Citizens and cities facing new hazards and threats

30th November to 4th December 2020

Session 6: IA, Cybersecurity and IT

Juan Francisco Carías

Cyber Resilience Awareness Training Cyber Range

By:
Juan F. Carías
Marta Iturriza
Saioa Arrizabalaga
Josune Hernantes

Cities

- Most people live in cities.
- Complex system of systems
  - Social systems
  - Economical systems
  - Natural Resources
  - Infrastructures
- City Stakeholders
  - Public companies
  - Private companies
  - Citizens

Cyber Threats

- Cyber incidents are one of the most important global risks today (WEF, 2016-2020).
- By 2021, the WEF estimates that cyber incident costs will be around 6 billion USD, the equivalent to the GDP of the third largest economy in the world.
- Since 2016, the average cost per incident per company per year was estimated between the hundreds of thousands and the millions of euros (ENISA, 2016).

Are cities safe?

- Considering their stakeholders there are many threats to cities:
  - Cyber terrorism is the most generalized.
  - Ransomware, Cyber sabotage, Cyber bullying, etc. all affect the stakeholders and thus the city.
- Given this, are the countermeasures enough? Is cybersecurity enough?
  - Traditionally cybersecurity was concerned with protection i.e. being fail-safe.
  - Is it possible to be fail-safe anymore? What if the protection fails?

Cyber Resilience

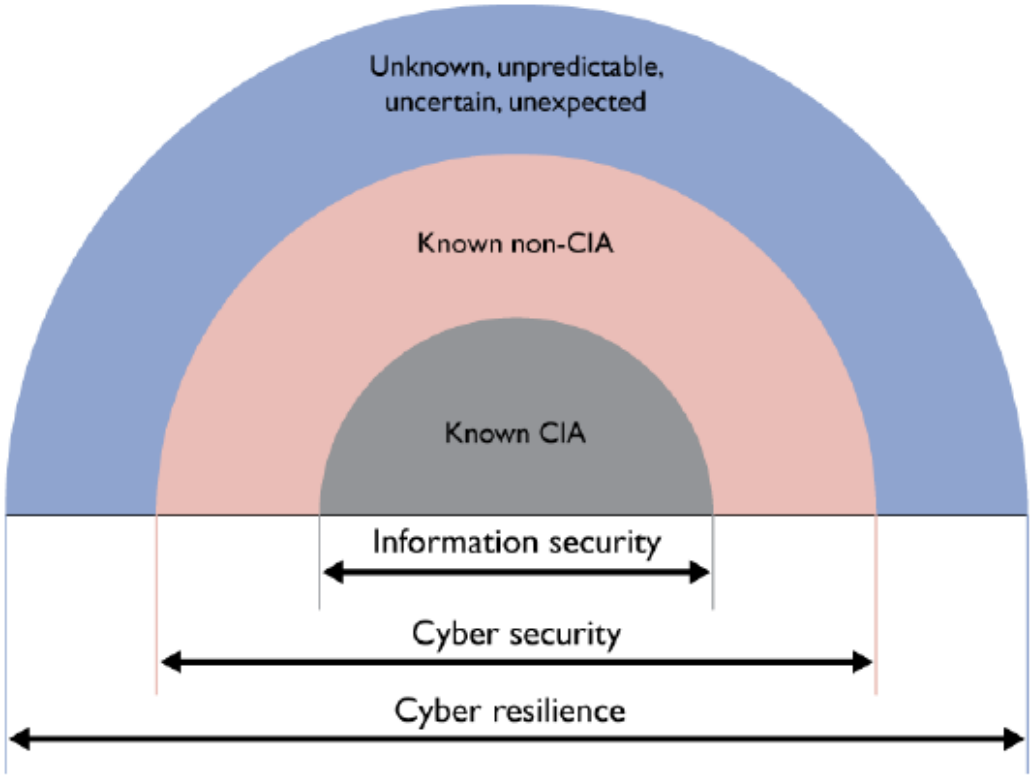
"Ability of a process, business, organization, or nation to anticipate, [detect], withstand, recover, and evolve in order to improve their capabilities in face of adverse conditions, stress, or attacks to the cyber resources it needs to function"

—INCIBE, 2019

Cyber Resilience vs Cybersecurity

Aspect	Cybersecurity	Cyber Resilience
Objective	Protect IT systems	Ensure business continuity
Intention	Fail-safe	Safe-to-fail
Architecture	Single layered protection	Multi layered protection
Scope	Atomistic, one organization	Hollistic, network of organizations

Cyber Resilience vs Cybersecurity



Sharkov, G. (2016)

Problem

- Cyber Resilience is multidimensional and multidisciplinary.
- Operationalization requires experience and knowledge.
- Companies usually lack this knowledge, especially SMEs which are 95+% of companies.

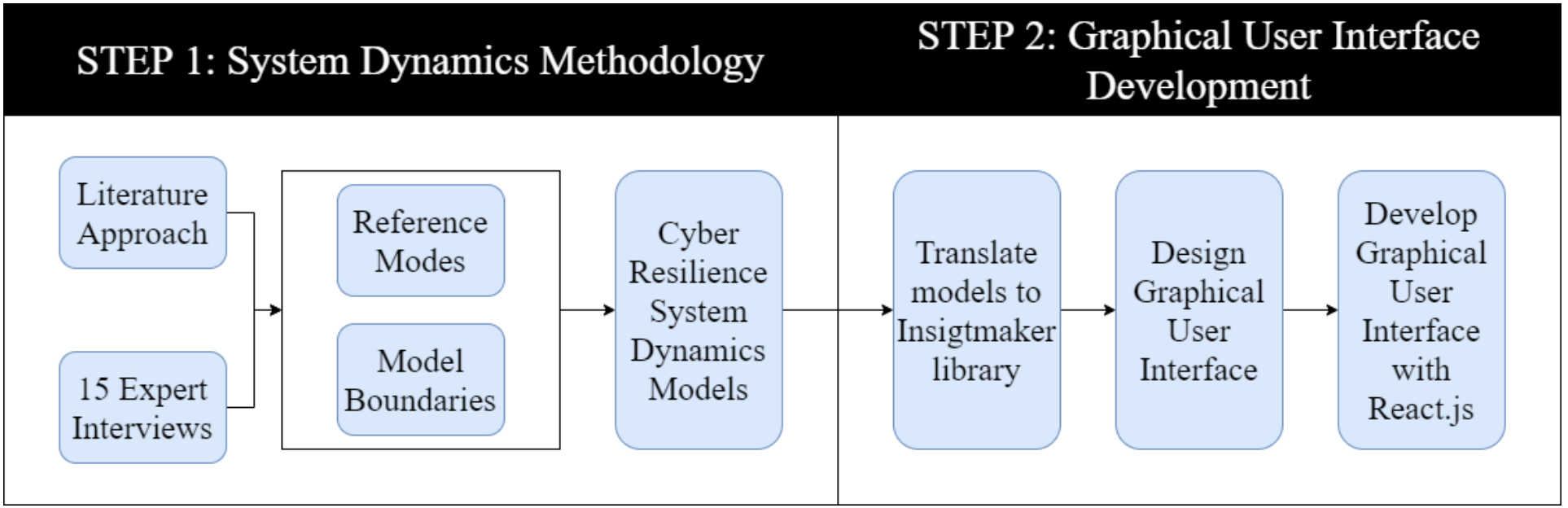
Current solutions

- Frameworks (NIST, WEF, Linkov, etc.)
- Metrics (Mitre, INCIBE, etc.)
- Maturity Models (C2M2, BC2M2, etc.)
- Standards (ISO 27000, ISA 62443, etc.)
- All of these are oriented towards the “what” to do, but “why?” and “when?”
- How do companies prioritizewhen they have limited knowledge?

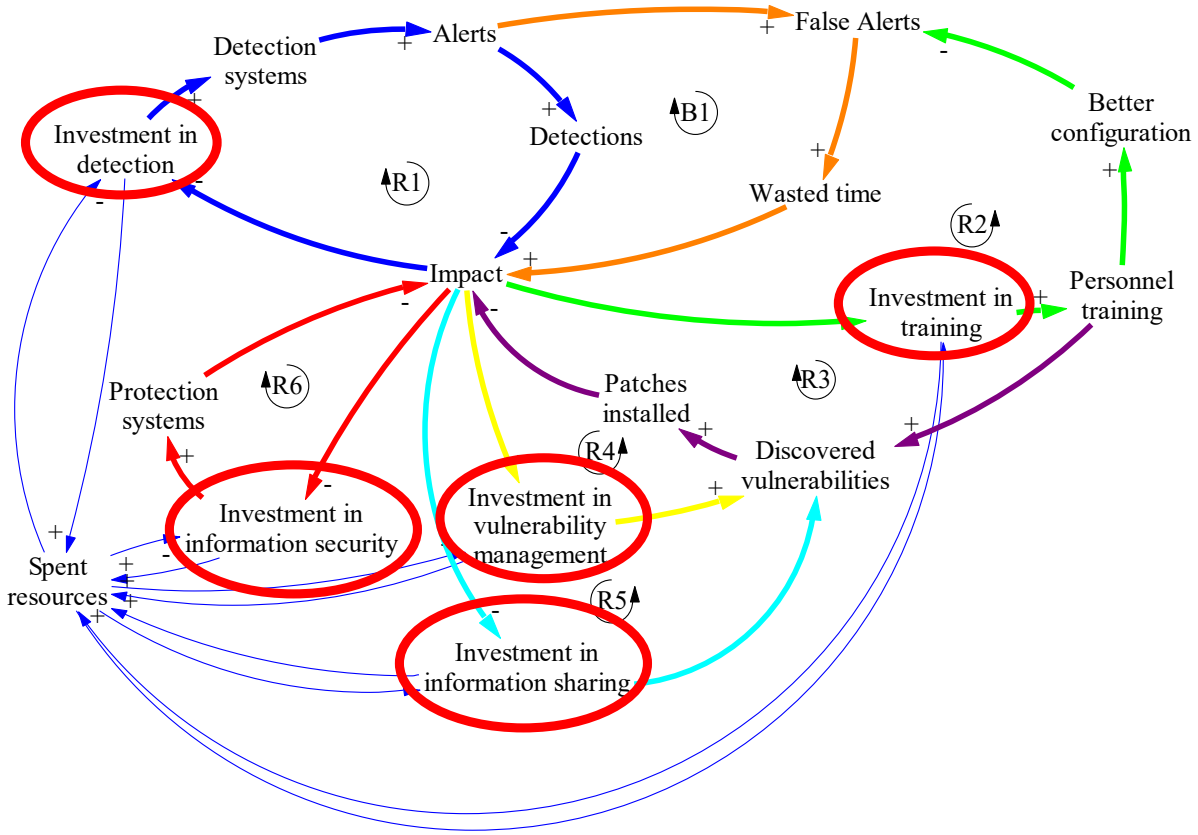
Proposal: Cyber ranges

- Cyber ranges as a form of serious game have been proven to be effective awareness raising tools.
- They let decision-makers understand and experiment with different investment strategies without compromising real assets.
- Gaining awareness could help decision-makers develop effective and informed strategies.

Methodology



Causal Loop Diagram



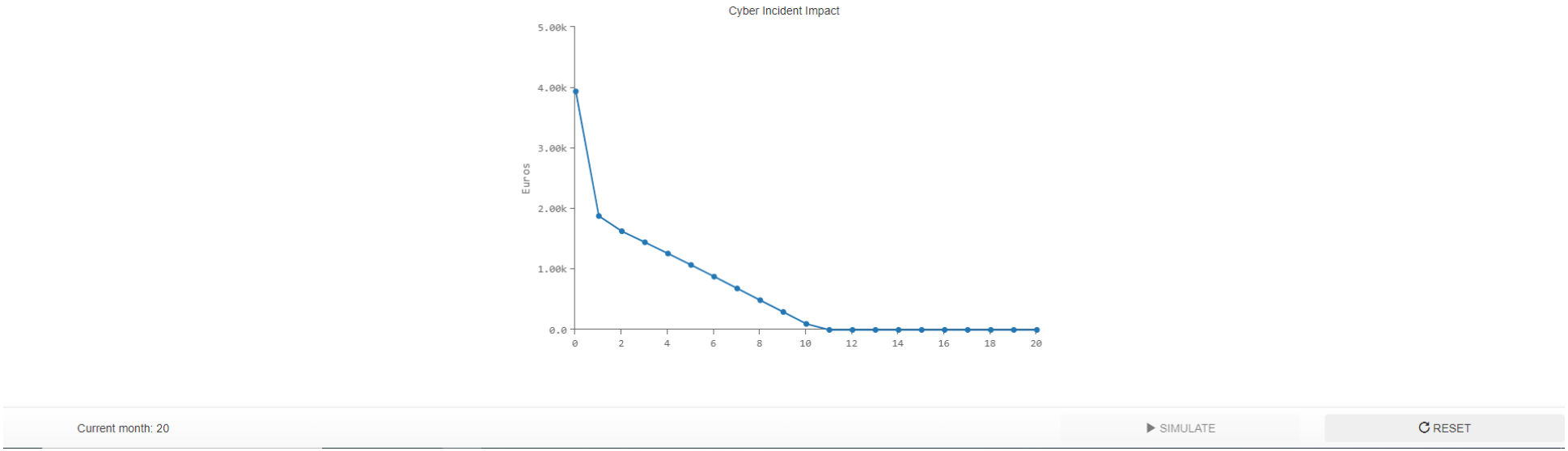
GUI: Investment Plan

Cyber Resilience Awareness Training Cyber Range

Please indicate the percetange of the budget you wish to allocate to each policy you would like to implement:

POLICIES	Investment %
Information security investment	0%
Detection processes and continuous monitoring investment	0%
Awareness and training investment	0%
Information sharing & communication investment	0%
Threat and vulnerability management investment	0%

GUI: Graph


Cyber Incident Impact
5.00k
4.00k
3.00k
2.00k
1.00k
0.0
Euros
0
2
4
6
8
10
12
14
16
18
20
Current month: 20
SIMULATE
RESET

Conclusions

- SD models with interfaces can be useful cyber ranges for decision-makers to gain awareness and develop effective strategies towards cyber resilience operationalization.
- These results can not only improve the knowledge and awareness of decision-makers but also reinforce the implementation of other cyber resilience operationalization aiding tools in the current literature.

Limitations

- The model has yet to be calibrated with real data to make a reality check and prevent it from being too theoretical.
- The use of serious games in the field of cyber resilience has yet to prove that it has similar benefits as in other areas.

Cyber Resilience Awareness Training Cyber Range

Thank you!
Questions?