An Adversarial Risk Analysis Framework for Cybersecurity

David Ríos, david.rios@icmat.es

AXA-ICMAT Chair in ARA and Real Academia de Ciencias

Joint with A. Couce, J.A. Rubio, D. Rasines, K. Musaraj, CYBECO team

Agenda

- **Motivation**
- Cyber Risk Management
- An ARA framework for cybersecurity resource allocation
- Case
- Discussion

Motivation

- Aurora attack ***targeted*** Google in 2009
- Attack ***targeted*** Sony to prevent release of *The Interview*
- Stuxnet, Flame, Duqu,… ***targeted*** Iran's nuclear program
- MANDIANT ***targeted*** Hong Kong
- ARAMCO ***targeted*** attack
- Russian ***targeted*** attack over Estonia

- Wannacry. ***Non-targeted***. Stops UK National Health service,…

- 50000M€ impact over German Economy
- Spain, 3rd country most attacked (with caution), mainly from Russia and China

Motivation

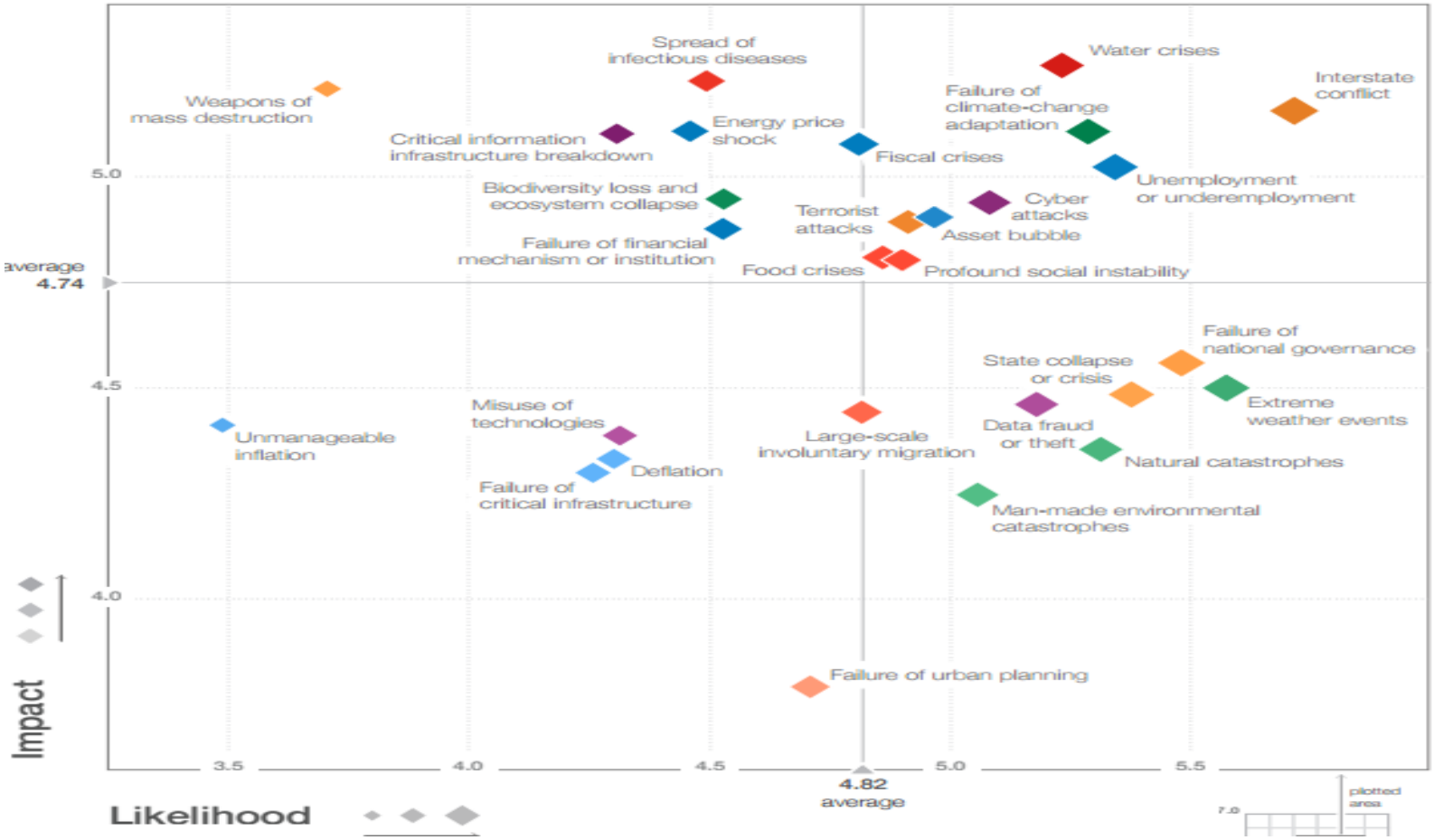
- **Increasingly relying on ICT:**
  - Cars, planes, medical systems, investing platforms, …
  - Critical infrastructure, voting systems, …
- **Increasingly interconnected systems:**
  - 10000 M devices connected to Internet

- **Variety of attackers:**
  - Countries, cybercriminals, internal actors, …
- **Increasing variety, and number, of threats:**
  - Virus, Worms, Trojan-horses, Spyware, APTs, Ransomware, …
- **Increasingly sophisticated, technologically but also socially.**
- **Response times tend to be excessive.**

- **Cause immense damage:**
  - Economic, environmental, health, …
  - Competitive intelligence, national security, reputation,...

- **Basic tools for cyber risk management**

Motivation



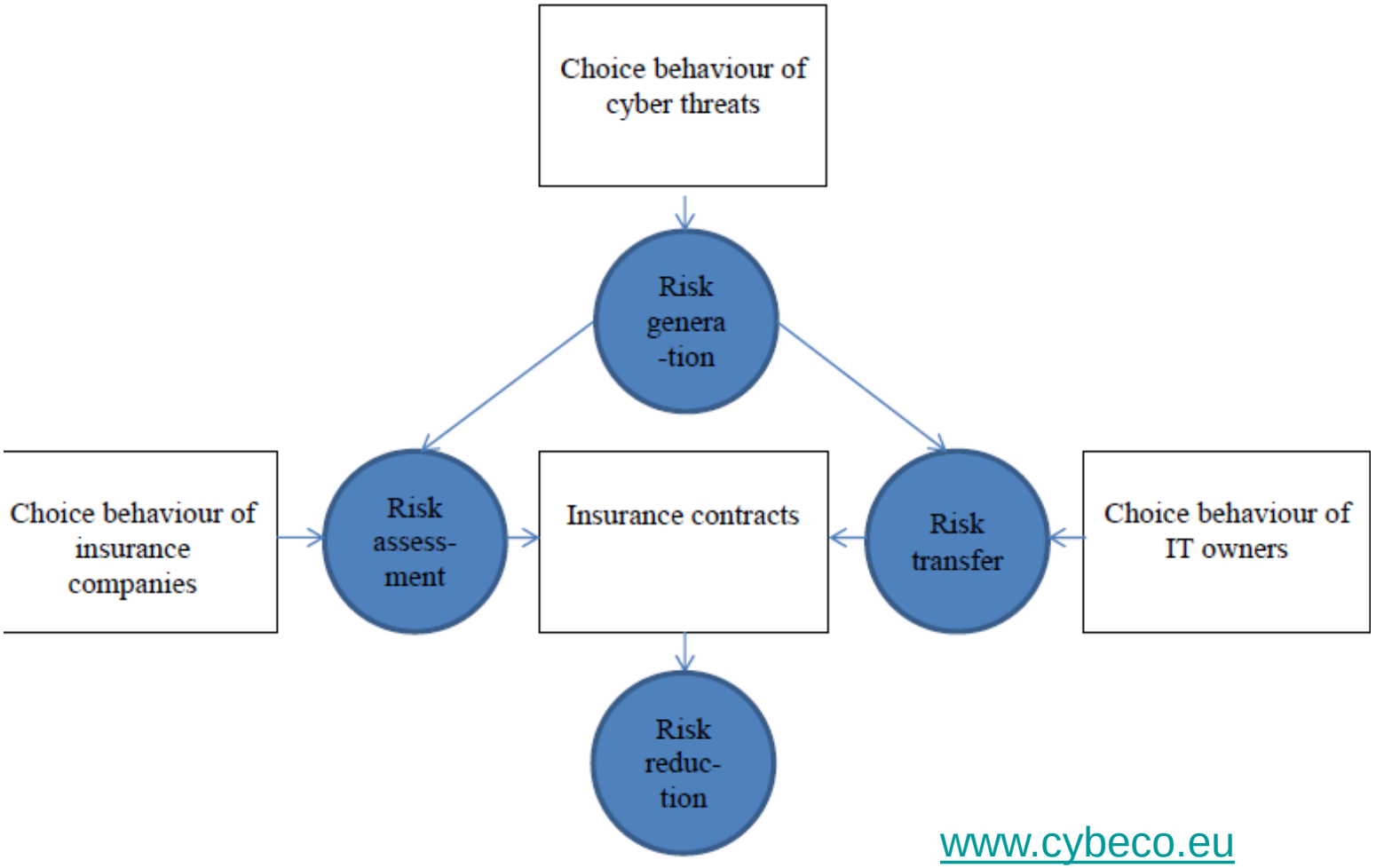
World Economic Forum. Global Risks Map for 2017

Motivation. Cyberinsurance

- Relatively recent products, Comparatively small market.
- Potentially enormous global costs.
- Data scarce, specially for losses. Companies not disclosing data breaches.

- Accumulation problems. Network effects.
- Moral hazard problems. Incentives for improving cybersecurity at large.
- Little data available. Structured expert judgement.
- Valuing information assets, reputation,… multi-attribute utility theory.

CYBECO. GA 740920. Digital Security



www.cybeco.eu
Tw:@CYBECO_project
LN: www.linkedin.com/company/cybeco

Agenda

- Motivation
- **Cyber Risk Management**
- An ARA framework for cybersecurity resource allocation
- Case
- Discussion

Approaches

- Risk analysis frameworks: CRAMM, EBIOS, ISAMM, Magerit, ISO 27005, MEHARI, NIST 800-30, ISO 31000,...
- Frameworks for Control Assessment and Compliance: ISO27001, ISO 27002, SANS Critical Security Controls, Common Criteria, Data Protection Laws, ISO 27031, Cloud Security Alliance Cloud Controls Matrix,…

Approaches

Excellent catalogues of assets, threats, countermeasures but…

VH	100	Very frequent	Daily
H	10	Frequent	Monthly
M	1	Normal	Yearly
L	1/10	Infrequent	Every few years
VL	1/100	Very infrequent	Every century

Risk		Probability				
		VL	L	M	H	VH
Impact	VH	H	VH	VH	VH	VH
	H	M	H	H	VH	VH
	M	L	M	M	H	H
	L	VL	L	L	M	M
	VL	VL	VL	VL	L	L

Impact		Degradation		
		1%	10%	100%
Value	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

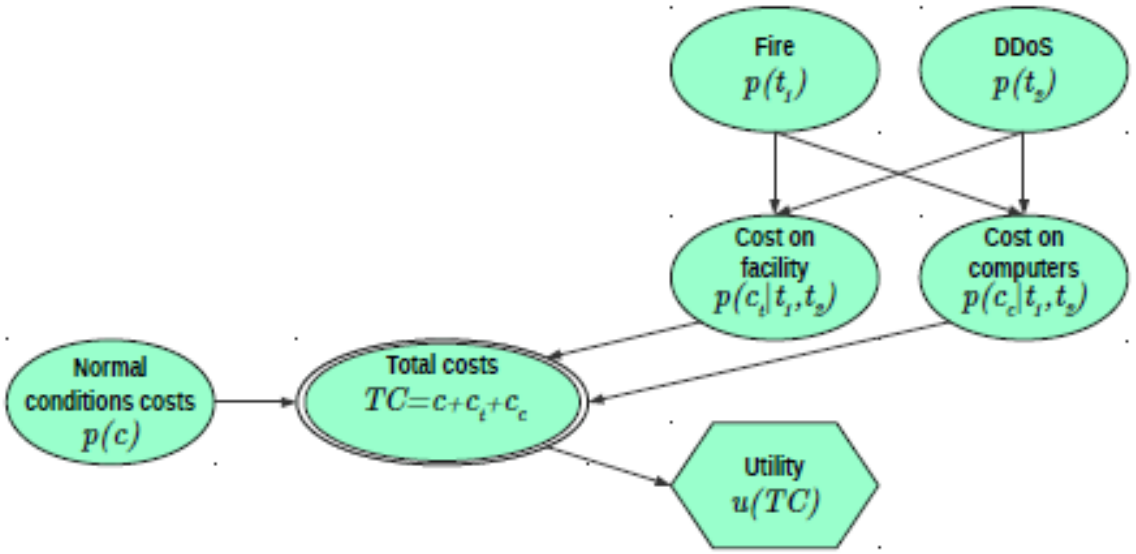
Defects reported in Cox (2008)
Intentionality?? HMG Standard 1

Little data

Agenda

- Motivation
- Cyber Risk Management
- **An ARA framework for cybersecurity resource allocation**
- Case
- Discussion

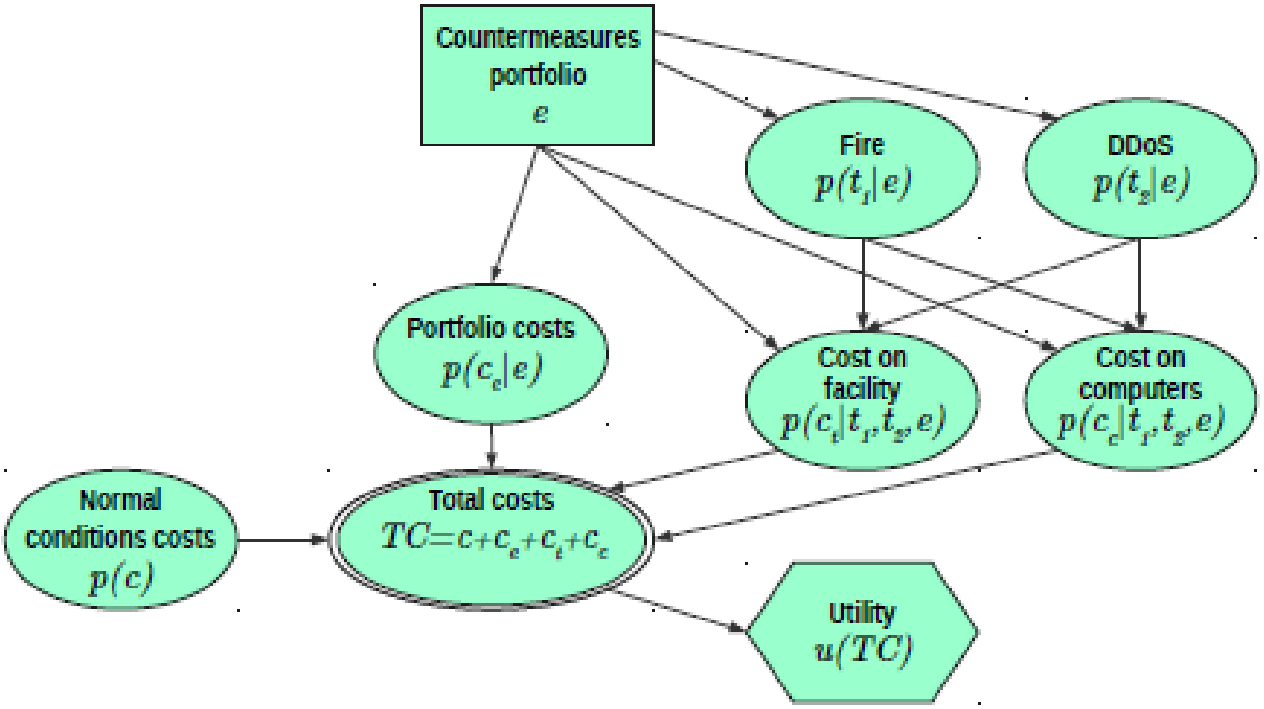
Cybersec risk assessment



$$\psi_r = \int \dots \int u(c + c_t + c_c)\, p(c)\, p(c_t, c_c|t_1, t_2)\, p(t_1, t_2)\, dt_1\, dt_2\, dc_t\, dc_c\, dc$$

$$\psi_n - \psi_r$$

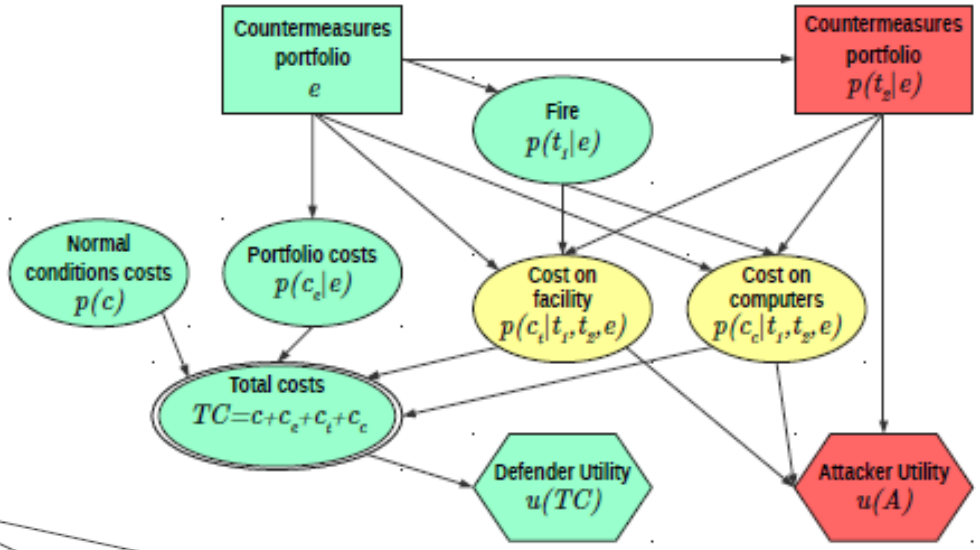
Cybersec risk management

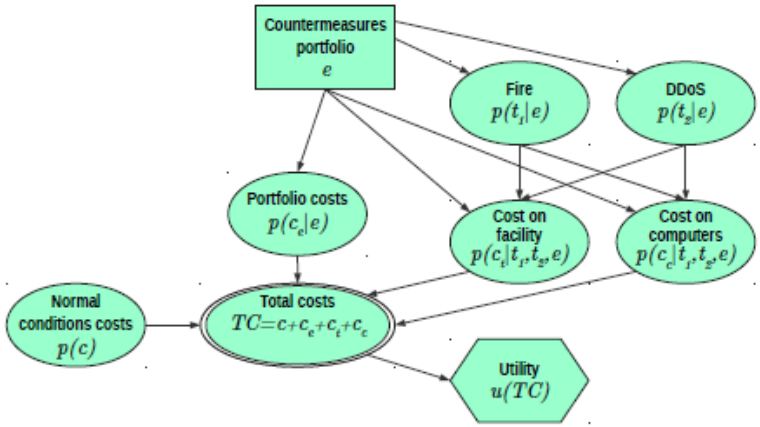


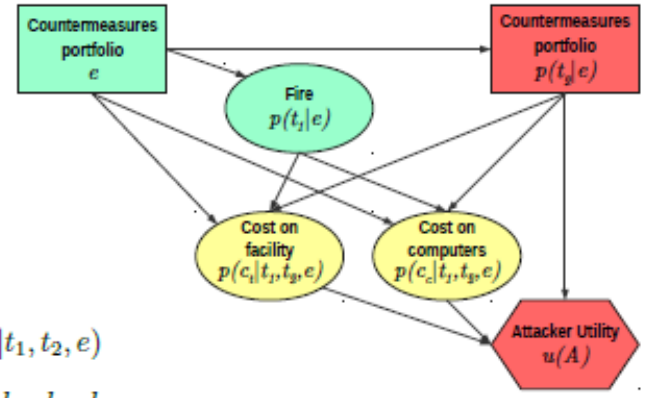
$$\psi(e) = \int \dots \int u(c_e + c_t + c + c_c)\, p(c)\, p(c_e|e) p(t_1|e)\, p(t_2|e)\, p(c_t|t_1, t_2, e)\, p(c_c|t_1, t_2, e)$$
$$dt_1\, dt_2\, dc_t\, dc_c\, dc_e\, dc$$

$$\psi_e^* = \max_{e \in E} \psi(e)$$

ARA in cybersec

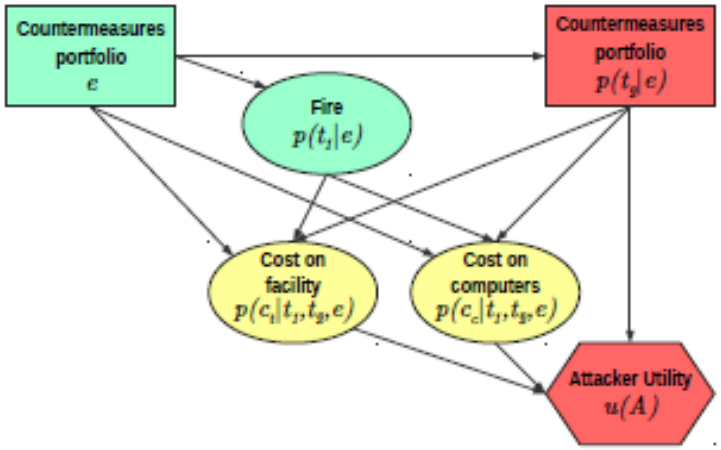






$$\psi(e) = \int \dots \int u(c_e + c_t + c + c_c)\, p(c)\, p(c_e|e) p(t_1|e)\, p(t_2|e)\, p(c_t|t_1,t_2,e)\, p(c_c|t_1,t_2,e)$$
$$dt_1\, dt_2\, dc_t\, dc_c\, dc_e\, dc.$$

ARA in cybersec



$$\psi_A(t_2|e) = \iiint u_A(t_2, c_t, c_c) p_A(t_1|e) p_A(c_t|t_1, t_2, e) p_A(c_c|t_1, t_2, e) dt_1 dc_t dc_c$$

$$\max_{t_2 \in T_2} \psi_A(t_2|e),$$

$$T_2^*(e) = \arg\max_{t_2 \in T_2} \iiint U_A(t_2, c_t, c_c) P_A(t_1|e) P_A(c_t|t_1, t_2, e) P_A(c_c|t_1, t_2, e) dt_1 dc_t dc_c.$$

$$F = (U_A, P_A(t_1|e), P_A(c_t|t_1, t_2, e), P_A(c_c|t_1, t_2, e))$$

Algorithm 1 Calculation of distribution over attacks.

For each e

  For $i = 1, \ldots, K$

    Generate

$$\left(U_A^i(t_2, c_t, c_c), P_A^i(t_1|e), P_A^i(c_t|t_1, t_2 e), P_A^i(c_c|t_1, t_2 e)\right) \sim F$$

    Compute

$$t_2^i = \arg\max_{t_2} \iiint U_A^i(t_2, c_t, c_c)\, P_A^i(t_1|e)\, P_A^i(c_t|t_1, t_2, e)\, P_A^i(c_c|t_1, t_2, e) dt_1\, dc_t\, dc_c$$

  end

  Approximate

$$\hat{p}_A(t_2|e) = \frac{\#\{t_2^i = t_2\}}{K}$$

end

Agenda

- Motivation
- Cyber Risk Management
- An ARA framework for cybersecurity resource allocation
- **Case**
- Discussion

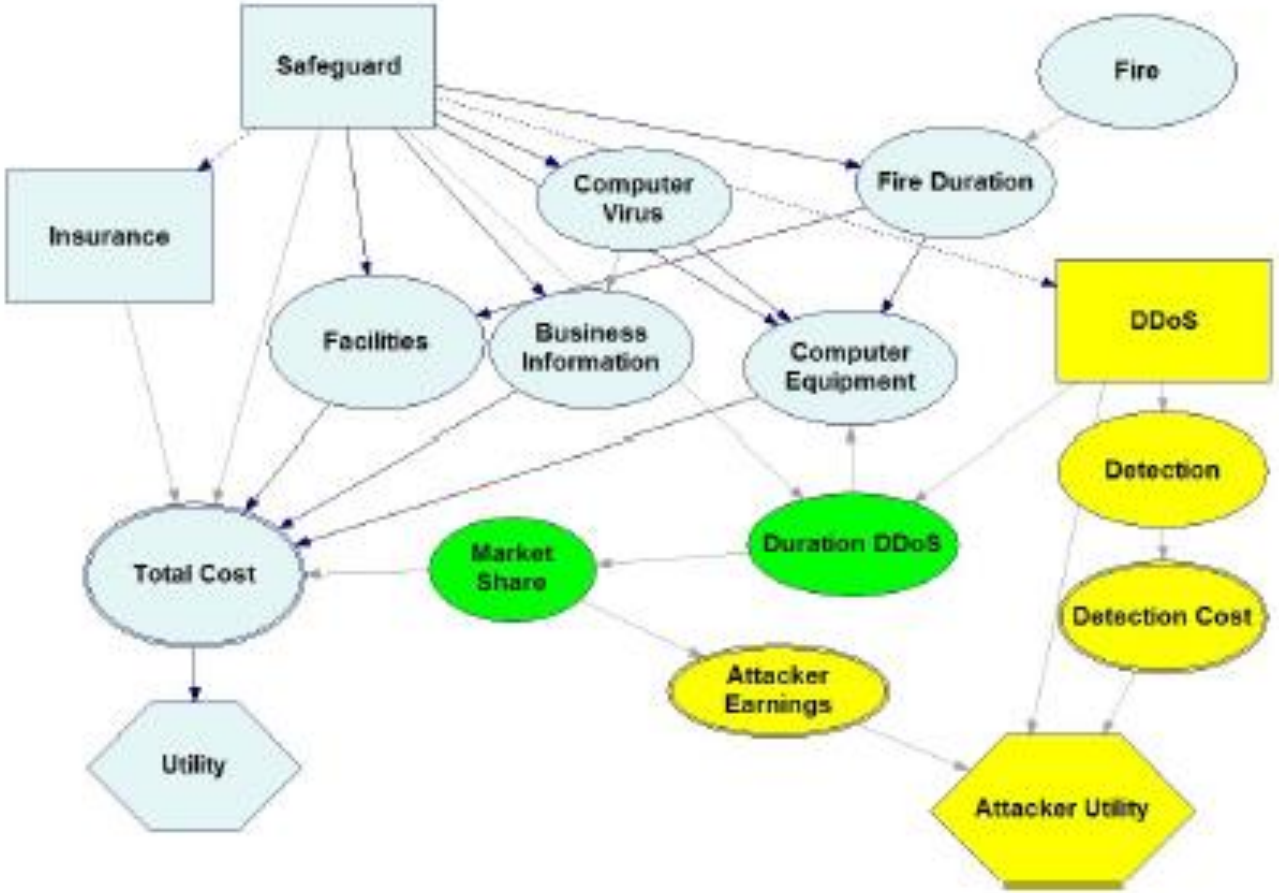
Case study: Process

- Problem structuring. Multiagent Influence Diagram
  - Assets
  - Impacts
  - Nonintentional threats
  - Environmental uncertainties
  - Intentional threats (and authors)
  - Attacker uncertainties
  - Safeguards
  - Insurance
  - Preferences
- Defender problem
- Attacker(s) problem(s)

Case study: Process

- Assessing defender's non adversarial beliefs and preferences
- Assessing attacker's random beliefs and preferences
- Simulating from the attacker problem to forecast his attacks
- Solve the defender problem to find optimal resource allocation and insurance
- Sensitivity analysis

Case study


Safeguard
Fire
Insurance
Computer Virus
Fire Duration
DDoS
Facilities
Business Information
Computer Equipment
Detection
Total Cost
Market Share
Duration DDoS
Detection Cost
Attacker Earnings
Utility
Attacker Utility

Case study

- Assets

Computer equipment, Facilities, Market share, Business info

- Non intentional threats

Fire, Virus

- Intentional threats

DDoS (different gbps) from a competitor

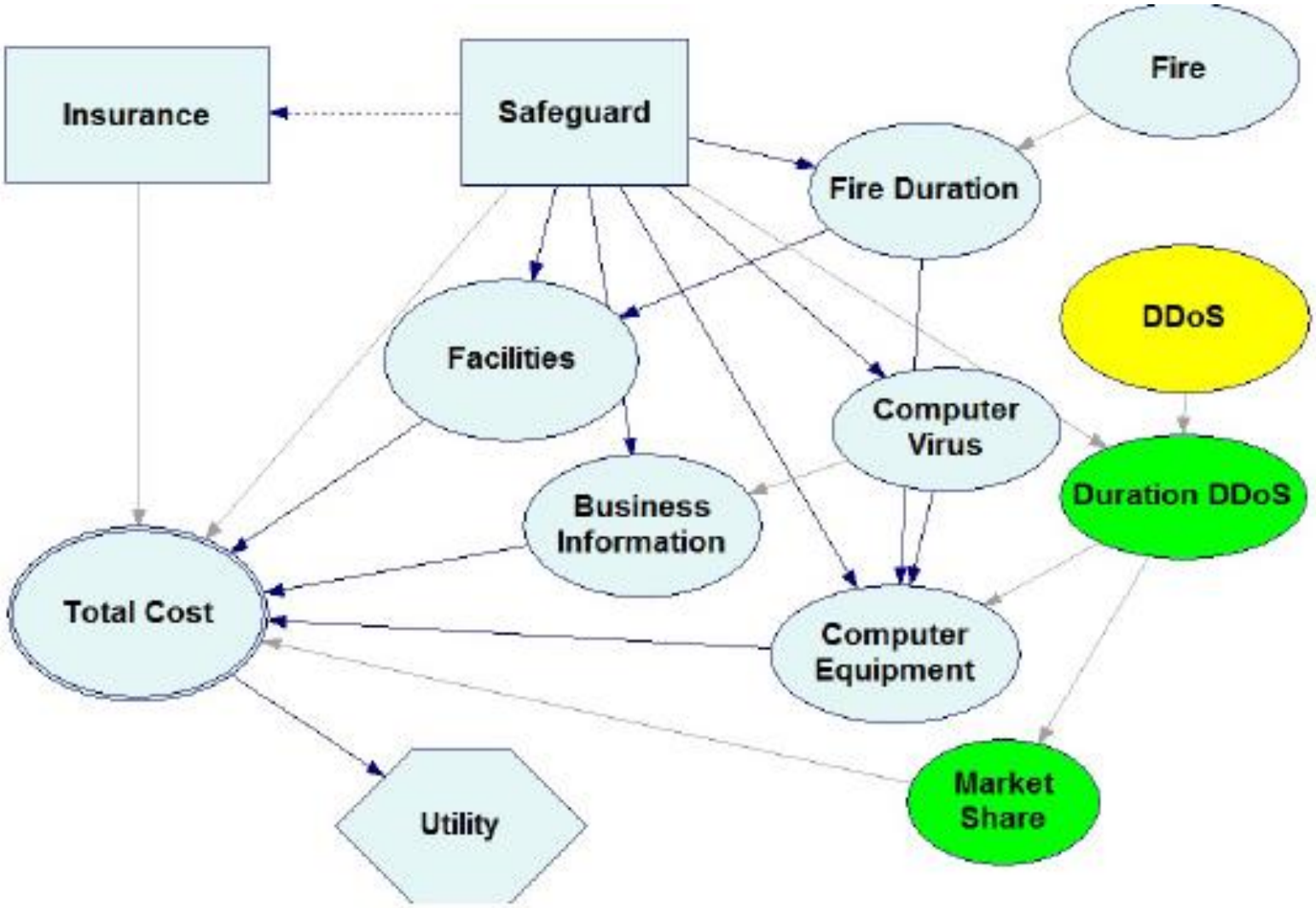
- Safeguards

Antifire, firewall, ISO risk mitigation procedures, Cloud based DDoS protection

- Insurance

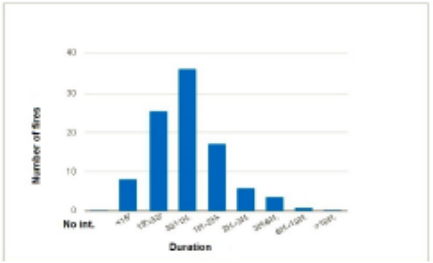
None, Fire, Cyber, Comprehensive

Case study

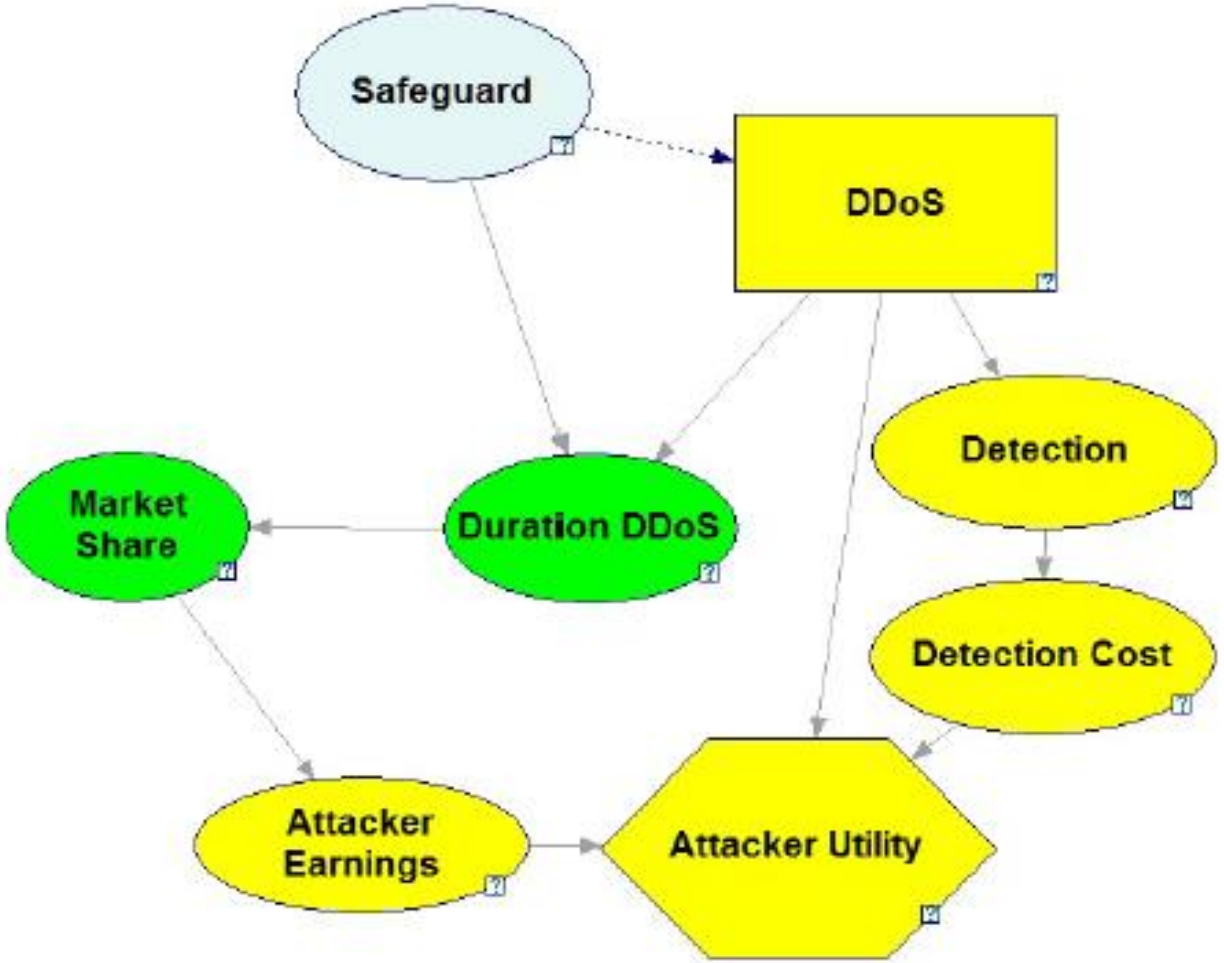

Insurance
Safeguard
Fire
Fire Duration
DDoS
Facilities
Computer Virus
Duration DDoS
Business Information
Total Cost
Computer Equipment
Utility
Market Share

Case study

- Fire
  - Likelihood
  - Duration
  - Impact on facilities and equipment
- Virus
  - Likelihood
  - Impact
- DDoS
  - Likelihood?
  - Duration
  - Impact



Case study

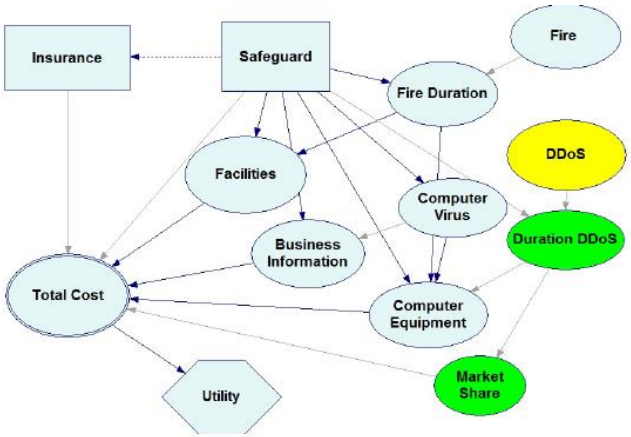

Safeguard
DDoS
Detection
Market Share
Duration DDoS
Detection Cost
Attacker Earnings
Attacker Utility

Case study

- DDoS duration. Random distribution
  - If no firewall is included in the portfolio of countermeasures, we model it as Gamma distribution with parameters a and p, with a uniformly distributed in $[3.5, 4.5]$ and p uniformly distributed in $[0.8, 1.2]$.
  - If, on the other hand, a firewall is included in the portfolio of countermeasures, we model it as a Gamma distribution with parameters a and p, with a uniformly distributed in $[0.3, 0.7]$ and p uniformly distributed in $[0.8, 1.2]$.
- Simulation model

$$A^*(s) = \arg\max_a \int ... \int U_A(ae, a, dc) P_A(ae|ms) P_A(ms|dd) P_A(dd|s, a) P_A(dc|d) P_A(d|a) dae...dd.$$

Case study



Anti-fire decision	Firewall decision	Procedure decision	DDoS protection decision	Insurance decision	Expected utility
no anti-fire	firewall	no procedure	10 gbps	traditional	0.9995698
anti-fire	no firewall	no procedure	10 gbps	comprehensive	0.9994854
anti-fire	no firewall	procedure	10 gbps	comprehensive	0.9994546
anti-fire	firewall	no procedure	10 gbps	comprehensive	0.9994381
no anti-fire	firewall	no procedure	10 gbps	comprehensive	0.9993949
...	...	...	...	...	...
no anti-fire	no firewall	procedure	no protection	cyber	0.9451530
no anti-fire	firewall	procedure	no protection	no insurance	0.9444523
no anti-fire	no firewall	no procedure	no protection	cyber	0.9444453
no anti-fire	firewall	procedure	no protection	cyber	0.9443398
no anti-fire	no firewall	no procedure	no protection	no insurance	0.9434914

Case study

- Sensitivity analysis
  - Maximum price willing to pay for insurance
  - Change in virus probability
- Budget constraints
- Return on risk mitigation investments

Agenda

- Motivation
- Cyber Risk Management
- An ARA framework for cybersecurity resource allocation
- Case
- **Discussion**

Discussion

- ARA provides opportunities from improved modeling of intentionality in cybersecurity
- Allows better forecasting of actions. Fermi-tising the questions
- Integrates cyberinsurance together with portfolio.
- Integrates preference modelling
- Problem discussed: IT owner deciding security investment

- The view from the insurance company?
  - Behavioral experiments to determine pricing
  - Behavioral experiments to segment market
- The view from reinsurers

Grazie

Collabs welcome!!!

david.rios@icmat.es

SPOR DataLab ICMAT.
https://www.icmat.es/spor/