Towards a Digital Single Market for NIS Products and Services - FINDINGS

Simon Forge| SCF Associates Ltd – Colin Blackman| CEPS

Athanasios Drougkas, Dimitra Liveri | ENISA

Validation Workshop| Brussels| 12 October 2016

European Union Agency for Network and Information Security

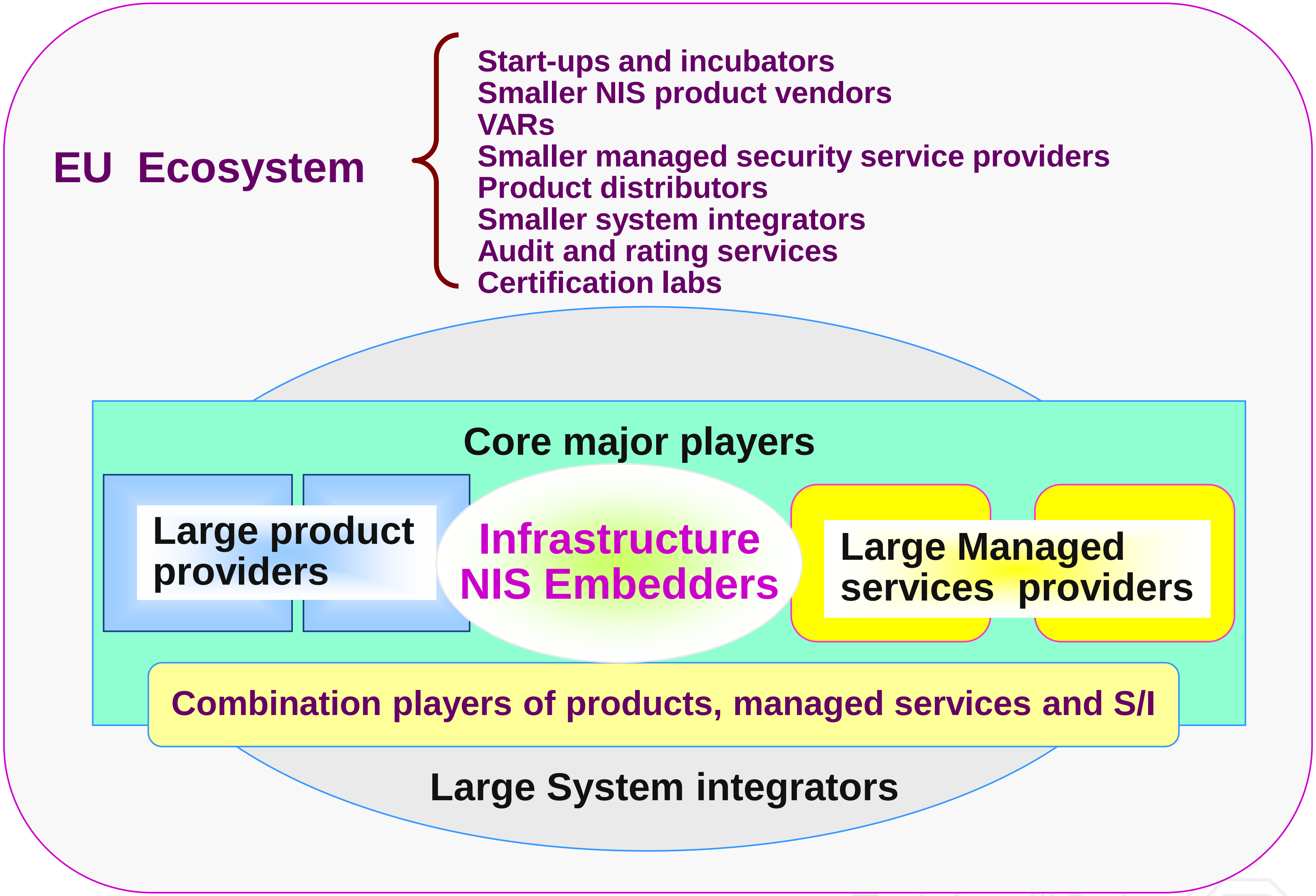
Agenda

1. Study overview – objectives – scope – methods
2. The EU’s Current NIS Market Landscape
3. Threats to the EU Economy and Society
4. Key drivers for the NIS market
5. Strengths and Weaknesses of EU suppliers
6. The Resulting Industry structure
7. Characteristics of Successful Suppliers in the EU Market
8. Six Overall Lessons from the Study

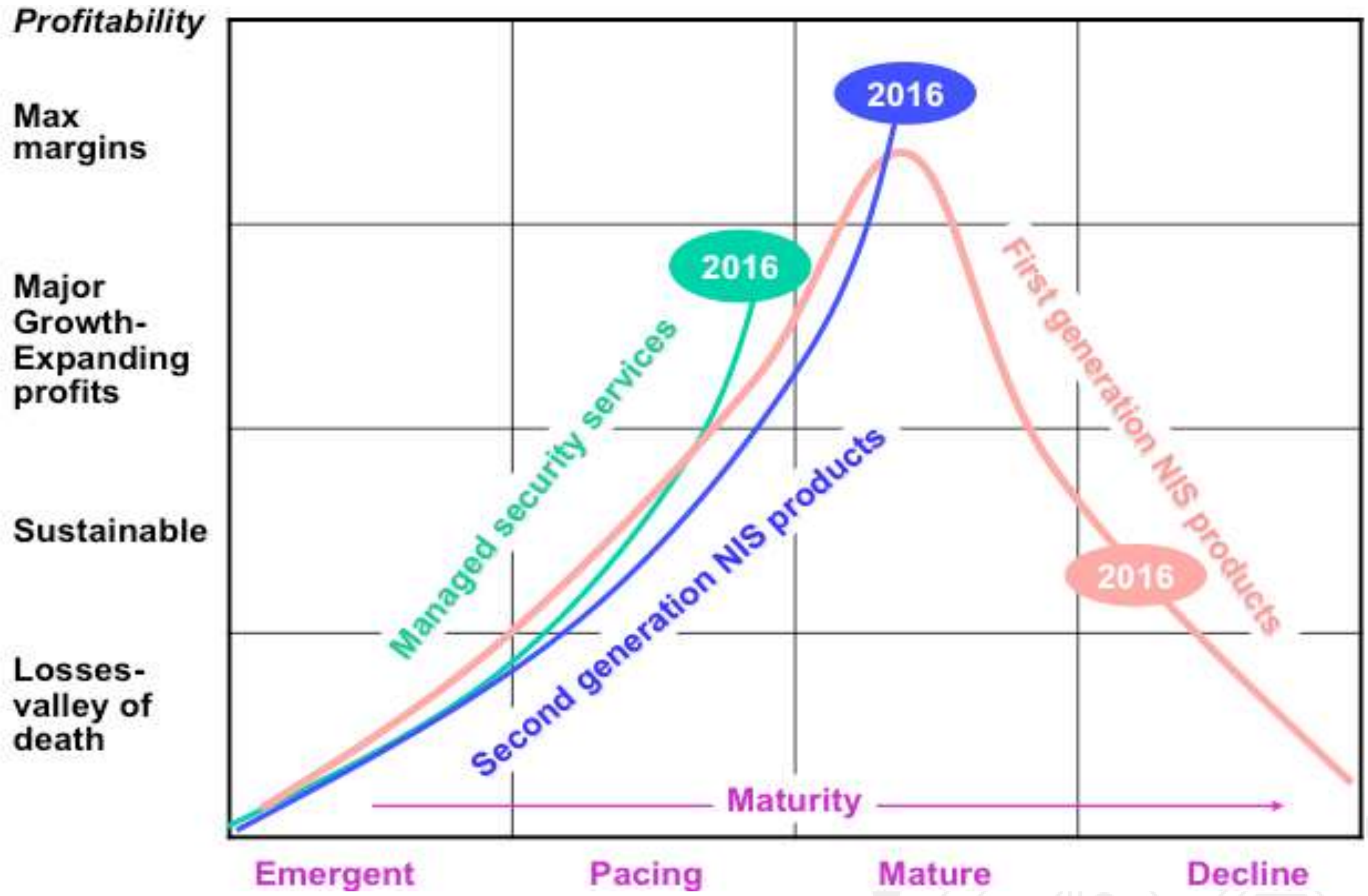
Study Overview

- Objectives
  - Understand which NIS products/services are successful in 5 specific sectors, whether from EU suppliers or not and to find ways to improve the growth and market penetration of EU suppliers
  - Recommendations for development of a more effective European NIS industry to protect the DSM
- Scope
  - The 5 specific sectors
  - Services and products
  - The EU market
  - Target audience - policy makers and end-user senior management in the private sector and management in the NIS sector
- Methods
  - Interviews with users in 5 sectors:- Online banking, Online marketplaces, Online media, Cloud storage, Wireless telecoms
  - Interviews with NIS suppliers
  - Desk research on market background
  - Online Survey

The EU NIS Ecosystem


EU Ecosystem
Start-ups and incubators
Smaller NIS product vendors
VARs
Smaller managed security service providers
Product distributors
Smaller system integrators
Audit and rating services
Certification labs
Core major players
Large product providers
Infrastructure NIS Embedders
Large Managed services providers
Combination players of products, managed services and S/I
Large System integrators

Maturity by Product/service Segment



The Demand Side by sector - Online Banking

Products	Services
•Database encryption – especially for customer records, with effective key management •Mobile devices - end to end encryption with customer identity and access management with strong authentication •Standard point product sets – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools •Automated remote back-up and recovery for security purposes (e.g. for ransomware) •Evidential and integrated SIEM (security information and event management)	•Threat intelligence •Managed security services with intrusion detection/protection/recovery services, 24x7 and EFT (Electronic Funds Transfer) surveillance •Audit services for rating and certification of corporate security levels with gap recognition and banking standards conformance checks •Sector-wide comparison service for security levels, with ranking •Business recovery services/ SIEM as a service •Cyber attack test exercises •Incident sharing service for the whole sector

The Demand Side
- Online Marketplaces

Products	Services
•Database encryption – especially for customer records, with effective key management •Mobile devices - end to end encryption with customer identity and access management with strong authentication •Standard point product sets – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools •Evidential and integrated SIEM	•Threat intelligence •Managed security services with intrusion detection/protection/ recovery services, 24x7 •Cyber attack test exercises •SIEM as a service

The Demand Side - Cloud Storage

Products	Services
•Database encryption – for all stored data (especially customer records); key management •Standard point product sets – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools •Automated infrastructure configuration management (OS and application patching) •Evidential and integrated SIEM •Federated identification and authentication	•Threat intelligence •Managed security services with intrusion detection/protection/ recovery services, 24x7 •Life cycle risk analysis with continuous tests for malfunction with hacking checks and incident reporting, especially data breaches •Cyber attack test exercises

The Demand Side - Wireless Telecommunications

Products	Services
•Database encryption – for customer records with effective key management •Automated configuration and patching manager (possibly using AI) for maintenance of global scale networks (could be an external service) •Standard point product sets – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools	•Threat intelligence •Managed security services with intrusion detection/protection/recovery services, 24x7 •SIEM as a service

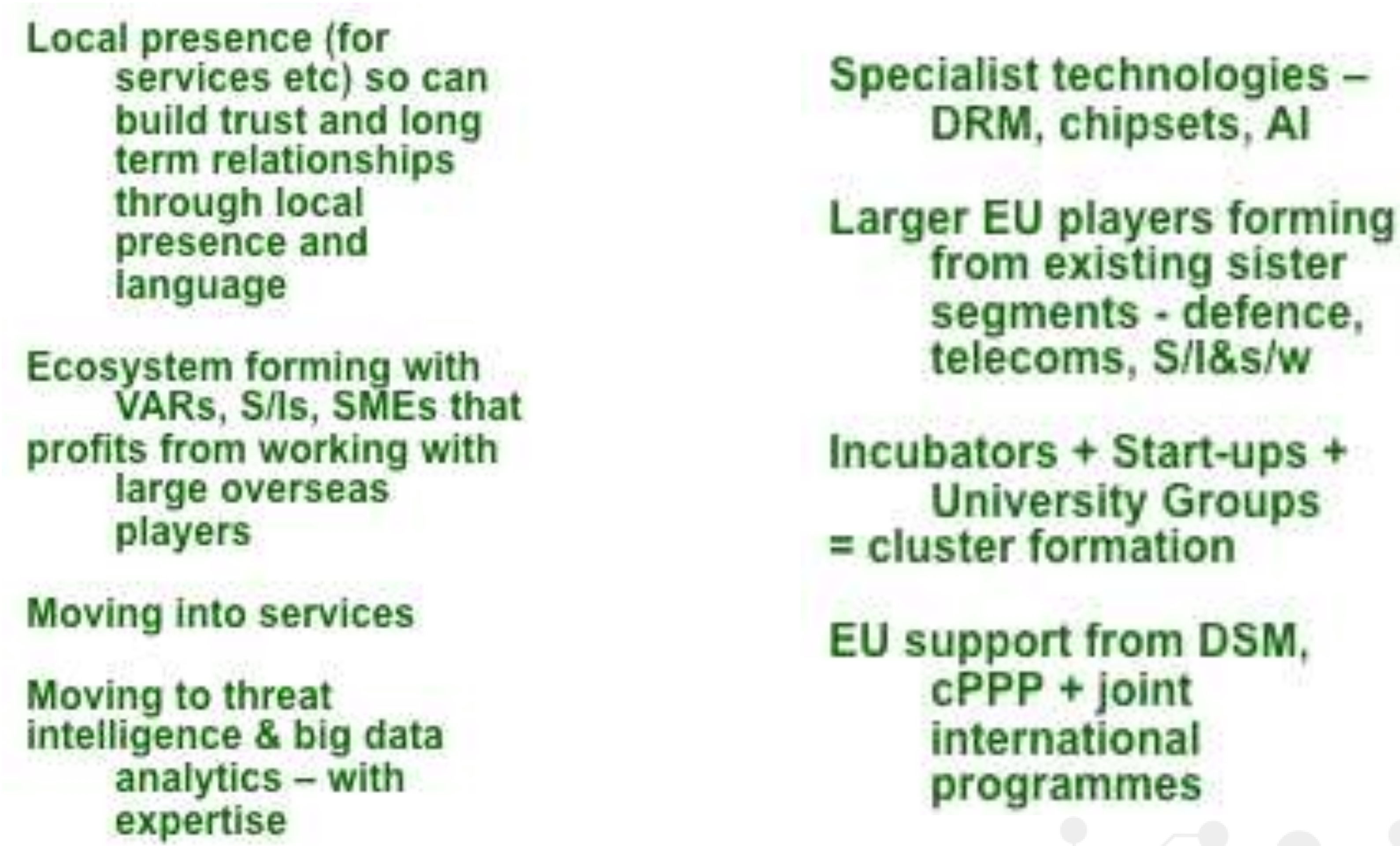
The Demand Side - Online Media

Products	Services
•Database encryption – for customer records with effective key management •Content data base encryption with effective key management •Content anti-theft software – for DRM and embedded watermarking •Secure multi-screen online distribution for mobile and other devices (STBs, smart TVs, game consoles, etc) •Identity and access management with strong authentication for customer access control, for OTT VOD streaming, audio, etc •Embedded and external smart TV hardware decoders and chipsets for conditional access •Standard point product sets – firewalls, anti-virus, attack alert and identification tools including IDS/IPS products and anti-DDOS tools	•Threat intelligence •Global managed security services with intrusion detection/protection/recovery services, 24x7 Digital forensic investigation/ SIEM as a service •Evaluation of security level of firmware, hardware and software •Device penetration testing •Security training and outsourced expert staff

Key Drivers for the NIS Market

- The IoT will have major security problems
- Mobile services and mobile apps are insecure
- Migration to outsourcing disrupts protection
- Software as a Service (SaaS)
- Increasing need for cryptography and better encryption management
- Improved authentication is needed
- Lack of effective public key infrastructure tools
- Verification and audit capabilities needed for Software Defined Networks
- Virtualisation - a further major market opportunity

SWOT Analysis - Strengths



Local presence (for services etc) so can build trust and long term relationships through local presence and language

Ecosystem forming with VARs, S/Is, SMEs that profits from working with large overseas players

Moving into services

Moving to threat intelligence & big data analytics – with expertise

Specialist technologies – DRM, chipsets, AI

Larger EU players forming from existing sister segments - defence, telecoms, S/I&s/w

Incubators + Start-ups + University Groups = cluster formation

EU support from DSM, cPPP + joint international programmes

SWOT Analysis - Weaknesses

Fragmented EU market – smaller players divided by language so lack critical mass of finance for EU and overseas expansion

Most EU players small and many are start-ups – few have EU wide presence

Fragmented national certification - not one certificate for Europe

Most underlying technology used in EU from USA, especially key software

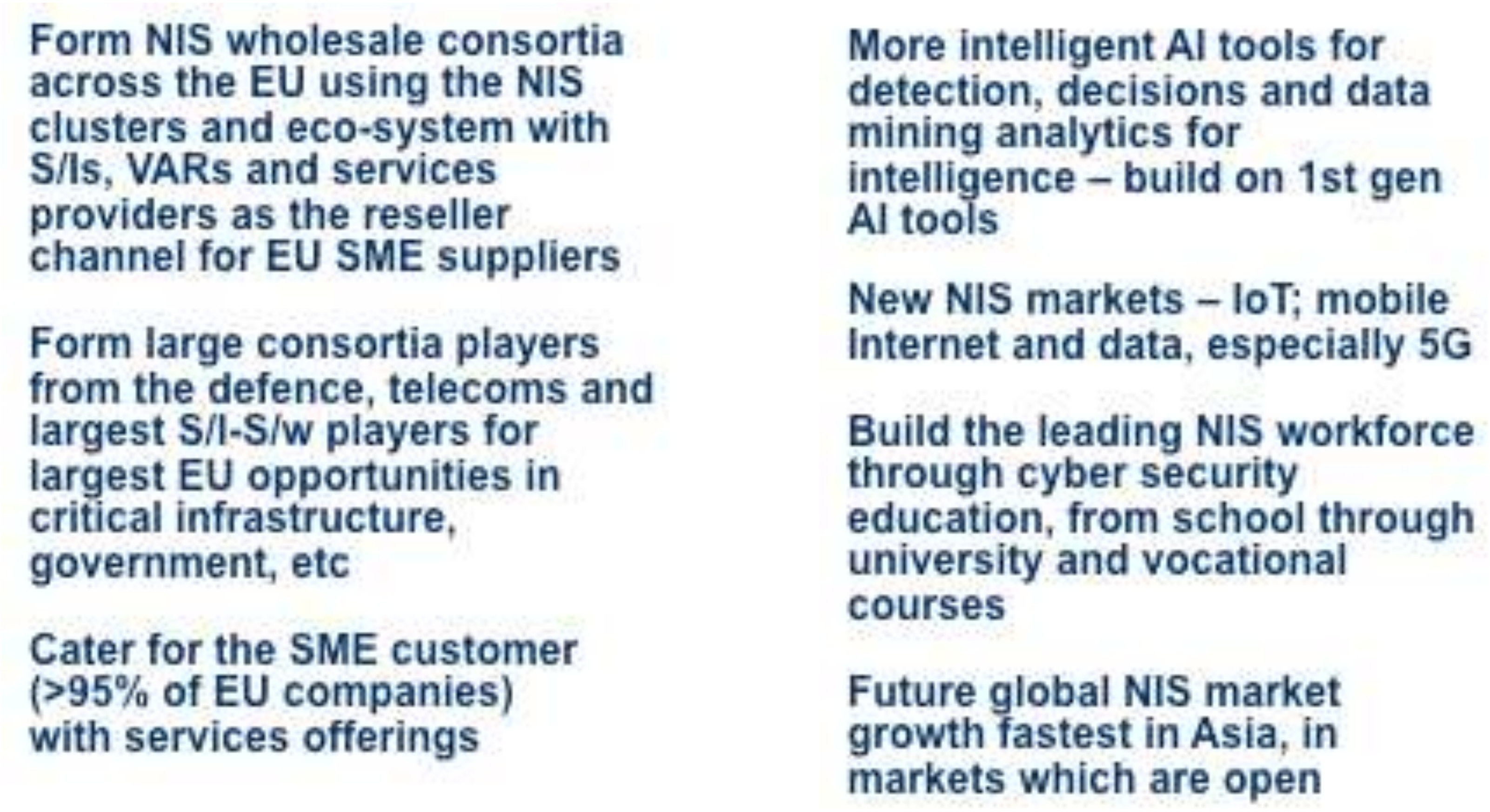
Lack of seed funding & commercial industrialisation support

EU NIS firms are relatively poor at marketing

Lack of support for exports to developing world

In these conditions, some EU NIS players have less ambition to expand globally – so await their buy-out

SWOT Analysis - Opportunities



Form NIS wholesale consortia across the EU using the NIS clusters and eco-system with S/Is, VARs and services providers as the reseller channel for EU SME suppliers

Form large consortia players from the defence, telecoms and largest S/I-S/w players for largest EU opportunities in critical infrastructure, government, etc

Cater for the SME customer (>95% of EU companies) with services offerings

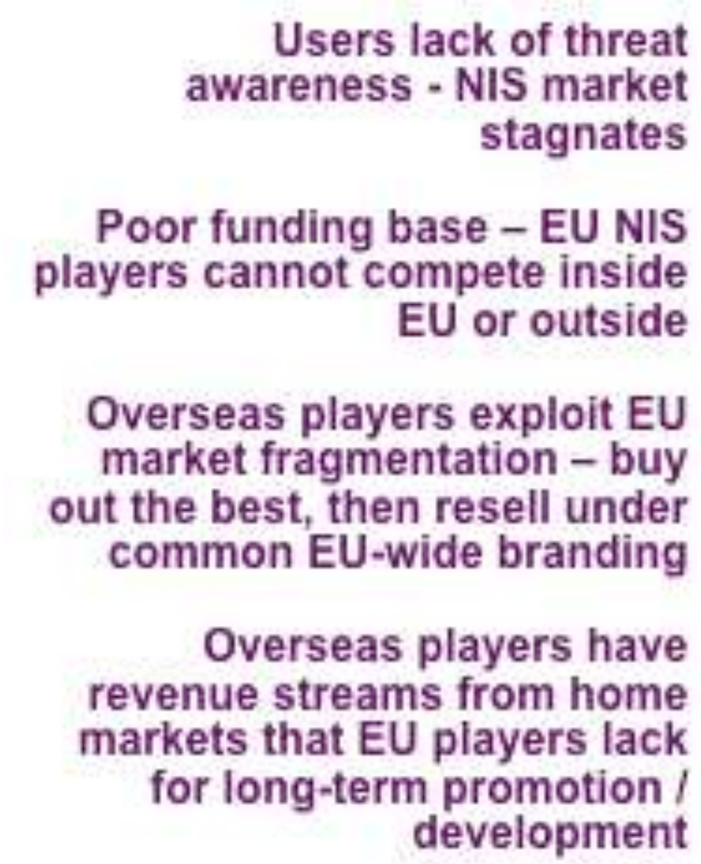
More intelligent AI tools for detection, decisions and data mining analytics for intelligence – build on 1st gen AI tools

New NIS markets – IoT; mobile Internet and data, especially 5G

Build the leading NIS workforce through cyber security education, from school through university and vocational courses

Future global NIS market growth fastest in Asia, in markets which are open

SWOT Analysis - Threats

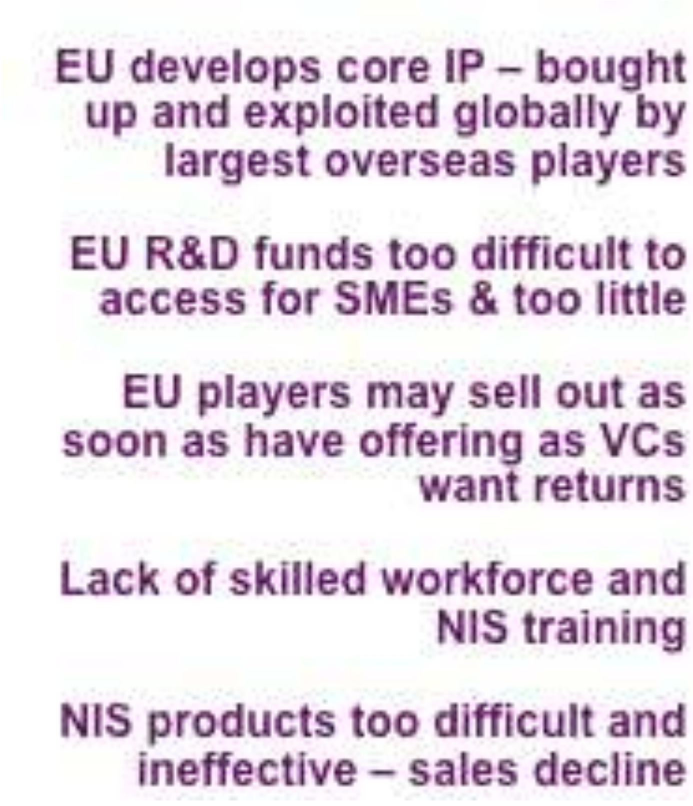


Users lack of threat awareness - NIS market stagnates

Poor funding base – EU NIS players cannot compete inside EU or outside

Overseas players exploit EU market fragmentation – buy out the best, then resell under common EU-wide branding

Overseas players have revenue streams from home markets that EU players lack for long-term promotion / development



EU develops core IP – bought up and exploited globally by largest overseas players

EU R&D funds too difficult to access for SMEs & too little

EU players may sell out as soon as have offering as VCs want returns

Lack of skilled workforce and NIS training

NIS products too difficult and ineffective – sales decline

The Future Industry Structure

- A larger service segment than point products
- A structure focused on relationships between vendors, both EU and headquartered outside
- Faster threat intelligence and detection
- More CERTs as a key industry resource
- Focus on user protection in online financial transactions, identity theft and use of mobile devices

Characteristics of Successful Suppliers in the EU Market (1)

- Successful suppliers operate in many sectors
- Offer both services and some products, or services only
- Invest in new technology for greater intelligence or automation
- Use the EU ecosystem for multiple channels to market, with emphasis on marketing and presence building
- Privacy is a USP for the EU NIS industry, which other regions do not have to the same extent.

Characteristics of Successful Suppliers in the EU Market (2)

- Successful suppliers nurture start-ups and incubators
- Cope with a fragmented EU market often divided by language and culture
- Take a more human-centric approach to security, for instance in retail banking
- Integrate with the rest of the global supply chain either as a service provider, systems integrator or distributor or product OEM supplier

Overall Lessons from the Study (1)

- EU market demand is fragmented and does not have the USA's single market or investment capital
- But reality is complex – some member states lag but some are leading the way, and some suppliers are at the forefront
- Many users are not aware of the risks – especially SMEs
- Move towards holistic rather than point solutions
- Indirect channels strategy of the major global product vendors opens the door for EU service providers

Overall Lessons from the Study (2)

- VARs and SIs are now moving more into managed security services

- Strongest future players in the EU NIS industry are likely to be based on software services and systems integration

- Players in the VAR & S/I segments see overseas product suppliers as partners not competitors

- A significant brake on growth is recruiting skilled personnel

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu