

Modelos estadísticos para la seguridad y la lucha contra el terrorismo

Curso de Verano UCLM

David Ríos, Real Academia de Ciencias
Octubre, 2013

Año Internacional de la Estadística 2013

Reconocimiento a nivel mundial de la contribución que la Estadística ha realizado a lo largo de los años al progreso de nuestra sociedad.

- Incrementar el conocimiento sobre el impacto que la estadística tiene en todos los aspectos de la sociedad.
 - Promocionar la estadística como profesión, especialmente entre los jóvenes
 - Promover el desarrollo de las ciencias estadísticas.
-
- INE, SEIO, UCLM

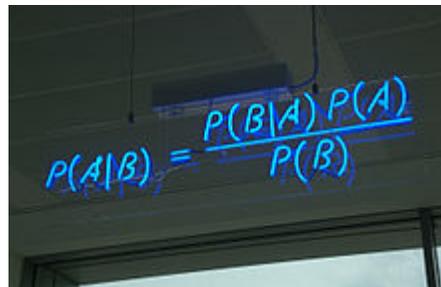


Año Internacional de la Estadística 2013



Thomas Bayes

1763

A photograph of a whiteboard with the formula for Bayes' theorem written in blue marker. The formula is
$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Sixto Ríos
1913-2008



Agenda

- El concepto de riesgo
- Análisis de riesgos
 - Conceptos generales
 - Un marco
 - Un ejemplo de seguridad en aviación
- 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

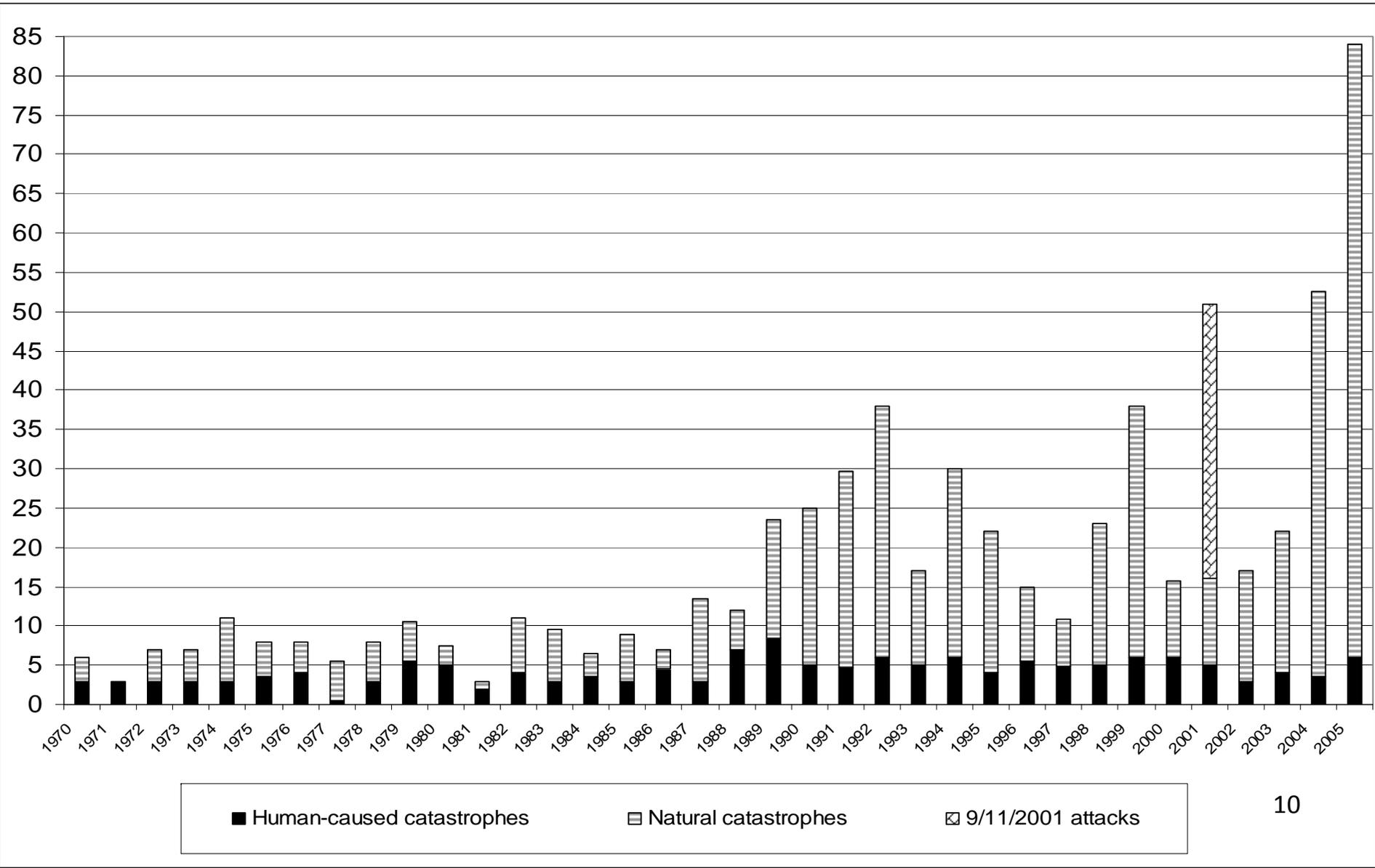
Riesgos

- 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)
 -

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...

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 amenaza.
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)

		<i>degradation</i>		
		1%	10%	100%
<i>value</i>	VH	M	H	VH
	H	L	M	H
	M	VL	L	M
	L	VL	VL	L
	VL	VL	VL	VL

		<i>frequency</i>			
		PF	FN	F	MF
<i>impact</i>	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

Escenario de partida

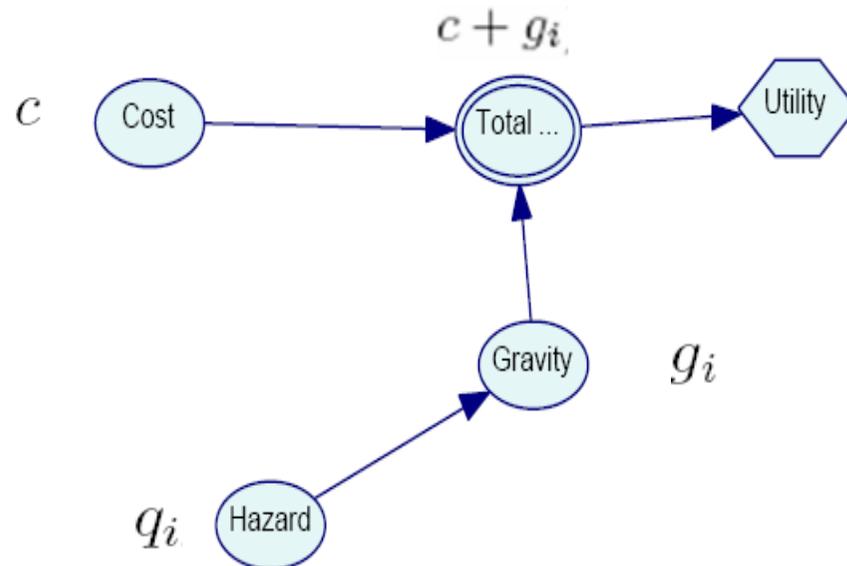
- Diseño dado (no hay intervenciones, status quo)
- Se identifican los costes (aleatorios)
- Se calcula la utilidad esperada



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

Evaluación de riesgos

- Verosimilitud e impacto de las amenazas identificadas



Ocurren con cierta probabilidad y conllevan un coste adicional

- Calculamos utilidad esperada después de evaluar riesgos

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

- Impacto:

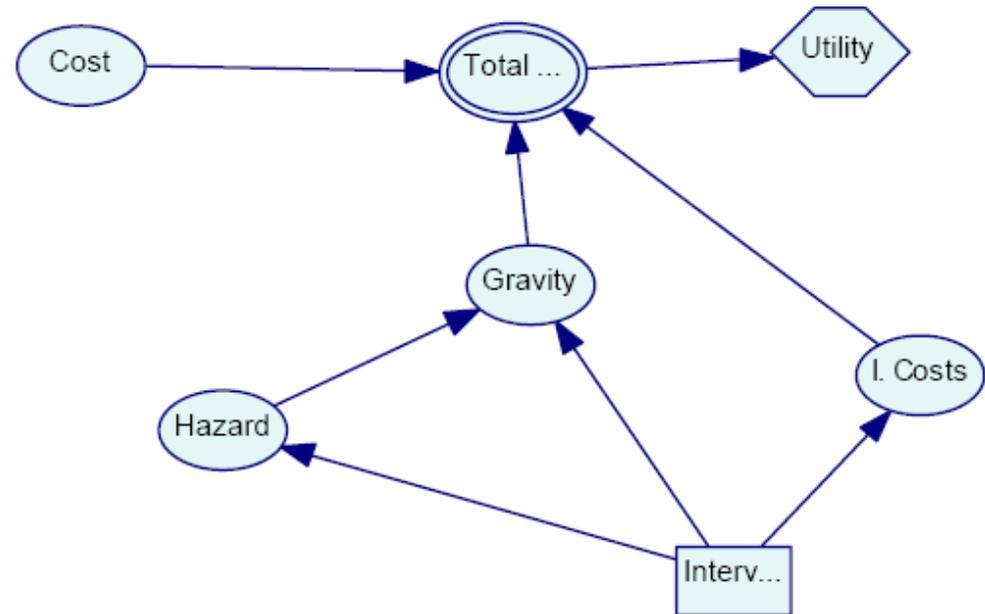
$$\Psi - \Psi_r$$

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 ...

Un ejemplo real: Despliegue no intencionado de rampas

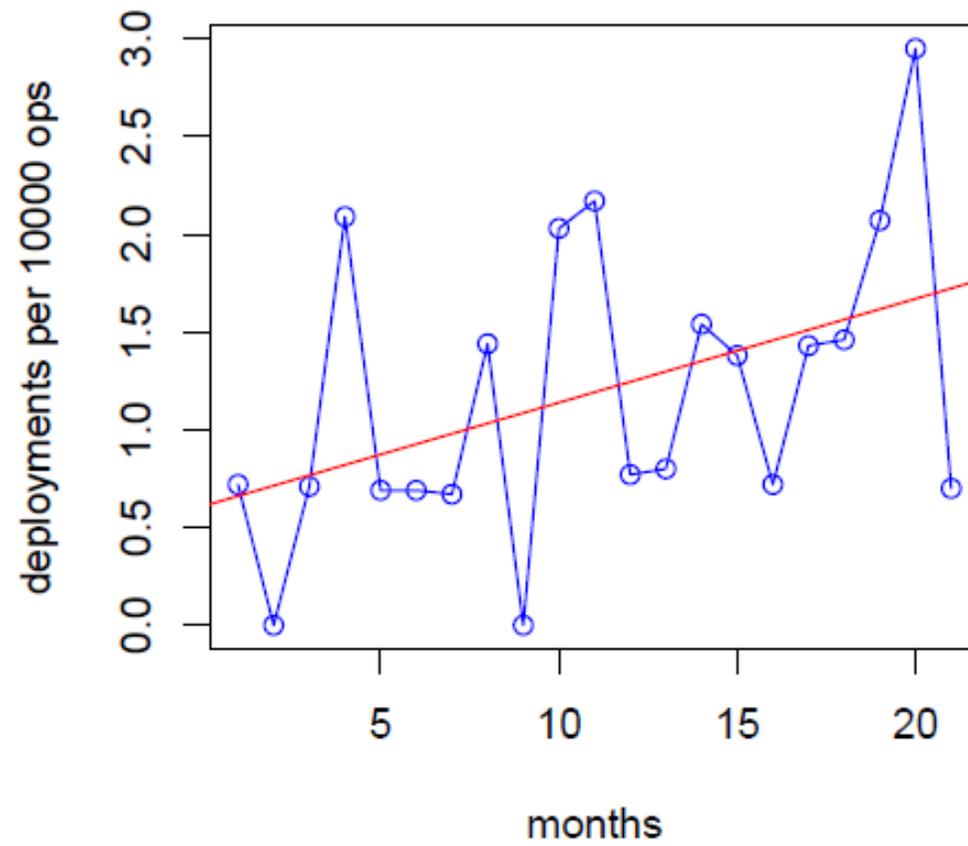


Información de partida

- 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

$$(x_i, n_i, y_i), i = 1, \dots, k$$

$$y_i | \theta_i \sim \text{Bin}(n_i, \theta_i)$$

$$\text{logit}(\theta_i) = \alpha + \beta x_i$$

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

$$T_d = p_0 I_0 + p_1 F_d$$

$$p_0 + p_1 = 1$$

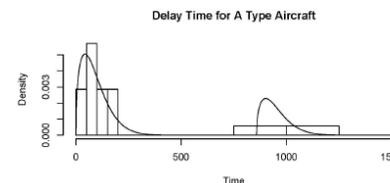
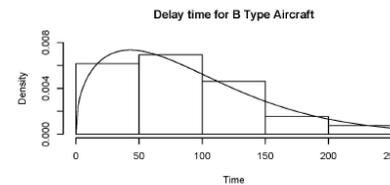
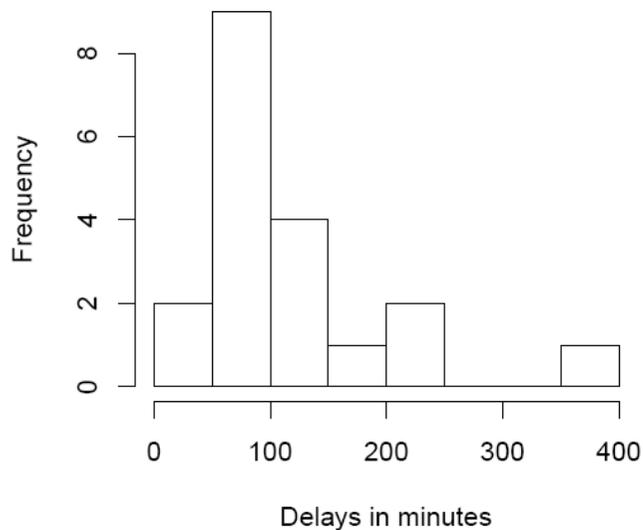
$$p_0, p_1 \geq 0$$

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

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

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

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



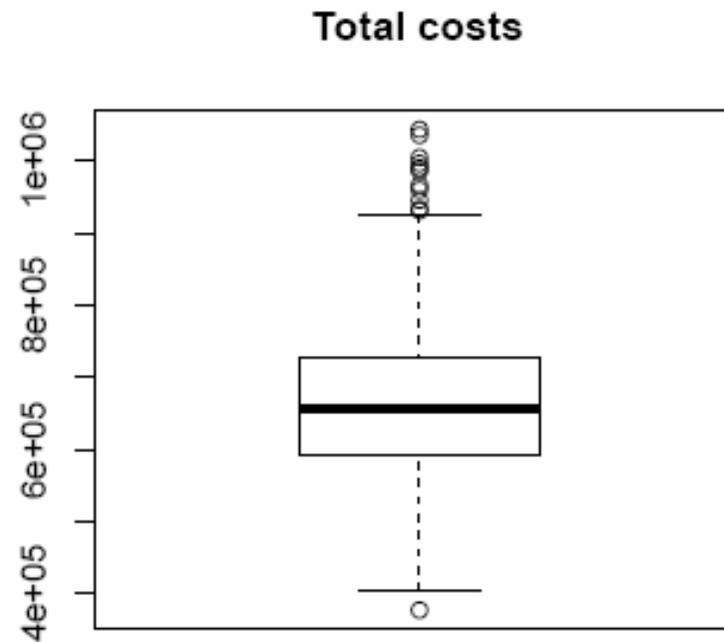
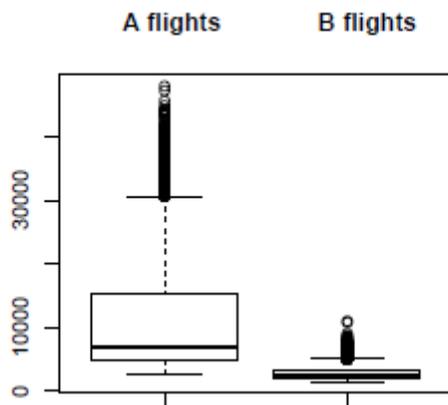
Costes por demoras

- 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	Coste esperado actualizado Neutro al riesgo
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	

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

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

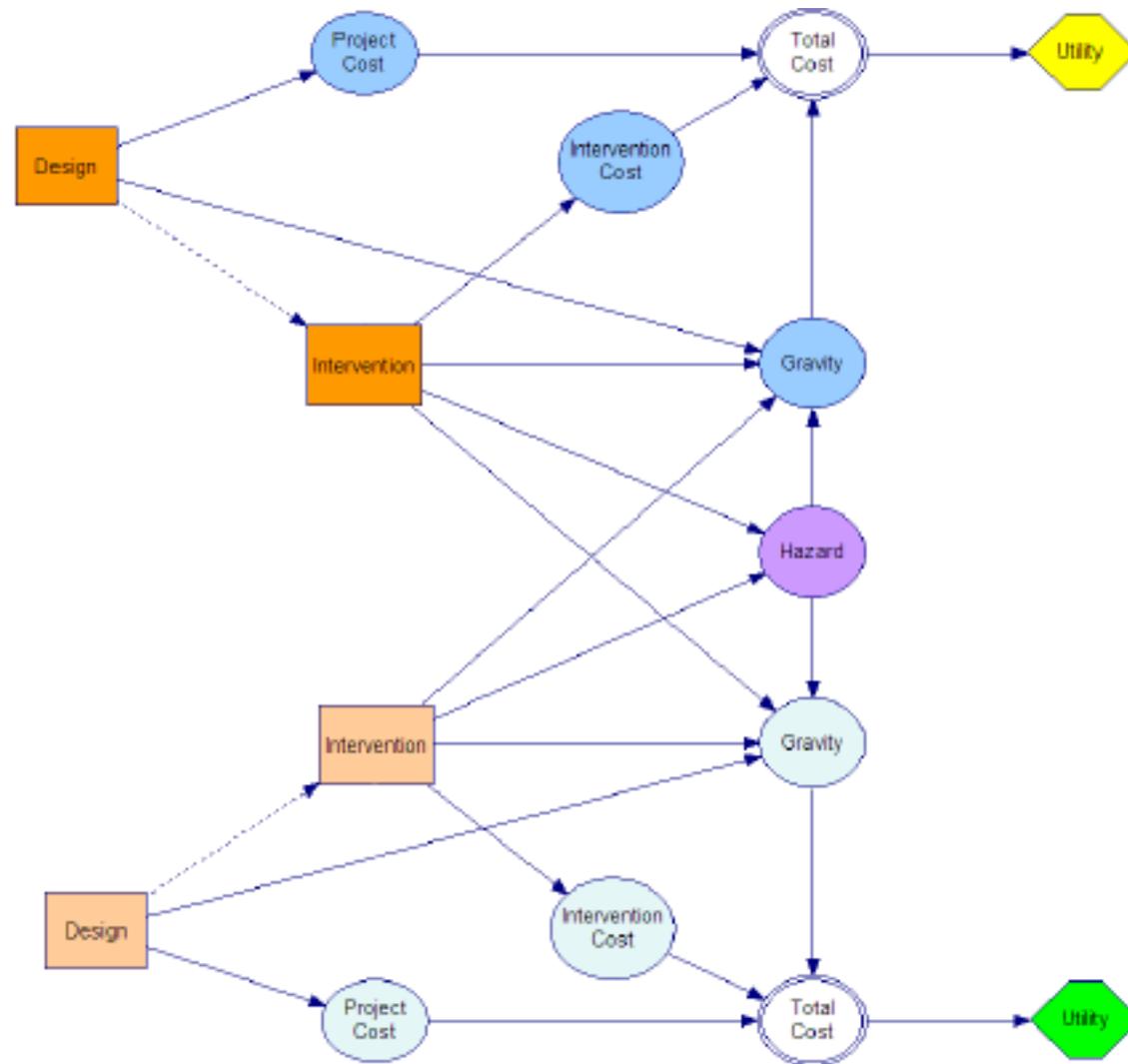
Diseñar políticas mantenimiento

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
 - Suponemos 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 aplicaciones a modelos counterterrorism (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

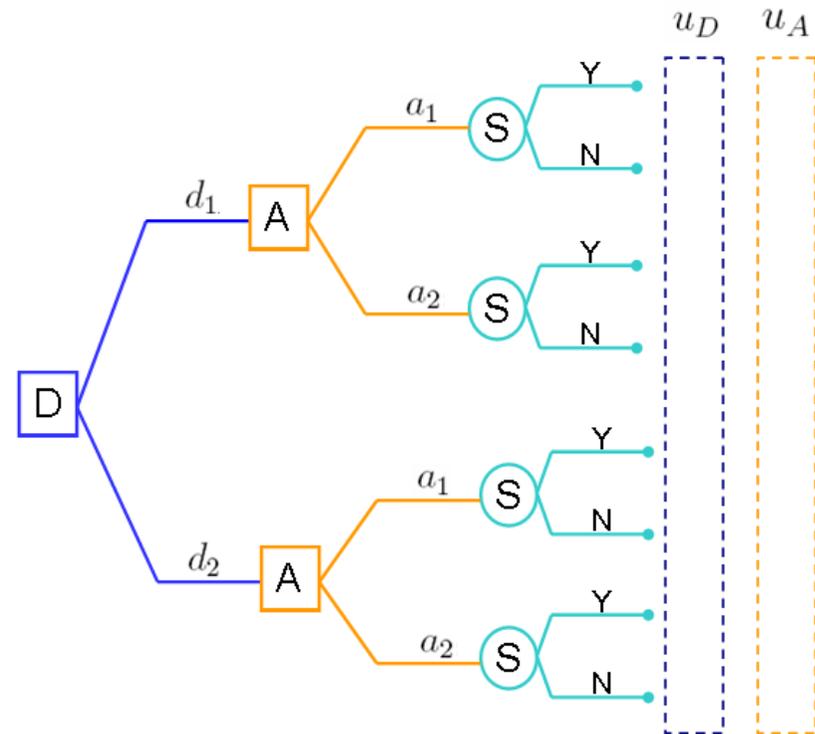
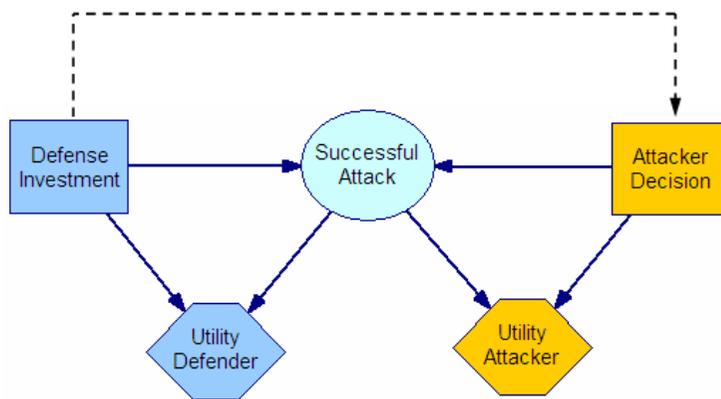
Safety vs Security

- Safety. Naturaleza, Accidentes
- Security. A propósito (terrorismo,...)
- Frecuentemente disociadas (Incluso para asignación de recursos!!!)

Safety vs Security



Juegos secuenciales: Primero Defensor, Luego Atacante

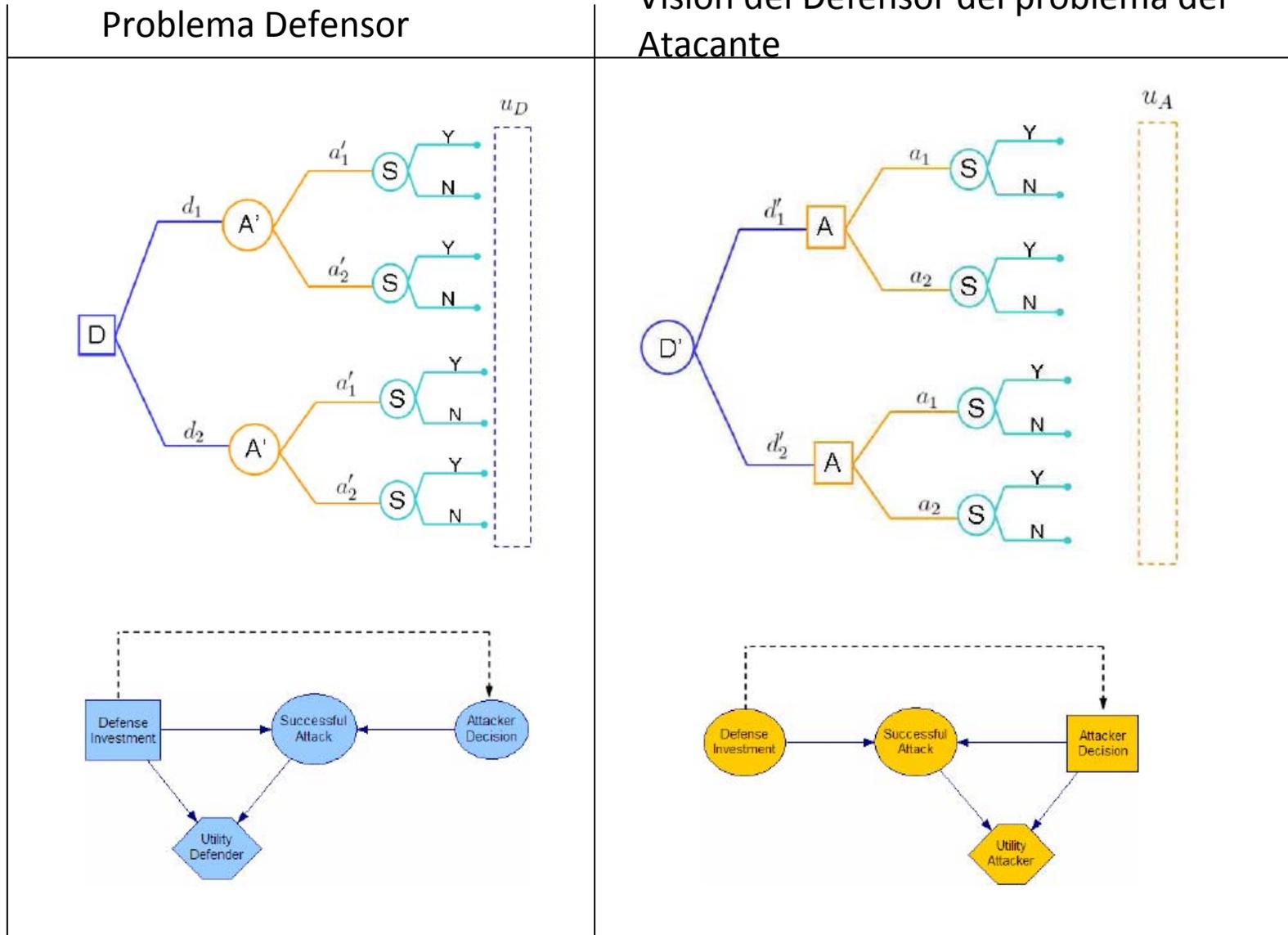


$$a^*(d) = \arg \max_{a \in X_A} u_A(d, a)$$

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

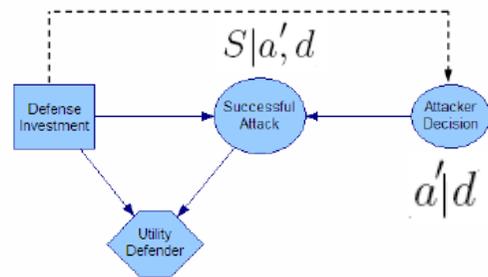
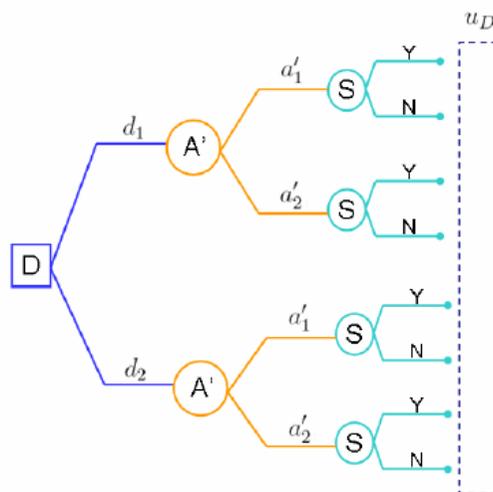
Sol Nash: $(d^*, a^*(d^*))$

Juego secuencial: Apoyo al Defensor



Apoyo al Defensor

Problema del defensor



Solución del defensor

$$\psi_D(d, a') = u_D(d, S = Y) p_D(S = Y | X_D = d, X'_A = a') + u_D(d, S = N) p_D(S = N | X_D = d, X'_A = a')$$

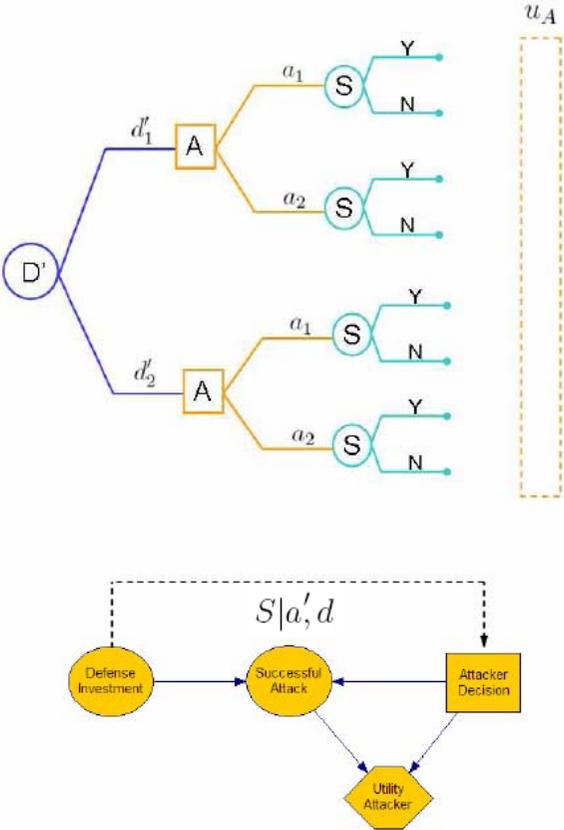
$$\psi_D(d) = \psi_D(d, a'_1) p_D(a'_1 | d) + \psi_D(d, a'_2) p_D(a'_2 | d)$$

$$d^* = \arg \max_{d \in X_D} \psi_D(d)$$

Input :

$$p_D(S|a', d) \quad p_D(a'|d) \quad ??$$

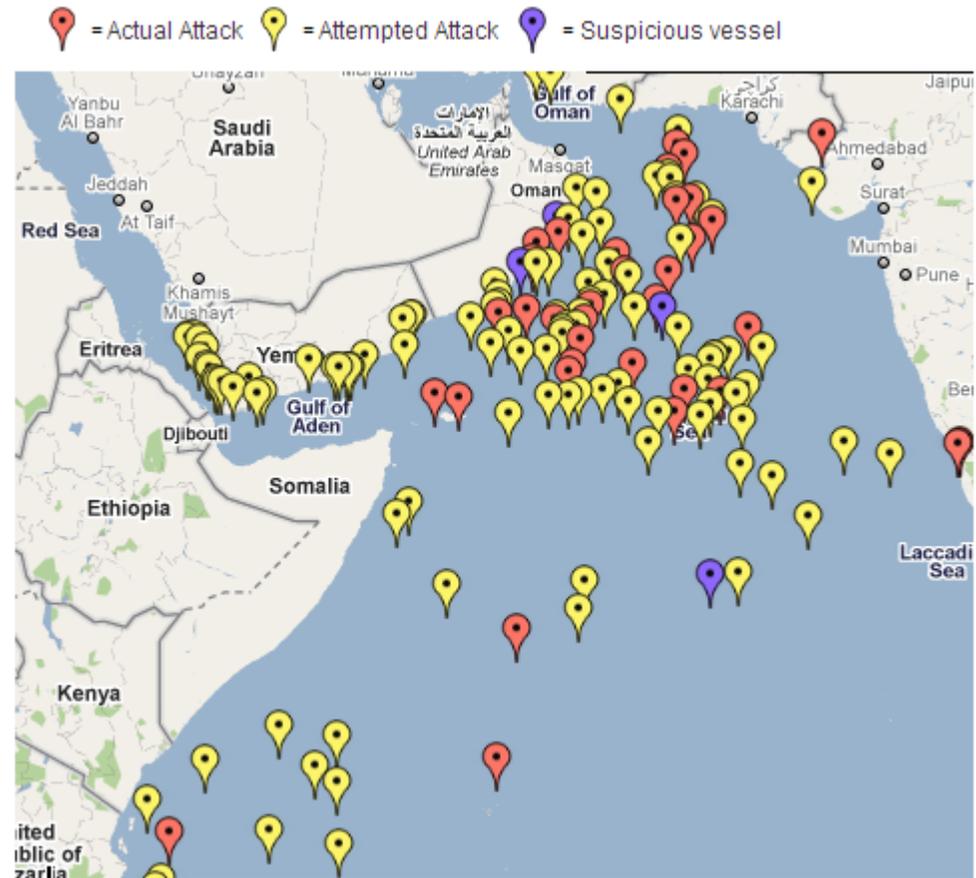
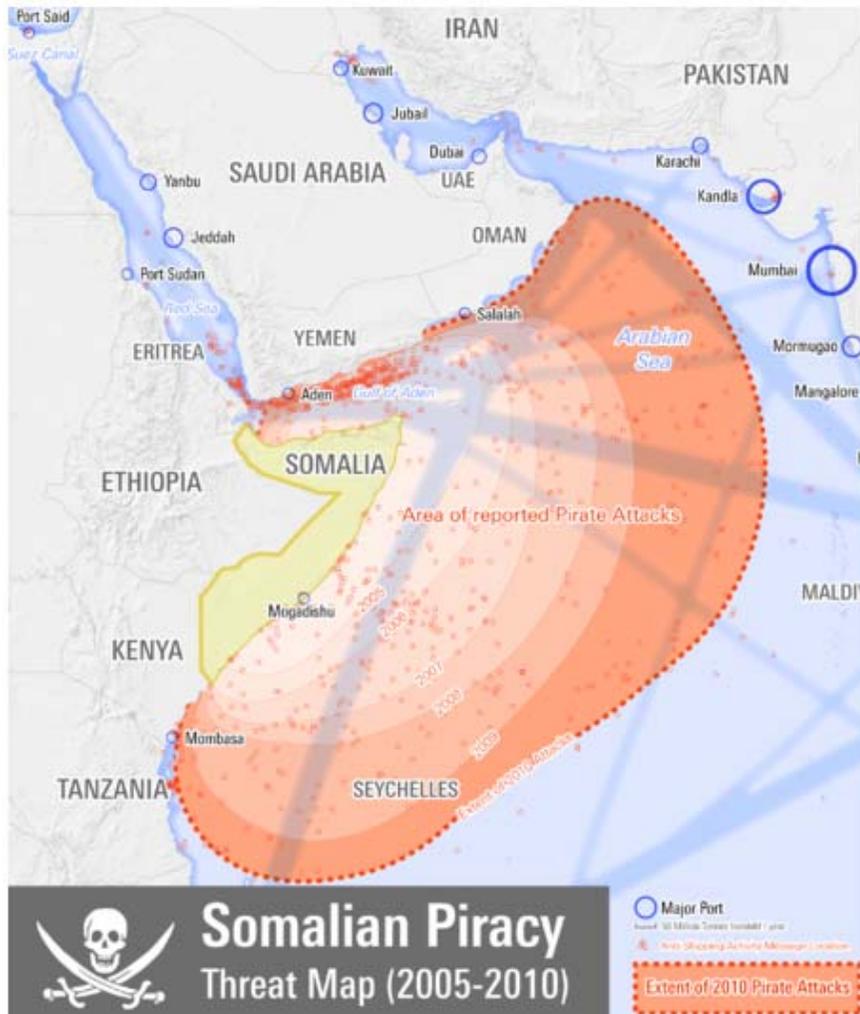
Apoyo al Defensor: Problema de asignación

Visión del Defensor del problema del Atacante	Asignación de $p_D(a' d)$
 <p>The diagram illustrates the defender's perspective of the attacker's problem. It starts with a decision node D' (blue circle) that branches into two defense strategies, d'_1 and d'_2 (blue lines). Each strategy leads to an attacker's decision node A (yellow square). From each A node, the attacker chooses between two actions, a_1 and a_2 (orange lines). Each action leads to a success (S, blue circle) or failure (N, blue circle) state. From each S state, the attacker chooses between two utilities, Y and N (blue lines). A dashed yellow box labeled u_A encloses the utility nodes. Below the tree is a flowchart with four nodes: 'Defense Investment' (yellow circle), 'Successful Attack' (yellow circle), 'Attacker Decision' (yellow square), and 'Utility Attacker' (yellow diamond). Arrows show the flow from 'Defense Investment' to 'Successful Attack', from 'Successful Attack' to 'Attacker Decision', and from 'Attacker Decision' to 'Utility Attacker'. A dashed arrow labeled $S a', d$ points from 'Attacker Decision' back to 'Successful Attack'.</p>	<p>A maximiza EU</p> <p>D tiene creencias $(\hat{u}_A, \hat{p}_A) \sim F$</p> $\hat{\psi}_A(d', a) = \hat{u}_A(a, S = Y) \hat{p}_A(S = Y X'_D = d', X_A = a) + \hat{u}_A(a, S = N) \hat{p}_A(S = N X'_D = d', X_A = a)$ $\hat{\psi}_A \sim \hat{\Psi}_A$ $p_D(a' d) = Pr \left[a' = \arg \max_{x \in X'_A} \hat{\Psi}_A(d, x) \right]$ <p><u>Simulación MC</u></p> $\hat{p}_D(a d) \approx n^{-1} \sum_i \#\{a = \arg \max_{x \in A} \hat{\psi}_A^i(x, d)\}$ <p>where $\hat{\psi}_A^i \sim \hat{\Psi}_A, i = 1, \dots, n$</p>

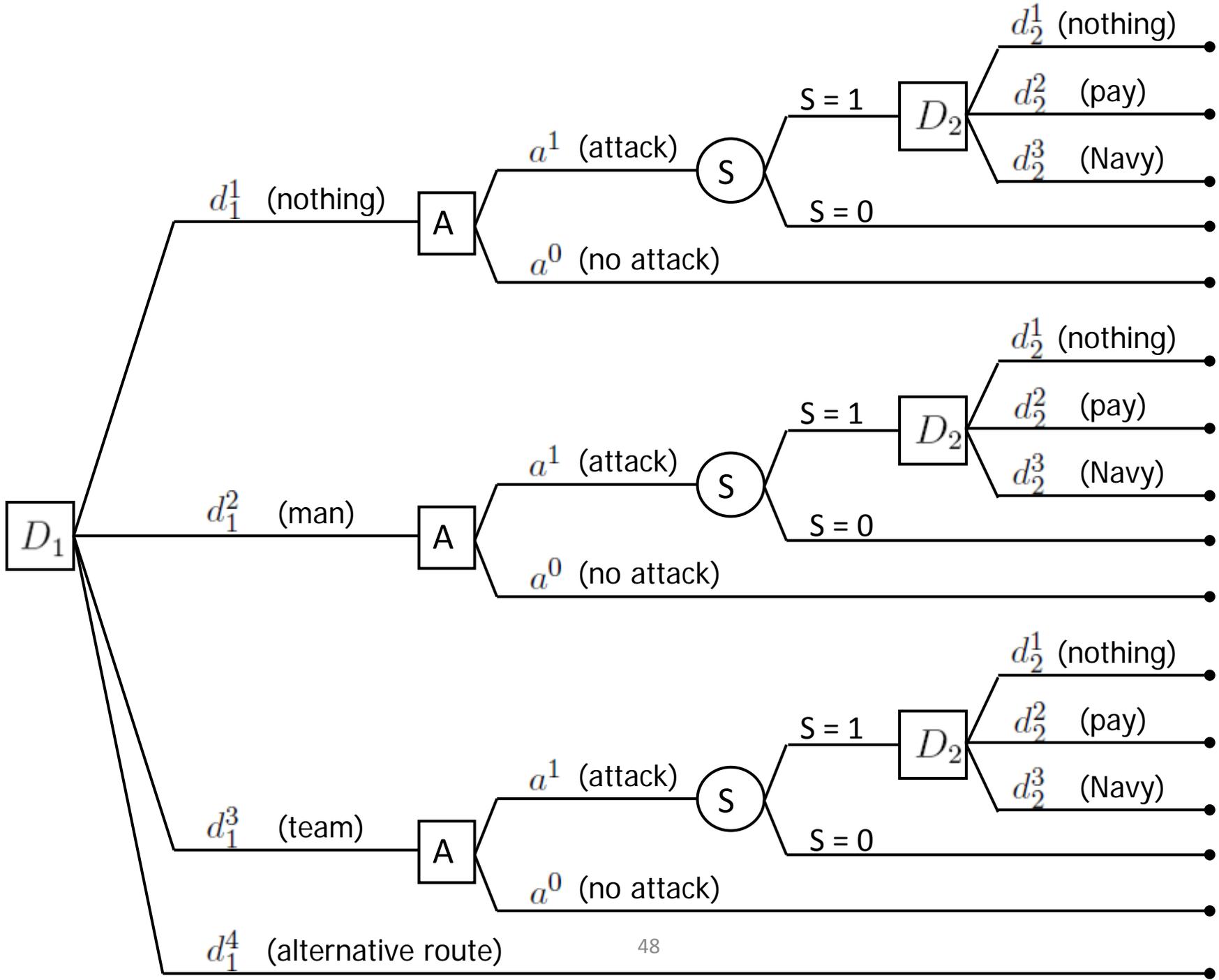
Ejemplos

- 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**

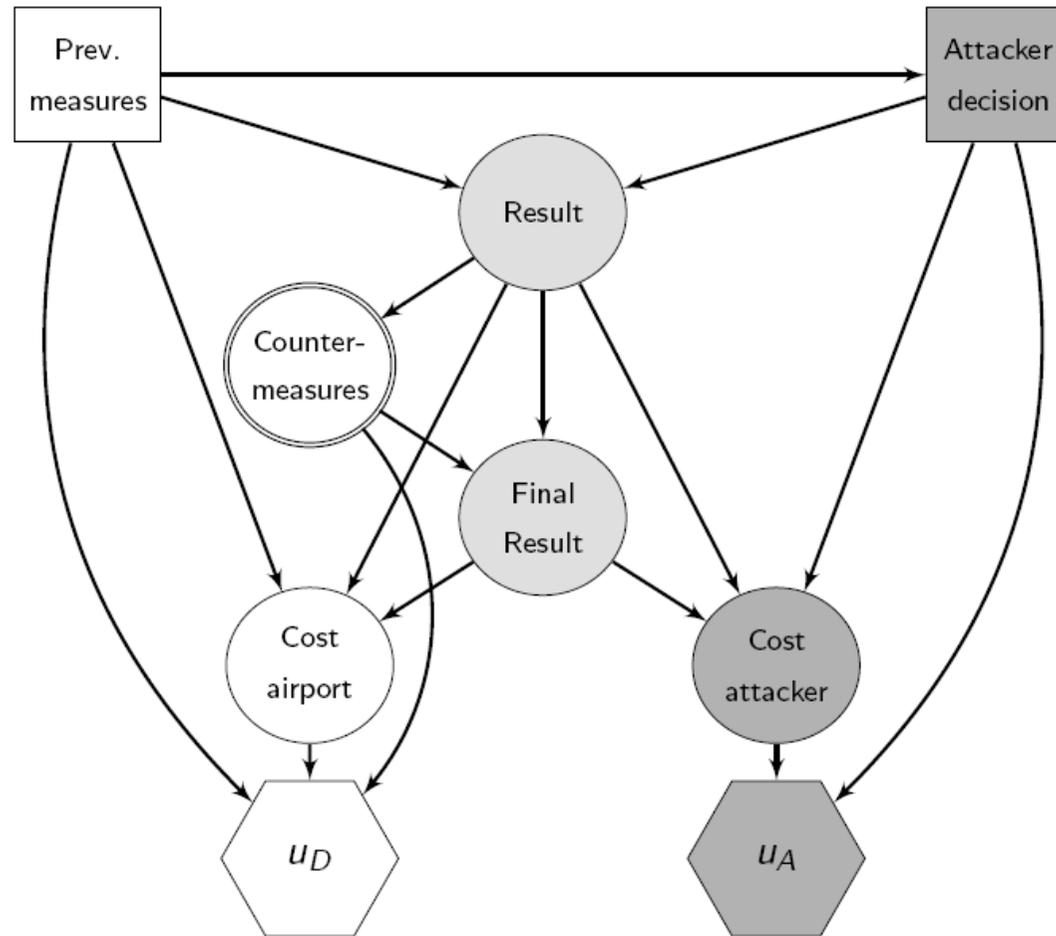
Piratería en Somalia



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



Seguridad en Aeropuerto

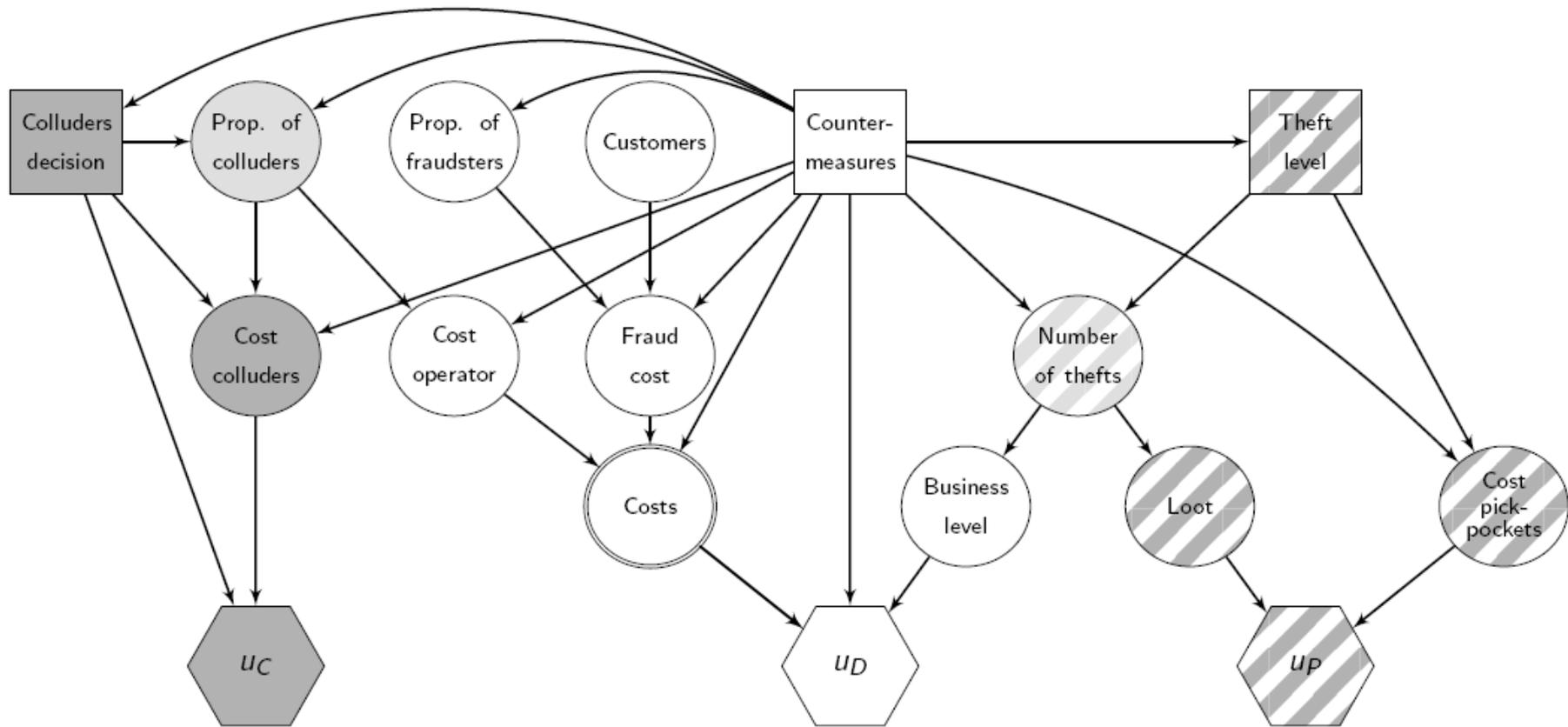


Cartera óptima de recursos defensivos

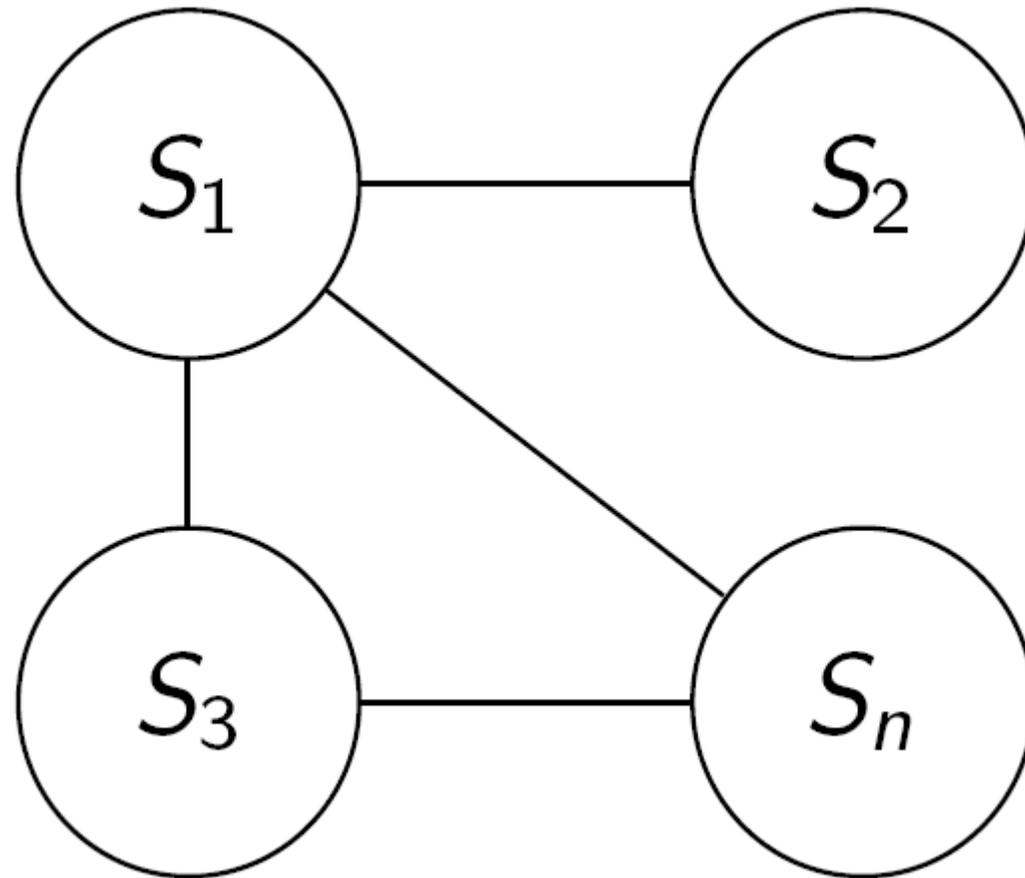
Measure	Max	Annual cost (€)/unit	Deterrence	Detection
Cameras	4	650	Moderate-high	Moderate (persons)
Metal detectors	1	6,500	Moderate	High (material)
X-ray devices	1	90,000	Moderate	High (material)
Police	5	19,200	High	High (persons)
Private security	9	15,600	High	Moderate (persons)

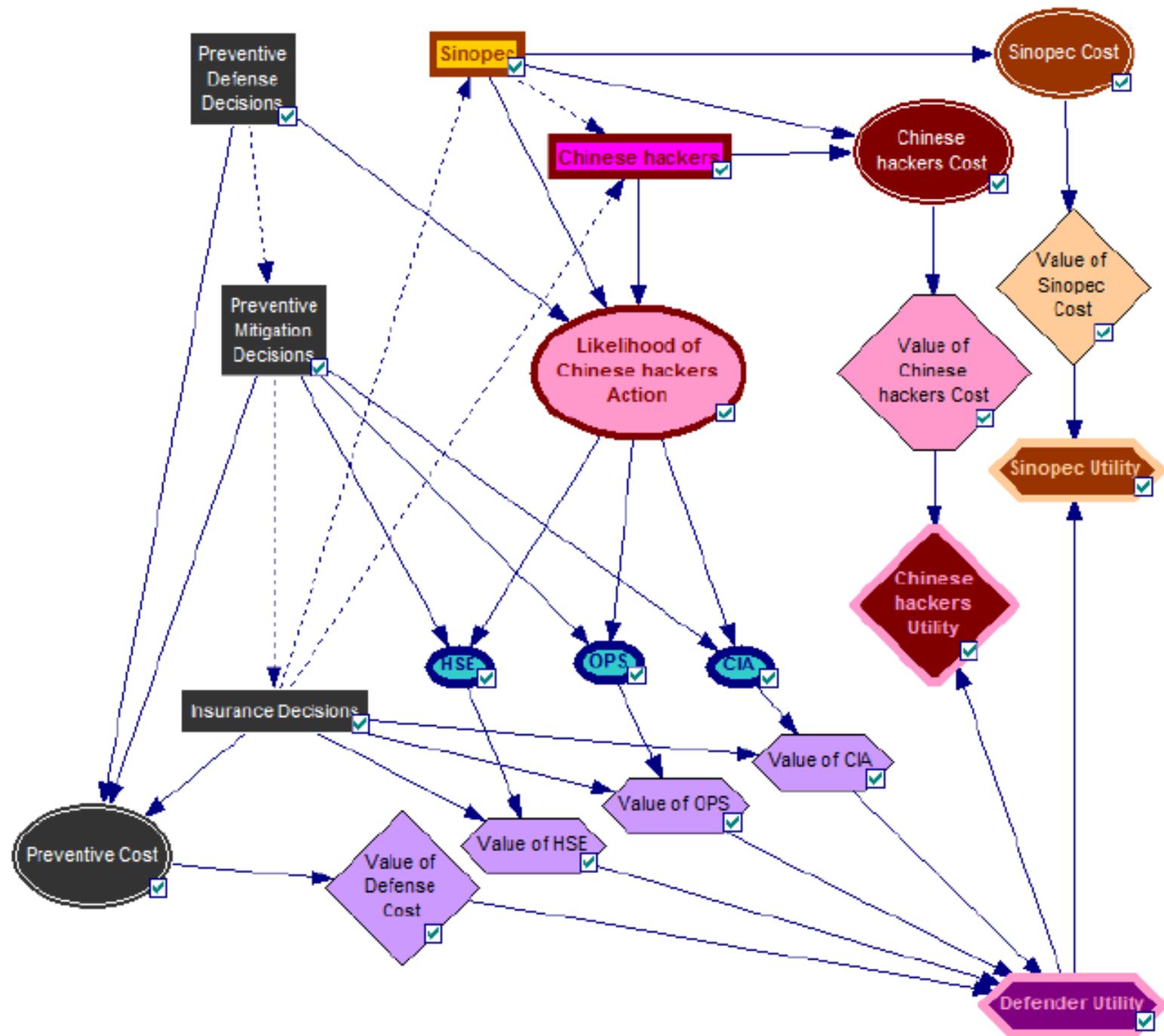
x	Investment	$P_{a,x}$					
		0	1	2	3	4	5
(4, 1, 0, 5, 1)	120700	0.60	0.26	0.08	0.03	0.02	0.01
(4, 0, 0, 0, 0)	2600	0	0.12	0.24	0.19	0.32	0.13
(0, 1, 0, 0, 0)	6500	0.01	0.05	0.18	0.2	0.23	0.33
(0, 0, 1, 0, 0)	90000	0	0.12	0.18	0.22	0.21	0.27
(0, 0, 0, 5, 0)	96000	0.45	0.28	0.13	0.07	0.05	0.02
(0, 0, 0, 0, 9)	140400	0.48	0.28	0.08	0.1	0.05	0.01
(4, 1, 1, 1, 2)	149500	0.28	0.37	0.13	0.09	0.09	0.04
(4, 1, 0, 0, 9)	149500	0.43	0.35	0.11	0.06	0.03	0.02
(3, 0, 1, 3, 0)	149550	0.35	0.29	0.15	0.13	0.07	0.01
(3, 0, 0, 2, 7)	149550	0.54	0.3	0.09	0.02	0.04	0.01
(1, 1, 0, 5, 3)	149950	0.48	0.37	0.06	0.07	0.01	0.01

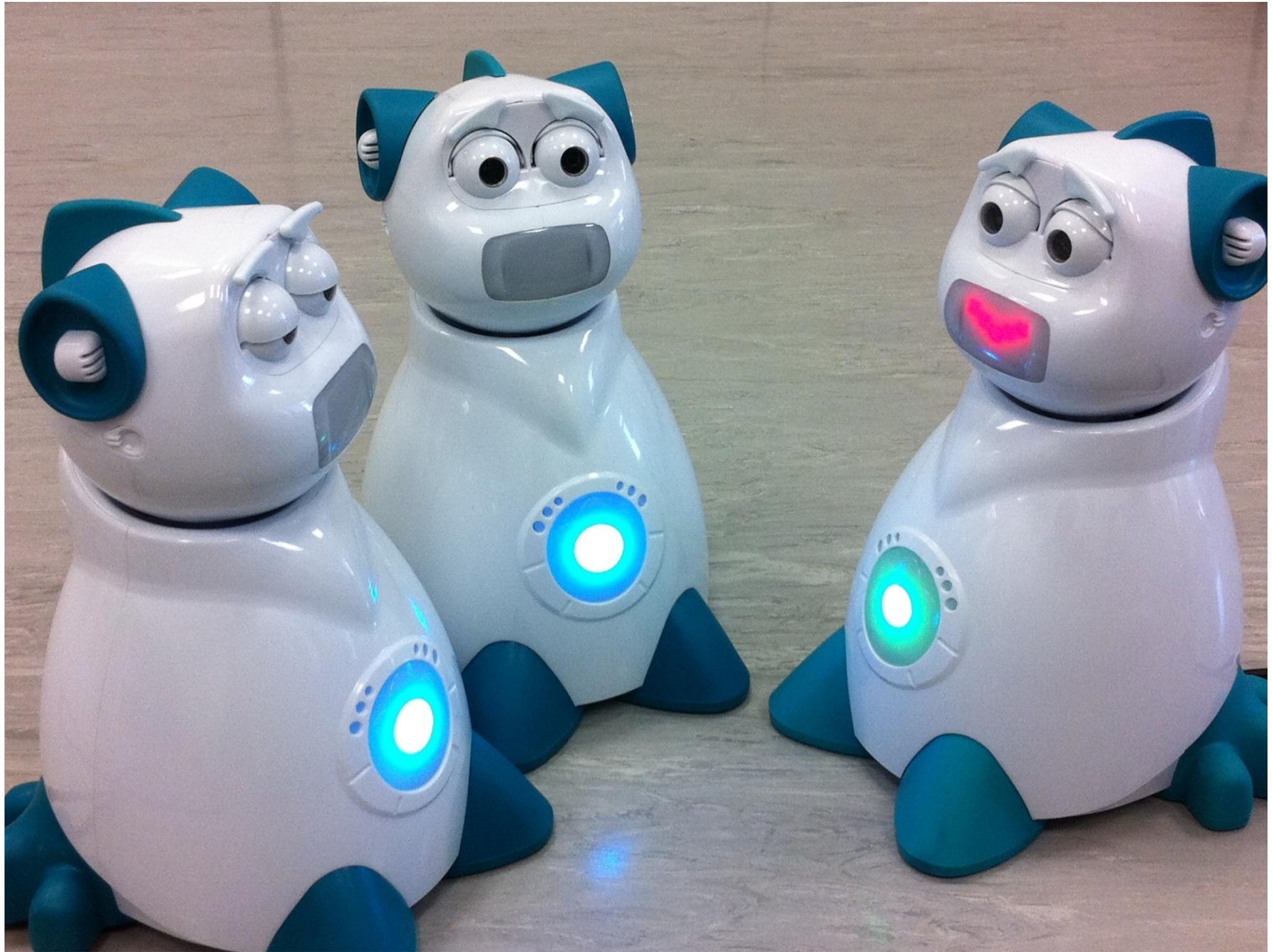
Metro de Barcelona



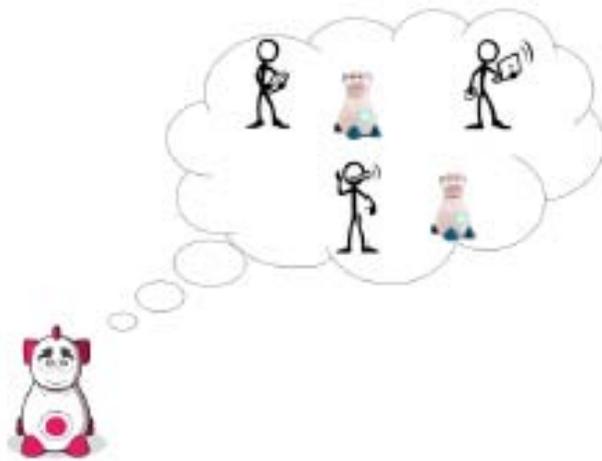
Estaciones múltiples



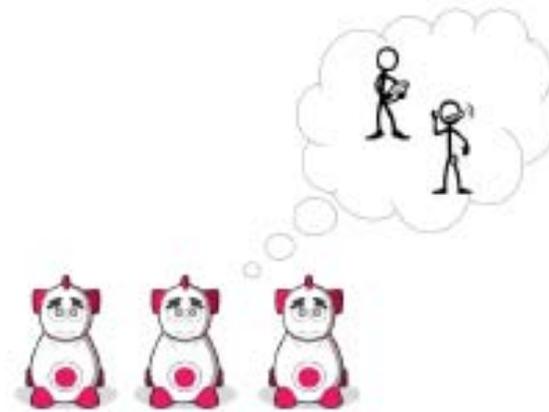




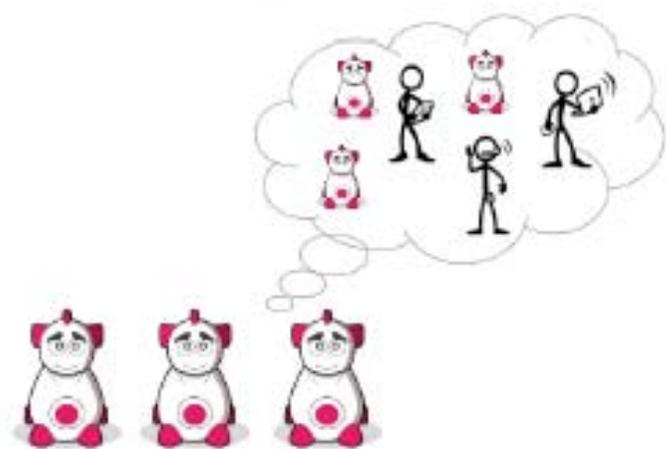
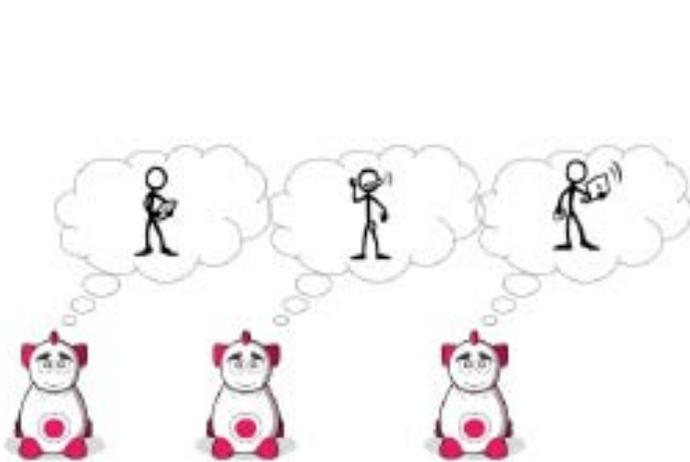
Marco básico



(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

Gracias

david.rios@urjc.es

www.analisisderiesgos.com

www.aisoy.com

www.skites.es