




tet

Securing Latvia's digital tomorrow

Dmitrijs Nīkitins

Tet CTO

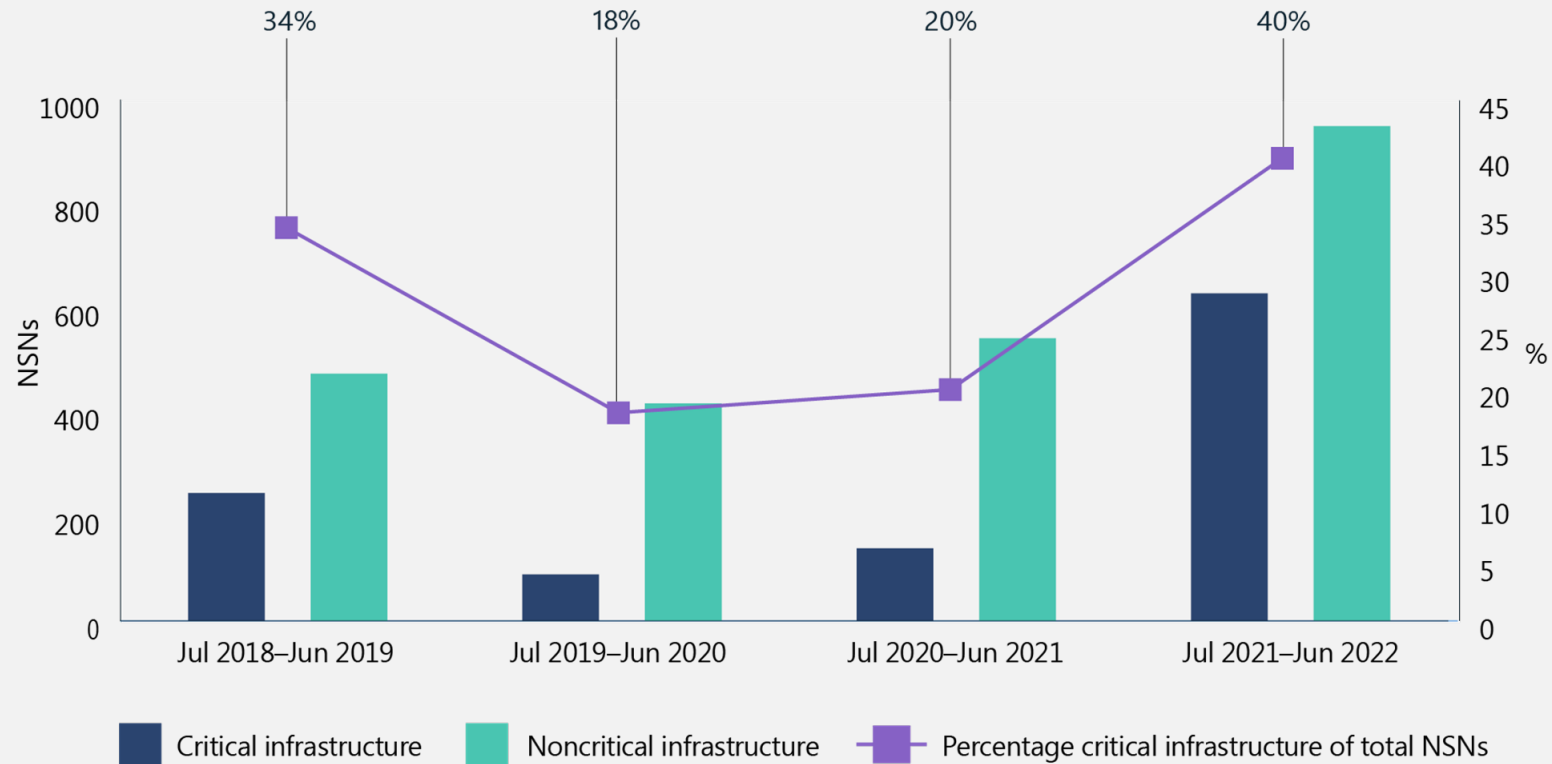


Critical infrastructure is the backbone of a nation's functioning, encompassing power grids, transportation systems, and financial institutions — all of which rely heavily on digital technologies.

A breach = catastrophic consequences for national security and stability.

During the past year, cyberattacks targeting critical infrastructure around the world jumped from **20%** of all nation-state attacks to **40%**.

Critical infrastructure trends



Source: Microsoft Digital Defense Report 2022

By 2025,

30%

of **critical infrastructure organizations** will experience a security breach resulting in the halting of a mission-critical system.

Our role

Tet plays a vital role in fortifying Latvia's digital resilience and security by:

safeguarding our own infrastructure (handling **50%** of internet traffic in the country)



safeguarding information space (providing **50%** of all TV subscriptions)



offering protection to local businesses and government (servicing **80%** of corporate segment companies)

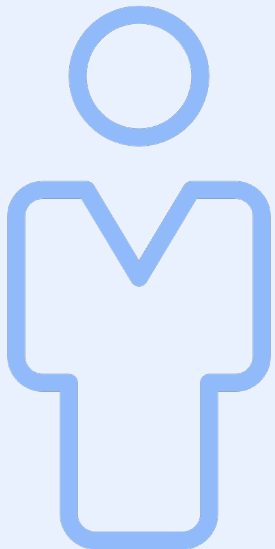


**Our goal is
to ensure the
digital security
of the country.**

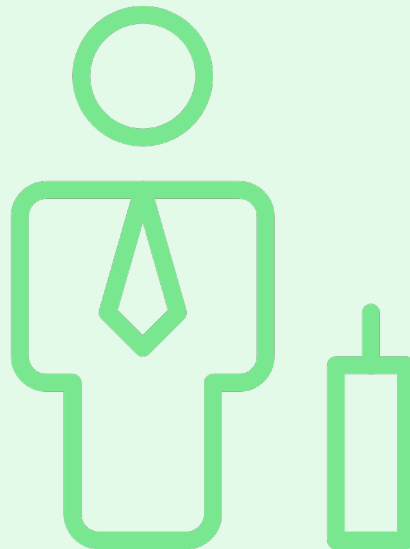


Securing the country by

Securing oneself



Securing
Latvian companies



Securing
Latvian society





SECURING ONESELF

- **One of our main tasks - protecting the integrity of data centres and the data within them.**
- **7 data centres** - only ones in Latvia with a Tier III certification.
- We verify and identify our data centre clients and respond quickly to breaches, disconnecting suspicious ones.
- Integrity and the way our data centre resources are used are crucial.

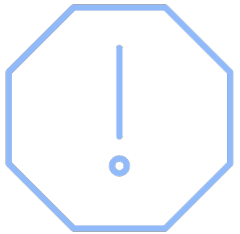




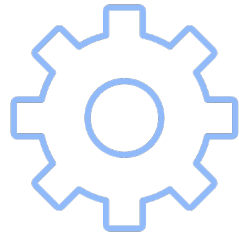
SECURING ONESELF

We are resilient and as strong as possible.

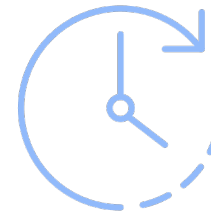
Providing
critical system
redundancy



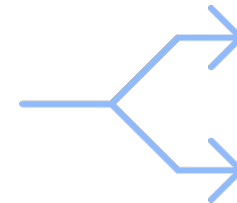
Maintaining
spare capacity



Working 24/7



Building
resilient
systems





SECURING ONESELF



Protecting the core – preventing DDoS attacks

2762 DDoS
attacks

27% classified
as significant

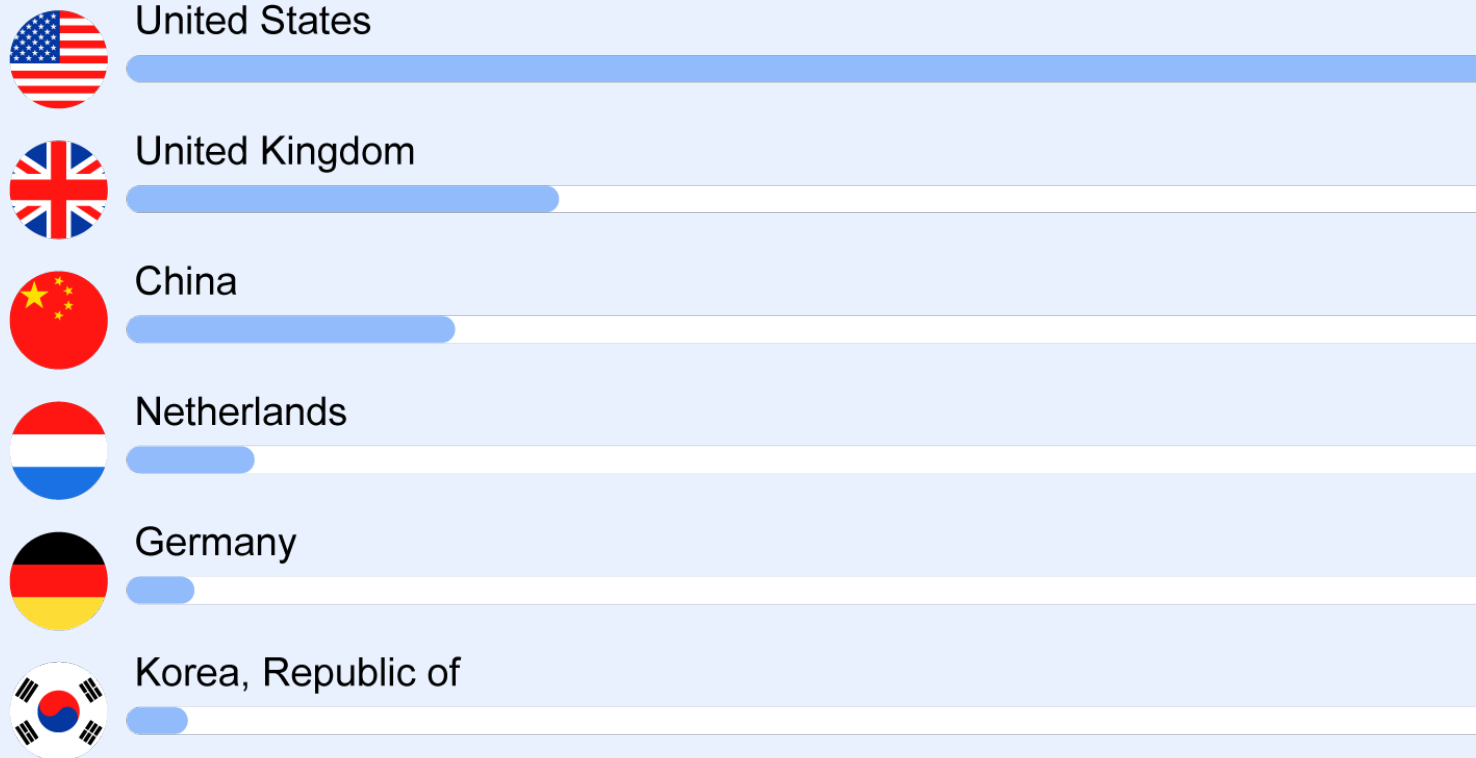
45% attacks are coming from
sources within Europe





SECURING ONESELF

Top attacking geolocations





SECURING LATVIAN COMPANIES

Cybersecurity Operations Centre or SOC provides a full range of cybersecurity management for large organizations in Latvia, which are also a part of the **national critical infrastructure** and offers essential services to society.



Educating the new generation

Tet school of digital security for pre-schoolers:
digitaladrosiba.lv



Cooperation with Riga Tech Girls and universities of Latvia to educate new IT and cyber security professionals

Sharing knowledge on cyber risks and ways to protect yourself and your business through media campaigns, free webinars, and the **annual cybersecurity forum, CyberShield**



Protecting the information space

Tet has blocked certain domains, including Russian websites and Russian TV channels that provide disinformation and false news.



Malware and phishing on the Internet

This year we have stopped 46,7M suspicious e-mails on reaching their targets.

From which 218 706 were virus containing e-mails.



**All this sounds
good, right?**

We are battling symptoms, not the root cause.

We mitigate DDoS attacks, filter out spam and virus emails, and block fraudulent websites on the Internet. However, this is an ongoing battle with repercussions - **blocking one domain results in a new one.**

Direct action is needed against the owner or controller of these harmful resources. That requires support of authorities and changes in the law.



For example

+44 (2045) 77-00-00 Abuse

We respond to all inquiries and complaints

This company is a white label for [PQ.Hosting](#), we are not a bulletproof hosting, we provide information to the police.

[Go to PQ.Hosting](#)

**CERTIFICATE OF INCORPORATION
OF A
PRIVATE LIMITED COMPANY**

Company Number **13206017**

The Registrar of Companies for England and Wales, hereby certifies that

STARK INDUSTRIES SOLUTIONS LTD

is this day incorporated under the Companies Act 2006 as a private company, that the company is limited by shares, and the situation of its registered office is in England and Wales

Given at Companies House, Cardiff, on **10th February 2022**

Unified action

- Establishment of a **centralized cyber risk management system** for cross-border collaboration and immediate response to cyber threats accross Europe
- **Empower companies to combat cyberattacks** by enabling quick blocking of fraudulent webpages and stopping DDoS attacks coming from local sources



Take action against the gray area companies

Information space

There are still many unlicensed providers and illegal broadcasters (satellites, illegal overhead lines etc.) providing untraceable content.

For situation to improve, we believe that government of Latvia must take more stricter approach.



In a crisis - one alone is not a warrior

Tet has developed its own crisis plan, like every company, that is a part of critical infrastructure. But these plans are **not coordinated between different companies**, instead developed based on assumptions.

Companies need to work together to create a comprehensive crisis management and disaster prevention plan.



Taking steps on educating our society

1 million
euros

Is the amount of money that is
defrauded from the citizens of Latvia
every month



3 steps to a secure cyberspace in Latvia

1
Legislation

2
Society

3
**Business
sector
support**

tet

Thank you!

The background features several overlapping, semi-transparent geometric shapes. A large light blue shape is prominent in the lower-left and center. A smaller green shape overlaps its top-right corner. A yellow shape is in the lower-right, overlapping a purple shape. A large beige shape is in the upper-right, overlapping the blue and green shapes. The overall composition is modern and minimalist.