Bridging the Gap between Cybersecurity Industry Needs and Tertiary Education Graduates Skills

Anna Felkner

Cybersecurity Research and Development Division, NASK

ECCO Community Group on Skills, 6 November 2024

SCIENCE NASK

The most important competences

Transversal competences	Professional competences
critical thinking	security risk assessment
ethical thinking	risk prevention management
strategic thinking	knowledge of vulnerabilities and exploits of systems
holistic thinking	understanding of secure web communications and technologies
creativity	understanding of system logic
problem solving	ability to write script or code
teamwork	knowledge of network security
interdisciplinary thinking	knowledge of operating systems security
business knowledge	knowledge of mobile and IoT security
lifelong learning	knowledge of cloud computing security
oral communication skills	
written communication skills	
handling complexity	
open mindedness	

https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/

SCIENCE NASK

Bridging the Gap between Cybersecurity Industry Needs and Tertiary Education Graduates Skills

- There is a clear gap between what business expects and what higher education gives
- Gaps related to professional and transversal competences
- Respondents from business industry placed approximately 10% more importance on both transversal and professional skills than the education sector

Recommendations:

1. Improve education and training
2. Back to basics
3. Raise awareness of the importance of cybersecurity at all levels of education
4. Improve collaboration between industry and education
5. Boost diversity
6. Upgrade recruitment procedures
7. Scale up knowledge-sharing and good practice

https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/

SCIENCE NASK

Bridging the Gap between Cybersecurity Industry Needs and Tertiary Education Graduates Skills

Pluses:

- both the industry-business and education sectors worldwide recognize the existence of the competence gap and express similar opinions about the core competences
- both universities and business see the need to propose different kinds of solutions to fill this gap

Proposals:

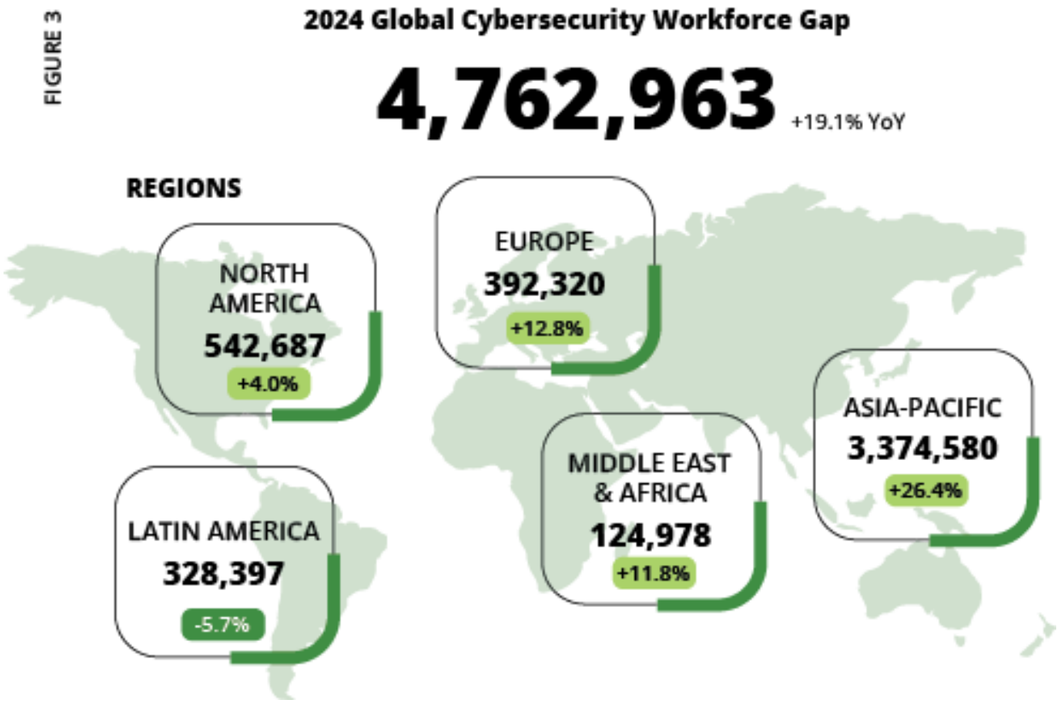
- *industry-business sector*: training
- *education sector*: collaboration and experience exchange with industry, in order to be able to build realistic forward-looking learning programmes

https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/

SCIENCE NASK

ISC2 2024 Cybersecurity Workforce Study

This year, the workforce gap was 4,762,963 people.



64% of respondents believe that **skills gaps have a more significant negative impact** than a staffing shortage.

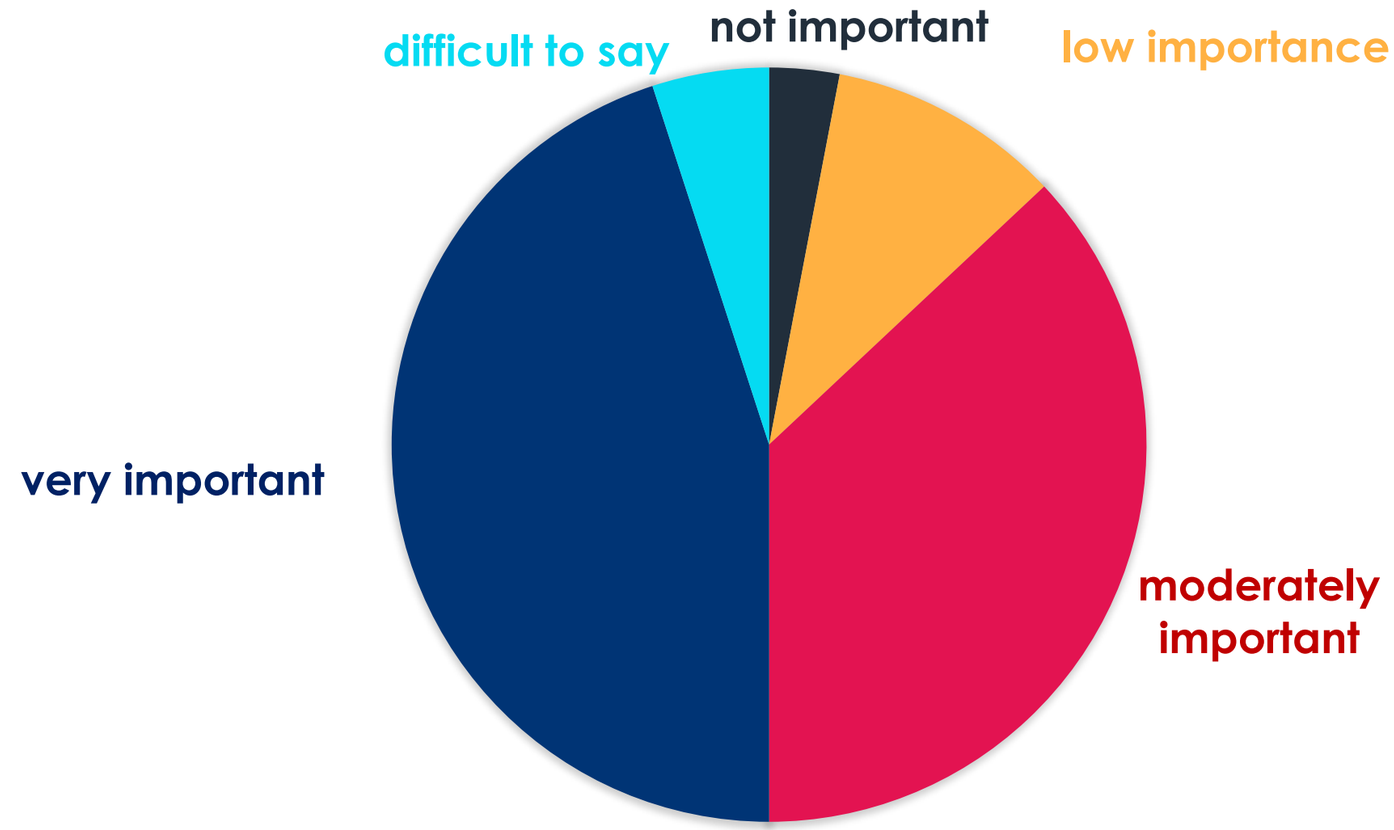
https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

SCIENCE NASK

Transversal competences

82% - very important or moderately important

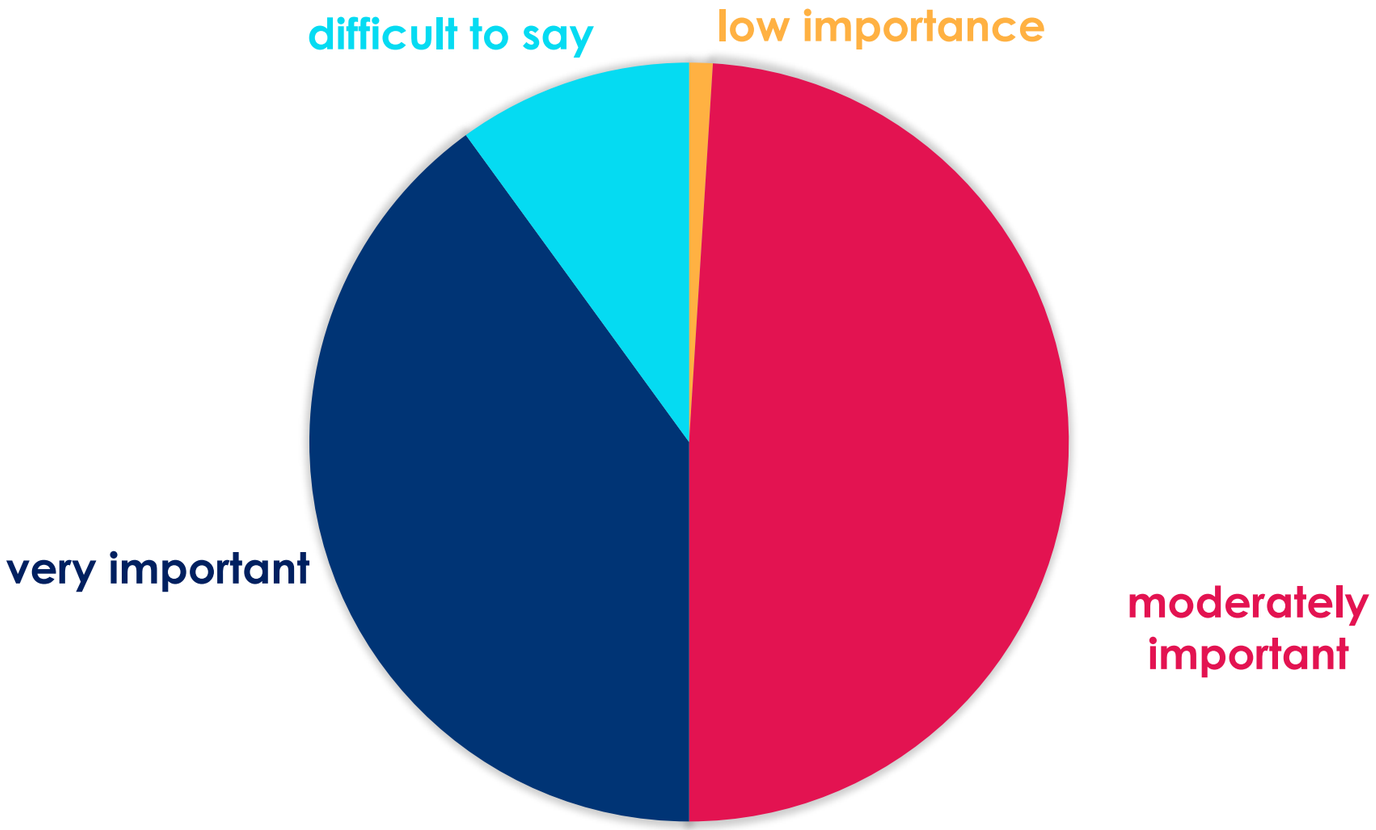
- lifelong learning
- critical thinking



Professional competences

89% - very important or moderately important

- knowledge of vulnerabilities and exploits of systems
- understanding of system logic



Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in a broader area, not just one specific area of interest

discernment in various topics and general knowledge

SCIENCE NASK

Additional competences

openness to knowledge sharing

assessing the impact of a given action further than one step ahead

elementary knowledge of psychology

„nit-pick", trying to spoil, substandard actions

search for information

analytical thinking, analysis of information

curiosity

synthesis of information (inference)

discernment in various topics and general knowledge

discernment in a broader area, not just one specific area of interest

SCIENCE NASK

Competence gaps

Lack of:

- the ability to go above and beyond
- responsibility/commitment to the objectives of the activities undertaken
- knowledge of tools used in cybersecurity
- more detailed technical knowledge of aspects of cybersecurity in networks
- defensive side of cybersecurity
- practical application of AI
- project and process management
- practical knowledge/practical use of tools
- the ability to assess the situation by looking at the problem more broadly

How serious a problem is this for your organization?

discourages recruitment
of young graduates

long time to implement
the employee

significant

large

quite large

huge

serious

very large

The most difficult roles to fill

- penetration tester
- cybersecurity manager
- network engineer
- information security architect
- cybersecurity researcher
- application security tester
- incident handling specialist
- malware analyst
- IT technology auditor

The most difficult roles to fill

- penetration tester
- cybersecurity manager
- network engineer
- information security architect
- cybersecurity researcher
- application security tester
- incident handling specialist
- malware analyst
- IT technology auditor

Why exactly these?

They:

- demand the most creativity and a lot of cross-cutting knowledge in many fields
- require comprehensive preparation and extensive (diverse) practice
- small pool of candidates (pentester, malware analyst)
- level of knowledge too low/lack of experienced people

Best practices

- knowledge sharing
  - information exchange channel
  - knowledge base
  - discussion club
  - invited seminars
  - cooperation with other teams
  - organization of inter-team meetings

- external and internal training
  - technical
  - developing creativity
  - training plans tailored to individual needs
  - widespread access to e-learning platforms

- encouraging young employees to increase commitment, independence
- rewarding employees who excel
- temporary work in other cybersecurity roles
- cyclical evaluations

Best practices

- knowledge sharing
  - information exchange channel
  - knowledge base
  - discussion club
  - invited seminars
  - cooperation with other teams
  - organization of inter-team meetings
- external and internal training
  - technical
  - developing creativity
  - training plans tailored to individual needs
  - widespread access to e-learning platforms
- encouraging young employees to increase commitment, independence
- rewarding employees who excel
- temporary work in other cybersecurity roles
- cyclical evaluations

Best practices

- knowledge sharing
  - information exchange channel
  - knowledge base
  - discussion club
  - invited seminars
  - cooperation with other teams
  - organization of inter-team meetings

- external and internal training
  - technical
  - developing creativity
  - training plans tailored to individual needs
  - widespread access to e-learning platforms

- encouraging young employees to increase commitment, independence
- rewarding employees who excel
- temporary work in other cybersecurity roles
- cyclical evaluations

Proposed solutions

- practice
  - simulating real-life events
  - presentations of real cases conducted by employers at universities
  - including extensive practical scenarios
  - compulsory apprenticeships
- collaboration between universities and employers in the context of shaping study programs
- prerequisite competency tests
- competitive salaries
- increased emphasis on active student participation in the cybersecurity environment
  - tracking publicly available sources of information
  - use of open training tools (hack the box, etc.)
  - participation in open source projects to holistically understand the state of the industry

Proposed solutions

- practice
  - simulating real-life events
  - presentations of real cases conducted by employers at universities
  - including extensive practical scenarios
  - compulsory apprenticeships
- collaboration between universities and employers in the context of shaping study programs
- prerequisite competency tests
- competitive salaries
- increased emphasis on active student participation in the cybersecurity environment
  - tracking publicly available sources of information
  - use of open training tools (hack the box, etc.)
  - participation in open source projects to holistically understand the state of the industry

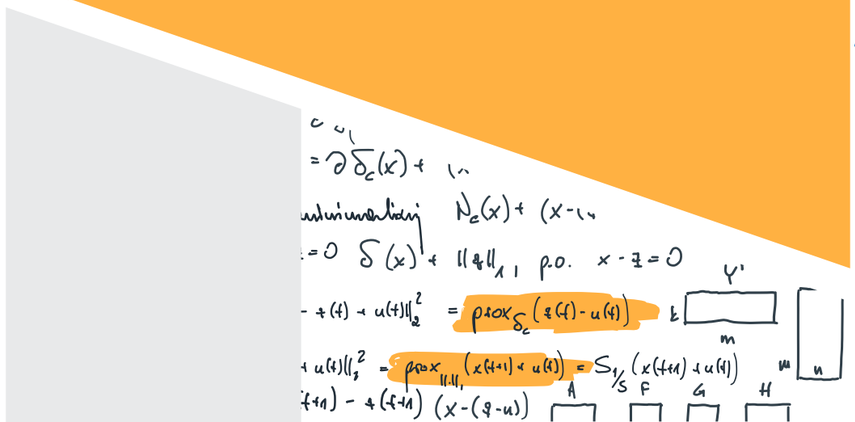
Proposed solutions

- practice
  - simulating real-life events
  - presentations of real cases conducted by employers at universities
  - including extensive practical scenarios
  - compulsory apprenticeships
- collaboration between universities and employers in the context of shaping study programs
- prerequisite competency tests
- competitive salaries
- increased emphasis on active student participation in the cybersecurity environment
  - tracking publicly available sources of information
  - use of open training tools (hack the box, etc.)
  - participation in open source projects to holistically understand the state of the industry

Thank you!

Anna Felkner, NASK

Anna.Felkner@nask.pl



SCIENCE NASK

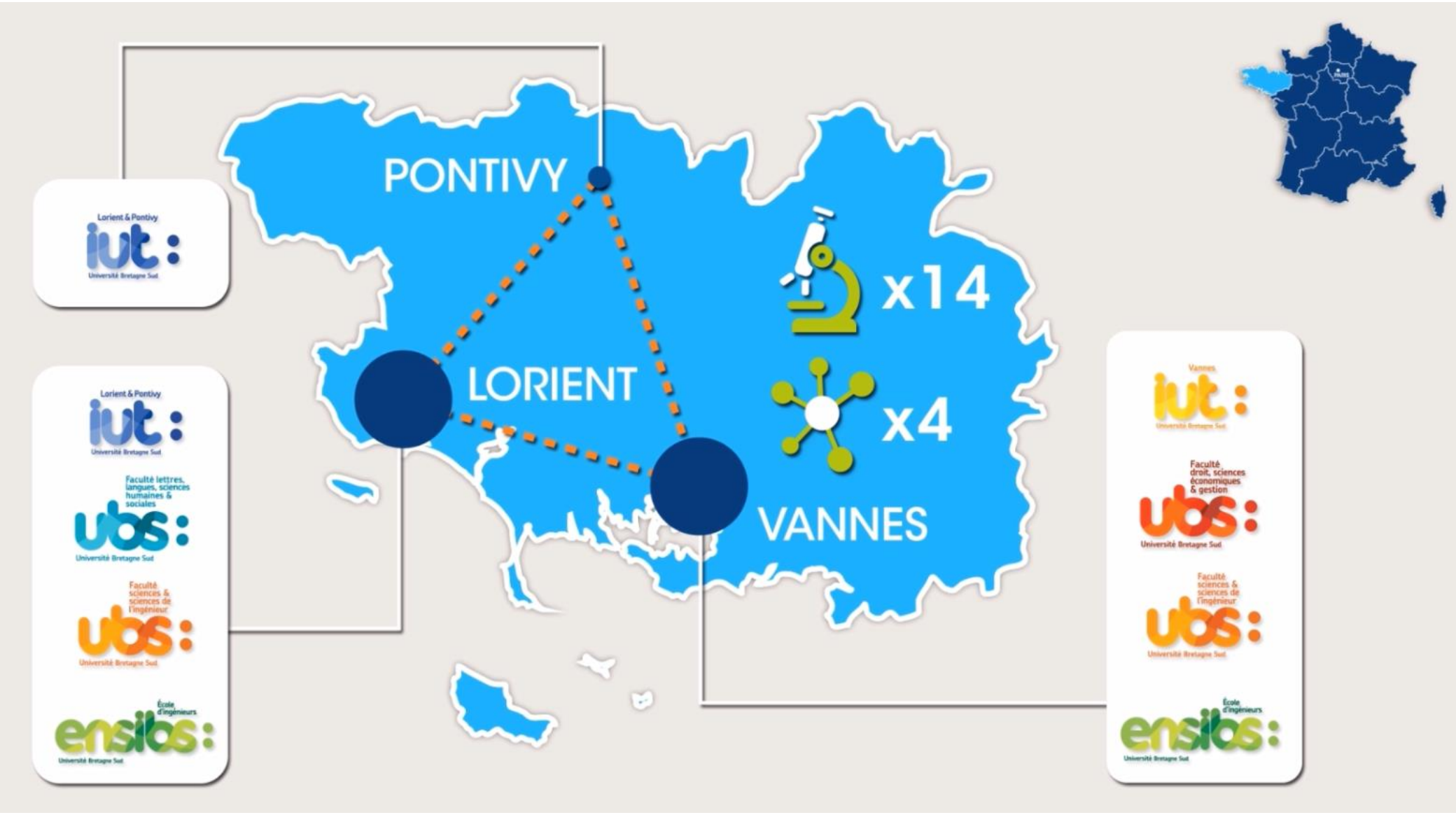
Presentation

Educational Curricula Alignement to Market Needs

From Student to Job in Cyber: switching Education Programs to Skill Blocks - Deciphering how French higher educational institutions are restructuring the courses based on demand for cyber security jobs

November 6, 2024

Université Bretagne Sud
cyber :


PONTIVY
LORIENT
VANNES
x14
x4
Lorient & Pontivy
iut :
Université Bretagne Sud
Faculté lettres, langues, sciences humaines & sociales
ubs :
Université Bretagne Sud
Faculté sciences & sciences de l'ingénieur
ubs :
Université Bretagne Sud
École d'ingénieurs
ensibs :
Université Bretagne Sud
Vannes
iut :
Université Bretagne Sud
Faculté droit, sciences économiques & gestion
ubs :
Université Bretagne Sud
Faculté sciences & sciences de l'ingénieur
ubs :
Université Bretagne Sud
École d'ingénieurs
ensibs :
Université Bretagne Sud

Sea & Coasts

Université Bretagne Sud
ubs:
Innovation Ecosystems

Cyber & Data

Industry of the future

Environment & Health


Université
Bretagne Sud
cyber :

General overview

- **RESEARCH (since 2015)**
  - **Applied research and federation of 5 laboratories**
  - **Transdisciplinarity**

Université Bretagne Sud
cyber :

Cyber Research

Our philosophy : *Secure by design*

6 focuses

- **Embedded systems & IOT**
- **Industrial cybersecurity**
- **Socio-technical systems of systems**
- ***Big data* & intrusion detection in massive data streams**
- **Human factor**
- **Cyberdefence**

+ Cybersecurity Chair for Large Public Events

Université Bretagne Sud
cyber :

General overview

- **CYBER CRISIS MANAGEMENT TRAINING**
  - **Cyber Range - Methodology & scenarios**
  - **PCA & PRA (continuity plan /recovery plan)**
  - **Hybrid Simulation + industrial plateform**

- **TERRITORY LINKAGE AROUND INNOVATION**

Université Bretagne Sud
cyber :

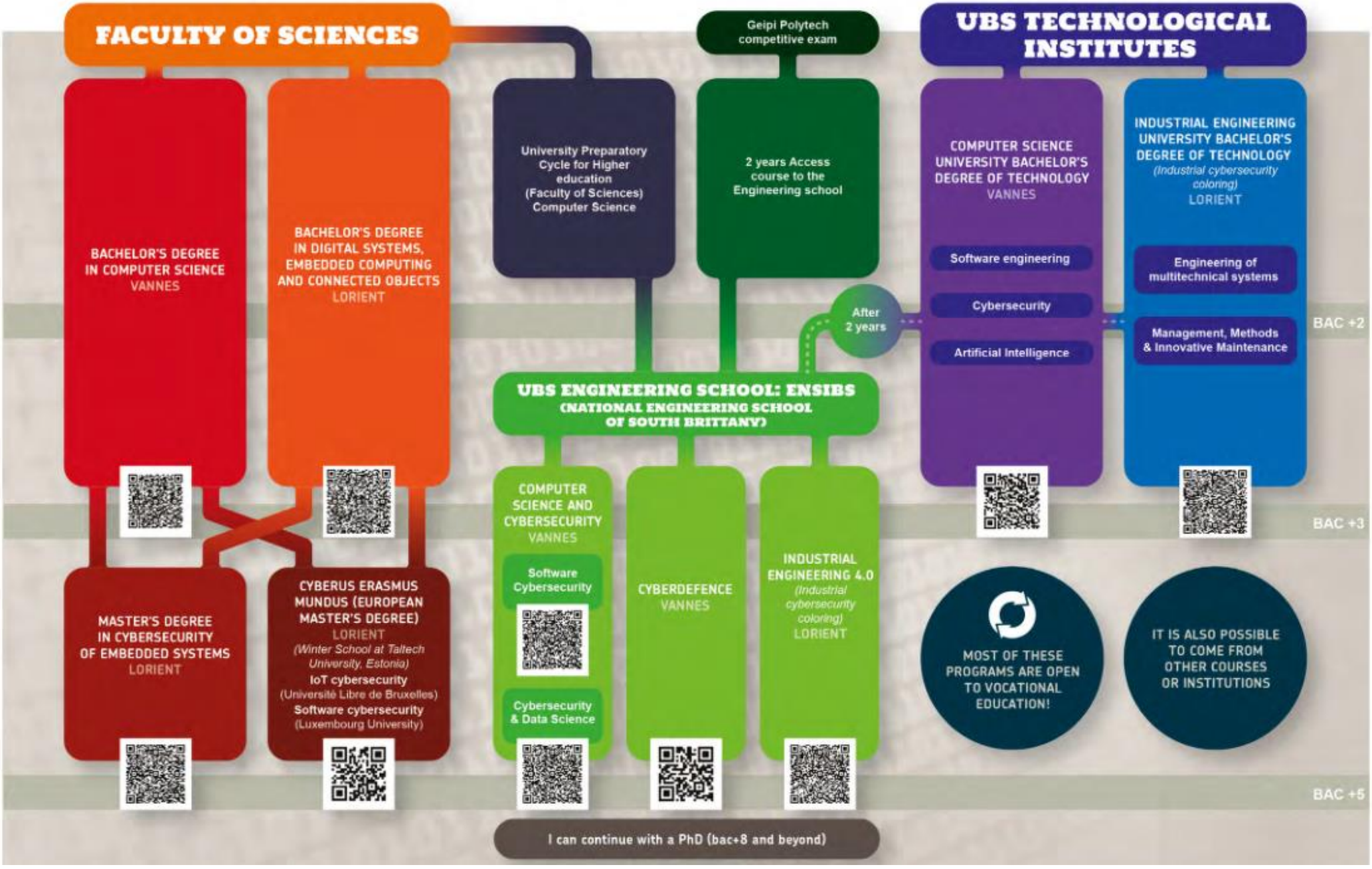
General overview

- **EDUCATION (since 2013)**
  - Continuum from completion of high school up to post-doctorate (1000 students / New Cyber and DataScience Campus in 2026)
  - Coverage of a wide spectrum of cyber : Software (Cyberdefence, software vulnerabilities…) & Hardware (embedded systems, IOT, ICS…)
  - ANSSI labelling and EU recognition
  - Vocational training
  - Tripartite Cooperations/Co-Training&Co-Evaluation
  - Continuing education / professional training (« University Diplomas ») – Reskilling/Upskilling
  - Students come from all over France and the World (25 nationalities Cyberus Erasmus Mundus)
  - Only 10-15% Women
  - All the students find a job after university
  - 20-30% go to State Agencies or Cyber Command as a first Professional experience
  - First salary (Engineers School) ~ 40k€ (up to 80 k€) per year
  - Some have created their own businesses
  - No PhD student has yet created his own business

Université Bretagne Sud cyber :

I'VE COMPLETED HIGH SCHOOL (BAC), I WANT TO GO ON WITH CYBER AT UBS

A COMPREHENSIVE EDUCATION PROGRAM



Some highlights

- Emphasis on projects and internships
- International mobility & Language training
- From education programs to skill blocks – Cyberskills matrix

Université Bretagne Sud
cyber :

Cyber Skills Matrix

https://wiki.campuscyber.fr/images/1/19/Matrice-comp_metiers_connexes.pdf

Université Bretagne Sud
cyber :

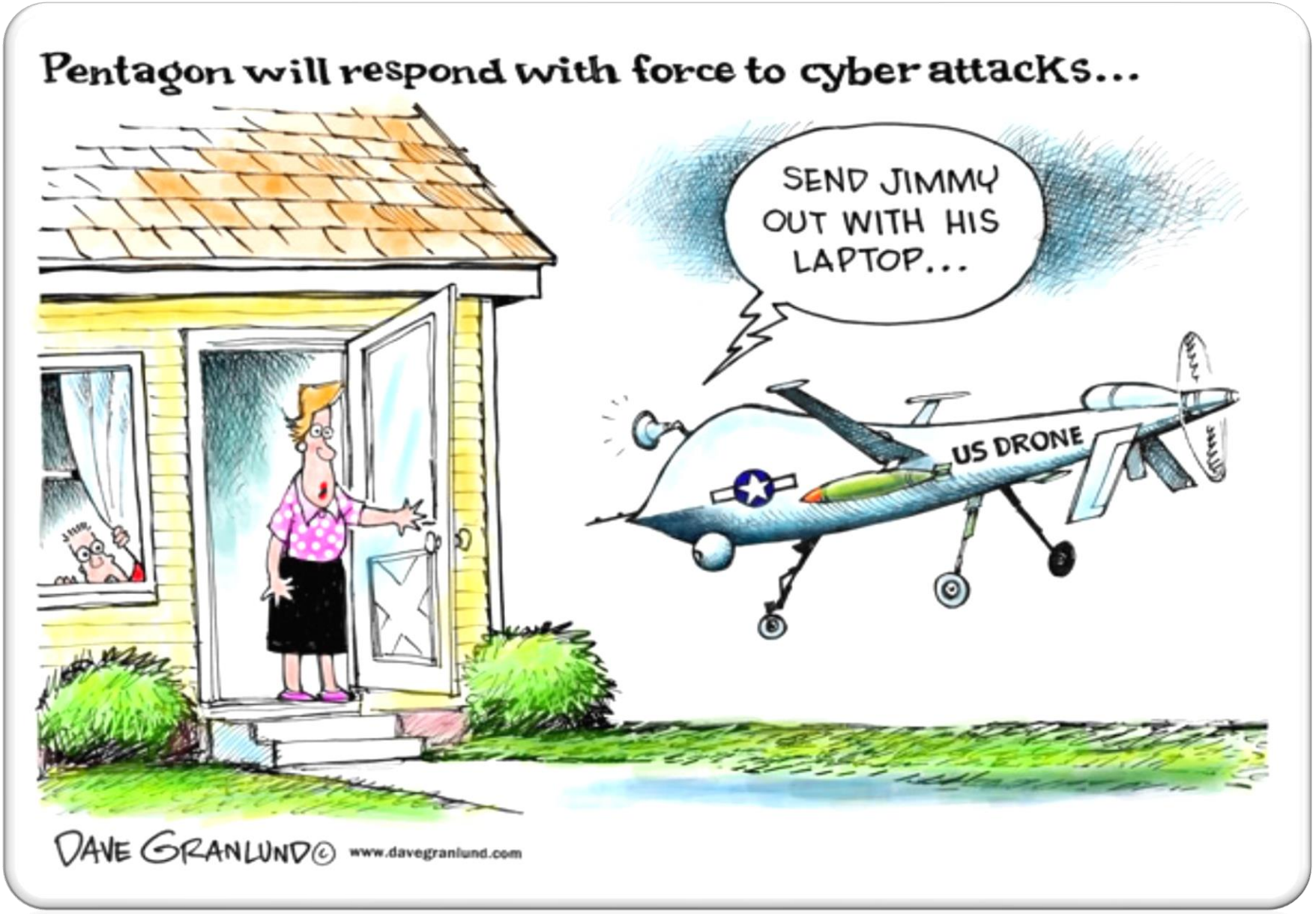
Some highlights

- Emphasis on projects and internships
- International mobility & Language training
- **From education programs to skill blocks – Cyberskills matrix**
  - **Approaching professions through skills**
  - **Grouping jobs not by function but by skills needed for their proper execution**
  - **Facilitate access and adaptation to a targeted profession**
  - **View to employability, enabling employees to be flexible and evolve throughout their working lives**
- **Education *vs.* Certification ?**
- **Evolution – Cybersecurity skills # Technology skills**
  - **Sometimes an engineer, sometimes a lawyer**
  - **Example, convergence CISO & DPO**
  - **« General practitioner » (Cyberdefence branch) or specialist? (No need to be an expert to manage a company's cyber policy or to ensure compliance)**
  - **Soft skills (leadership, teamwork, communication…)**
  - **Pentester or Ethical hacker ~5% of the job market and more and more automated through AI**

- ***How to take into account the evolving nature of the threat***

Université Bretagne Sud cyber :

QUESTIONS ?



Université Bretagne Sud
cyber :

Jack NOEL

Cybersecurity Innovation Engineer
Coordinator *Cyber:UBS*

+ 33 (0)6 66 99 38 05

jack.noel@univ-ubs.fr

Université Bretagne Sud
cyber: