De la gestión de riesgos a la gestión de riesgos adversarios: Aplicaciones en seguridad aérea y lucha contraterrorismo

U. 11 de Novembro, Cabinda

David Ríos, Real Academia de Ciencias

Septiembre, 2013

Agenda

- El concepto de riesgo
- Análisis de riesgos
  - Conceptos generales
  - Un marco
  - Un ejemplo
  - Un ejemplo de aviación
  - Otros ejemplos
- Análisis de riesgos adversarios
  - Conceptos básicos
  - Un ejemplo contraterrorismo
  - Otros ejemplos
- Discusión final

El concepto elusivo de riesgo

Conceptos relacionados con riesgo en numerosos campos

- Teoría de la Decisión Estadística:

Función de riesgo, Riesgo Bayes

- Estadística

Modelos de sucesos extremos, Fiabilidad

- Economía

Decisiones en riesgo vs Decisiones en incertidumbre

- Finanzas

Valor en Riesgo (y conceptos relacionados)

- Seguros

Pérdida Esperada Anual

- Seguridad

Riesgos Adversarios

El concepto elusivo de riesgo

- Estar vivo significa buscar oportunidades tomar riesgos
- Hay incertidumbre sobre el resultado y es posible que sea negativo (pero no necesariamente!!!)
- Posible definición
  - Situación en la que es posible una desviación adversa de un resultado deseable que se espera.

    1. Lista de sucesos potenciales
    2. Probabilidad de que ocurra un suceso adverso
    3. Consecuencias del suceso adverso

Riesgos

- Muchos tipos de riesgos: ambientales, financieros, políticos, tecnológicos,…
- Clasificaciones estándar:
  - Financieros y no financieros
    - Financieros: Crédito, Mercado, Operacional,…
  - Estáticos y Dinámicos
    - Asociados con funcionamiento status quo (pérdidas posibles), Asociado con cambios (pérdidas, ganancias)
  - Fundamentales y Particulares
    - Grupo (terremoto), Individual (fuego)
  - Puros (pérdida, no pérdida) y especulativos (pérdida y ganancia)
  - …..

Global Risks

2012. WEF

Riesgos: Su carga

- Algunas pérdidas llegan a ocurrir: Evitar o aliviar su impacto
- La incertidumbre es una carga: asegurar, reservar fondos, invertir en protección,…
- Frena el crecimiento económico, impacta en el coste del capital
- Crea sentimiento de frustración e intranquilidad (aunque hay aficionados al riesgo y aficionados al riesgo inteligentes)
- Más riesgos y más variados
  - De la naturaleza y los depredadores, a los riesgos asociados con la energía nuclear, el transporte aéreo, las tecnologías de la información, el terrorismo, el cambio climático,…
- Con pérdidas más severas
  - Cada catástrofe parece superar la anterior…
  - Más riqueza, más inversión, más activos expuestos a pérdidas…

Riesgos: retos en un mundo complejo

- Accidente del aeropuerto de Sao Paulo

La población ha crecido: Instalaciones antes alejadas, ahora cercanas a la población

- Cambio climático

Opinión pública mucho más consciente de las amenazas sobre la vida

- Ciberataque sobre Estonia

Necesidad de proteger infraestructuras críticas para garantizar la continuidad de una nación. Infraestructuras internacionales interconectadas. Ciberguerra fría.

- Interdependencia creciente a escala global. Lockerbie

Sistemas de seguridad interdependientes. Cada compañía es parte de un sistema interconectado y decide independientemente si adopta o no estrategias de portección. Puede sufrir si no adoptan medidas similares.

- Katrina, Tsunami, Haiti, Japón, Volcanes islandeses,…..

Los grandes desastres naturales...

- 11-S, 11-M, Piratas somalies,…

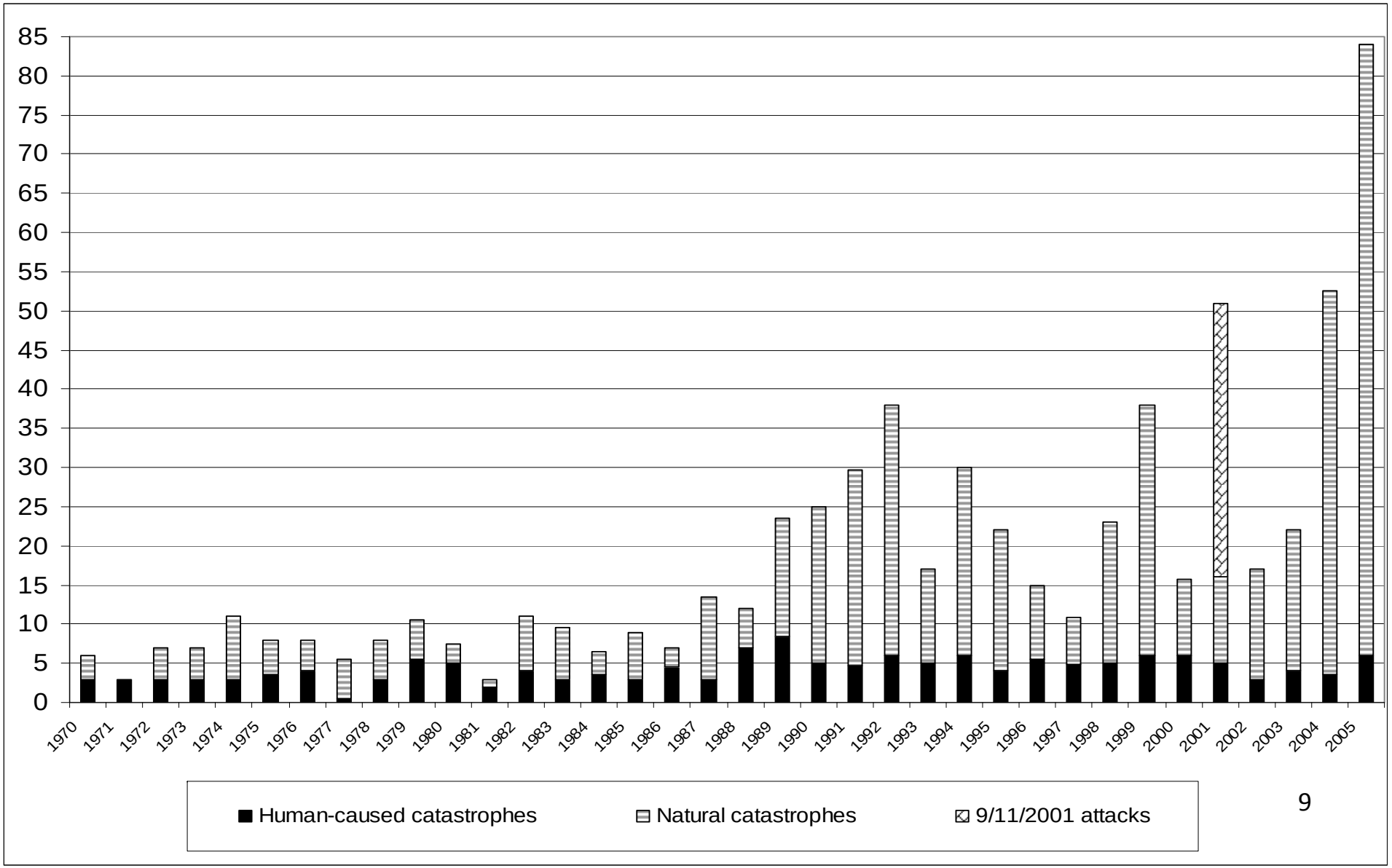
Organizaciones delictivas y terroristas globales dirigidas empresarialmente (capitalismo de degüello)

- Accidente de Air France

El factor humano

Sucesos de baja probabilidad y altas concecuencias parecen más frecuentes

Evolución Mundial de Pérdidas Catastróficas Aseguradas 1970-2005



Riesgos en un mundo moderno

La gestión de riesgos es prioridad principal para la alta dirección de las principales compañías.

Hace siete años: Gestión de recursos humanos y del talento (Accenture)

Demanda creciente de seguridad en una economía globalizada, presión de los reguladores,…

Análisis de riesgos

Un proceso analítico sistemático para evaluar, gestionar y comunicar el riesgo, que se realiza para entender la naturaleza de las consecuencias negativas, no deseables para la vida humana, la salud, la propiedad y/o el medio ambiente (para reducir o eliminarlas)

1. **Evaluación de riesgos**. Información de la relevancia y las características de los riesgos atribuidos a una amenza.
2. **Gestión de riesgos**. Actividades dirigidas a controlar las amenazas.
3. **Comunicación de riesgos**. Intercambio de información y opiniones en relación con el riesgo y sus factores entre evaluadores de riesgo, gestores de riesgo y otros participantes.

Evaluación de intereses. Se emplea para analizar la percepción de riesgo, entender el problema y evaluar los intercambios entre riesgos y beneficios. (1')

Análisis de riesgos: Para qué??

Gestión de riesgos para una instalación/sistema existente o propuesta

Desarrollo de regulaciones/normativas

Demostración de cumplimiento de regulaciones

Demostración de la necesidad de mejorar en el cumplimiento de regulaciones

Litigios

Investigación científica

Análisis de riesgos: Una historia breve

- Predada inicialmente por el sector seguros
- El impacto de las ciencias/ingeniería de la decisión
- Seguridad de sistemas (militar, ingeniería aeroespacial, industria nuclear)
- Gestión: Identificados y evaluados los riesgos a que estamos expuestos, podemos evitar la ocurrencia de ciertas pérdidas y minimizar el impacto de otros. El coste del riesgo puede gestionarse y reducirse a sus niveles mínimos.
- La presencia de adversarios inteligentes: análisis de riesgos+teoría de juegos

Matrices de riesgos!!! (SIC)

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

risk		*frequency*			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

Proceso

1. Determinar objetivos
    1. Mantener/Mejorar la eficacia operativa de una organización
2. Identificación de amenzas
3. Evaluación de amenazas
4. Considerar alternativas y seleccionar mejor tratamiento
5. Implantar la decisión (Comunicar!!!)
6. Evaluar y revisar

Un marco para el análisis de riesgos: Hipótesis iniciales

- Sólo interesados en costes…
- Una alternativa existente…
- Sólo mi organización es relevante
- Objetivo. Maximizar la utilidad esperada

Marco para el análisis de riesgos

- Predecir **costes** bajo circunstancias normales
- Identificar amenazas, estimar probabilidades e impactos en los costes (costes adicionales inducidos)
- Predecir costes (un modelo de mixturas).
- Calcular cambios en la utilidad esperada. Si demasiado grandes…
- Identificar intervenciones, estimar impacto sobre probabilidades y/o costes.
- Calcular utilidades esperadas. Escoger la mejor intervención (si la ganancia es suficiente)

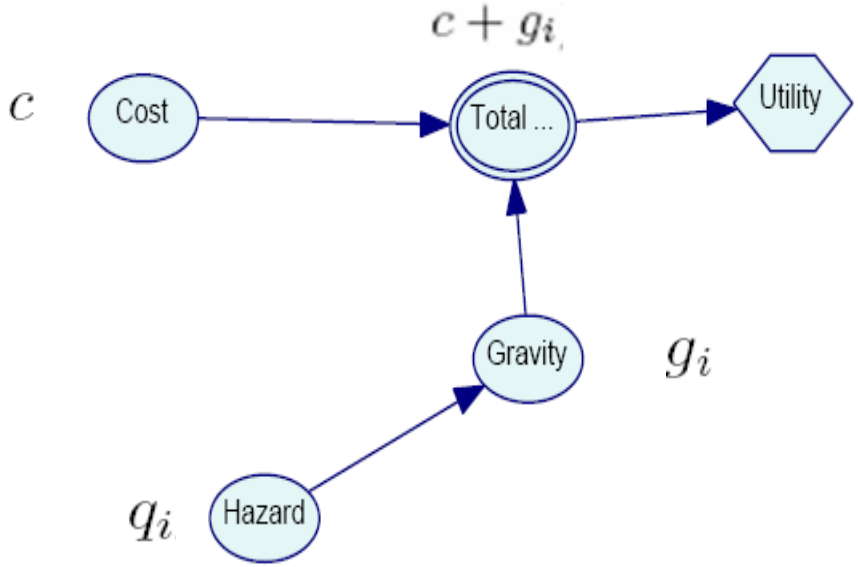
Escenario de partida

- Diseño dado (no hay intervenciones, status quo)
- Se identifican los costes (aleatorios)
- Se calcula la utilidad esperada

$$\Psi = \int u(c)\pi(c)dc$$

Evaluación de riesgos

- Verosimilitud e impacto de las amenazas identificadas



Ocurren con cierta probabilidad y conllevan un coste adicional

- Calculamos utilidad esperada despues de evaluar riesgos

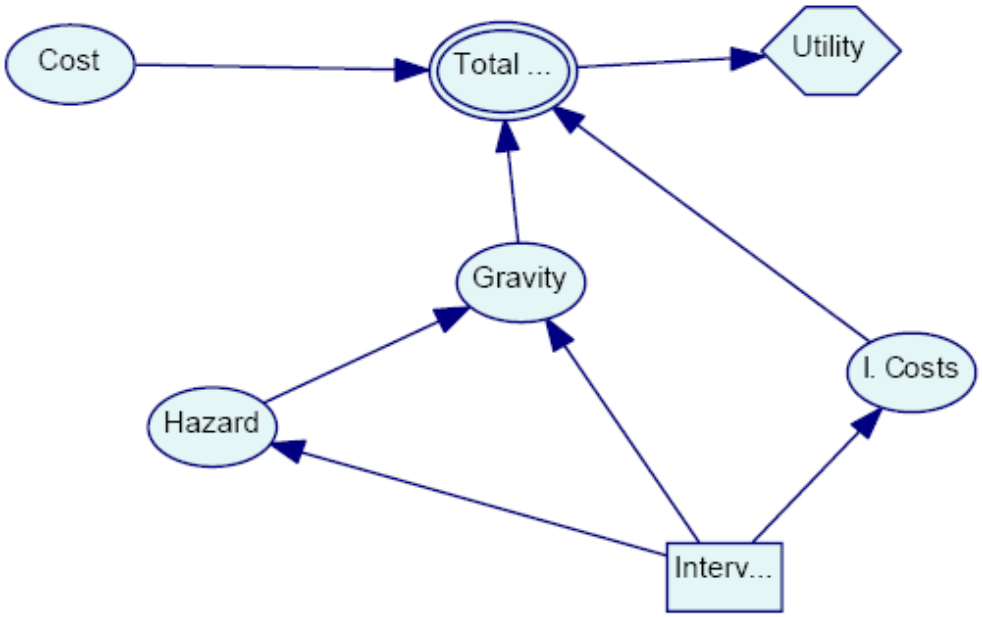
$$\Psi_r = \int \int \int \sum q_i u(c + g_i)\pi(q)\pi(g)dqdg \;\; \pi(c)dc$$

- Impacto: $\Psi - \Psi_r$

Si el impacto es muy grande, necesitamos gestionar los riesgos

Gestión de riesgos

- Intervención a escoger:



Tienden a reducir la verosimilitud de las amenazas y su gravedad... pero conllevan un coste

$$\Psi_d = \max_d \Psi_r(d) = \max_d \int\int\int\int \sum q_i u(c+g_i+c_d)\pi(q|d)\pi(g|d)dq\ dg\pi(c)\pi(c_d)\ \ dc_d\, dc$$

- Ganancia con riesgo gestionado : $\Psi_d - \Psi_r$

Escoger intervención que aporta mayor ganancia, si es suficientemente grande ...

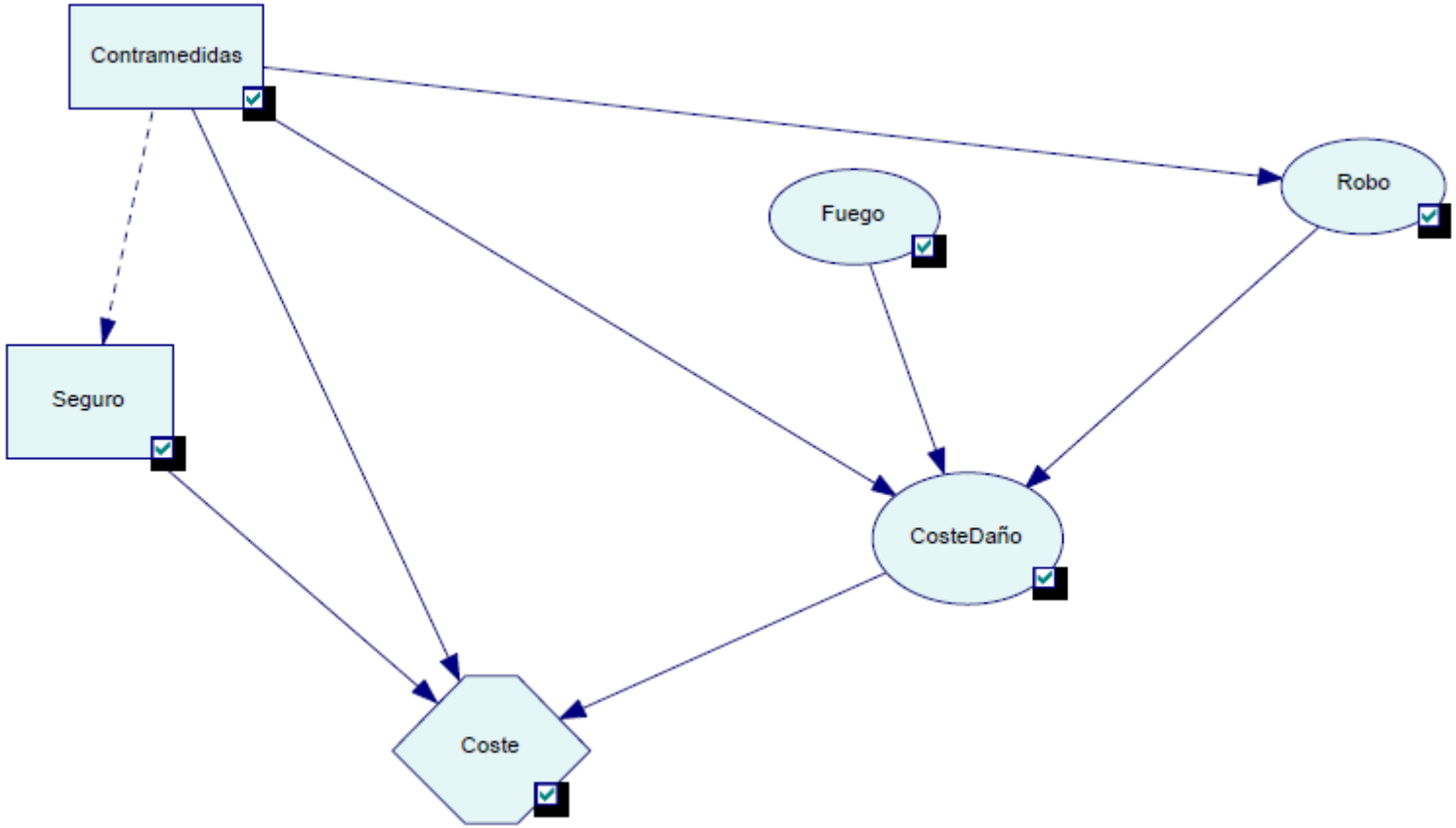
Análisis de riesgos: Un ejemplo sencillo

- Consideramos la adopción de contramedidas y compra de seguros para un local de una empresa.
- Amenazas: Nada, Fuego, Robo
- Contramedidas:
  - Alarma. Hace muy improbable un robo
  - Detector. Hace menos severo un fuego
  - No hay presupuesto para implantar ambas

Análisis de riesgos: Un ejemplo sencillo (bis)

- Seguro:
  - Cubre todos los costes de fuego o robo.
  - Es más barato si se implantan contramedidas
- Las cantidades involucradas son pequeñas para la empresa por lo que suponemos neutralidad frente al riesgo.

Análisis de riesgos: Un ejemplo sencillo



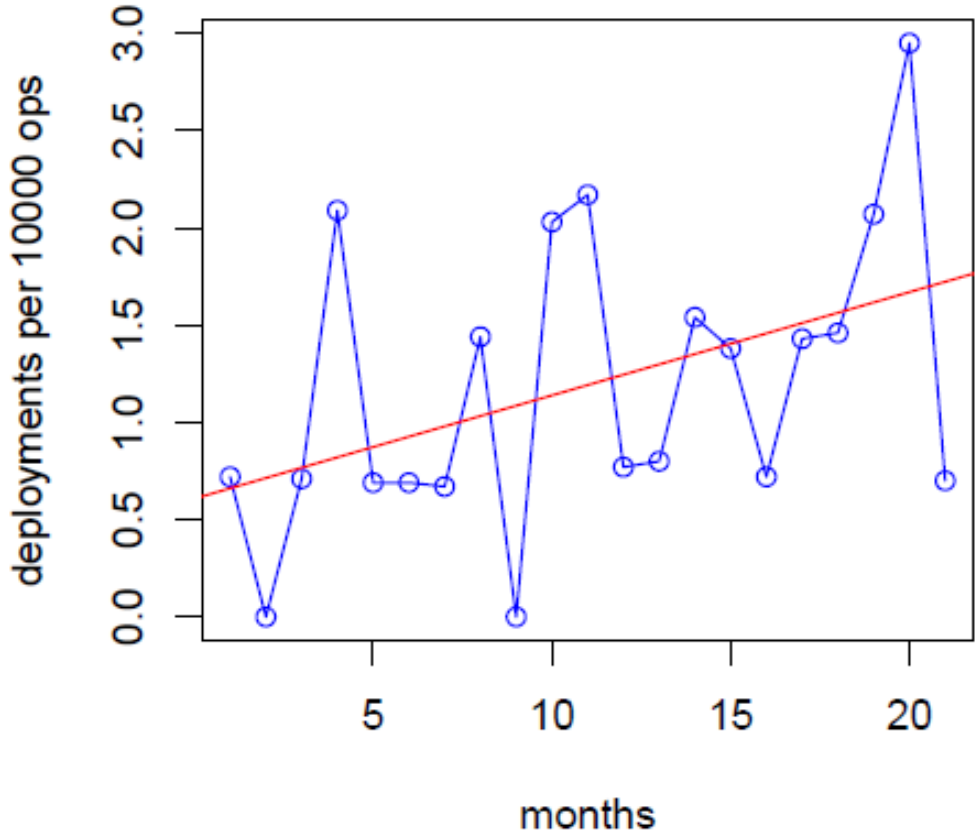
Un ejemplo real: Despliegue no intencionado de rampas

Información de partida

- Seguridad es un factor crítico en la industria aérea
- Creciente competitividad fuerza la reducción de costes, más aun en tiempos de crisis. Afecta a la seguridad?

- Despliegue no intencionado de rampas en condiciones normales
- Coste anual (esperado??) de 20 million USD para toda la industria

El problema



Análisis de incidentes

- Se identificaron los siguientes factores potenciales

Factor	Relevance	Factor levels
Aircraft type	Yes, Moderate	A > B
Airport	No	Nearly 50
Pairing day	Yes	First > Second > Third
Flight turn	Yes	First > (Second, Third)

Análisis de incidentes

- Modelo de regresión logística

$$(x_i, n_i, y_i), i = 1, ..., k$$

$$y_i|\theta_i \sim Bin(n_i, \theta_i)$$

$$logit(\theta_i) = \alpha + \beta x_i$$

Case	Operations	Incidents	Exp.Variables	Coding
i	n_i	y_i	(fleet,day,turn)	x_i
1	29702	3	B,Fst,1	1,1,1
2	59661	7	B,Fst,Oth	1,1,2
3	44159	6	B,Snd,1	1,2,1
4	46257	6	B,Snd,Oth	1,2,2
5	28910	2	B,Thrd,1	1,3,1
6	55193	4	B,Thrd,Oth	1,3,2
7	15245	6	A,Fst,1	2,1,1
8	1516	0	A,Fst,Oth	2,1,2
9	13713	1	A,Thrd,1	2,3,1

Análisis de incidentes

- Fase de operaciones relevante y personal involucrado

Factor	Relevance ranking
Operational phase	Arrival > Departure >> Refueling > Preflight = Stopover
Staff involved	(A, B) > (C,D,E,F,G,H,I)

7 errores, 9 interrupciones del procedimiento, 19 no cumplimiento del procedimiento

Análisis de costes

- Costes
  - De remoción
  - De transporte
  - De reparación
  - Asociados a demora

$$C = Lab \times T_m + C_t + C_m + C_d \times T_d,$$

Costes relacionados con retardos

Distinguimos entre demoras cero y positivas. Entre éstas distinguimos entre las A y las B. Para las A, distinguimos entre demoras cortas y largas

$$T_d = p_0 \; I_0 + p_1 \; F_d$$

$$p_0 + p_1 = 1$$

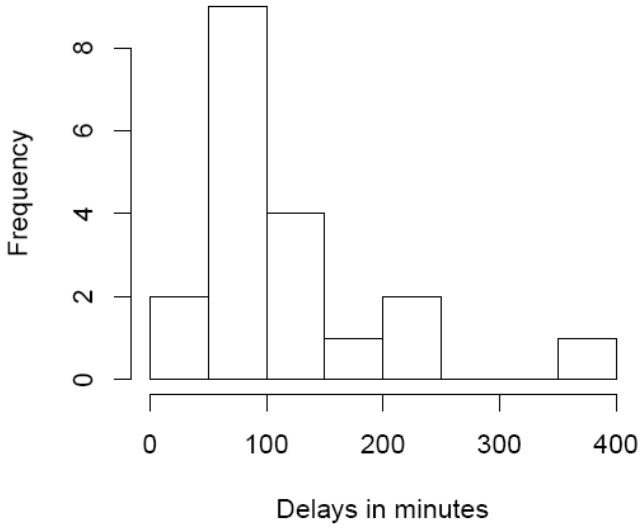
$$p_0, p_1 \geq 0$$

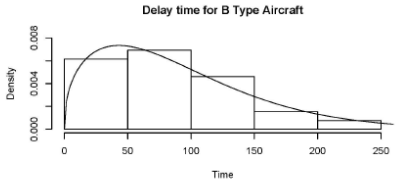
$$p_0|data \sim Be(14, 23)$$

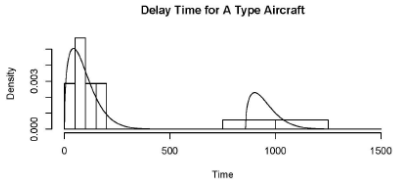
$$F_{d_B} \sim Wei(\theta = 0, \alpha, \beta)$$

$$F_{d_A} \sim p \; Wei(\theta = 0, \alpha, \beta) + (1 - p) \; Wei(\theta, \alpha, \beta),$$

$$f(x \mid \theta, \alpha, \beta) = \alpha \frac{(x - \theta)^{\alpha - 1}}{\beta^{\alpha}} \exp(-((x - \theta)/\beta)^{\alpha})$$







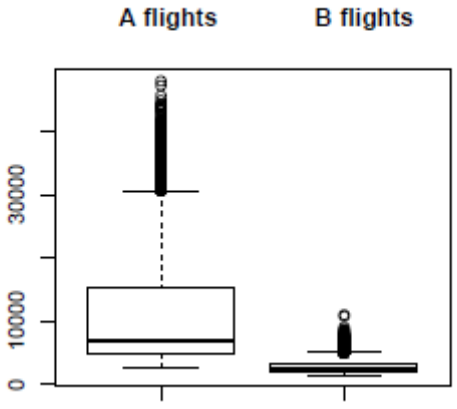
Costes por demoras

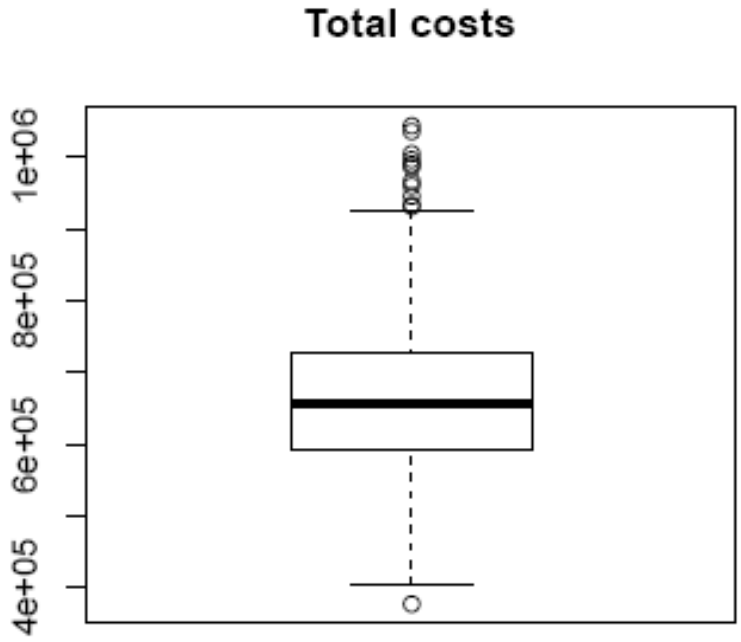
- Basado en Cook and Tanner (2009)

	A Flights	B Flights
	(Min, most likely, max)	(Min, most likely, max)
Passenger Hard Costs	(0.12, 0.19, 0.24)	(0.12, 0.19, 0.24)
Passenger Soft Costs	(0.06, 0.19, 0.22)	(0.06, 0.19, 0.22)
Marginal Crew Costs	(0.00, 14.00, 39.00)	(0.00, 7.90, 16,59)
Marginal Maintenance Costs	(0.65, 0.81, 0.97)	(0.38, 0.47, 0.56)
Total Costs	(0.83, 15.19, 40.27)	(0.56, 8.75, 17.61)

Costes debidos a los incidentes

	Type A	Type B
Mean	10970	2959
Median	6808	2590
$Q_{0.95}$	30481	5503
$Q_{0.98}$	35189	6129





Gestión de riesgos

- Contramedidas
  - Cambiar procedimiento (para ‘eliminar’ interrupciones y mitigar errores, prácticamente sin coste)
  - Cursos de entrenamiento al personal clave (para mitigar errores y no cumplimientos, prácticamente sin coste)
  - Campaña de sensibilización al personal clave con boletines, etc… (mismo objetivo, coste 6000 euros)
  - Warning en las puertas (para mitigar errores, interrupciones y no conformidades, 2500 euros por puerta) (o sólo las clave)
  - Pegatinas en las puertas (it., coste 120 euros por puerta) (o sólo las clave)
- Sólo afectamos, esencialmente, la verosimilitud de los incidentes, no su severidad

Gestión de riesgos

Countermeasure	1 year	5 years
Procedure revision	252902	1214935
Awareness campaign	524477	2492943
Warning devices, St. 1	1307393	1335514
Warning devices, St. 2	616058	2137866
Visual reminders, St. 1	631403	2881078
Visual reminders, St. 2	677329	3228759
None	663400	1490047

Coste esperado actualizado
Neutro al riesgo

Countermeasure	1 year	5 years
Awareness campaign	123724	567739
Warning devices,St. 1	1302529	1312149
Warning devices, St. 2	352862	873480
Visual reminders, St. 1	273448	1161478
Visual reminders, St. 2	236060	1108918
None	252902	1214935

Conclusión

- Se implantó una revisión de procedimientos y una campaña de sensibilización.
- Comunicación no sencilla.
- Pero los resultados (4 frente a 18) apoyan la gestión realizada

Otros ejemplos realizados

- Mejores remedios frente a fenómenos meteorológicos extremos (riadas y sequía) en Jiqulisco (El Salvador)
- Evaluación de riesgos de salidas de pista (Iberia)
- Fuel para la operación de holding (Iberia)
- Plan nacional de gestión de riesgos aéreos (AENA)
- Protección frente a impagos de tarifa en el metro (TMB)
- Riesgo operacional en bancos y aseguradoras (Basel III, Solvency II,…) (First Rand, Old Mutual,…) SKITES
- Riesgos en auditorías (CODELCO)

Análisis de Riesgos Adversarios

- Análisis de Riesgos con adversarios dispuestos a incrementar nuestros riesgos.
- Análisis de Riesgos + Teoría de Juegos

Cuál es la mejor asignación de recursos de seguridad en una ciudad?

Ciudad como un mapa con celdas

Cada celda tiene un valor

Para cada celda, modelo predictivo de actos delictivos

Asignar recursos (restricciones)

Para cada celda, predecir el impacto de la asignación de recursos

Asignación óptima de recursos

NB: Los 'malos' operan de forma inteligente y organizada!!!

Cuál es el mejor mantenimiento HW/SW para el ERP de una organización?

Modelizar sistema HW/SW (bloques HW y SW que interactúan)

Predecir fiabilidad bloque

Predecir fiabilidad sistema

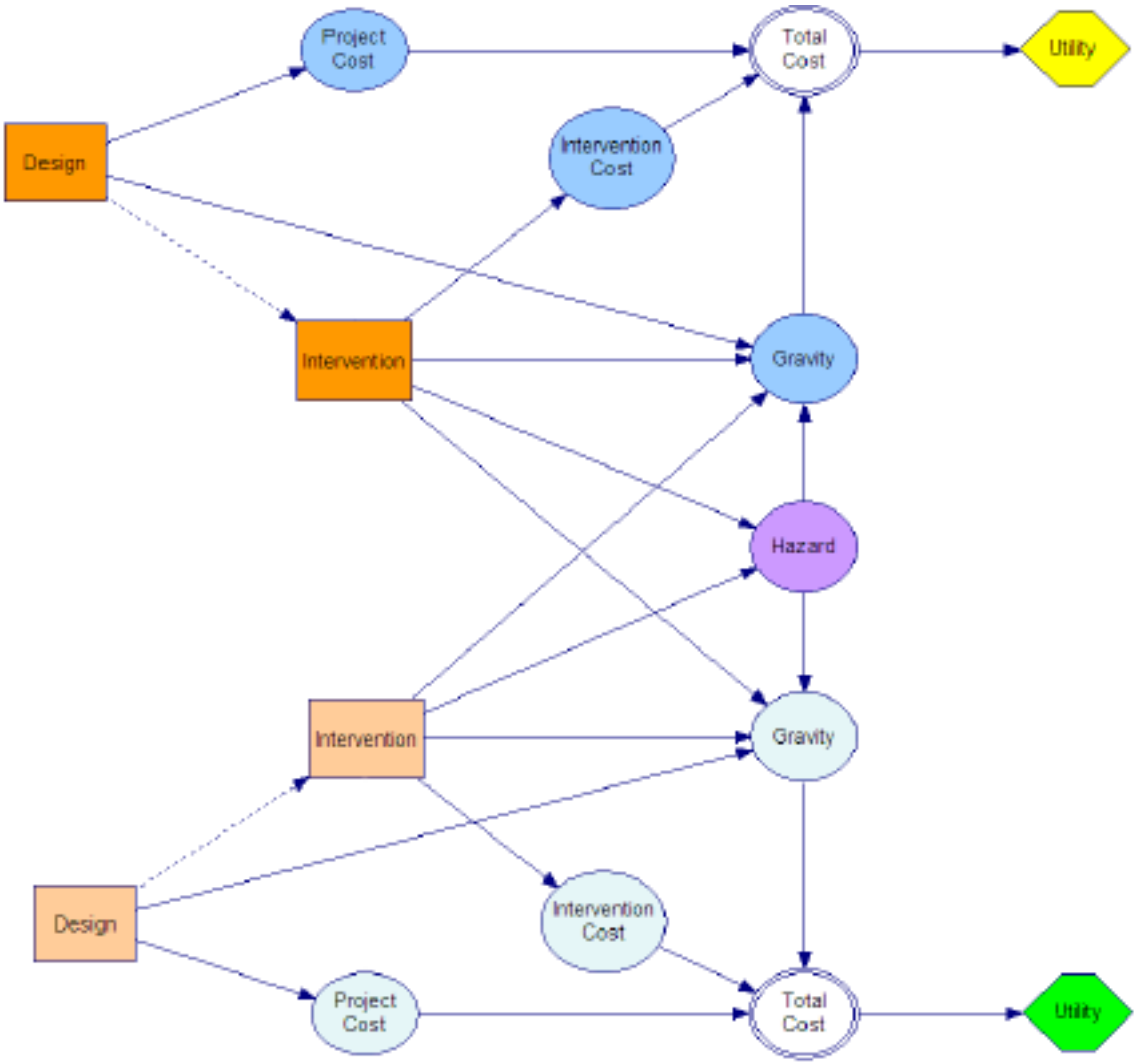
Diseñar políticas mantenimiento

Predecir impacto sobre fiabilidad (y costes)

Política óptima de mantenimiento

NB: Qué pasa con los ‘malos’ que atacan nuestro sistema?

Análisis de riesgos adversarios



Motivación

- AR tradicional extendido para incluir adversarios

- S-11, M-11 condujeron a grandes inversiones globales de seguridad algunas muy criticadas
- Muchos esfuerzos de modelización para asignarlos eficientemente
- Revisión de Parnell et al (2008) NAS
  - Métodos estándar de fiabilidad y riesgos no tienen en cuenta la intencionalidad
  - Aproximaciones teoría de juegos. Hipótesis de conocimiento común
  - Aproximaciones análisis de decisiones. Predicción de la acción del adversario
- Merrick, Parnell (2011) revisan aproximaciones comentando favorablemente sobre ARA

ARA

- Marco para gestionar riesgos debidos a las acciones de adversarios inteligentes (DRI, Rios, Banks, JASA 2009)

- Apoyo prescriptivo unilateral
  - Usa modelo SEU
  - Trata las decisiones del adversario como incertidumbres

- Método para predecir acciones del adversario
  - Suponenos que maximiza UE
    - Modelizar su problema de decisión
    - Asignar sus utilidades y probabilidades
    - Encontrar su acción de máxima utilidad esperada
  - Pero otros modelos descriptivos son posibles

- Incertidumbre en la decisión del atacante proviene de
  - *Nuestra* incertidumbre sobre sus probabilidades y utilidades
  - Pero esto conduce a una jerarquía de problemas de decisión anidados

(aleatorio, no informativo, nivel.k, heurística, espejo) vs (conocimiento común)

ARA

- ARA alicaciones a modelos countraterrorism (Rios, DRI, 2009, 2012 Risk Analysis)
  - Sequential Defend-Attack
  - Simultaneous Defend-Attack
  - Sequential Defend-Attack-Defend
  - Sequential Defend-Attack with private information

- Caso piratas Somalia (Sevillano, Rios, DRI, 2012 Decision Analysis)
- Juegos rutas (guerra anti IED) (Wang, Banks, 2011)

- Juegos Borel (Banks, Petralia, Wang, 2011)
- Subastas (DRI, Rios, Banks, 2009; Rothkopf, 2007)

- Kadane, Larkey (1982), Raiffa (1982), Lippman, McCardle (2012)
- Stahl and Wilson (1994,1995) D. Wolpert (2012)
- Rotschild, MacLay, Guikema (2012)

Seguridad

- Uno de los ‘The World’s (23) Biggest Problems´ (Lomborg, 2008)
  - Proliferación de armas
  - Conflictos
  - Corrupción
  - Terrorismo
  - Drogas
  - Lavado de dinero

Una prioridad en el FP7 y el Horizon2020. SECONOMICS

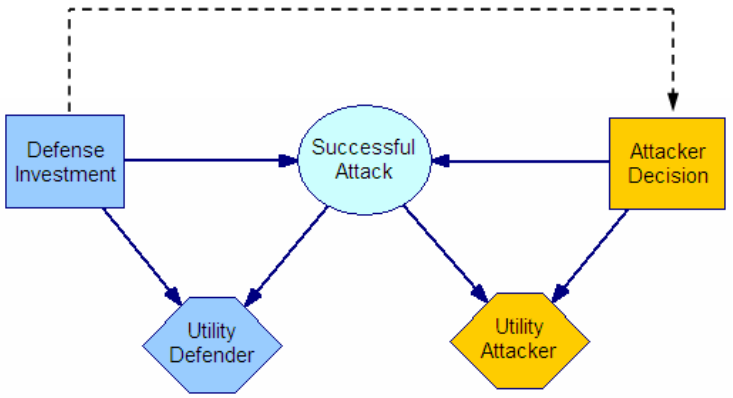
Safety vs Security

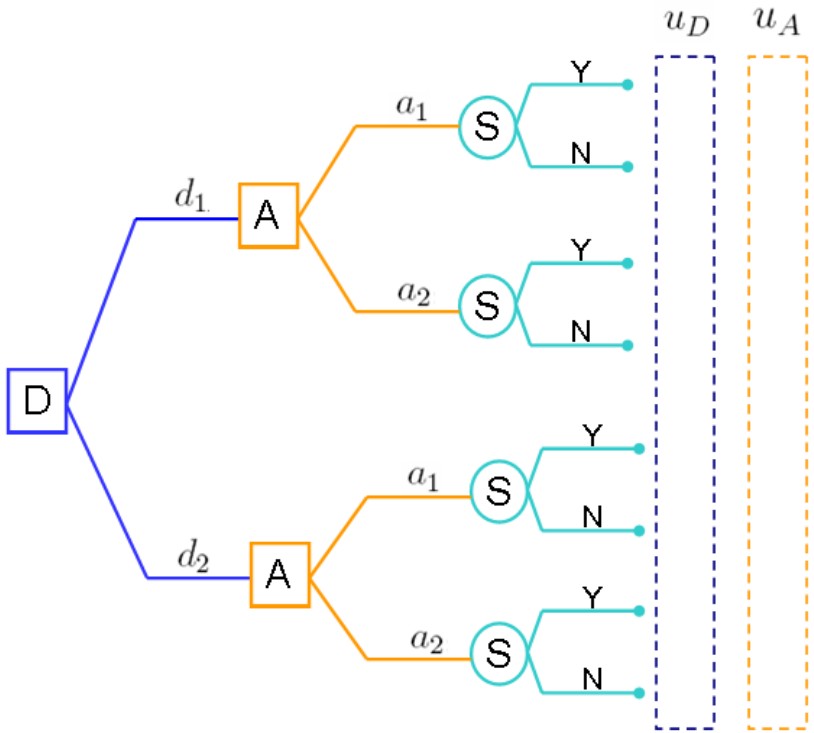
- Safety. Naturaleza, Accidentes
- Security. A propósito (terrorismo,…)

- Freceuntemente disociadas (Incluso para asignación de recursos!!!)

Safety vs Security

Juegos secuenciales:
Primero Defensor, Luego Atacante





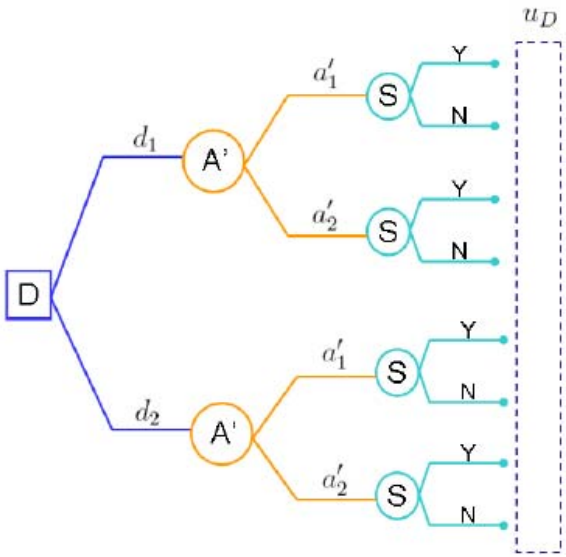
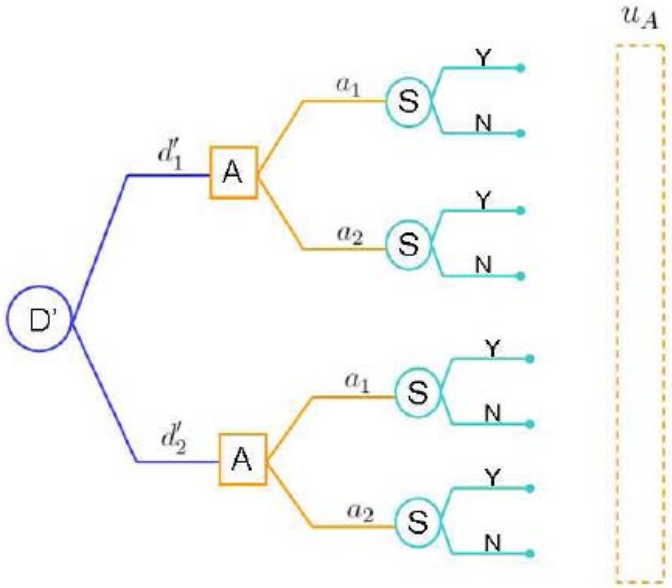
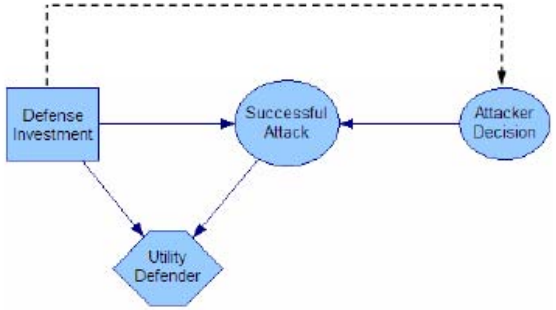
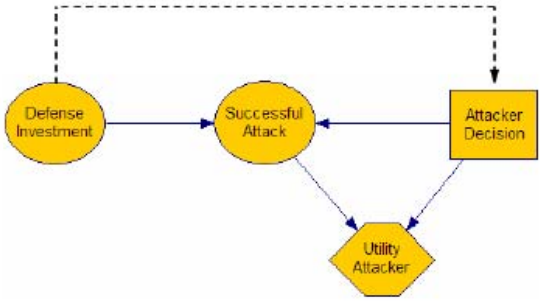
$$a^*(d) = \arg\max_{a \in X_A} u_A(d, a)$$

$$d^* = \arg\max_{d \in X_D} u_A(d, a^*(d))$$

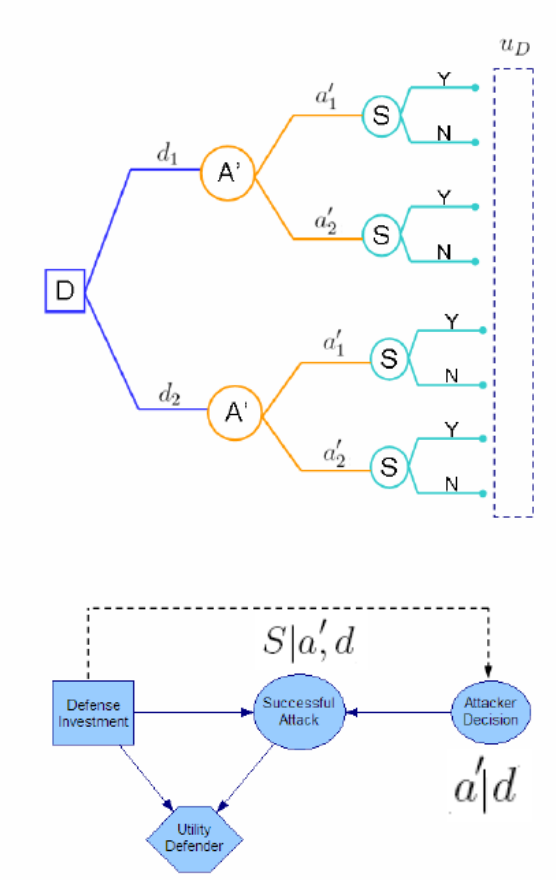
Sol Nash: $(d^*, a^*(d^*))$

Teoría Juegos

Juego secuencial: Apoyo al Defensor

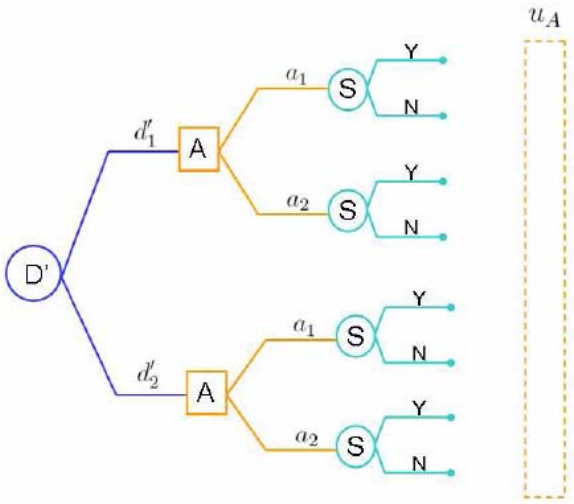
Problema Defensor	Vision del Defensor del problema del Atacante
	
	

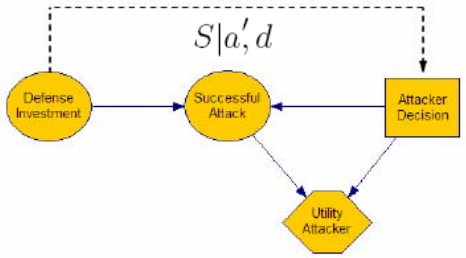
Apoyo al Defensor

Problema del defensor	Solución del defensor
	$\psi_D(d,a') = u_D(d,S=Y)\, p_D(S=Y \mid X_D=d, X'_A=a') + u_D(d,S=N)\, p_D(S=N \mid X_D=d, X'_A=a')$ $\psi_D(d) = \psi_D(d,a'_1)\, p_D(a'_1 \mid d) + \psi_D(d,a'_2)\, p_D(a'_2 \mid d)$ $d^* = \arg\max_{d \in X_D} \psi_D(d)$ Input : $p_D(S \mid a', d)$ $p_D(a' \mid d)$??

Apoyo al Defensor: Problema de asignación

Visión del Defensor del problema del Atacante





Asignación de $p_D(a'|d)$

A maximiza EU

D tiene creencias $(\widehat{u}_A, \widehat{p}_A) \sim F$

$$\hat{\psi}_A(d', a) = \hat{u}_A(a, S = Y)\, \hat{p}_A(S = Y \mid X'_D = d',\ X_A = a) + \hat{u}_A(a, S = N)\, \hat{p}_A(S = N \mid X'_D = d',\ X_A = a)$$

$$\hat{\psi}_A \sim \widehat{\Psi}_A$$

$$p_D(a'|d) = Pr\left[a' = \arg\max_{x \in X'_A} \widehat{\Psi}_A(d, x)\right]$$

Simulación MC

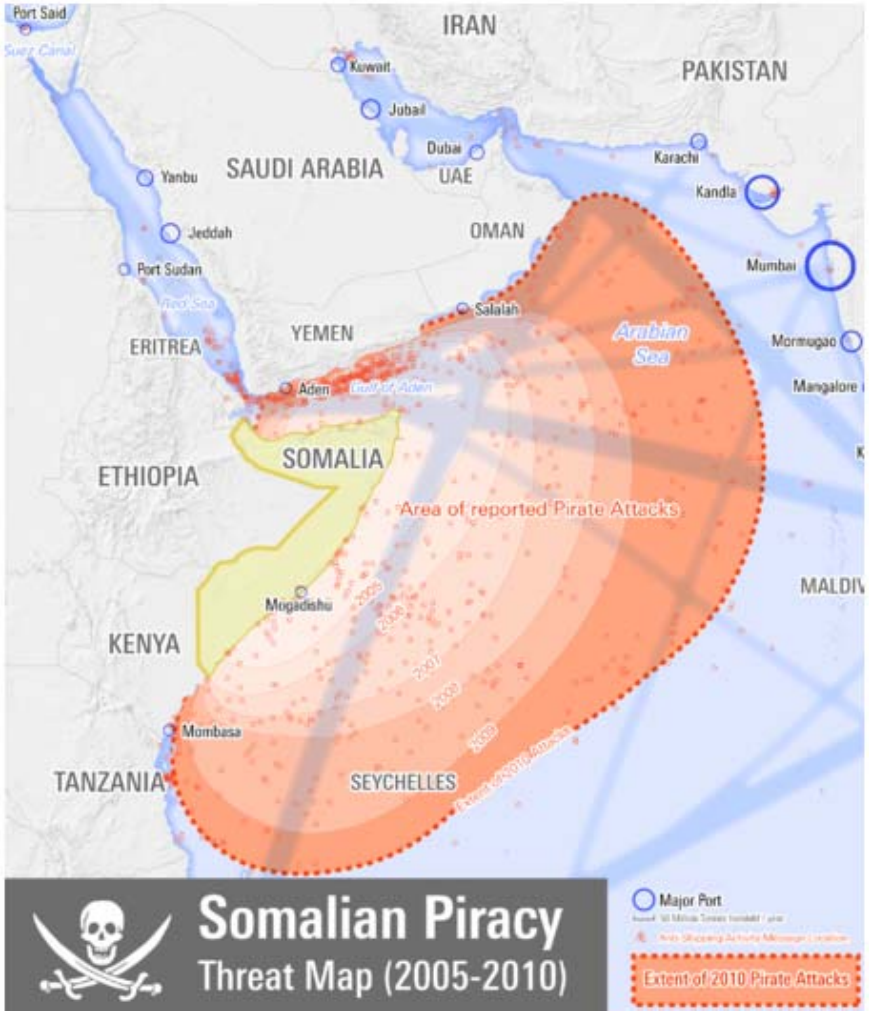
$$\hat{p}_D(a|d) \approx n^{-1} \sum_i \#\{a = \text{argmax}_{x \in \mathcal{A}}\, \hat{\psi}_A^i(x, d)\}$$

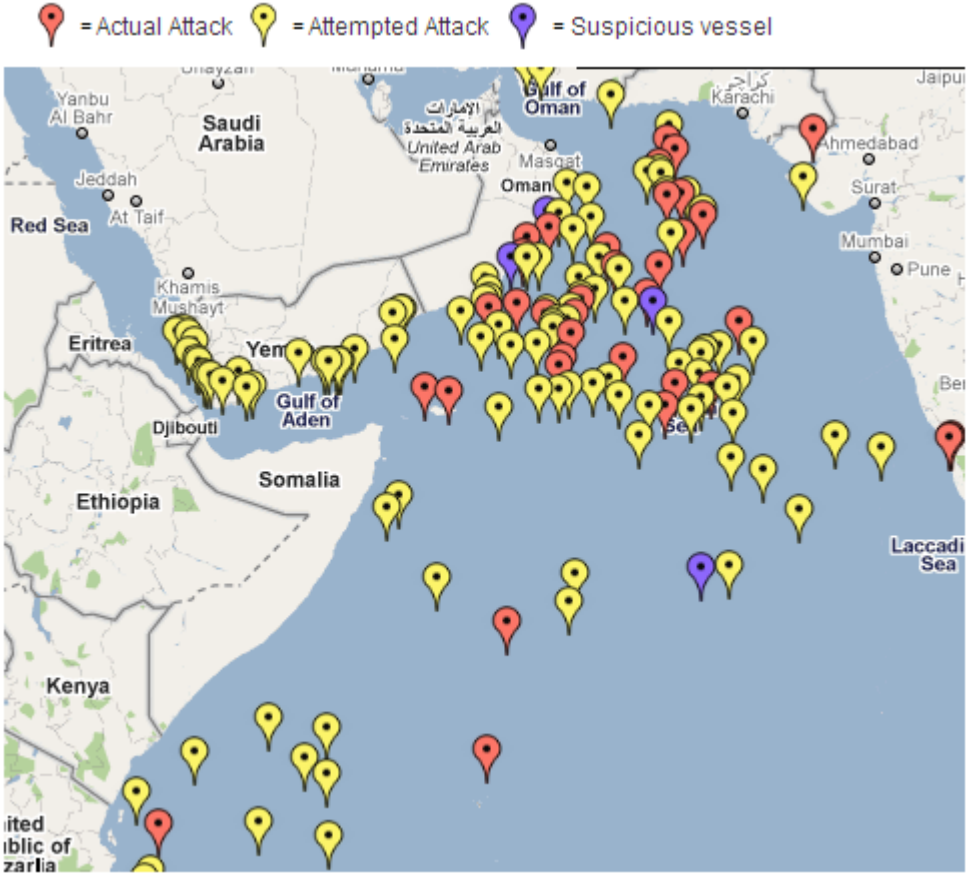
where $\hat{\psi}_A^i \sim \widehat{\Psi}_A,\ i = 1, \ldots, n$

Otros ejemplos

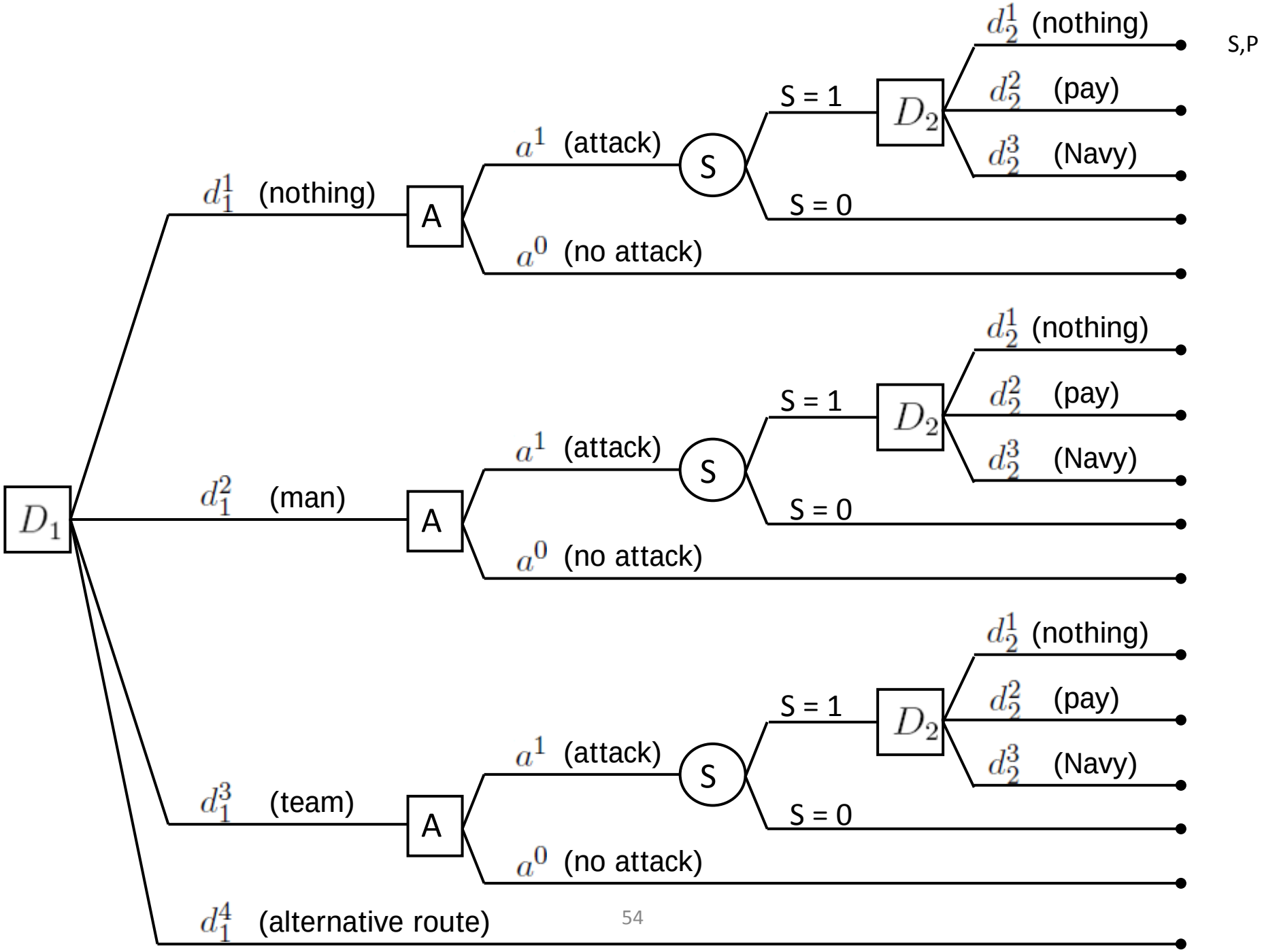
- Seguridad urbana
- **Seguridad frente a piratas en Somalia**
- Seguridad en el Metro de Barcelona
- Seguridad en el aeropuerto de Anadulu
- Seguridad en la red eléctrica de Reino Unido
- Seguridad en rutas anti-IED (Irak)
- **Ciberseguridad en sistemas de control en plataformas petrolífera**
- Subastas
- Poker (Sencillo)
- **Sociedades de robots**

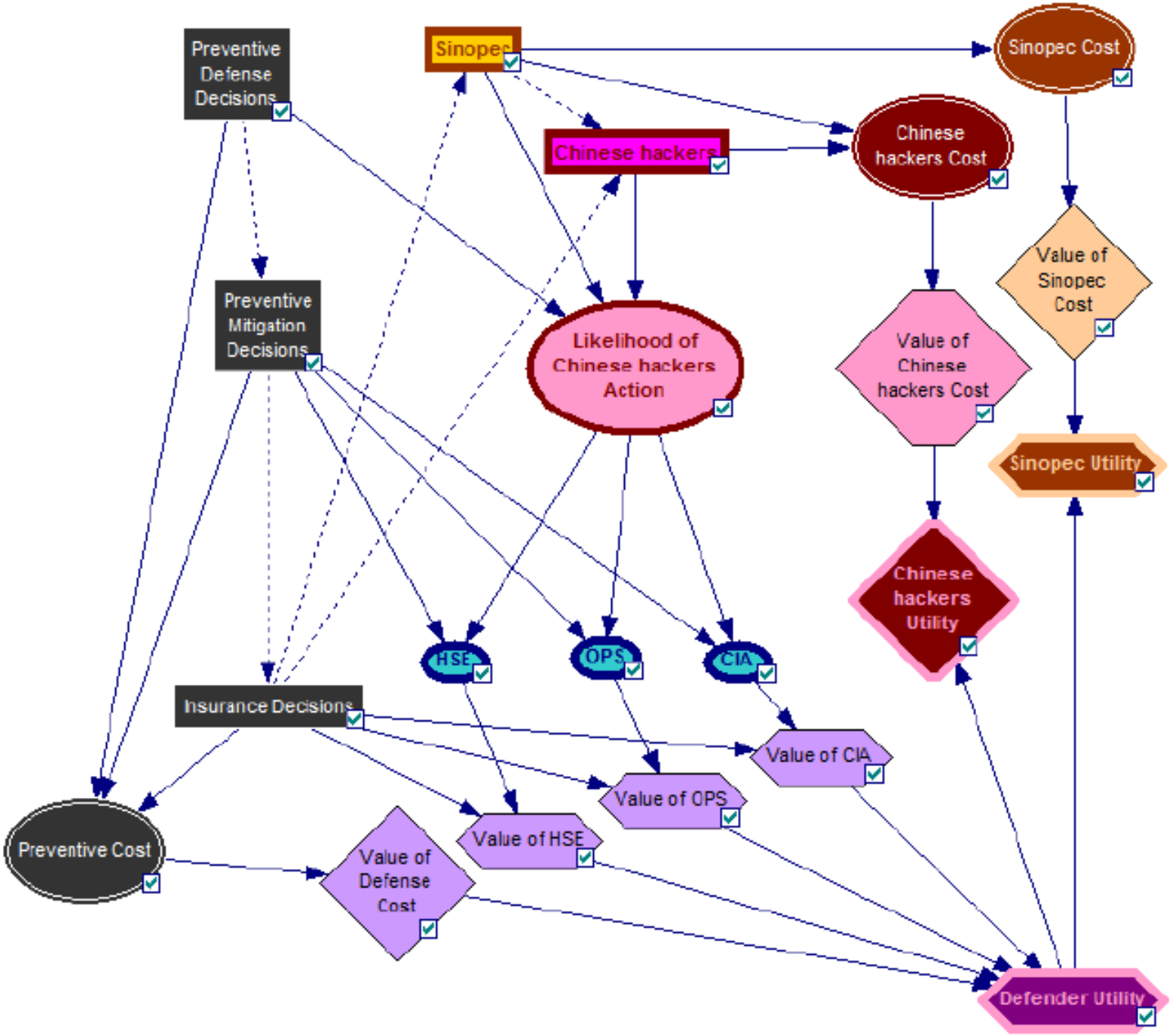
Piratería en Somalia

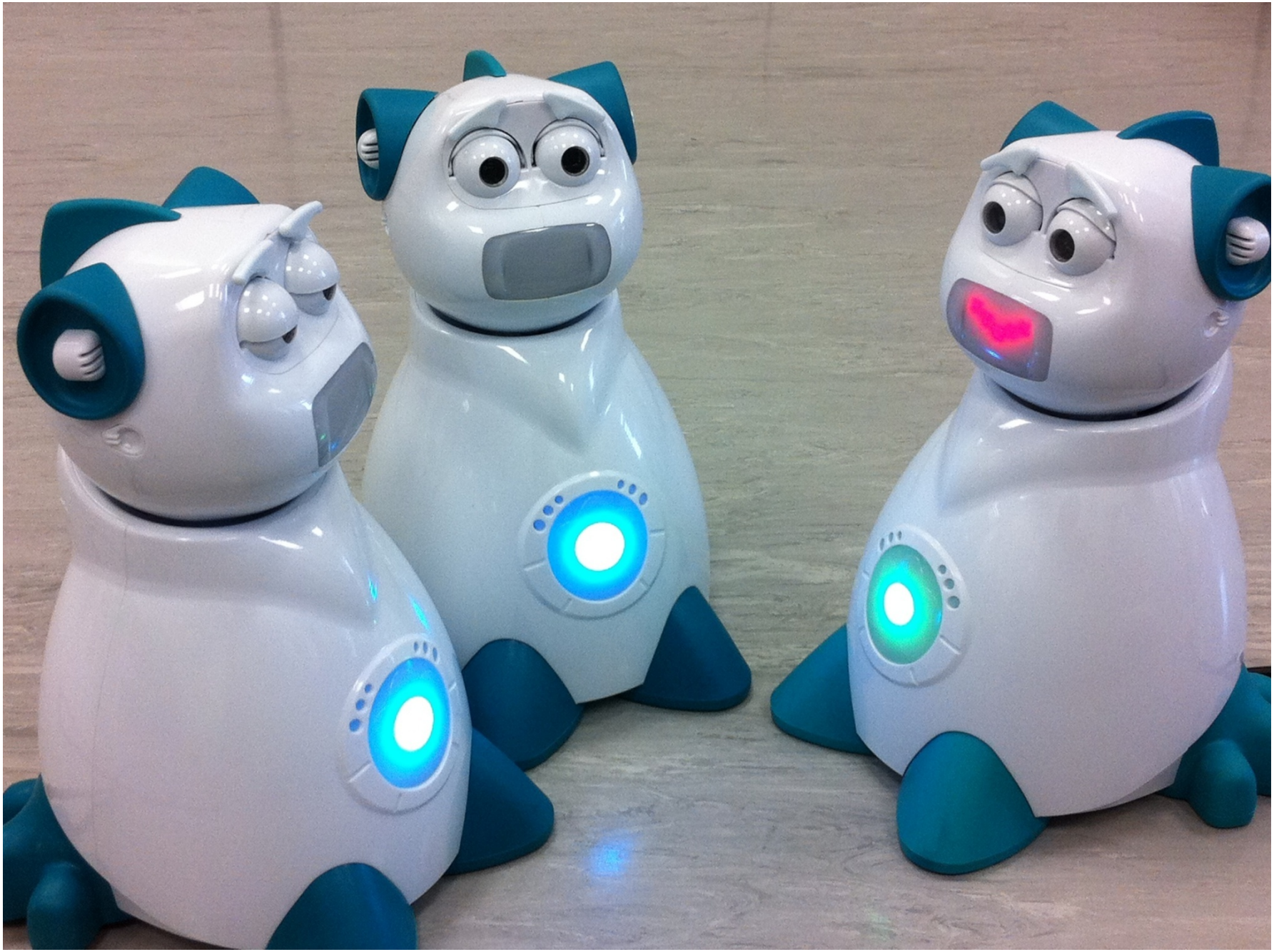




Piracy and armed robbery incidents reported to the IMB Piracy Reporting Centre 2011

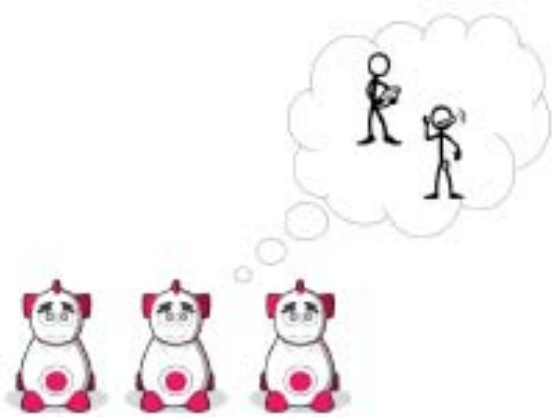

D_1
d_1^1 (nothing)
d_1^2 (man)
d_1^3 (team)
d_1^4 (alternative route)
A
A
A
a^1 (attack)
a^0 (no attack)
a^1 (attack)
a^0 (no attack)
a^1 (attack)
a^0 (no attack)
S
S
S
S = 1
S = 0
S = 1
S = 0
S = 1
S = 0
D_2
D_2
D_2
d_2^1 (nothing)
d_2^2 (pay)
d_2^3 (Navy)
d_2^1 (nothing)
d_2^2 (pay)
d_2^3 (Navy)
d_2^1 (nothing)
d_2^2 (pay)
d_2^3 (Navy)
S,P


Preventive Defense Decisions
Sinopec
Sinopec Cost
Chinese hackers
Chinese hackers Cost
Value of Sinopec Cost
Preventive Mitigation Decisions
Likelihood of Chinese hackers Action
Value of Chinese hackers Cost
Sinopec Utility
Chinese hackers Utility
HSE
OPS
CIA
Insurance Decisions
Value of CIA
Value of OPS
Value of HSE
Preventive Cost
Value of Defense Cost
Defender Utility



Marco básico

(a)



(b)

Discusión

- Del Análisis de Riesgos
  - Aplicaciones (Matriz de Riesgos…)
- Al Análisis de Riesgos Adversarios
  - Teoría
  - Computación
  - Aplicaciones
  - Revisitar Teoría de Juegos
- Percepción de riesgo
- Comunicación de riesgo

Obrigado!!!

david.rios@urjc.es

www.analisisderiesgos.com

www.aisoy.com

www.skites.es