Game-Theoretic Foundations for Cyber-(Physical) Insurance Contracts.

(based on joint work with S. Shankar Shastry)

Galina Schwartz
Dept. of Electrical Engineering & Computer Sciences,
UC Berkeley, CA, USA

The Fourth Industrial Revolution for large-scale CPS: The Insurance

How to: measure, quantify, manage risks in large scale CPS

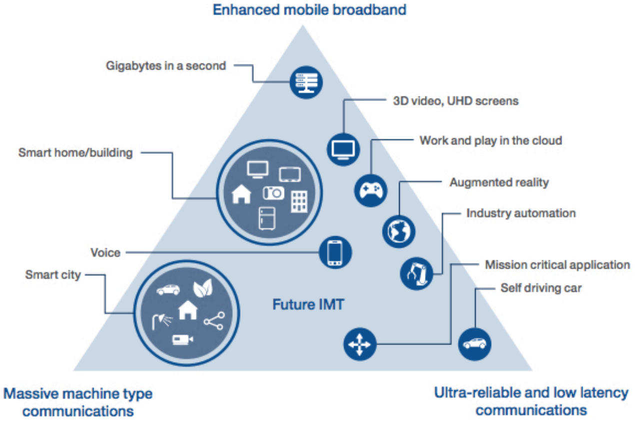
- Present:
  - cyber risks assessment is largely expert opinion-based
  - data is scarce
  - insurance pricing is adhoc
- Future: IDS risk framework $\longleftarrow$ FORCES meeting, 06-2016
  - Developing sound valuation theory for CPS risks (control theory; statistics)
  - Taking into account strategic risk nature (game theory)
- Future: Foundations of insurance $\longleftarrow$ Today's talk
  - Insurance contracts for large scale CPS with IDS risks
  - Effects on the magnitude of risk (microeconomic theory)
  - Policies (mandated vs. best practices) (IO, public policy)

Today's talk:

Insurance contracts
for large scale cyber-(physical) systems with IDS

Physical Infrastructures: The Fourth Industrial Revolution (4IR)

- From Cyber Risks to Cyber-Physical Risks
  [From Internet to Internet of Things]



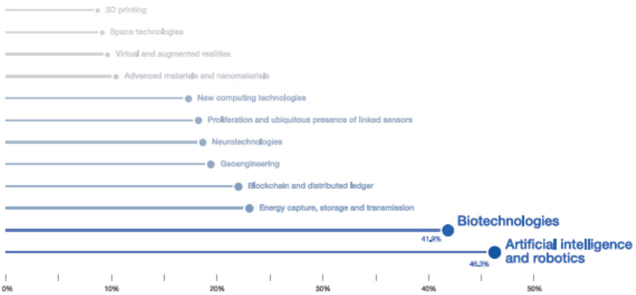
- World Economic Forum [WEF], World Economic Forum, Global Risk Reports, 2017

The Disruptive Impact of Emerging Technologies I

Disruptive technologies and governance (i.e, Institutions)

[disruptions of labor market ⟶ social instability]

Figure 3.1.3: Emerging Technologies Perceived as Needing Better Governance



Source: World Economic Forum Global Risks Perception Survey 2016.

A gradual disruption!? (oxymoron?)

Risk quantification and design of liability

(incl. insurance evaluation of institutional changes and social insurance)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The Fourth Industrial Revolution and large-scale CPS

- Transport (road, rail, waterways, airports)
- Energy (electricity, heat, fuel supply: gas, liquid and solid)
- Digital communications (fixed, mobile)
- Water (supply, waste water treatment, flood protection)

- MIT Forum and Infosys Risk Group, survey based MIT Global Risk Survey, 06-2016
  The nature of risk is changing [92.54 percent of companies]

CPS = IDS risks + disruptive technologies + insufficient governance $\longrightarrow$ an important question: how to design liability (risk sharing)

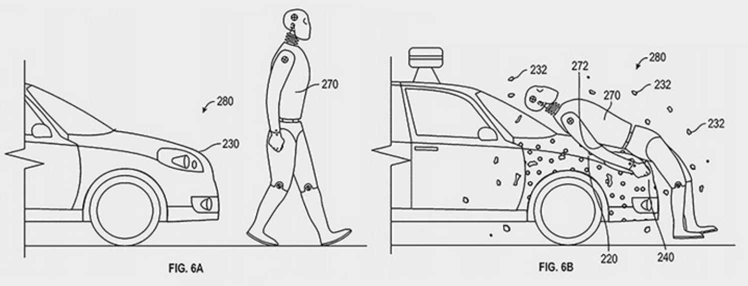
Motivating example: auto-insurance of driverless cars

Today: Flat rate $2.5 mln; Tomorrow: will depend on a vehicle and CIT

- vehicle features (+ internal CIT)
- vehicle interactions with external environment
  - humans
  - vehicles (multiple types: w/ human-driven, semi-automated and driverless)
  - road (physical environment and conditions; traffic rules)

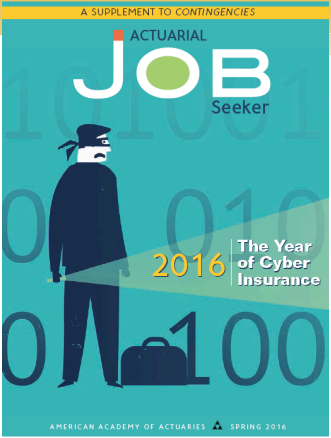
Implications of liability on technology

Google patent: Adhesive layer to protect pedestrians



Photograph: United States Patent and Trademark Office [patent granted on 05-17-2016]

Industry outlook on cyber-insurance



Approximate U.S. premiums:[5]

2015	$2.5 billion
2020	$7.5 billion[6] or $11.0 billion (assuming 35% annual growth)

Approximate global premiums:[7]

Near future: $85 billion

Miscellaneous errors	29.4%
Malware	25.1%
Insider misuse	20.6%
Physical theft/loss	15.3%
Web application attacks	4.1%
Denial of service	3.9%
Cyber espionage	0.8%
Point-of-sale intrusions	0.7%
Payment card skimmers	0.1%

Data: Contingencies Magazine, American Academy of Actuaries [Spring, 2016]

Verizon 2015 data breach investigations report

Historical outlook on cyber-insurance market

[hopes for 2016]

Data: US gross cyber premiums (bln $)

2005	[2.5] ("conservative" prediction)
2008	0.45
2009	0.5
2010	0.6
2011	0.8
2012	1
2013	1.3
2014	2
2015	2.5 - 2.75
2020	7 - 11 (prediction)

Betterley report 2010-2014, 2015, Marsh, Munich RE

... and emotions: 2010

Cyber risk is irreversible and geometrically expanding in 2010.

Cyber Insurance would very soon become a dominant instrument of risk transfer - reinventing an insurance market to transform from the physical to the virtual axes of risk.
World Economic forum, 2010

Benchmark: identical agents, no info asymmetries

Game between P (insurer) & A (potential insuree)

$$V = (1-p)U(W) + pU(W-D) \quad [\textit{no insurance } \alpha = (0,0)]$$

Contract $\alpha = (\alpha_1, \alpha_2)$

$$V = (1-p)U(W-\alpha_1) + pU(W-D+\alpha_2) \quad [\textit{with insurance } \alpha = (\alpha_1, \alpha_2) \neq (0,0)]$$

s	state $s = \{d, n\}$ (damage or no damage)
p	prob. of an accident (damage D from an accident)
W_s	agent's wealth in state s
$W_n = W$	no damage
$W_d = W - D$	damage D

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Benchmark (no info asymmetry)

Timing

P	offers a contract $\alpha = (\alpha_1, \alpha_2)$ to A
A	accepts $\alpha = (\alpha_1, \alpha_2)$ or rejects (aka $\alpha = (0, 0)$)
N	draws s from a dist. w/ known density P & A observe s (d or n)
P & A	payoffs Π^P *and* V^A

$$\Pi^P = \begin{cases} \Pi_n = \alpha_1 & \text{if } s = n \\ \Pi_s = -\alpha_2 & \text{if } s = d \end{cases}$$

$$V^A = \begin{cases} U_n = U(W - \alpha_1) & \text{if } s = n \\ U_s = U(W - D + \alpha_2) & \text{if } s = d \end{cases}$$

Benchmark (no info asymmetry): A solution
PC insurers (Principals) & Identical insurees (Agents)

Contract $\alpha = (\alpha_1, \alpha_2)$

$$\Pi^P = \begin{cases} \Pi_n = \alpha_1 & \text{if } s = n \\ \Pi_s = -\alpha_2 & \text{if } s = d \end{cases} \qquad V^A = \begin{cases} U_n = U(W - \alpha_1) & \text{if } s = n \\ U_s = U(W - D + \alpha_2) & \text{if } s = d \end{cases}$$

$$\Pi^P = (1-p)\alpha_1 - p\alpha_2$$

$$V^A = \begin{cases} (1-p)U(W) + pU(W-D) & \text{if uninsured, } \alpha = (0,0) \\ (1-p)U(W-\alpha_1) + pU(W-D+\alpha_2) & \text{if } \alpha = (\alpha_1, \alpha_2) \neq (0,0) \end{cases}$$

Under perfect competition: $\Pi^P = 0$, for any $\hat{\alpha}_2 \in (0, D)$

$$(1-p)/p = \alpha_2/\alpha_1 \quad or \quad \alpha_1 = p\hat{\alpha}_2 \qquad [\textit{actuarially fair contract}]$$

Risk averse agent buys full coverage ($\hat{\alpha}_2 = D$). Same utility in both states (d, n):

$$V^A = U(W - pD) \quad and \quad (\alpha_1, \alpha_2) = (pD, (1-p)D)$$

Next: Two agent types; differ only by the prob. of an accident

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Moral Hazard (MH): general notation

s	state $s = \{d, n\}$ (damage or no damage)	
p	prob. of an accident (damage D)	
w	agent's initial wealth	
x	random loss (damage);	$= L$ (or $= D$)
F	dist. $F(x, a)$	
f	cont.density of F: $f(x; a)$ on support $[0, \overline{x}]$	
a	$A's$ action (ex. effort to reduce loss x) [new]	
$v(a)$	$v'(\cdot) < 0$; $v''(\cdot) > 0$ [new]	cost of effort
u	agent's utility in state s; $u'(\cdot) > 0$; $u''(\cdot) < 0$	
Π	insurer profit	
V	agent's utility: 2 polar cases: separable V_{sep} & pecuniary V_{pec}	
V_{sep}	separable: $V = u(w) - v(a)$	$\longleftarrow$ standard assumption
V_{pec}	pecuniary: $V = u(w - a)$	
r	insurance premium	$= \alpha_1$
$I(x)$	coverage (if loss = x); $I(x) \leq x$	$= \alpha_2$
α	contract $(r, I(x))$	$= \alpha$
w_n	$w - r$	
w_s	$w - r - x + I(x)$	

Assumptions

- Increase in effort a reduces loss in a sense of first order stochastic dominance $\frac{\partial F(x,a)}{\partial a} \leq 0$; strictly positive if positive measure of a.
- concavity of F in a (for any x) $\frac{\partial^2 F(x,a)}{\partial a^2} \leq 0$;

MH: problem formulation I

Optimal contract $(r, I(x))$ for user with V_{sep}. User objective is to max V

$$\max_{(r,I(x)),a} V = \max_{(r,I(x)),a} \left\{ \int_0^{\overline{x}} u(w - r - x + I(x)) f(x; a) dx - v(a) \right\},$$

s.t. user IC and insurer IR (non-negative profit from offering contract $(r, I(x))$)

$$a = \arg\max_e \left\{ \int_0^{\overline{x}} u(w - r - x + I(x)) f(x; a) dx - v(e) \right\} \quad \text{[user IC]}.$$

User IC may have multiple solutions. Insurer IR:

$$r - \int_0^{\overline{x}} I(x) f(x; a) dx \geq 0 \quad \text{[insurer IR]}.$$

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

MH: Non-zero deductible is optimal I

Proposition

The individual's share of loss is non-decreasing in the size of the loss: $x - I(x)$ is non-decreasing in x (because $u'(x)$ is strictly decreasing)

Remark

Less than full coverage is optimal with MH = deductible is required.

Terminology

$x - I(x) =$ individual's share of loss = coinsurance = deductible

MH: the channels: reducing loss vs prob. of loss I

Two channels:

- reducing prob. occurrence of each realization x,
- reducing the amount of loss x, while keeping the dist. of prob.of losses constant. (exogenous prob. of loss) ex. earthquake

Ehrlich & Becker 1972 terminology:

- self protection = reducing prob. of an accident ⟵ standard in cyber security papers (ex. dangerous driving (speeding)),
- self insurance = reducing the amount of loss; the prob. of loss is fixed exogenously (ex. earthquake, electricity blackout (customers))

Arnott & Stiglitz 1991 - example of (i);
Reduction of prob. of an accident and optimal deductible [used in majority of cyber insurance papers]

Conventional vs cyber: the case of self protection

Reminder: Standard case of modeling the reduction of prob. of an incident (self-protection): User objective is $\max_{(r,I(x)),a} V$

$$\max_{(r,I(x)),a}\left\{(1-(p_0-a))u(w-r)+(p_0-a)\int_0^{\overline{x}} u(w-r-x+I(x))f(x)dx - v(a)\right\}.$$

$$r - p_i(a_i, a_{-i})I(r) \geq 0. \quad \text{[insurer IR]}$$

Simplification to a known fixed loss $x = L$, but make prob. of loss interdependent: $p_i = p(a_i, a_{-i}) := B(s_i, s_{-i})$.

Insurance with Moral Hazard and IDS

With insurance, user objective is $\max_{(r,I(r)),s_i} V$

$$\max_{(r,I(r)),s_i} \{(1 - B(s_i, s_{-i}))u(w - r) + B(s_i, s_{-i})u(w - r - L + I(r)) - h(s_i)\},$$

s.t. insured IC and insurer IR

$$r - B(s_i, s_{-i})I(r) \geq 0. \quad \text{[insurer IR]}$$

In IDS case:

$$B_i(s_1, ... s_n) = 1 - s_i + s_i \prod_{j \neq i}^{n} \{q(1 - s_j)\}. \quad (1)$$

$$B_i = 1 - s_i + s_i q_n \left\{(1 - \bar{s}) - \frac{(1 - s_i)}{n}\right\}, \quad (2)$$

where $q_n := q(n)n$ and $\bar{s}$ denotes average network security:

$$\bar{s} = \frac{1}{n} \sum_{j=1}^{n} s_j.$$

Competitive contracts: the definition I

Each insurer offers a single contract in *a class of admissible contracts*, or does nothing. A Nash eq = a set of admissible contracts s.t.:

- all contracts at least break even
- given incumbent-insurer contracts, no contract by an entrant-insurer will make a strictly positive profit
- given the set of existing offered contracts, no incumbent can increase his profits by altering his offered contract

Such contracts are called *competitive* because

- entry and exit are free
- no barrier to entry
- no scale economies are present

Following Rothschild-Stiglitz (1976): individual insurer cannon affect the aggregates; thus, each insurer takes network security as given.

Timing of the game

P: offers a contract $\alpha = (\alpha_1, \alpha_2)$ to A

A: accepts $\alpha = (\alpha_1, \alpha_2)$
or rejects (aka $\alpha = (0, 0)$); invests in security

N: draws *s* from a dist. w/ (computable) density
P & A observe *s* (*d* or *n*)

P & A: payoffs
Π^P *and* V^A

First (ex ante), network nodes (players) observe all contracts offered by cyber insurers; second, each node chooses which contract to accept (if any); third (ex post), the nodes choose their security level(s), (in both cases, with cyber contract or without). Contracts include a stipulation prohibiting to buy extra cyber insurance

Step 1: Optimal user action for a given contract

Notation

$\rho_c := r, L_c := l(r) - r.$

Let there exist some offered contract (ρ_c, L_c).

Proposition

For a given network security $\tilde{s}$, and contract (ρ_c, L_c), with $L_c > 0$, individual optimum $s = s^\dagger(\tilde{s}, \rho_c, L_c)$ is strictly lower than his optimal security $s = s^*(\tilde{s}, 0, 0)$ with $L_c = 0$ (no insurance):

$$s^\dagger(\tilde{s}, \rho_c, L_c) < s^*(\tilde{s}, 0, 0).$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Step 2: Properties of contracts viable for the insurers

Zero profit condition [given network security $\tilde{s}$]:

$$\rho_c = \rho_c(s_i, \tilde{s}, L_c) = B_i(s_i, \tilde{s})L_c,$$

Proposition

From user optimality, for any given network security s, and in symmetric equilibrium (identical), there exists a unique corresponding viable contract $(\rho_c, L_c) = (\rho_c^\dagger(s), L_c^\dagger(s))$, *and the derivatives* $\frac{dL_c^\dagger}{ds}$ *and* $\frac{d\rho_c^\dagger}{ds}$ *are negative.*

$$\frac{dL_c^\dagger}{ds} = \frac{[R' + \Delta_{c1} B' L_c]}{B\Delta_{c1} - U'(W - \rho_c - L + L_c)} < 0, \tag{3}$$

and

$$\frac{d\rho_c^\dagger}{ds} = B' L_c + B\frac{dL_c^\dagger}{ds}, \text{ and } B' < 0. \tag{4}$$

Step 3: Derivation of user preferred contract(s)

The problem is equivalent to finding s s.t.

$$\max_{s} \left\{ B \cdot U(W - L - \rho_c + L_c) + (1 - B) \cdot U(W - \rho_c) - h(s) \right\}.$$

From (3) or (4), and player optima: in eq., connect L_c and s

$$\frac{[B\Delta_{c1} + U'(W - \rho_c - L + L_c)]}{[B\Delta_{c1} - U'(W - \rho_c - L + L_c)]} = \frac{sqR - B\Delta_{c1} B' L_c}{B\,[R' + \Delta_{c1} B' L_c]},$$

where R, B, ρ_c and ρ_c are:

$$R(s) := \frac{h'(s)}{[1 - q(1 - s)]},$$

$$B = \left[1 - s(1 - q) - (s)^2 q\right],$$

$$\rho_c = BL_c,$$

$$\Delta_{c1} := \left[U'(W - \rho_c - (L - L_c)) - U'(W - \rho_c)\right] > 0.$$

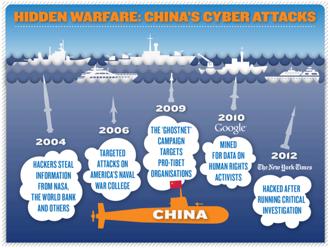
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Summary: Game theoretic framework

- Cyber-(physical) Insurance contracts
  - player choices are continuous
  - large scale IDS risks
  - strategic security investments
  - in the presence of moral hazard and adverse selection

- Novelty:
  - analytical solution for optimal contracts
  - modest requirements on data (aggregate data is sufficient for players)
  - tools to evaluate effects of different technologies
  - tools to evaluate policies
  - ready for applications in concrete CPS environments

Academic outlook on cyber-risks and cyber-insurance



Open questions

- Risk metrics: a hard question
- Data: scant and unreliable
  Technology advancement = [market is not in steady state]
- Adverse Selection: Lemon market (aka missing market) [econ jargon]
- Moral Hazard: difficulties with deductible

ex. prob. evals are expert based; Global Risks Report 2016

Actuarial evaluation?

Players (dominant + fringe)

AIG || Munuch RE Group || Lloyd's || Marsh || Beazley Group|| + 60+

Recent events

- UK govt'2015: World cyber-insurance center
- Marsh'2016: Cyber ECHO [capital]
- Lloyd's'2016: Standards [Core data requirements for cyber-insurance]
- Beazley & Munich RE'2016: Alliance [cyber and data breach insurance]

Treading (dangerous) waters?
From healthcare & mortgage risks to cyber risks?

Cyber-Insurance market is demand driven (lemon issues unresolved(?))

Cyber-Insurance is (almost) here