Using a socio-technical systems approach to design and support systems thinking in cyber security education

Erjon Zoto, Stewart J. Kowalski, Edgar A. Lopez-Rojas, Mazaher Kianpour
erjon.zoto@ntnu.no; stewart.kowalski@ntnu.no; edgar.lopez@ntnu.no; mazaher.kianpour@ntnu.no;

Abstract

- Information security (IS) - protecting confidentiality, integrity, availability, authentication and accountability
- **Gap between what entities do and what should be done**, related to internal IS policies according to a systems perspective

Aim of this paper

- Promoting the usage of the socio-technical systems approach to support the emerging role of systems thinking in cyber security education
- Using simulation-based teaching tools to raise awareness of Master students towards cyber security

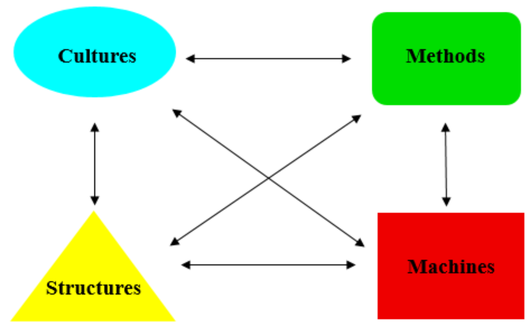
Introduction

Academia

- Developing new crosscutting concepts (Joint Task Force on Cybersecurity Education, 2017):
  - **Systems thinking**, considering the interplay between social and technical constraints to enable assured operations
  - **Adversarial thinking**, considering the potential actions of the opposing force working against the desired result

Background

Theoretical approach

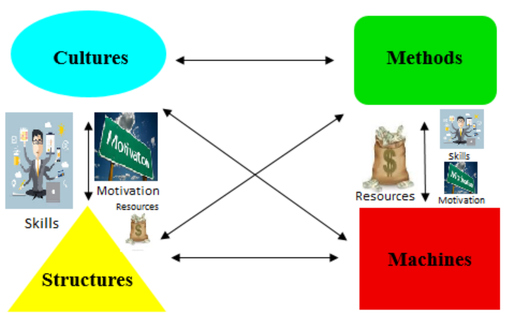


The socio-technical systems (STS) approach

Designing the CyberAIMs tool

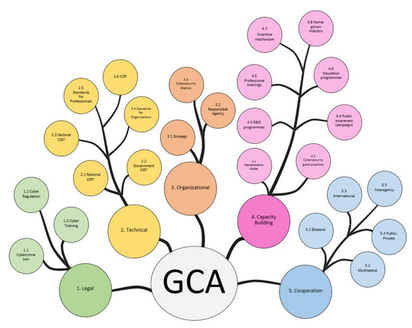
Defining main attributes

- Extending the STS approach to define main attributes for the tool



Skills

- Mapping values from Global Cybersecurity Index (ITU, 2017)



Resources

- Mapping values from different sources

Ponemon INSTITUTE

SANS IT Security Spending Trends

SIPRI Military Expenditure Database © SIPRI 2017

Defining initial values

Parameter	Side	Echelon/Category	*Range*
Resources	Defense	*Ind*	1-30
		SMB	1-40
		Corp	41-70
		States	60-100
	Attack	*Kid*	1-45
		Ideol	15-45
		Contract	45-67
		State	60-100
Skills	Attack / Defense	Low	1-30
		Moderate	31-70
		High	71-93
Motivation	Attack / Defense	Low	1-25
		Moderate Low	26-50
		Moderate High	51-75
		High	76-100

CyberAIMs

Simulation speed slider and ticks count

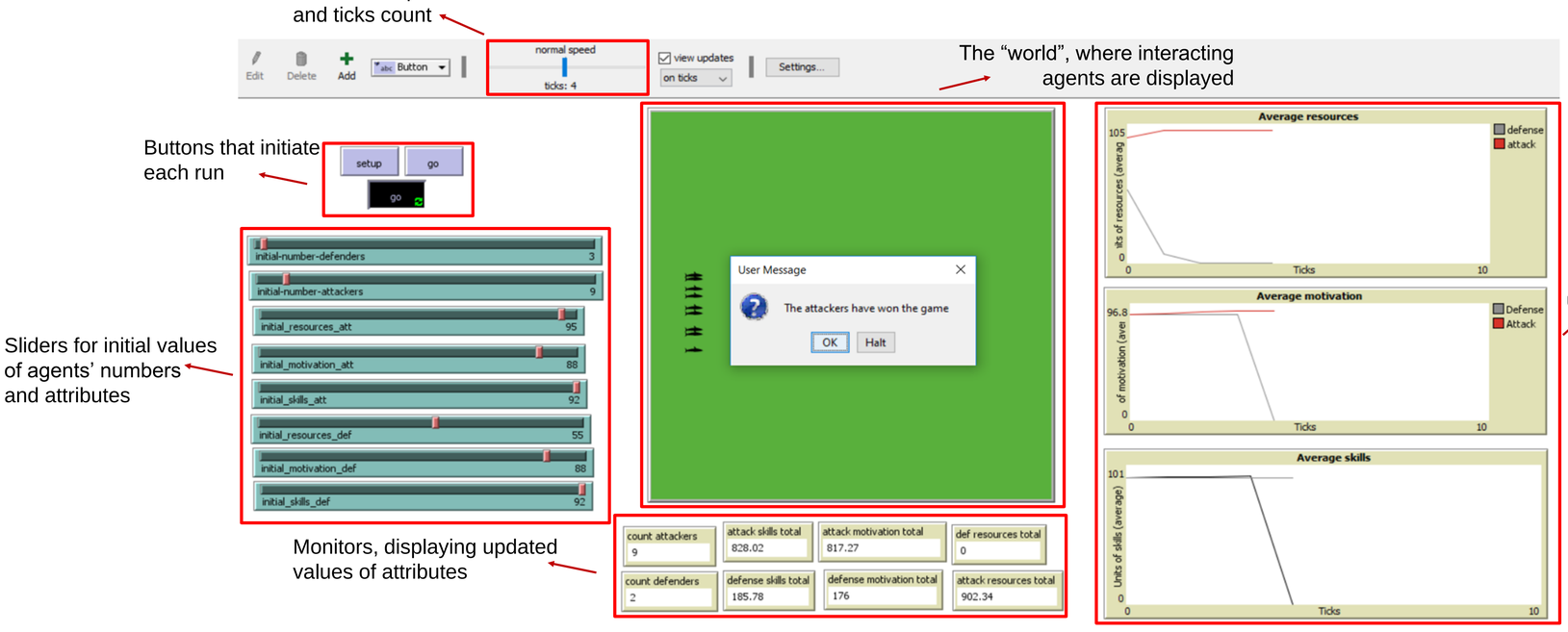
The "world", where interacting agents are displayed

Buttons that initiate each run

Sliders for initial values of agents' numbers and attributes

Monitors, displaying updated values of attributes

Plots, showing updated values



Current results

Using CyberAIMs with students

- Lab with 15 Master students in a cyber security course, NTNU Gjøvik
- Students have changed perspective on the main attributes affecting defense agents' performance after using the tool

Pre-lab results	***Post-lab results****
Defense Resources	***Attack Motivation***
Defense Skills	*Defense Motivation*
Defense Motivation	*Defense Skills*

**Preliminary results, with 3 matching respondents overall*

Conclusions & Future work

Conclusions

In this paper

- We presented how STS approach can be used in agent-based modeling and simulation, introducing the emerging role of systems thinking in cyber security education
- We created **CyberAIMs**, where we defined two sides of interacting agents, defense and attack, whose performance is related to their attributes values, namely *Resources*, *Skills*, and *Motivation*
- We used the tool as part of a lab within a course in cyber security, and current results show that students have changed their perspective as related to **systems** and **adversarial** thinking after using the tool.

Future Work

Increasing usability and coverage of the tool

- A deeper exploration of the *Motivation* attribute
  - MOMM's taxonomy
  - Protection Motivation theory
- A new version is already being tested
  - Randomized values of attributes
  - Introducing ratios for echelons (RAND, 2014)
- The STS approach will be further used
  - To analyze and interpret results from simulation runs
  - To develop the next versions of the tool
- A "teaching and training tool" for students and other potential targets
  - IS, Computer Science, Military, Health and Finance
  - Critical infrastructure agencies, suppliers and end users
- Increasing level of agents' intelligence
  - Raising knowledge of agents according to their opponents behavior

Acknowledgements

This work was carried out during the tenure of an ERCIM "Alain Bensoussan" Fellowship Programme, in the Information Security and Privacy Management research group, and supported further from the Systems Security and Digital forensics research groups at the Information Security and Communication Technology Department, NTNU in Gjøvik. We would like to express our special gratitude to our colleagues Basel Katt and Christopher Frantz, along with the other colleagues from NTNU in Gjøvik supporting this research and the Master students participating in the lab and answering related surveys.

NTNU Norwegian University of Science and Technology