UNIVERSITÀ DEGLI STUDI DI MILANO

Current training & educational opportunities: An academic approach & what the employers need

Marco CREMONINI

Computer Science Department

University of Milan, Italy

WORKSHOP CTI – EU | Bonding EU Cyber Threat Intelligence

30-31 October, Link Campus University, Rome, Italy

Who I am

- Assistant Professor
- Teaching
  - Risk Analysis and Management (Laurea Magistrale in Information Security)
  - (previous) Network Security, OS Security
- Research
  - Risk and Cybersecurity (vulns, markets, education)
  - Privacy/Data Protection
  - Complex Network Analysis (Social, Epidemics, Controllability)
- Other
  - Industrial collaborations, EU Projects, Mentoring, Op-Ed

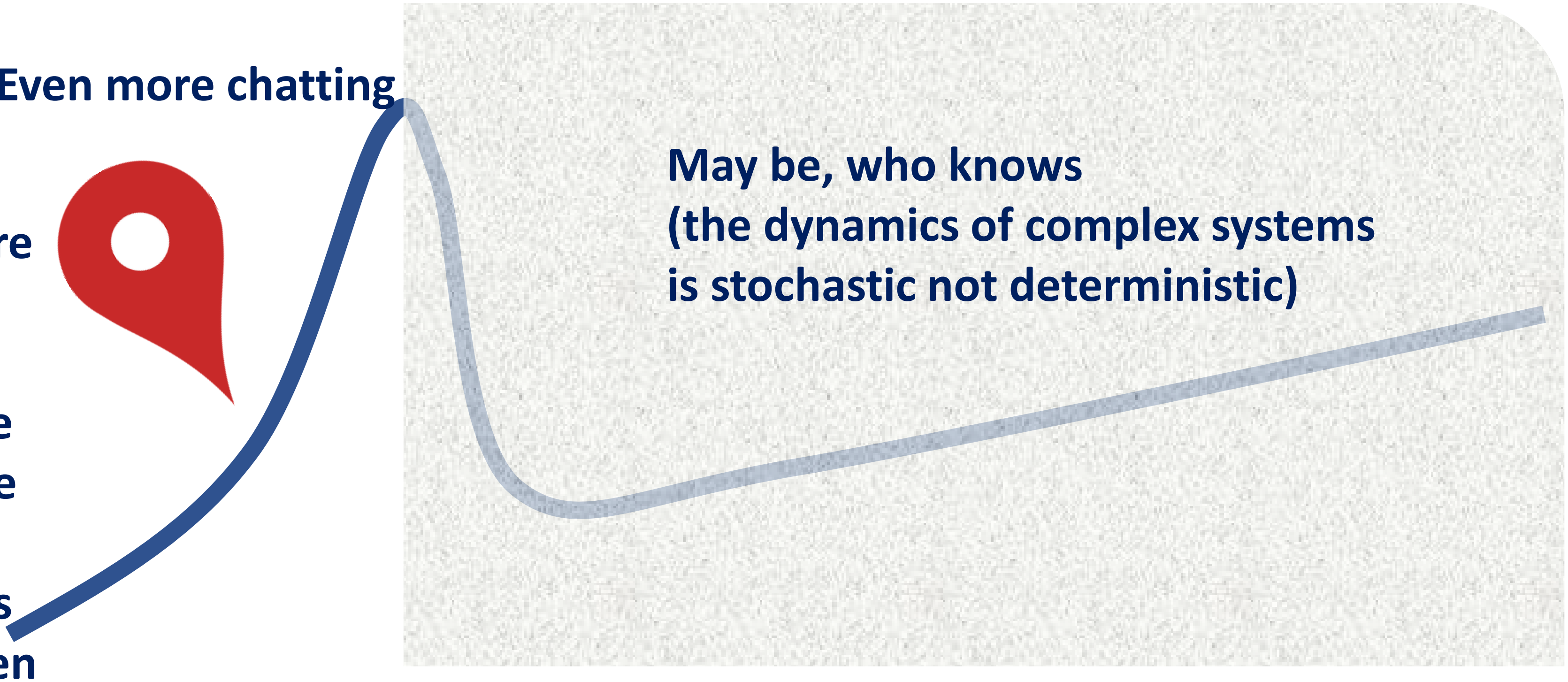
Outline

- Gloom and doom analysis
- A few small suggestions
- Take home message

Gloom and doom

CTI – It's complex

- Many had given/will give many different definitions of CTI
- A lot of ***promotion*** ("hype cycle" is branded)



Even more chatting

WE ARE HERE

A lot of chat, ties are forming, the complex network has no recognizable structure yet, phase transition still possible, clogging is very likely to happen

May be, who knows
(the dynamics of complex systems
is stochastic not deterministic)

CTI – It’s generic

- Many companies are now offering CTI services
- **Generically data-oriented** (OSINT, third-party info, ad-hoc collection)
- **Generically threat-oriented** (Try give a definition of threat)
- **Generically risk-oriented** (Try give a definition of risk)
- **Generically cybercrime-oriented** (but not always)
- **Generically industry-agnostic** (leaning towards the finance sector)

CTI – It’s naïve

- **Thread modelling confused** (web defacement a CTI issue? Where is espionage? Where are industrial sector analyses?)
- **Risk concepts messed up** (where are probability and loss estimates? CVSS is NOT a risk metric for vulns (by design))
- **Data analysis and analytics missing** (Did you employed data scientists?)
- **CTI effectiveness not measured** (You know what you can measure)
- **Goals undefined** (CTI is hopefully useful for something)
- **Customers mostly unfamiliar** (as usual)
- **Skills, competences undefined** (what is a CTI expert? Many apparently out there)

CTI – Training for what?

- **Traditional shortage of security skilled workforce** (still debated)
- **Traditional fight Practical Vs. Theoretic education** (please, refrain from taking side, believe me, it is not useful)
- **Traditional lack of measurement** (Which effectiveness of education/experience? Learning to learn or learning to do?)
- **Traditional difficulty (if not hostility) for interdisciplinary training** (vertical silos for knowledge domains is the norm)
- **Traditional solutionist approach for education** (education needs time to be tuned and time to produce first results, which are always stochastic)

A few small suggestions

Education for CTI – Principles

- **Education is a process not a product** (like for security and millions of other things, as you already know)
- **Education** IS NOT GOING TO SOLVE YOUR BUSINESS PROBLEMS, LACK OF MEASUREMENTS, DISORGANIZATION, AND POOR PRODUCT FEATURES
- **Garbage In Garbage Out holds for education too**
- **Education and experience together could be EXTREMELY effective**

CTI – Education goals

- **Academic education** (Master level, broad spectrum, mostly learn to learn)
- **Professional education** (specific training, mostly learn to do)
- **Address the complexity** (web defacement is not CTI, domain name scam is not CTI, Nessus scan is not CTI, CVSS is not CTI)
- Define the goals of CTI, explicitly
- Then define the goals of CTI education, explicitly
- It’s something brand new in Infosecurity, but already known outside of it

CTI – Key competences (top down)

- **CTI by nature crosses multiple technical/scientific disciplines:**
  - **Computer science** (everywhere)
  - **Information security** (not so common, increasing)
  - **Data science** (also not so common, increasing)
    - gathering (DBMS SQL/noSQL, web scraping, data fusion)
    - data mining, machine learning, statistics, text mining
    - visualization / HMI
  - **Network Science** (definitely not common, somehow increasing)
    - social networks, epidemics, diffusion
  - **Cybercrime** (not even a technical discipline, mostly anecdotic)
  - **Economics/Business/Legal** (everywhere but difficult to integrate)
  - **Risk Analysis and Mng.** (totally ignored in Infosec, shame on you!)
  - **Forensics** (established as a discipline)
  - ...

Take home message

Education for CTI – What to do?

- **Take it very seriously if you think that CTI will become strategic** (I believe so, although the name is naïve)
- **Nobody now has a clear and comprehensive picture in mind** (if someone pretend to have it, fire him/her)
- **It should be developed, piece by piece**
- **Beware the bullshit** (a lot to come)
- **Join the efforts/Share the interests** (professionals, academics, companies, public agencies)