ENISA Rome October 31st 2017

CTI – EU | Bonding EU Cyber Threat Intelligence

Session 5: CTI capabilities, skills, education training and research

Facilitators & Supporters

Facilitators - Jart Armin & Andreas Sfakianakis

Supporters – Adam Kozakiewicz, Ms Heidi Kivekäs, Selene Giupponi, Prof Latif Ladid, Prof Marco Cremonini, Jess Garcia

Session 5: CTI capabilities, skills, education training and research

During this session we will focus on different aspects of Cyber Threat Intelligence:

1. CTI analyst's skillset will be analysed regarding tactical, operational as well as strategic threat intelligence.
2. We will also discuss the current skills gap in the market, the high demand for capable CTI analysts and how this gap can be bridged.
3. Then, we will explore the current training opportunities, how a course syllabus would look ideal and what would be its content.
4. Finally, we will pay special attention to current EU research efforts in the area of CTI.

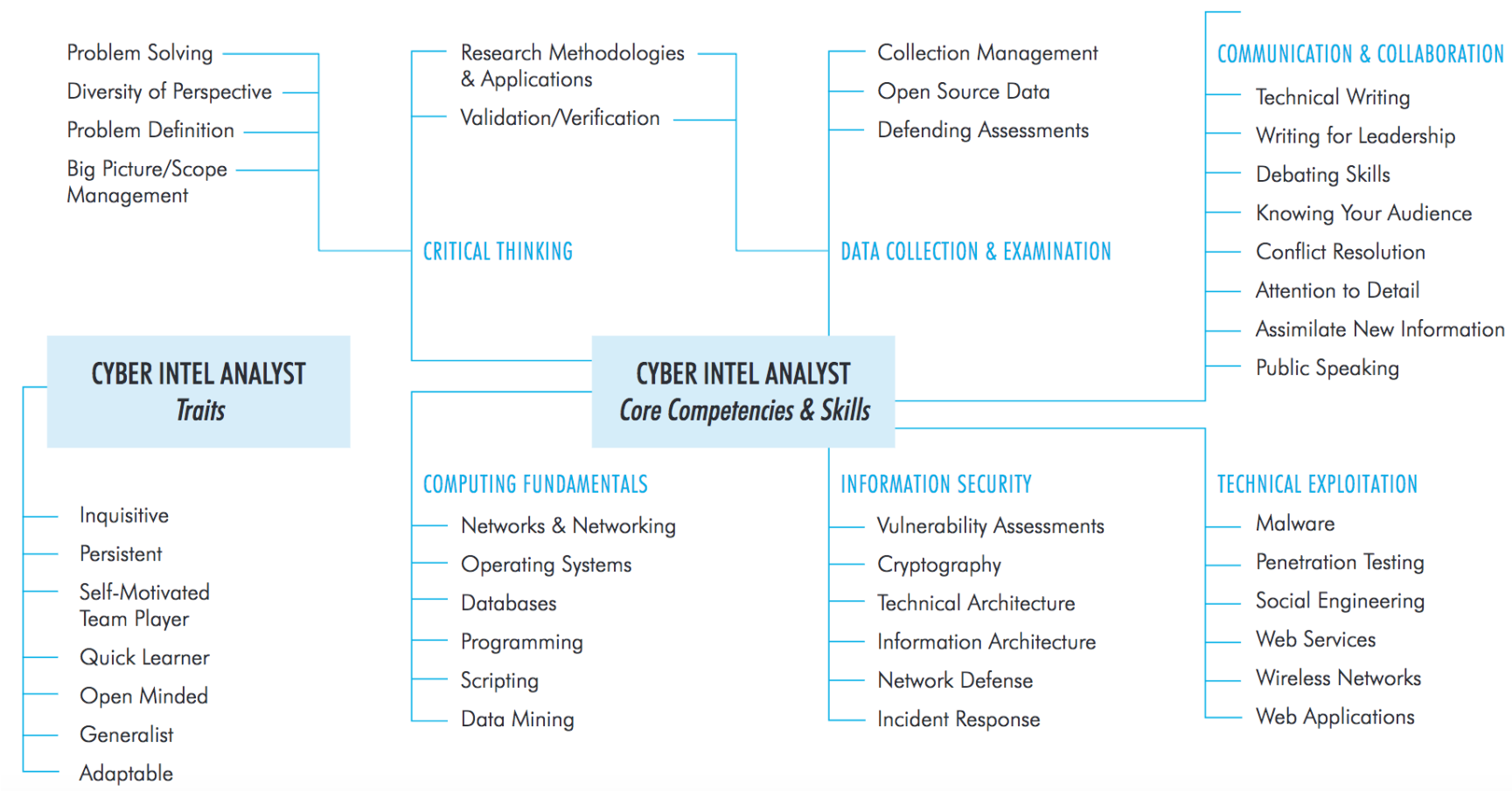
CTI capabilities- NCSC-FI

- Finland has one of the safest networks
- What can we learn from the approach of Finland?
- Regulation as a service
- Autoreporter tool
- Service proven value and orgs reach them on a voluntarily basis

Lessons learnt from teaching CTI

- Focus on syllabus – tactical – strategic and analytic skills
- Trainees background
- Professional background
- What Are Students Looking For?
- What Are Students Most Common Questions?
- What Are Students Most Common Complains / Needs?
- What Do Students Value Most from the Training?

CTI analyst skillset



Academic approach and what the employers need

- CTI education goals
- Difficulties in establishing a CTI curriculum
- Nobody now has a clear and comprehensive picture in mind
- It should be developed, piece by piece
- Beware the snakeoil ☺
- Join the efforts/Share the interests (professionals, academics, companies, public agencies)

DFIR and CTI, and other challenges

- Skills gap
- Lack of certified professionals
- High-value skills in critically short supply
- Inadequate levels of Training
- DFIR and CTI teams interaction
  - Challenges for corporate environments
  - Lack of processes and understanding

Overall recap + Recommendations

Challenge	Recommendations	Target
Lack of Competence Building Support	• Increasing government expenditure on cyber security training through matched funding and/or financial incentives; • Pushing for more cyber security programs in school and higher education.	Government
Lack of cyber security in Academia	• Partner with professional cyber security training vendors to offer extra extra-curriculum professional certifications and hands-on experience; • Organize Cyber Security Games and Competitions and/or facilitate students to participate.	Academia
Security Competition and Exercise	• Promoting gaming and technology exercises	Government
Companies Do not Invest Enough in Staff Training	• Shift spending from security systems to people and processes; • Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts.	Organizations
Cost of Training and Certifications	• Develop better competence building programmes, which can be delivered by competent in-house staff and pay for staff certification attempts.	Government, Academia and Organizations
Lack of Adequate Training	• Prioritize formal and structured training over online/self-learning especially to begin with	ALL
Young Professional Not Doing It Right!	• Follow a goal-oriented approach to produce tangible deliverables at every step of the learning process	Individuals

SAINT Objectives

1 - **Metrics for CTI**, cyber-security and cyber-crime market

2 - **New economic models** for the reduction of cyber-crime as a cost-benefit operation

3 - **Costs / Benefits** of information sharing regarding cyber-attacks

4 - **Privacy** and security level of internet applications, services and technologies

5 - **Automated analysis**, for behavioral, social analysis, cyber-security risk and cost assessment

6 - **Recommendations** to all relevant stakeholders including **policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies**

NASK

SISSDEN

Open to community collaboration

- Sign up in advance:

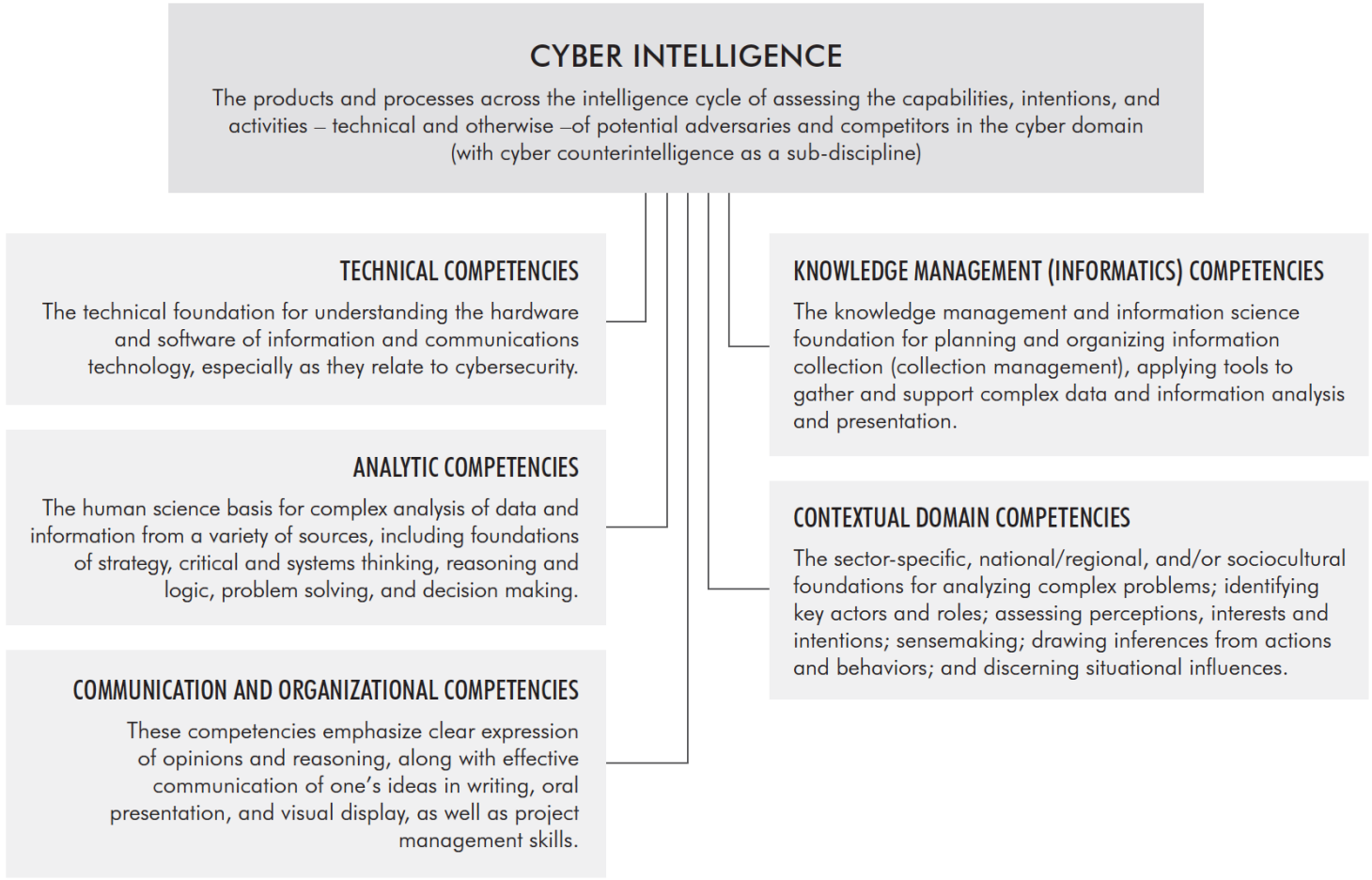
  https://sissden.eu

- Deploy sensors, provide IP space, VMs, physical servers
- Contribute new honeypot/sensor technologies
- Third party feeds welcome
  - integrate and help enrich curated data
- Academics willing to do research on the curated data set welcome
- Open to collaboration with LE initiatives with data on malware and botnet activity
  - existing example – Cuing.org

Wrapping up

- Master degree in CTI? … Universities are not currently rushing to propose a CTI curriculum
- Universities have difficulties in establishing a curriculum in a timely way.
- Need for intelligence trainings and courses for cyber security professionals.
- No courses accredited by intelligence services in EU. No EU intel agency to co-ordinate education/training
- University provides CTI foundation (“the same language”) and students that are enterprise ready. Organisations will provide the practical experience.
- Few organisation apply and invest on CTI training. Change of mind set needed.

CTI Knowledge domains



Thanks for your participation!!