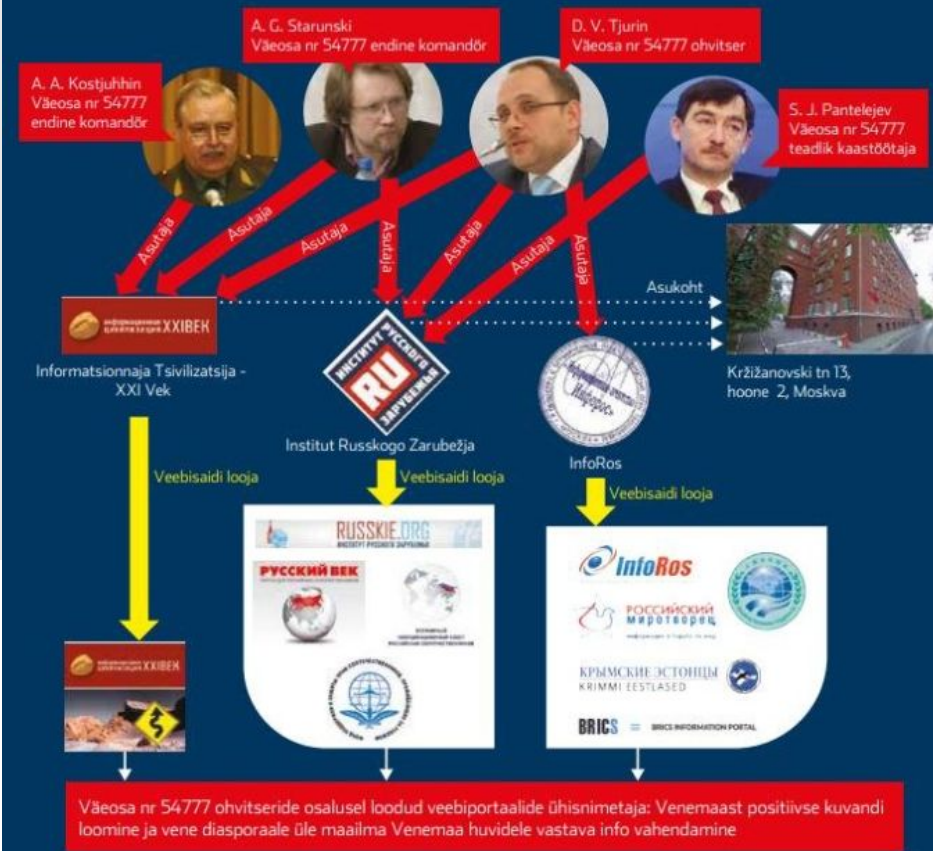
EEFIS collects, analyses and delivers information on Estonia's external security threats. The information gathered by EEFIS has a significant influence on Estonia's national defence and security policy making. EEFIS is in the front line of national defence, as intelligence ensures early warning for events that pose a threat to us.

History

Our history dates back to 1992 Office of the Republic of Estonia was subordinated to the Ministry of Internal Affairs.

In 2001, the Estonian Information Security Unit was subordinated to the Ministry of Intelligence of the former (CIS).

GRU PSÜHHOOLIGILISE VÕITLUSE KATTEORGANISATSIOONE



Psühholoogiliste operatsioonide sooritamiseks avalikus ruumis kasutab GRU sageli katteorganisatsioone ja nende loodud veebiportaale. Ülal on mõned näited GRU väeosa nr 54777 ohvitseride ja nendega lähedalt seotud isikute loodud projektidest.

- Home
- Press releases
- General Information
- Counterintelligence and foreign influence activities
- Disclosure of employees
- Corruption
- Economic security
- Extremism
- International crimes not subject to

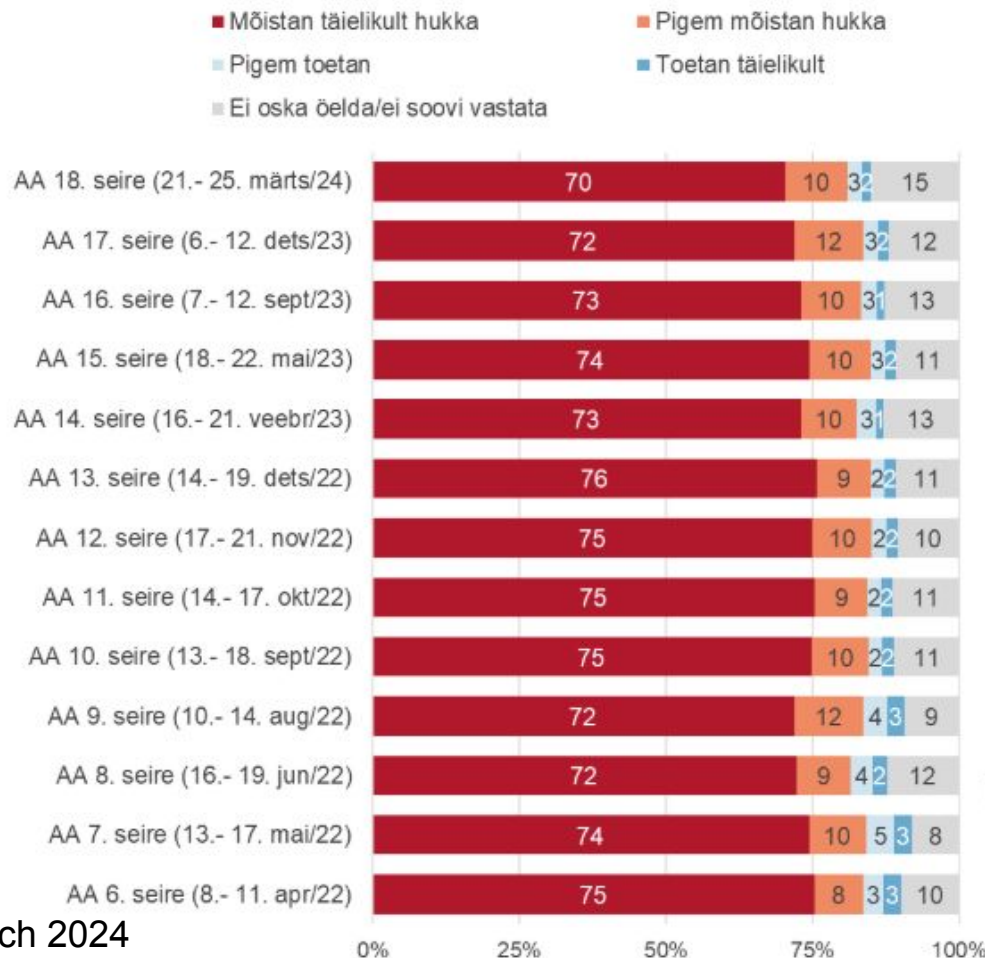
It's information space...



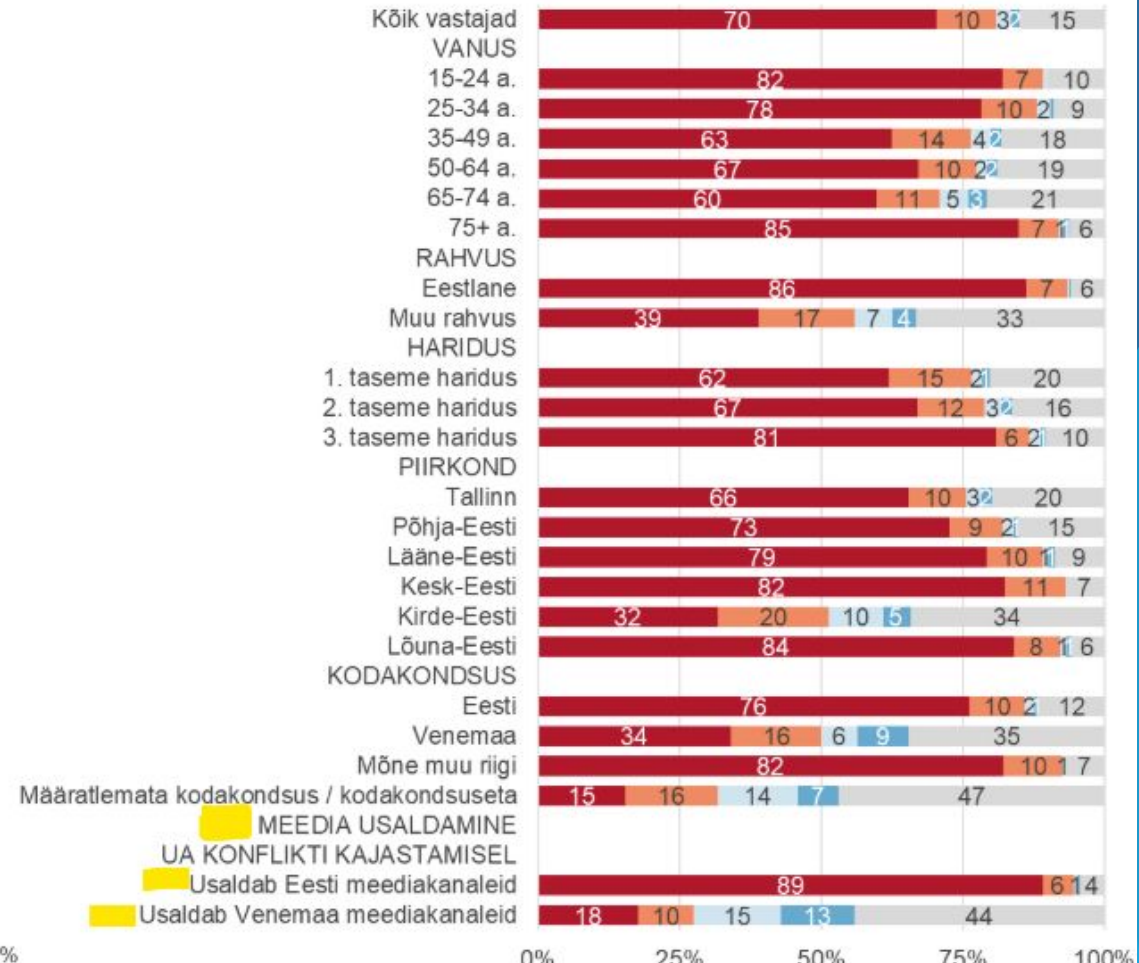
Suhtumine Venemaa sõjategevusse Ukrainas

Kõik vastajad, n=1260 (varasemates uuringutes 1252-1510 vastajat)

Kuidas Teie isiklikult suhtute Vene Föderatsiooni sõjategevusse Ukrainas?



Taustrühmade võrdlus, AA 18. seire



FIMI in recent elections: EU democracies

Did Russia Influence Brexit?



Photo: Stefan Rousseau-Pool/Getty Images

Blog Post by Donatienne Ruy
Published July 21, 2020

Contributor: Rachel Ellehuus

According to the UK Parliament's Intelligence and Security Committee, the UK government does not know and—incredibly—did not try to find out.

This was the question at the heart of the long-awaited “[Russia Report](#),” the 9-month delayed, 55-page assessment of Russia’s malign interference in UK politics. Produced by an independent committee of nine members of parliament from several political parties, including the ruling Conservatives, the report became highly controversial because Boris Johnson’s government tried to block its publication.

The report is damning. It says that the government, along with its intelligence and security services, “underestimated the response required to the Russian threat and



By Jean-Baptiste Jeangène Vilmer
With an introduction by Heather A. Conley

JUNE 2018

THE ISSUE

The 2017 French presidential election remains the clearest failed attempt by a foreign entity to influence an electoral process in recent years. Taking aim at presidential candidate Emmanuel Macron, Russian interference succeeded neither in interfering with the election nor in antagonizing French society. This Brief examines how France successfully withstood the disinformation and interference; how this failed attempt can be explained; and, looking to the future, what lessons can be learned from this experience?

INTRODUCTION

On Friday, May 5, 2017—just two days before the second and final round of the French presidential elections—gigabytes of data hacked from Emmanuel Macron’s presidential campaign team were released online. Months earlier an orchestrated disinformation campaign against the Macron presidential campaign had already begun. The so-called Macron Leaks—a combination of real emails and forgeries—could have been yet another example of a long list of attempts by Russia to interfere in a high-stakes transatlantic election. But the 2017 French presidential election may be the exception that proves the rule: it is the most clearly failed attempt. The Kremlin neither succeeded in interfering with the presidential election nor in dividing French society.

As the United States prepares to hold nationwide elections on November 6, 2018, the director of national intelligence, Dan Coats, has already warned in February of this year that “We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokespersons and other means of influence to try to exacerbate social and political fissures in the United States.” Calling Russian influence “pervasive,” Director Coats further noted that “The Russians have a strategy that goes well beyond what is happening in

the United States,” he said. “While they have historically tried to do these types of things, clearly in 2016 they upped their game. They took advantage, a sophisticated advantage of social media. They are doing that not only in the United States but . . . throughout Europe and perhaps elsewhere.” Because the United States is not well prepared for future elections, it is necessary to study the past.

This is why the 2017 French presidential election is a particularly important election to study and why we highlight French scholar Jean-Baptiste Jeangène Vilmer’s groundbreaking report on the Macron Leaks.¹ Drawing in part upon the work of CSIS visiting fellow Boris Toucas,² Vilmer’s forthcoming report will examine what happened during the French presidential election; who orchestrated the affair; how it was successfully countered; and what lessons can be learned. This Brief, which is part of the forthcoming CSIS comprehensive report, sums up the main lessons learned.

Myriad structural factors, luck, as well as effective anticipation and reaction by the Macron campaign staff, government and civil society, and especially the mainstream media, combined to successfully resist Russian malign influence.

—Heather A. Conley, CSIS



Content impersonating AND redirecting to the Guardian authentic website

Fake content produced by Doppelgänger



Figure 3 - Spot the difference: fake content on a cloned Guardian

So how can one spot the difference between one authentic media and its cloned counterpart? Not by its design but by its domain name. Looking for credibility, malicious actors targeted their efforts in buying alternative domain names for the media they wanted to impersonate, thus making very likely unauthorised use of their associated trademarks. Doppelgänger took advantage of the loopholes in the ecosystem of domain names and our lack of attention to this Internet vulnerability.

Protecting electoral integrity and information space

- ▶ Building trust and enhancing awareness
- ▶ Practical guidelines
- ▶ Revealing information
- ▶ Carefully considering amplification
- ▶ Cooperation and coordination

Providing public awareness protects
free competition of ideas and fear
elections

Thank you!