NTNU

Perspectives on research and development in cyber security in Europe and beyond

Sokratis K. Katsikas
Center for Cyber & Information Security
Norwegian University of Science & Technology
sokratis.katsikas@ccis.no
sokratis.katsikas@ntnu.no

Center for Cyber and Information Security

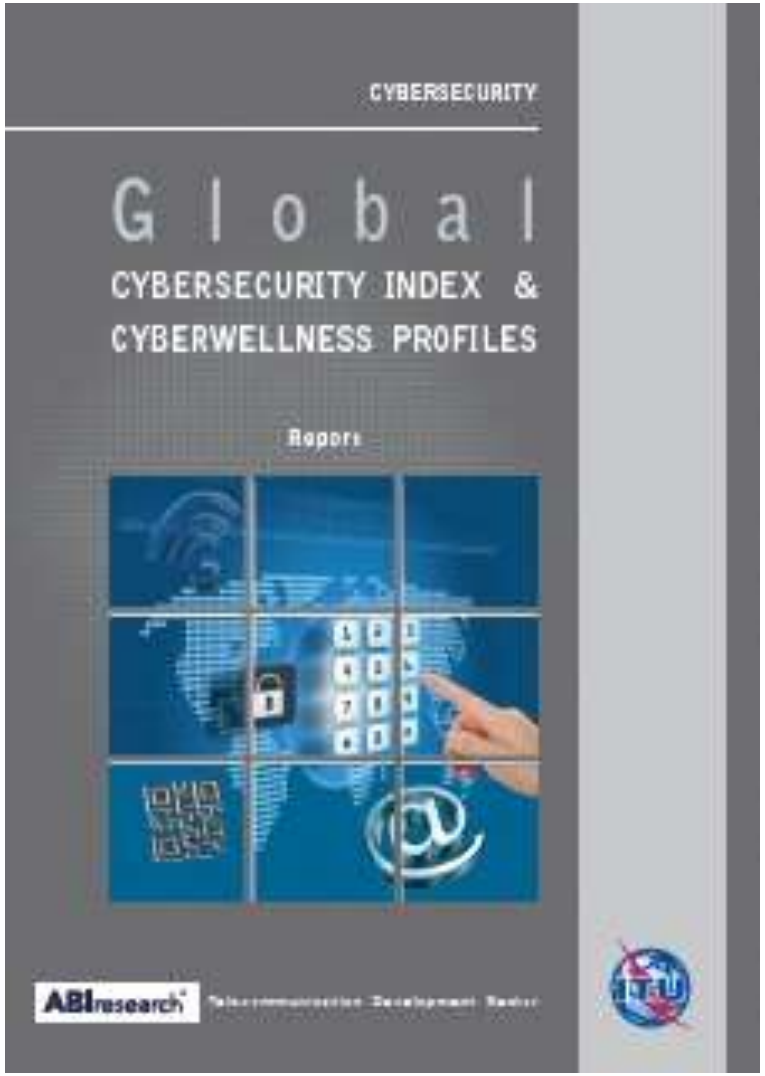
NTNU

- Largest University in Norway, 39000 students, approximately 400 PhD dissertations per year
- 4 Nobel laureates
- 120 research labs, more than 90 spinoffs
- 14 faculties and 70 departments and divisions
- Operating income: NOK 7.6 billion.
- FTE: 6700, of which 4053 are in teaching, research and outreach positions (39 % female).

Center for Cyber and Information Security

How well does a country stand in cybersecurity?

http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf



Criteria

- LEGAL MEASURES
  - CRIMINAL LEGISLATION
  - REGULATION AND COMPLIANCE
- TECHNICAL MEASURES
  - CIRT
  - STANDARDS
  - CERTIFICATION
- ORGANIZATION MEASURES
  - POLICY
  - ROADMAP FOR GOVERNANCE
  - RESPONSIBLE AGENCY
  - NATIONAL BENCHMARKING
- CAPACITY BUILDING
  - STANDARDISATION DEVELOPMENT
  - MANPOWER DEVELOPMENT
  - PROFESSIONAL CERTIFICATION
  - AGENCY CERTIFICATION
- COOPERATION
  - INTRA-STATE COOPERATION
  - INTRA-AGENCY COOPERATION
  - PUBLIC SECTOR PARTNERSHIP
  - INTERNATIONAL COOPERATION

Latvia: Global and regional ranking

Global Cybersecurity Index & Cyberwellness Profiles

Country	Index	Global Rank
Austria*	0.676	6
Hungary*	0.676	6
Israel*	0.676	6
Netherlands*	0.676	6
Singapore	0.676	6
Latvia*	0.647	7
Sweden*	0.647	7
Turkey		

Table 7: Europe region ranking by index

Europe	Legal	Technical	Organizational	Capacity Building	Cooperation	Index	Regional Rank
Norway*	1.0000	0.6667	0.7500	0.8750	0.5000	0.7353	1
Estonia*	1.0000	0.6667	1.0000	0.5000	0.5000	0.7059	2
Germany*	1.0000	1.0000	0.6250	0.6250	0.5000	0.7059	2
United Kingdom	1.0000	0.6667	0.7500	0.7500	0.5000	0.7059	2
Austria*	1.0000	0.3333	0.8750	0.7500	0.5000	0.6765	3
Hungary*	1.0000	0.6667	0.7500	0.6250	0.5000	0.6765	3
Israel*	1.0000	0.6667	0.6250	0.7500	0.5000	0.6765	3
Netherlands	0.7500	0.5000	0.8750	0.6250	0.6250	0.6765	3
Latvia*	1.0000	0.6667	0.7500	0.5000	0.5000	0.6471	4
Sweden*	0.7500	0.6667	0.6250	0.6250	0.6250	0.6471	4
Turkey	0.5000	0.6667	0.7500	0.7500	0.5000	0.6471	4
Finland	0.5000	0.6667	0.8750	0.5000	0.5000	0.6176	5
Slovakia	1.0000	0.6667	0.8750	0.2500	0.5000	0.6176	5
Denmark*	1.0000	0.6667	0.5000	0.5000	0.5000	0.5882	6

Why enhance cyber security capacity and capabilities?

- Risks to the economy and the society
  - Number of digital personal devices rapidly increasing, IoT, increasing connectivity, hence increased dependence on ICT
  - New cyber threats and vulnerabilities, with increased impact on critical infrastructures and societal functions
  - Cyber world easier to attack than the physical world
  - Need to balance security and privacy
- Digital sovereignty and autonomy
  - US leader in the global market – Europe lags behind
  - Non EU and non US manufacturers
- The economy and the market
  - Need to support the vision of the Digital Single Market
  - Need to develop the cybersecurity market and industry

The European industry perspective

- Make the EU more trustworthy and digitally secure
  - Level Playing Field
  - European cybersecurity monitoring and advising
  - Additional regulatory measures
- Support the successful development of European cybersecurity champions
  - Legislation
  - Security standards
  - European cybersecurity labels
- Cooperation between European Member States
- Supporting ecosystem for cybersecurity
  - Through academic and research involvement
  - Through policy and investment instruments

Recomendations on Cybersecurity for Europe", a Report to M. Günther H. Oettinger, European Commissioner for Digital Economy and Society. Study report compiled by European cybersecurity Industry Leaders. 2016.

Priority areas for action

- Information sharing
- Public Private Partnership
- Collaboration between Insurance sector and Cybersecurity industry players
- Cybersecurity by design
- Competitiveness and standardization / certification
- Support R&D
- People / Talent management
- European Cybersecurity Situation Centre & National Cybersecurity Situation Centre
- Certification of Service Providers (IT and Cybersecurity professional services)
- SCADA cybersecurity
- Digital Identity management
- Data Encryption
- Labels

Cybersecurity research and innovation: Research priorities

- Individuals' Digital Rights and Capabilities (Individual layer)
- Resilient Digital Civilisation (Collective layer)
- Trustworthy (Hyperconnected) Infrastructures (Infrastructure layer)
  - ICT Infrastructure
  - Smart Grids
  - Transportation
  - Smart Buildings in Smart Cities
  - Industrial Control Systems, including SCADA, in selected sectors (Water, Food/Agriculture, Nuclear, and Chemical Operation)
  - Public Administration and Open Government
  - Healthcare Sector
  - Automotive / Electrical Vehicles
  - Insurance
  - General Privacy Aspects for all Infrastructure Sectors

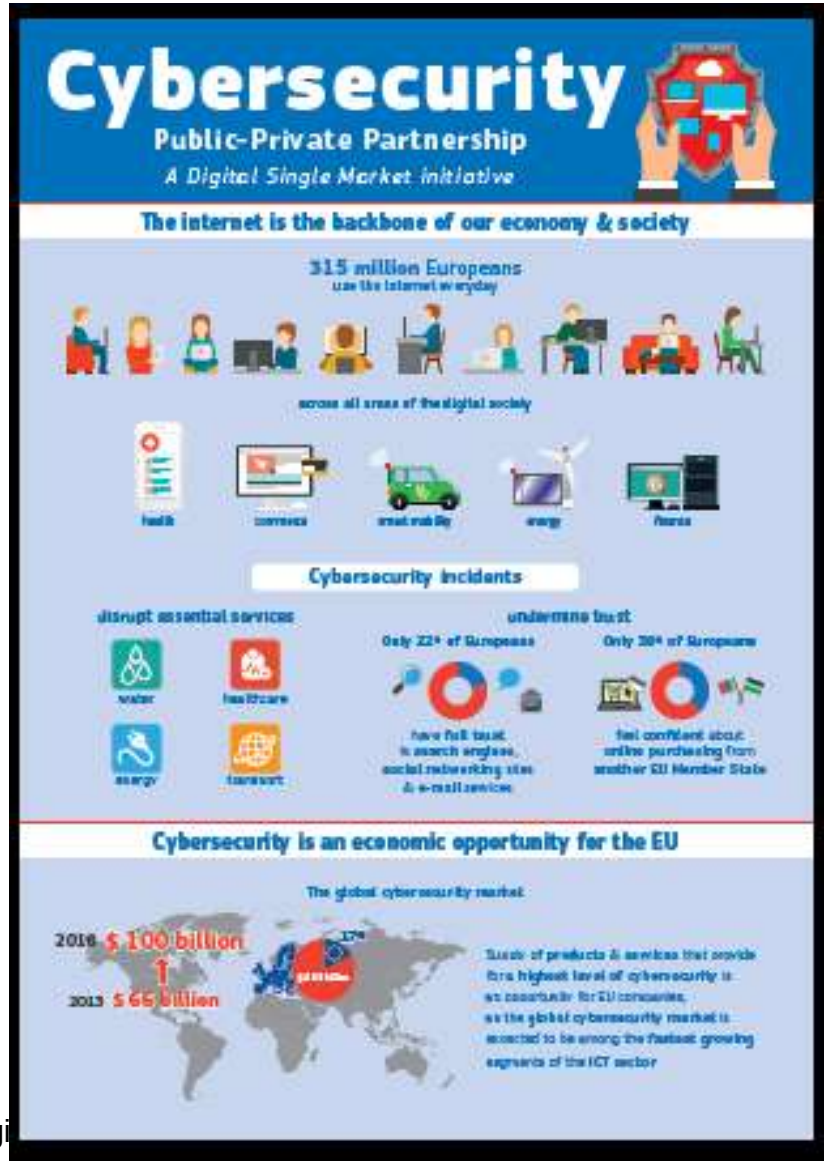
CYBERSECURITY STRATEGIC RESEARCH AGENDA – SRA. European Network and Information Security (NIS) Platform. 2015. http://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/cybersecurity-SRA-final-v0_96-ENISA.pdf

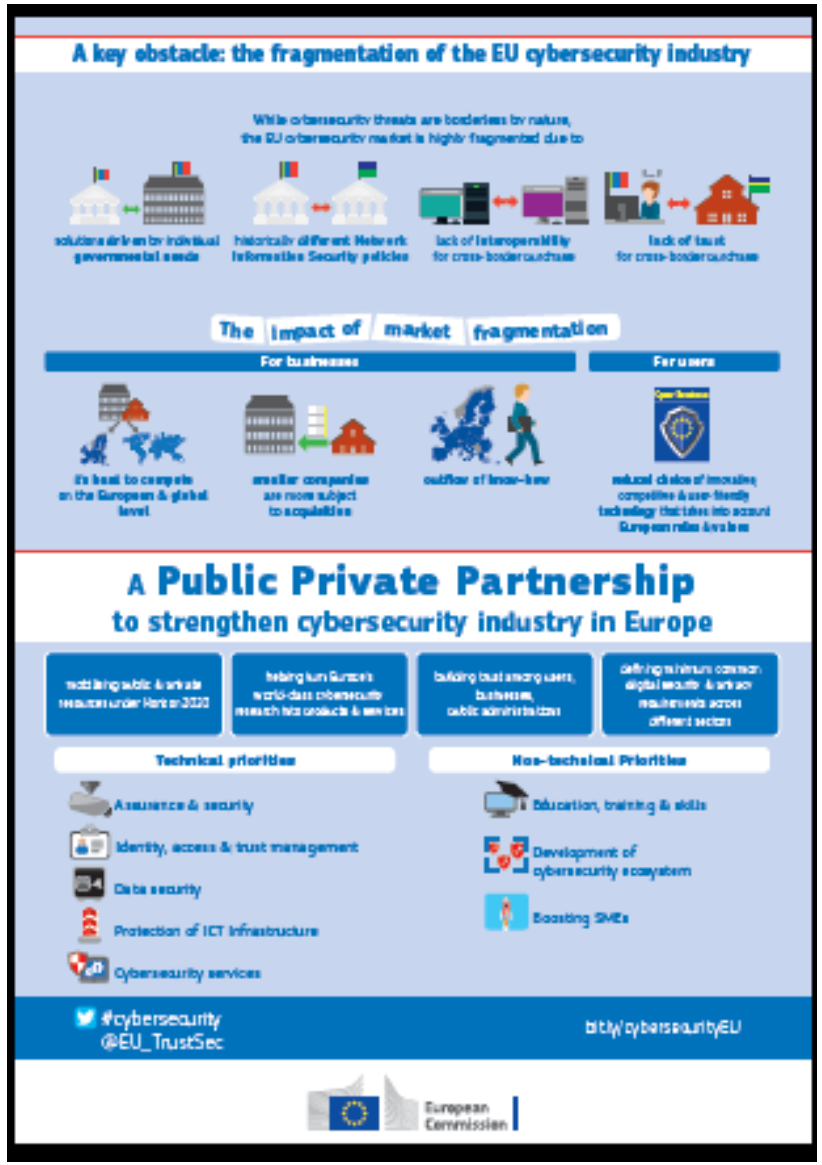
Cybersecurity research and innovation: R&D strategic priorities in the US

- Prioritize basic and long-term research in Federal cybersecurity R&D.
- Lower barriers and strengthen incentives for public and private organizations that would broaden participation in cybersecurity
- Assess barriers and identify incentives that could accelerate the transition of evidence-validated effective and efficient cybersecurity research results into adopted technologies, especially for emerging technologies and threats.
- Expand the diversity of expertise in the cybersecurity research community.
- Expand diversity in the cybersecurity workforce

FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT STRATEGIC PLAN. National Science and Technology Council. 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

Bringing the European cybersecurity stakeholders together: the cPPP





https://ec.europa.eu/digital-single-market/en/cybersecurity-industry

The strategy: facts and goals

- The cPPP is expected to trigger €1.8 billion of investment by 2020.
- The European Cyber Security Organisation (ECSO) http://www.ecs-org.eu/
- At the moment, the European cybersecurity market is about 24%, less than the contribution of Europe to Global GDP (i.e. about 26%) with an average yearly growth slightly larger around 6%, when the world market is growing at about 8% year, so **we must improve and do so fast.**
- **We need to show our leadership in the area of cyber security**; i.e. collect forces and provide solutions for the problems that are dampening the way toward a sustainable Digital Single Market.

The underlying trends: Factors affecting growth

- Europe’s share of global economy is declining due to lower growth
- EU market is fragmented in practice making growth difficult
- Funding shortages and entrepreneurial support
- Europe procurement policies focus too much on short-term savings without promoting customer-vendor partnerships needed for innovation
- Less investment in R&D and little market success
- Skill shortage
- European companies favour execution to strategic foresight

What to do?...

- Bring the major stakeholders together
  - European Union
  - Member States and Public Administration
  - Large Companies
  - Small and Medium Enterprises
  - Universities and Research Institutions
  - Venture Capitalist and Financial Institutions
- Formulate a Master Plan with clearly defined cybersecurity focused areas.

What to do?

- Focus on
  - high-end, B2B and business-to-government (B2G)
  - **economic sectors in which Europe has a comparatively strong position**, such as the defence, automotive, process industries, industrial machinery, utilities, telecom, and financial services
  - **cyber subsectors that will specifically address the challenges of these industries and create a home market for European players,** such as embedded systems, intelligent networks (e.g. smart grids), cyber-physical systems, ICT-enabled secure smart automation (Industry 4.0 strategy), complex software systems, security systems and big data and analytics solutions.
  - **the needs of these players and major EU buyers more than focusing on technology** to deliver solutions that give them competitive advantages**.**

How to do? The instruments…

- Cyber Coordination (Coordination and Support Actions)
- Cyber Pillars (socio-technical ecosystems for innovation and experimentation/training)
  - Cyber Pillar for Innovation – Cyber Trustworthy Innovation Ecosystem
  - Cyber Pillar for training/education/cyber experimentation facilities – Cyber experimentation and training Ecosystem

How to do? The instruments…

- Technical projects
  - Security and Privacy by Design
  - Security Assurance along the supply chain
  - Identity and Trust Management
  - Privacy and Data Security
  - ICT Infrastructure Protection
  - Security Services
  - User-centric security and privacy
  - Quantum-resistant cryptography

How to do? The instruments…

- Trustworthy Cyber Infrastructures
  - Cross-cutting topics
    - Digital Citizenship
    - Security Assessment and Risk Management
    - Information Sharing and Analytics
  - Functional topics
    - High-assurance prevention and protection
    - Enhanced anomaly and attack detection and analysis of cyber-threats
    - Advanced cyber-incident response and recovery towards cyber-threats

How to do? The instruments…

- Cyber Pilots
  - Industry 4.0 (Industrial Control Systems - ICS)
  - Energy (Smart grids, Electricity generation, water supply)
  - Smart Buildings & Smart Cities
  - Transportation (Smart cars, UAVs, Maritime, Aviation)
  - Public services / E-government
  - Healthcare
  - Finance / Insurance
  - Telecom, media, and content

Conclusions

- Cybersecurity is not an expense; it is an investment that can create wealth and secure prosperity
- Major paradigm shifts in computing and ICT create significant multiple cybersecurity R&D challenges
- Cybersecurity is high in the R&D agenda in both Europe and the US
- Many opportunities exist for obtaining funding for exciting R&D projects in Europe
- Collaboration at all levels and among sectors is a key enabler

Thank you!