DREAMLAB
TECHNOLOGIES

Majandus- ja Kommunikatsiooniministeerium
Suur-Ameerika 1
10122 Tallinn
Estonia

Bern/Switzerland, October 2024

Cyber sovereignty - measure and monitor your nation's cyberspaces

Dear Minister of Economic Affairs and Infomation Technology Tiit Riisalo

Dreamlab Technologies is a Swiss cybersecurity innovation pioneer which partners with the UN's ITU (International Telecommunication Union) for its Cyber for Good initiative and the 2024 Global Cybersecurity Index (GCI) report - by utilising the CyObs platform.

CyObs is the Swiss made software solution (www.cyobs.com) that has the ability to scan an entire's nation cyberspace and create a full repository of the public attack surface. With this, CyObs provides unparalleled visibility on all cyber assets' attack surfaces and supply chain dependencies.

Key features include:

- Analyse: Complete a high-precision, high-speed analysis of the nation's digital infrastructure.
- Identify: Provide full visibility of vulnerabilities and anomalies.
- Protect: Reduce your nation's public attack surface to improve the overall security.
- Monitor: Stay ahead with automated alerts and notifications regarding potential threats.

We already sent you a copy of your country report some weeks ago. As we believe that the protection of your cyberspace is a critical undertaking in the digital age, we herewith attach another copy for your perusal.

Please contact us for further information and a demonstration on how CyObs can help you protect your nation's cyberspace.

With kind regards,

Nicolas Mayencourt
Founder and Global CEO
Dreamlab Technologies AG
nick@dreamlab.net

MAJANDUS- JA
KOMMUNIKATSIOONIMINISTEERIUM
06. 11. 2024
Nr. 9-2/2806-1

CYOBS
SEE THE CYBER

Cyber Attack Surface & Risk Profile: Estonia

Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

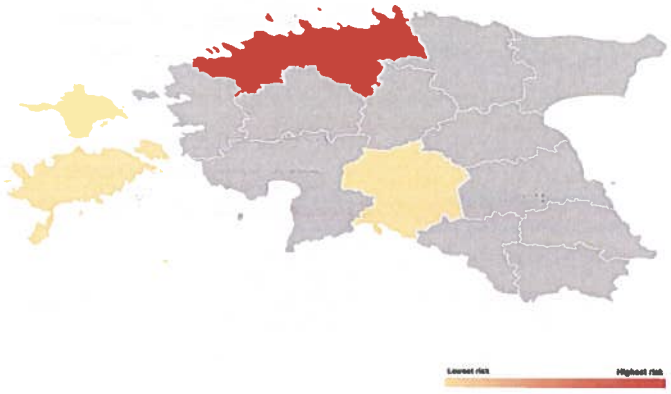
National Cyberspace Metrics

Decoding Estonia's Invisible Cyberspace

Risk Vectors by Regions

Harjumaa	
Total IPv4	1,263,847
Active IPv4	313,693
Total Domains	186,914
Active Domains	173,578
Open Ports	303,478
Vulnerabilities	356,061

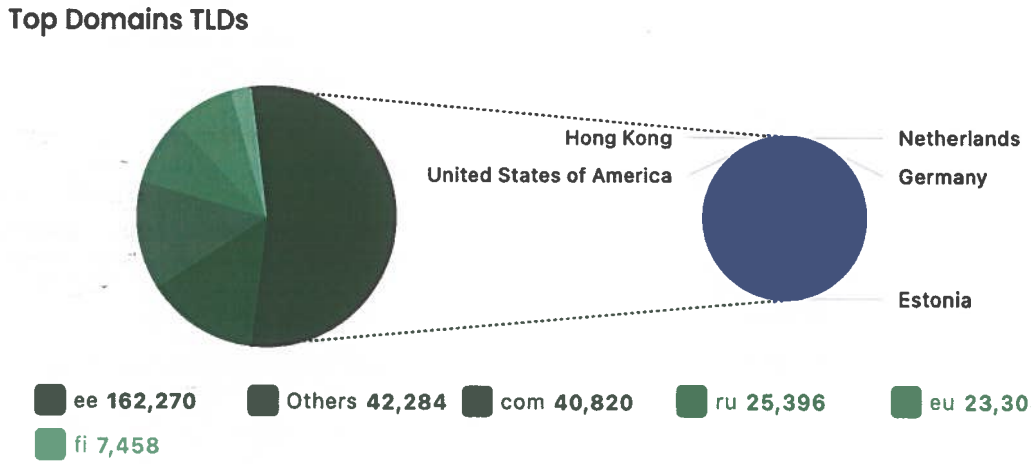
Security risks overview



Overall Assets Monitored and Level of Threat

Active IPv4	348,780 + 35,705 (11.4%)	1.506.931 Total
Open Ports	447,220 + 370,890 (485.9%)	998 Unique
Active Domains	202,658 + 18,183 (9.9%)	301.928 Total
Vulnerabilities	678,259 + 441,418 (186.4%)	678.259 Potential

Geo-Dependencies of Top-Level Domains Hosting



In this example, the majority of the .ee domains (dark green) are hosted (blue pie) in the country, but we see a portion of them hosted in Germany, Netherlands, Hong Kong and the USA.

Cyber Attack Surface & Risk Profile: Estonia

Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

National Attack Surface Metrics

Attack Surface Risks (Overall)

Vulnerabilities

678.259 Total
1.966 Unique
27.388 Host
37.055 Applications

List of Vulnerabilities by Criticality and CVEs

Critical	131,819
High	243,217
Medium	274,459
Low	28,764

Top Vulnerabilities

All | Critical | High | Medium | Low

			Quantity
1	CVE-2023-48795	Medium	14,993
2	CVE-2023-51385	Medium	14,655
3	CVE-2023-38408	Critical	14,379
4	CVE-2021-36368	Low	11,274
5	CVE-2016-20012	Medium	11,208

Vulnerable Assets found in the Country's Cyberspace

6,400
Email Servers

11,841
Web Servers

931
Databases

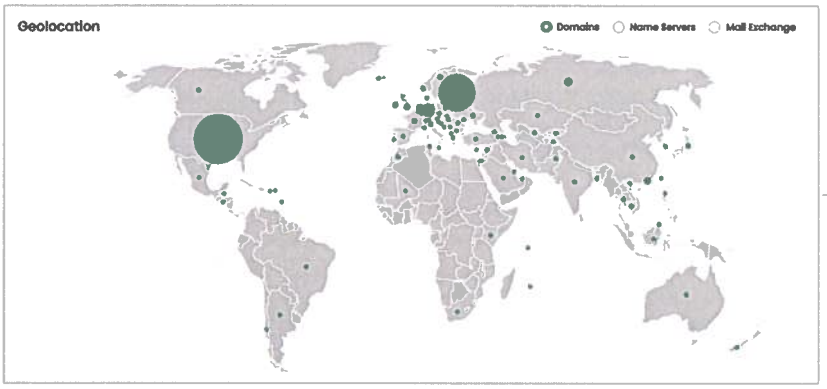
CYOBS
SEE THE CYBER

Cyber Attack Surface & Risk Profile: Estonia

Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

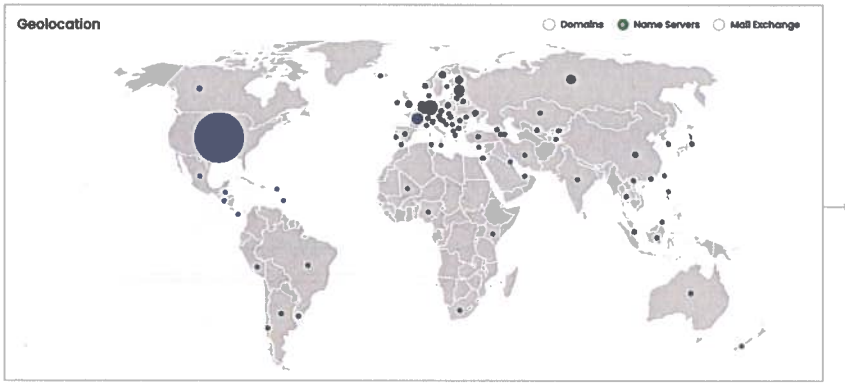
Nation's Cyberspace Geopolitical Dependency

Domains: **301.928**



Active Domains
202,658
202,658 Serving a service
301,295 SOA configured

Global spread of domain hosting globally.



Name Servers
16,348
14,938 Unique IP addresses
310,911 Namespaces with NS

Global spread of DNS server hosting globally.

Mail Exchange
71,155
15,333 Unique IP addresses
203,484 Namespaces with MX

Global spread of mail server hosting globally.

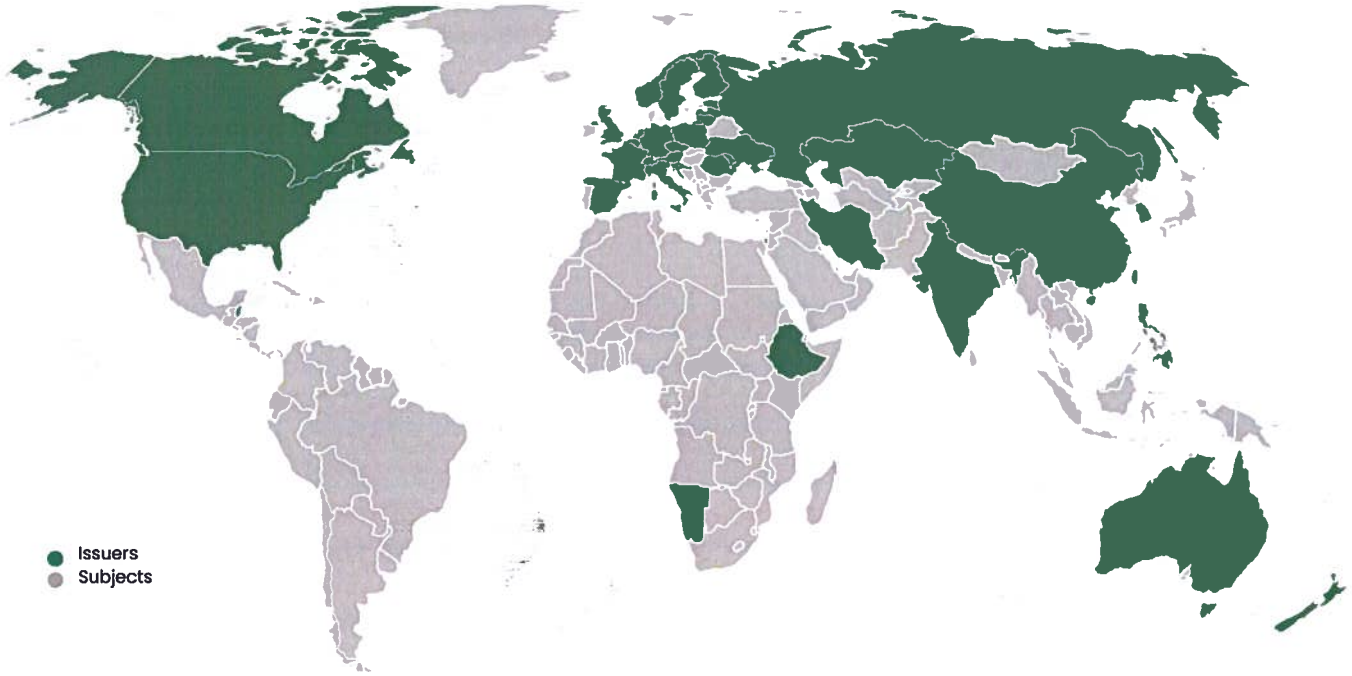
The more services, such as domains, DNS, and mail servers, are hosted outside the jurisdiction of a nation-state, the greater the dependence becomes. This also leads to an increased likelihood of eavesdropping, cyber espionage, and loss of control over the service and associated data.

Cyber Attack Surface & Risk Profile: Estonia

Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

National Trust & SSL Analytics

Certificates	**24.421**
Issuers	**4.733**
Services with certifications	**42.150**
Self-signed certificates	**24.637**
Expired certificates	**12.410**



Top Organizations

Issuers | Subjects

		Quantity
1	Let's Encrypt	5,061
2	Companyname	3,535
3	FASTVPS	2,386
4	Sectigo Limited	842
5	DigiCert Inc	433

CYOBS
SEE THE CYBER

Cyber Attack Surface & Risk Profile: Estonia

Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

Software & OS Landscape Detected at National Level

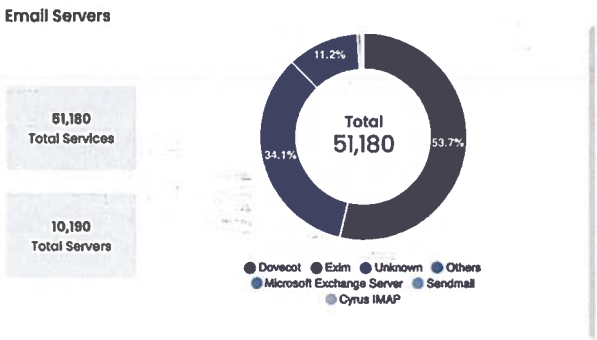
Unique software	**1.357**
Unique OS	**72**
Host exposing software	**31.124**
Host exposing OS information	**23.346**

Top Software

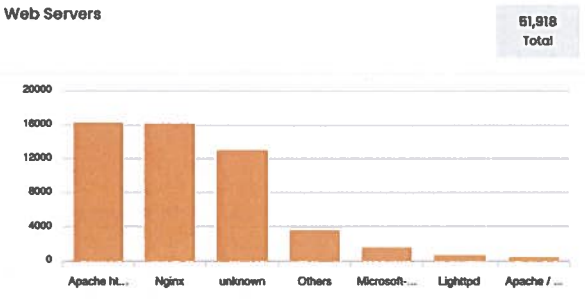
		Quantity
1	OpenSSH	14,801
2	Apache httpd	13,209
3	Nginx	10,935
4	Dovecot	7,342
5	Exim	6,290

Statistics and Detailed Views on Services Exposed Directly on the Internet

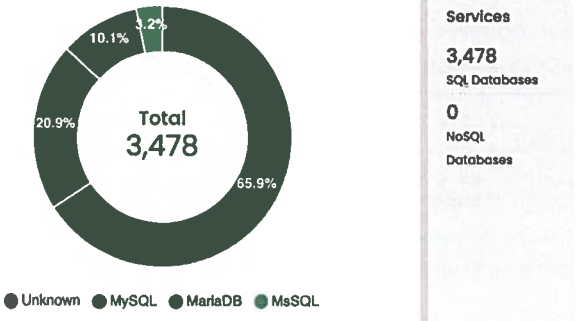
Email Servers



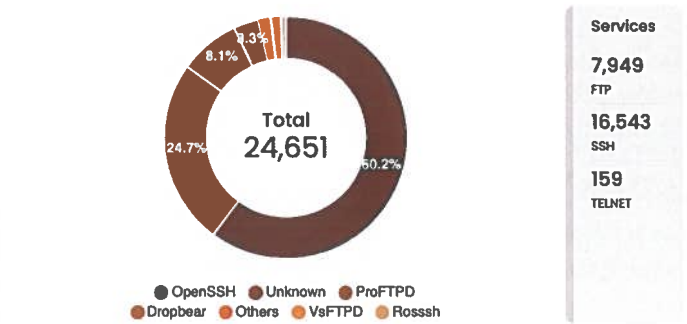
Web Servers



Databases



Remote Administration Interfaces (RAI)



Cyber Attack Surface & Risk Profile: Estonia

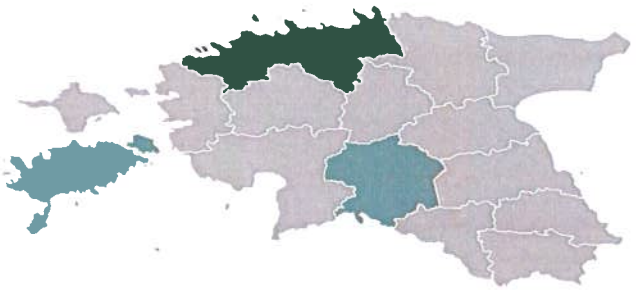
Scientific, non-intrusive scan as of July 2024 based on allocated IPv4 addresses and identified domains

Spotlight Risk - Dynamic Queries showing Vulnerable System from Specific CVE

EXPLORE RESULTS

vulnerability.cve = CVE-2023-38408 ×

Showing 1 to 10 of 14379 results.



CVE-2023-38408 - A vulnerability was found in OpenSSH (before 9.3p2 version). The PKCS#11 feature in the ssh-agent in OpenSSH has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system (the code in /usr/lib is not necessarily safe for loading into ssh-agent). This flaw allows an attacker with control of the forwarded agent-socket on the server and the ability to write to the filesystem of the client host to execute arbitrary code with the privileges of the user running the ssh-agent.

July 6, 2023: The initial advisory draft and patch were submitted to OpenSSH.

July 19, 2023: A coordinated disclosure and patch release were executed.

Top Locations

Name	Quantity
Harjumaa	6895
Ida-Virumaa	6855
Tartumaa	441
Parnumaa	50
Laanemaa	18

We found 14.379 vulnerable assets (CVE-2023-38408) in the cyberspace of Estonia.