ADAPTATION OF THE NIS2 DIRECTIVE IN SECURITY TECHNOLOGIES

Kārlis Apalups, MBA
ZEVS
BA "Turība"

ZEVS SECURITY

Agenda

01

Security risks

02

NIS2

03

Strategic perspective

ZEVS SECURITY

SECURITY RISKS

ZEVS SECURITY

Sources of risks

Reasons why security people do not sleep at night

1

Russia

2

People's Republic of China

3

Terrorism & Organised crime

01 Russia

- Potential future NATO - Russian war
- "Wind of Change" FSB letters
- Modus operandi - exploit security systems

ZEVS SECURITY

THE Sun UK Edition

News Sport Fabulous TV Showbiz Money Travel Health

UK News World News Health News Politics Opinion

News > World News

TWISTED MIND How 'deluded' Putin thought Ukraine invasion would break up Nato & have West bowing down to Russia, leaked docs show

euronews. Latest Europe World EU Policy Business Euroviews Next Green Health Cultur

my.europe > Europe News

Russia could attack NATO by end of decade, German intelligence chief warns

Copyright Alexander Zemlianichenko/Copyright 2024 The AP. All rights reserved.

RadioFreeEurope RadioLiberty

UKRAINE

Investigation: China's Hikvision, Dahua Security Cameras Heighten Risks Of Russian Attacks On Ukraine

February 08, 2024 14:18 GMT

By Kyrylo Ovsyaniy

Ukraine's security service says Russia can hack certain security cameras for the purpose of gathering intelligence, which can be used to carry out attacks on its western neighbor. (file photo)

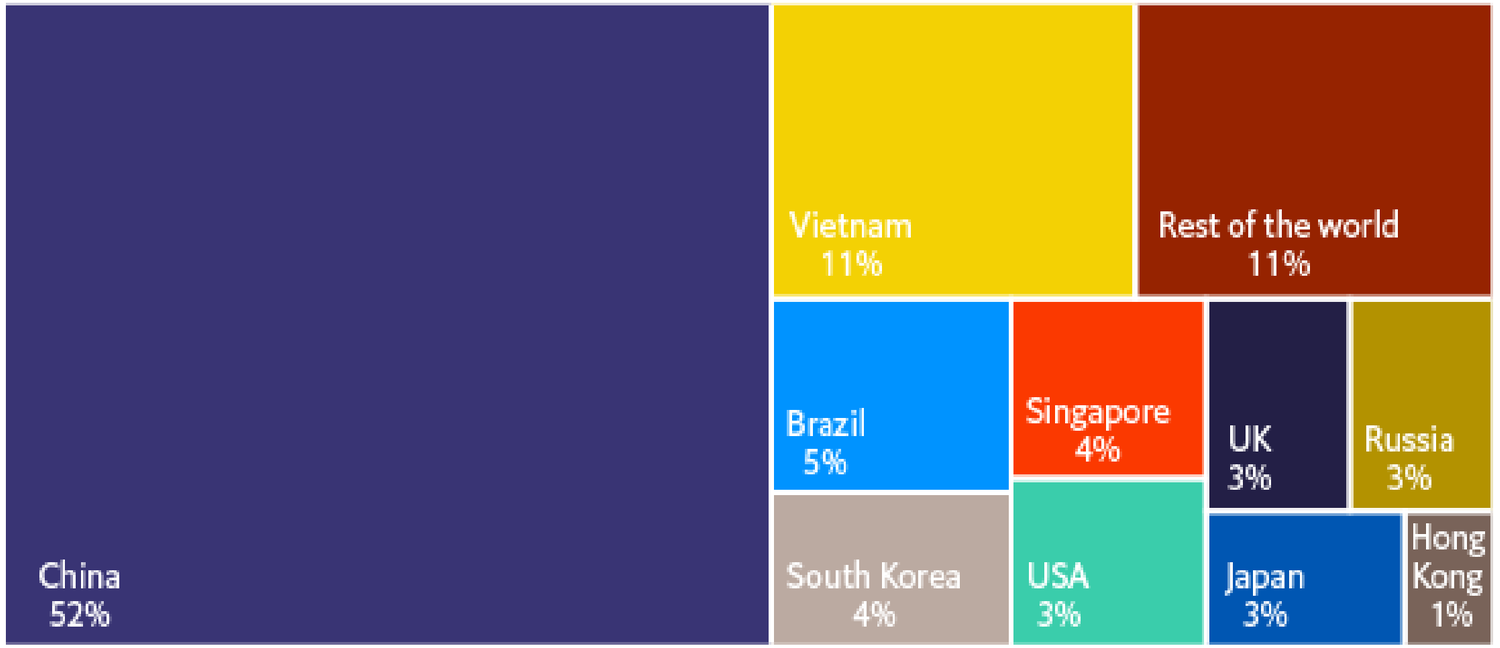
02 China

- Ambitions against Taiwan (+ Russian ally)
- Advanced (cyber)espionage (economy-oriented)
- Controls supply chains for electronics

ZEVS SECURITY

China accounts for half of the strategic imports the EU is highly dependent on

(share of import value by origin of the 137 strategic products the EU is most dependent on)



Source: European Commission, based on BACI database.

BBC

Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live

Mystery of alleged Chinese hack on eve of Ukraine invasion

7 April 2022

Share Save

Gordon Corera
Security correspondent, BBC News

Getty Images

Allegations of Chinese cyber activity as the recent conflict broke out in Ukraine have been emerging.

03

Terrorism & Organised crime

- Clashes of ideologies
- Digitalisation of organised crime
- Cooperation with national threat actors

ZEVS SECURITY

ZEVS SECURITY

NIS2

ZEVS SECURITY

REASONS FOR THE INTRODUCTION OF NIS2

01 Insufficient cyber resilience for EU companies

02 Uneven cyber resilience between Member States and sectors

03 There is no common understanding of the EU's threats

04 There is a lack of a common crisis response between Member States.

How is the security industry affected?

ZEVS SECURITY

The cybersecurity industry by itself, but also:

1

Internal security structures

Important and essential service providers

2

Security companies

Security service providers (Medium or large - Important)

and security system installers/servicers

(Large – Essential / Medium - Important)

3

Accredited training centres

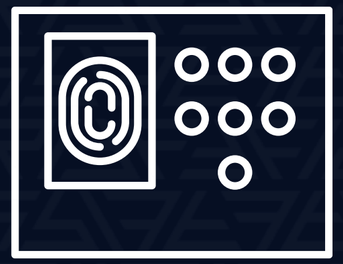
Accredited training centres (regardless of their size) processing personal data in educational information systems

What security technologies does NIS2 cover? (Article 22 of the NCSL)

ZEVS SECURITY

The law uses the term "Network and Information System"

Electronic communications network



Devices carrying out digital data processing

Digital data processed..., for protection purposes.

Simplisticly speaking...
applies to all security technologies

ZEVS SECURITY

ZEVS SECURITY

NIS2 restricts purchases of equipment and services from EU/EEA/NATO ONLY

Category A systems

All types of technical resources and maintenance (Hence, all equipment and all services from EU/EEA/NATO)

Category B systems

Network equipment (routers, switches, etc.), cyber defence systems (IDS, ISP, Antivirus, etc.) as well as (physical) protection and surveillance services and equipment of these systems only from EU/EEA/NATO (So, Hikvision, Dahua, etc. should not be used to protect these systems)

ZEVS SECURITY

STRATEGIC PERSPECTIVE

Key things to expect with NIS2

ZEVS SECURITY

Cyberphysical convergence

IT and security department must take care of security together

EU/EEA/NATO orientation

From the point of view of both long-term security risks and NIS2 requirements, a reorientation in the acquisition of security technologies from partner countries.

Physical security "upgrade"

The emphasis on cybersecurity will increase in the physical security sector, thereby reducing the vulnerability of the service provider

Innovation

The new requirements will boost innovation in the security sector, which in turn can also lead to new cyberphysical products

ZEVS SECURITY

Let's get ready for evolution!

Thank you for your attention.

karlis@zevs.lv | +371 26622419