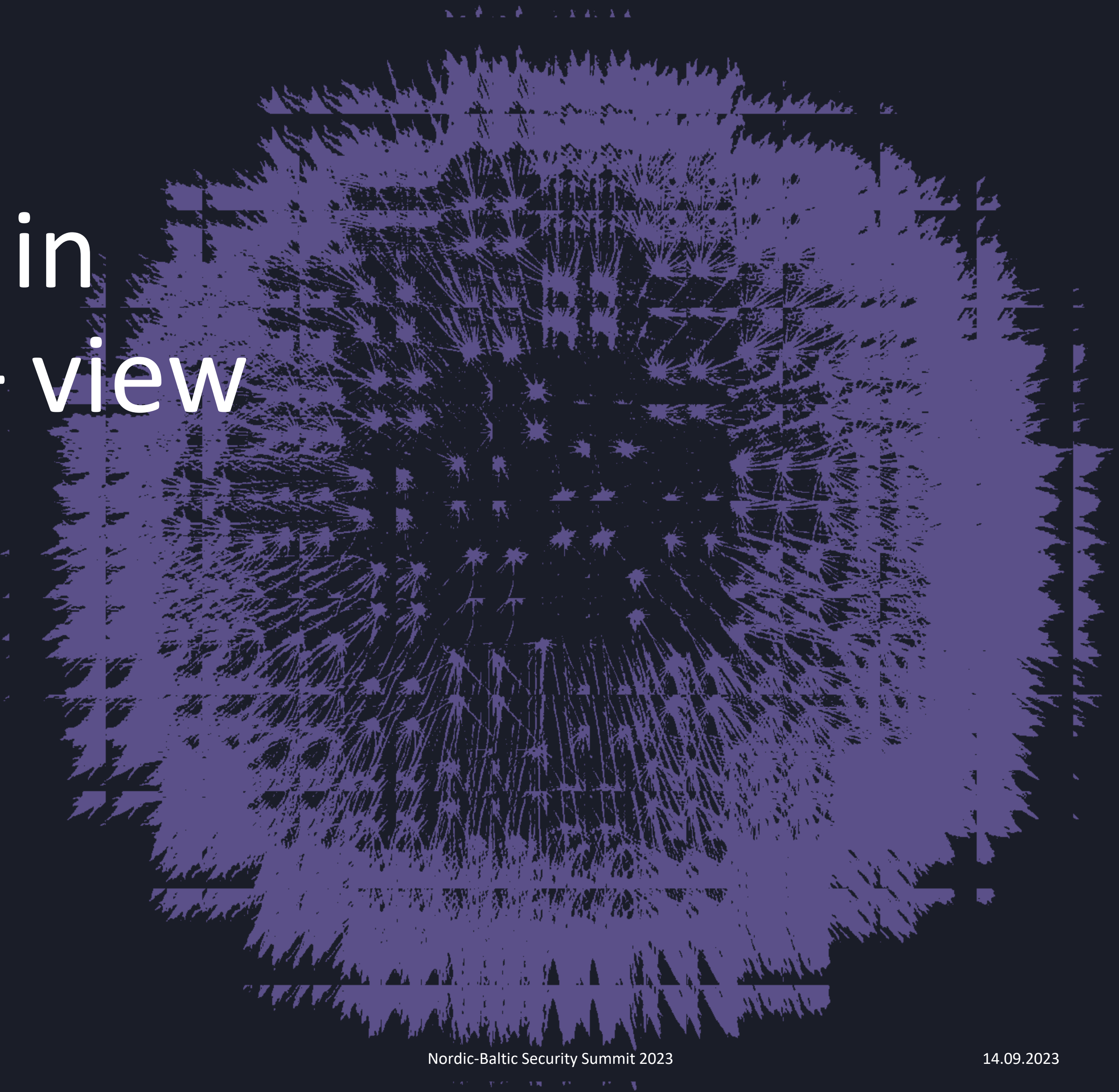
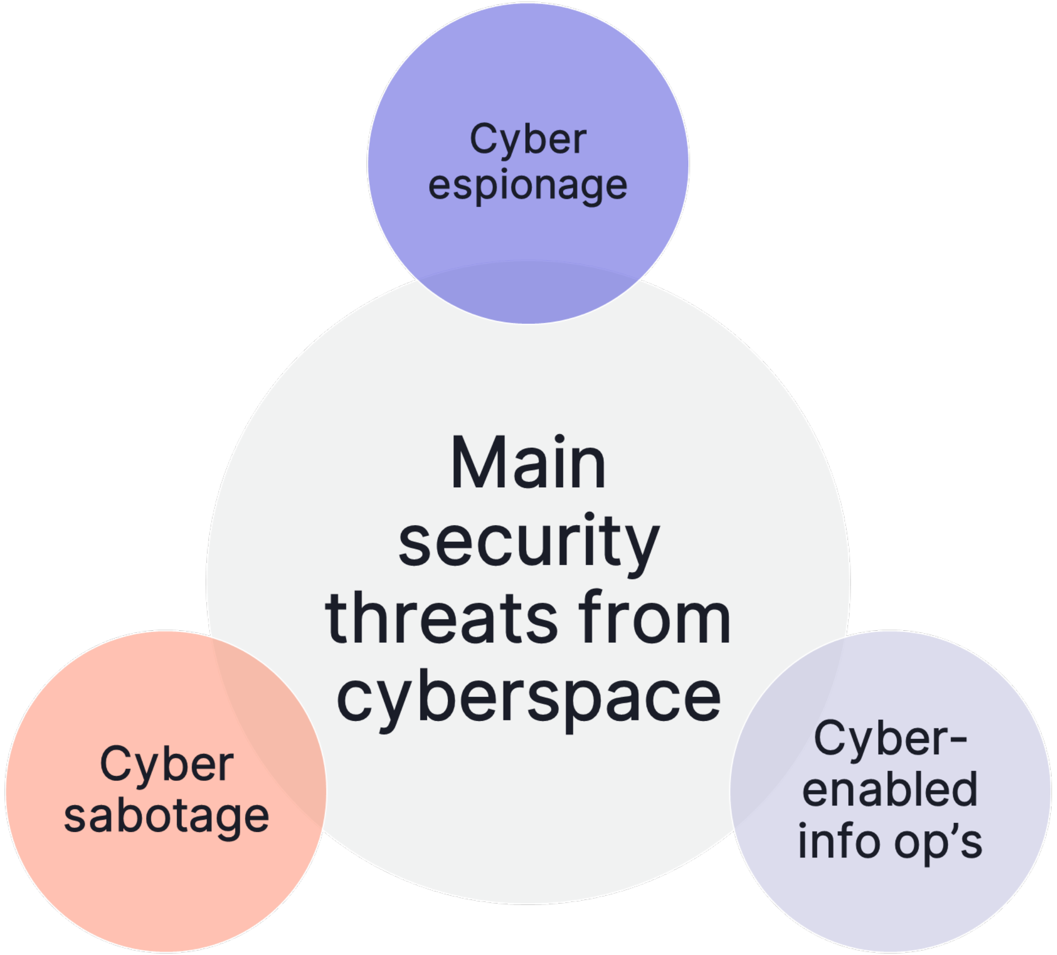


Security Threats in Cyber Domain – view from EFIS

Kaupo Rosin

Director General

Cyber Threat Landscape

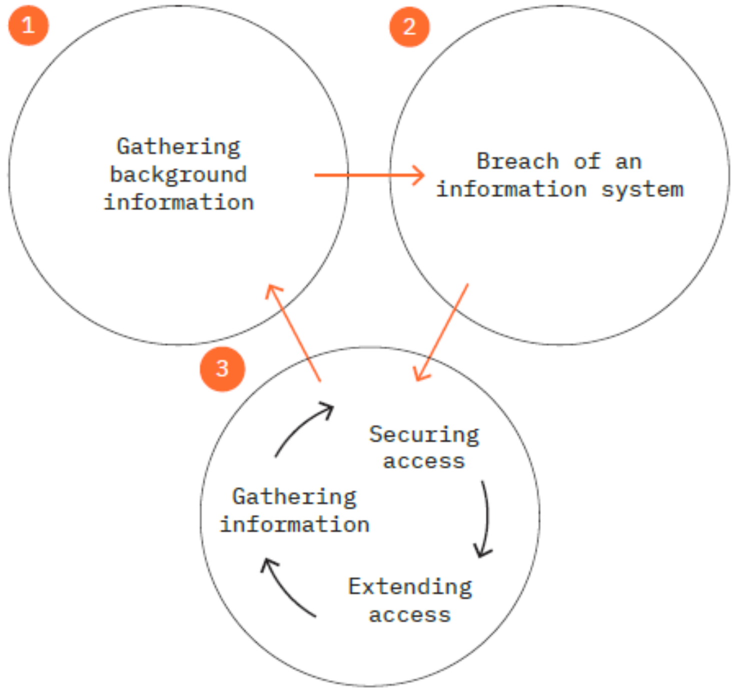


Understanding Cyber Espionage

Cyber espionage

- **Constant threat**
- **Targets: government institutions, critical information systems and entities, private sector, people**
- **The goal of the attackers is to stay hidden as long as possible in order to preserve access to the systems**

Stages of Russian special services' cyber espionage operation

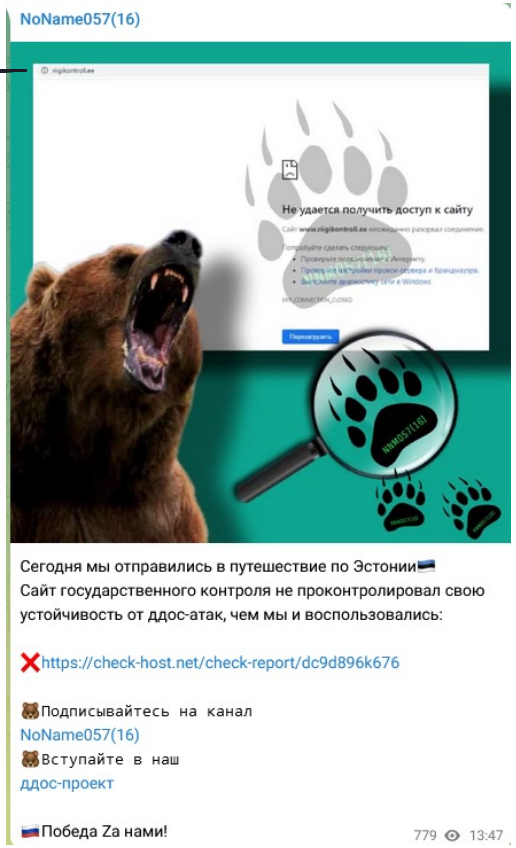

1
Gathering background information
2
Breach of an information system
3
Securing access
Extending access
Gathering information

Understanding Cyber as a Means for Influence

Cyber-enabled informatio op’s

- **DDoS attacks, defacements, hack-and-leak *etc***
- **Targets: government institutions, critical information systems and entities, private sector**
- **The goal of the attackers is to gain publicity, cause anxiety among citizens and undermine the target nation**

Riigikontroll.ee



NoName057(16)

riigikontroll.ee
Не удается получить доступ к сайту
Сайт www.riigikontroll.ee неожиданно разорвал соединение.
Попробуйте сделать следующее:
Проверьте подключение к Интернету.
Проверьте настройки прокси-сервера и брандмауэра.
Выполните диагностику сети в Windows
ERR_CONNECTION_CLOSED
Перезагрузить
NNM057(16)

Сегодня мы отправились в путешествие по Эстонии🇪🇪
Сайт государственного контроля не проконтролировал свою устойчивость от ддос-атак, чем мы и воспользовались:

❌https://check-host.net/check-report/dc9d896k676

🐻Подписывайтесь на канал
NoName057(16)
🐻Вступайте в наш
ддос-проект

🇷🇺Победа Za нами!

779 👁 13:47

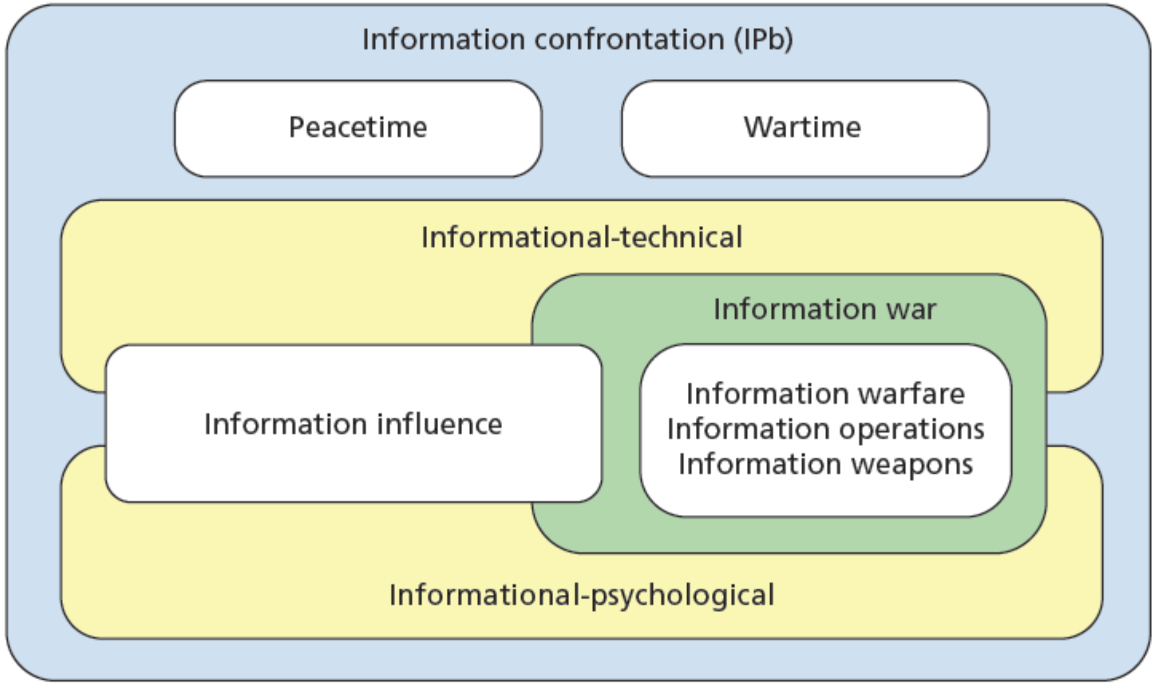
Understanding Cyber Sabotage

Cyber sabotage

- **The goal is to disrupt critical services, stress society on a bigger scale**
- **Targets: energy, communication, military sectors**
- **Low number of incidents, but wide impact**

How does Russia see the cyber domain?

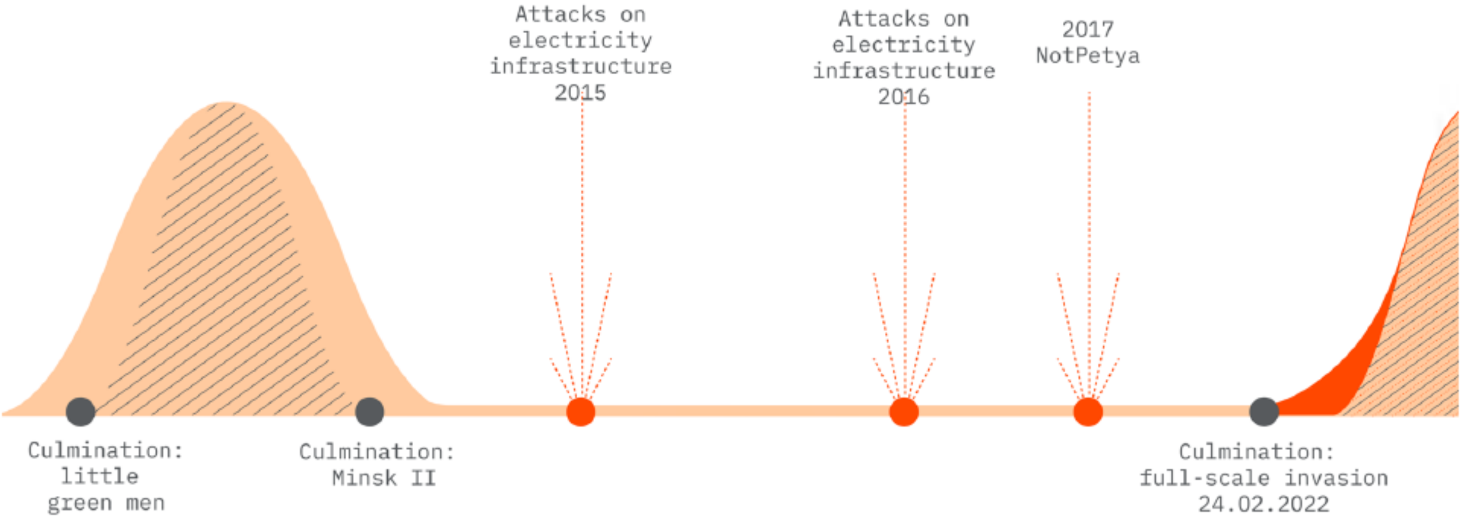
- **The West distinguishes between cyberattacks and influence operations**
- **Russia interprets them as a single concept – information confrontation – which consists of technical and psychological measures**
- **The Russian Armed Forces' doctrine: exert informational, technological and psychological influence on another country, protect Russia itself from such influences**



Grisé, M., et al. Rivalry in the Information Sphere: Russian Conceptions of Information Confrontation. RAND Corporation (2022)

Cyber in Ukraine

- **Ukraine has been a constant target of cyberattacks by Russian special services since 2014**
- **Cyber attacks intensified before the full-scale invasion and have been ongoing ever since**
- **DDoS attacks, defacements, data leaks, wipers, cyber espionage**
- **Targets: critical infrastructure, military systems, media, local governments *etc***
- **Russia’s cyberattacks against Ukraine highly likely aimed to support its general goals**



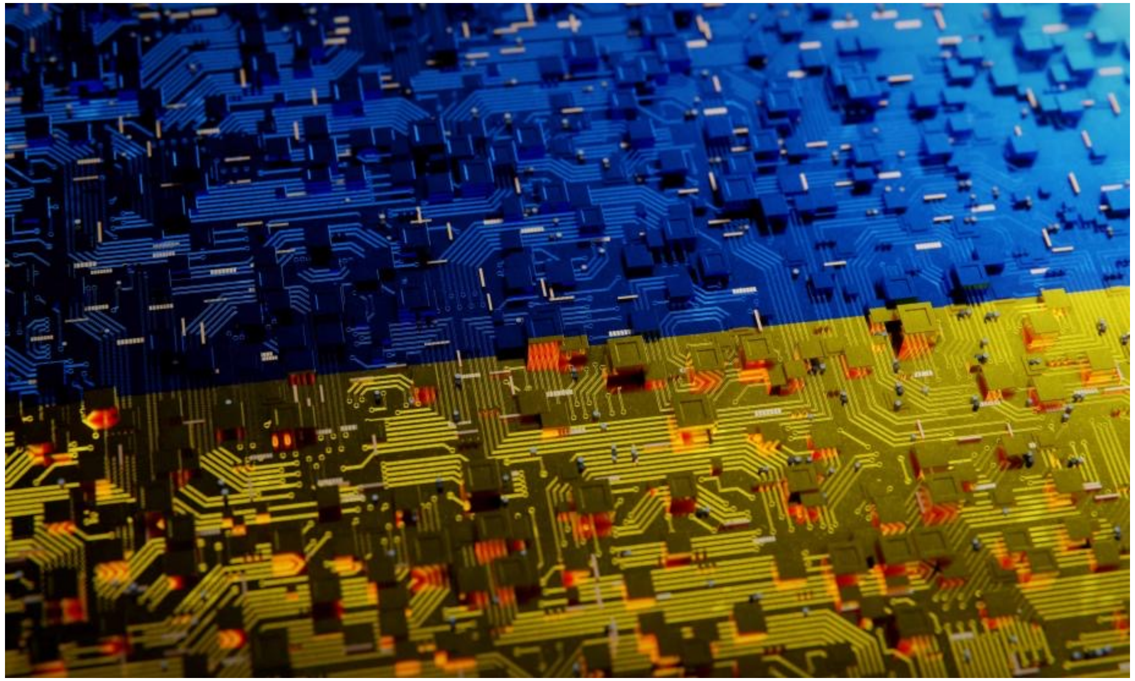
▨ **Active phase of kinetic warfare**

🟧 **Cyberattacks to obtain information and support influence operations**

🟥 **Cyber extortion**

Ukraine’s resilience in cyberspace

- **Ukraine’s resilience in cyberspace has been remarkable**
- **Russia underestimated the resilience of Ukraine’s cyberspace and the help it receives from Western countries and cybersecurity companies**
- **Ukrainian society remains united and trusts its government despite threats posted on social media and data leaks**



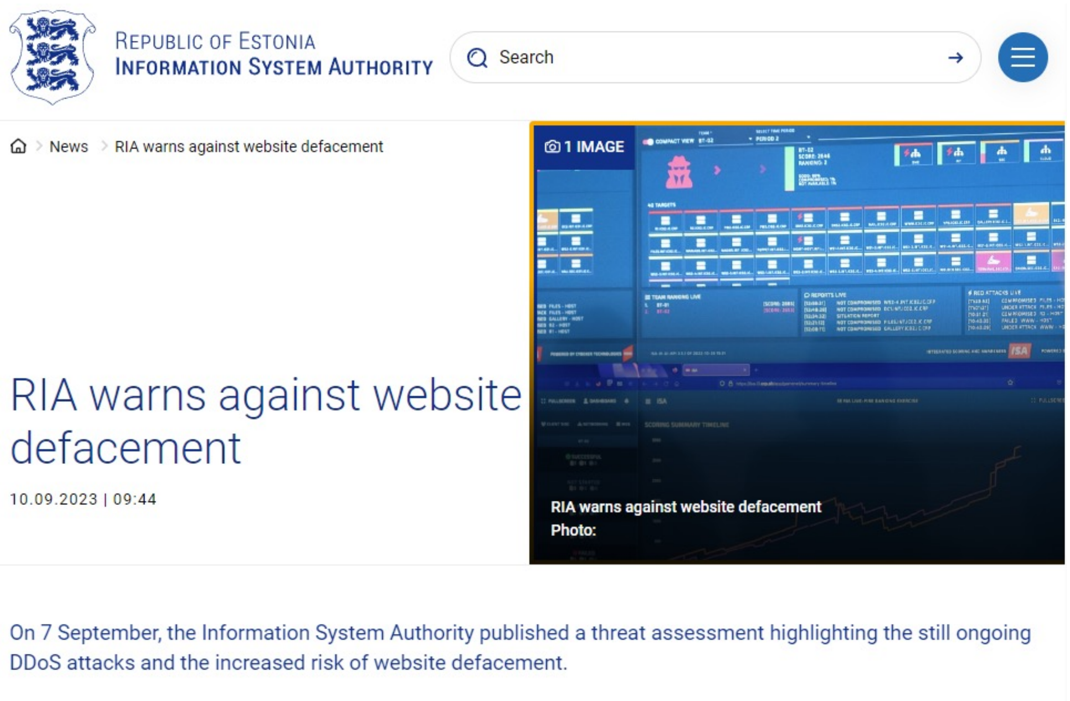
Malicious Cyber Activities Outside Ukraine

Increased cyber threat level for Estonia and other Western countries due to:

- **possible spill-over efect from cyber attacks against Ukraine;**
- **becoming a target because of the support for Ukraine.**

Malicious activities of the „hactivists“:

- **constant cybet attacks against the Western countries since the Russian full-scale invasion of Ukraine;**
- **the impact as high as promoted by the hackers;**
- **waves of cyber attacks often as a reaction to certain political activities or decisions disliked by Russia;**
- **main purpose is psychological/influencial.**



Republic of Estonia
Information System Authority

RIA warns against website defacement

RIA warns against website defacement

10.09.2023 | 09:44

RIA warns against website defacement
Photo:

On 7 September, the Information System Authority published a threat assessment highlighting the still ongoing DDoS attacks and the increased risk of website defacement.

View Forward

- **Other cyber threat actors of concern**
- **China cyber actors have shown more interest in Europe overt the past years**
- **Deny hacktivists wider publicity, as that is their main goal (so far)**
- **The cyberspace is of global nature and cooperation between the civil, military and private sector is crucial**

Estonian Foreign Intelligence Service