Cyber(in)security in Digital Services: the Unintended Effects of Interoperability

Stefano Comino[1] Alessandro Fedele[2] Fabio M. Manenti[3]

[1]University of Udine [2]Free Univ. of Bolzano [3]University of Padova

Economics of the DMA Workshop, JRC
– Bruxelles, September 2025 –

⇒ This paper is about the interplay between (A) - **interoperability** and (B) - **cybersecurity** in digital services

(A) Interoperability:

- The ability of different digital products and services to 'work seamlessly together' e.g.
  - send a text message from one messaging service to another
  - run different app stores on the same operating system
  - travel data seamlessly between cloud environments

⇒ This paper is about the interplay between (A) - **interoperability** and (B) - **cybersecurity** in digital services

(A) Interoperability:

- The ability of different digital products and services to 'work seamlessly together' e.g.
  - send a text message from one messaging service to another
  - run different app stores on the same operating system
  - travel data seamlessly between cloud environments
- Viewed favorably:
  - generates greater direct/indirect network externalities
  - reduces switching costs between different services
  - increases markets contestability

⇒ This paper is about the interplay between (A) - **interoperability** and (B) - **cybersecurity** in digital services

(A) Interoperability:

- The ability of different digital products and services to 'work seamlessly together' e.g.
  - send a text message from one messaging service to another
  - run different app stores on the same operating system
  - travel data seamlessly between cloud environments
- Viewed favorably:
  - generates greater direct/indirect network externalities
  - reduces switching costs between different services
  - increases markets contestability
- Broad consensus: regulators should mandate interoperability
  - art. 7 of the DMA: interoperability between messaging services
  - Chapters VI and VIII of the European Data Act: interoperability of data and data sharing mechanisms and services

(B) Cyberattacks and cybersecurity:

- Huge concern about cyberattacks on firms, public admins., individuals
  - threats include: damage and destruction of data, stolen money, service disruption, theft of IP, theft of personal and financial data ...
- Famous example: Target (US retail corporation) cyberattack (2013)
  - hackers exploited a vulnerability in Fazio Mechanical Services, a third-party HVAC contractor for Target (*indirect* attack)
  - installation of the Citadel malware on the vendor's systems, then used to gain unauthorized access to Target's network through a vendor portal

(B) Cyberattacks and cybersecurity:

- Huge concern about cyberattacks on firms, public admins., individuals
  - threats include: damage and destruction of data, stolen money, service disruption, theft of IP, theft of personal and financial data ...
- Famous example: Target (US retail corporation) cyberattack (2013)
  - hackers exploited a vulnerability in Fazio Mechanical Services, a third-party HVAC contractor for Target (*indirect* attack)
  - installation of the Citadel malware on the vendor's systems, then used to gain unauthorized access to Target's network through a vendor portal
- Broad consensus: need to take actions against these threats to ensure cybersecurity
  - global spending on cybersecurity projected to reach $213 billion in 2025, a nearly 10% increase from 2024 (Gartner, 2024)

Interoperability and cybersecurity: an inevitable tension

- Interoperability requires, e.g., the standardization of common functionalities and interfaces (Bourreau et al., 2022)
- This is considered to be risky by experts and companies in several sectors
  - health sector: interoperability aimed at enhancing access to patients data may expose personal info to cyber-risk (Gates, 2024)
  - text messaging services: interoperability threatens end-to-end encryption (Blessing and Anderson, 2023)

Interoperability and cybersecurity: an inevitable tension

- Interoperability requires, e.g., the standardization of common functionalities and interfaces (Bourreau et al., 2022)
- This is considered to be risky by experts and companies in several sectors
  - health sector: interoperability aimed at enhancing access to patients data may expose personal info to cyber-risk (Gates, 2024)
  - text messaging services: interoperability threatens end-to-end encryption (Blessing and Anderson, 2023)

- Where does the higher risk may come from?
  1. Interoperability creates larger targets for malicious actors
     - evidence shows that hackers are attracted by large targets (e.g. Villeneuve, 2011; Geer et al., 2020)
  2. As digital services are more interoperable, 'entry points' for hackers multiply
     - expanded attack surface
     - creation of backdoors: hidden entrances that bypass security measures

This paper

- We build a model with three types of agents:
  - *i*) Two competing firms/platforms selling digital services
  - *ii*) Users buying such services
  - *iii*) Hackers performing malicious activities to attack platforms

- **Main assumption**: Interoperability stimulates hackers' malicious activities
  $\Rightarrow$ a greater mass of data can be compromised

- Our aim:
  - Examine platforms' incentives to invest in cybersecurity
  - Compare private *vs* social incentives for interoperability

Plan of the talk

- Related literature
- Baseline model
- Private *vs* social incentives for interoperability
- Extensions *(not today)*
- Sophisticated and naive users
- Ad-funded platforms
- Uncovered market

Related literature

1. Incentives to invest in cybersecurity. Main focus either on (Fedele and Roner, 2022):
   - (a) technical spillovers: firms use a common/interconnected IT infrastructure but aren't competitors; or
   - (b) market spillovers: competing firms using an independent/non-connected infrastructure
   - $\Rightarrow$ However, in digital markets (a) and (b) may come together, especially with interoperability

2. Oligopolistic competition in markets with congestion (e.g., De Borger and Van Dender, 2006; Matsumura and Matsushima, 2007)
   - lower investment in quality $\Rightarrow$ lessens the intensity of price-competition
   - De Corniére and Taylor (2024) focus on investment in cybersecurity

Related literature

3. Compatibility and standardization in network industries
   - Katz and Shapiro (1985); Farrell and Salorner (1986); Crémer et al. (2000)
   - recent contributions investigating the interplay between interoperability and multihoming (Bourreau and Kraemer, 2022; Dhakar and Yan, 2024)

Timing of the game

Firms/platforms located at the end-points of a unit-length Hotelling line

They offer **interoperable** services

For a given **degree of interoperability** $g \in [0, 1]$:

- t_1: Firms invest in cybersecurity, $\alpha_i \in [0, 1]$ and $\alpha_j \in [0, 1]$
- t_2: Firms compete on prices, p_i and p_j
- t_3: Users observe firms' choices and decide which one to patronize: m_i and m_j mass of users on platform i and j
- t_4: Hackers observe users' and firms' choices, then decide how much to invest in malicious activities
- t_5: Payoffs

$\Rightarrow$ focus on symmetric equilibrium with full market coverage

Hackers

- Two groups of hackers of mass 1: type i and j (alternatively, two hackers)
- Type-i hackers specialized in malicious activities targeting platform i
  - their payoff increases with the mass of users that can be reached (proxy for the amount of data that can be compromised): $m_i + g\, m_j$
    - $\Rightarrow$ interoperability g makes an attack targeted to platform i useful to compromise users on the other platform too
- Let denote with q_i the probability of a successful attack from type-i hackers:
  - each hacker spends $c(q_i)$ to increase q_i, with $c'(q_i) > 0$
  - the cost increases the higher α_i, i.e. the more secure platform i:
    - $\Rightarrow$ $c(q_i) = \frac{1}{2}\frac{q_i^2}{1-\alpha_i}$

Hackers

- Type-i Hacker's optimization problem:

$$\max_{q_i} \; q_i(m_i + g\, m_j) - \frac{1}{2}\frac{q_i^2}{1-\alpha_i} \quad \Rightarrow q_i^* = (1-\alpha_i)(m_i + g\, m_j),$$

  $\Rightarrow$ q_i^* is the prob. of a successful attack from type-i hackers targeting platform i (so called **direct attack**)

Hackers

- Type-i Hacker's optimization problem:

$$\max_{q_i} \; q_i(m_i + g\, m_j) - \frac{1}{2}\frac{q_i^2}{1-\alpha_i} \quad \Rightarrow q_i^* = (1-\alpha_i)(m_i + g\, m_j),$$

  $\Rightarrow$ q_i^* is the prob. of a successful attack from type-i hackers targeting platform i (so called **direct attack**)

Tension between cybersecurity and interoperability (**Driver 1**):

- interoperability, g, stimulates hacker's malicious activities

$\Rightarrow$ interoperability increases incentives to invest in security

Indirect attacks and probability of a breach

- **Indirect attacks**: performed by type-j hackers on platform j but, due to interoperability, can compromise platform i as well
- The overall probability of platform i being breached is $q_i^* + g\, q_j^*$:

$$prob_i(\alpha_i, \alpha_j, g) = \underbrace{(1-\alpha_i)(m_i + g\, m_j)}_{\text{direct attacks}} + \underbrace{g\,(1-\alpha_j)(m_j + g\, m_i)}_{\text{indirect attacks}}.$$

$\Rightarrow$ $prob_i(\alpha_i, \alpha_j, g)$ consistent with the idea that interoperability (via the use of shared protocols) creates backdoors that hackers may use

Indirect attacks and probability of a breach

- **Indirect attacks**: performed by type-j hackers on platform j but, due to interoperability, can compromise platform i as well
- The overall probability of platform i being breached is $q_i^* + g\, q_j^*$:

$$prob_i(\alpha_i, \alpha_j, g) = \underbrace{(1-\alpha_i)(m_i + g\, m_j)}_{\text{direct attacks}} + \underbrace{g\,(1-\alpha_j)(m_j + g\, m_i)}_{\text{indirect attacks}}.$$

$\Rightarrow$ $prob_i(\alpha_i, \alpha_j, g)$ consistent with the idea that interoperability (via the use of shared protocols) creates backdoors that hackers may use

Tension between cybersecurity and interoperability (**Driver 2**):

- interoperability, g, opens the door to indirect attacks
- it generates public-good effect of the investment in cyber-security

$\Rightarrow$ interoperability reduces incentives to invest in cybersecurity

Users

Utility of a user located at x on the Hotelling line and purchasing from i

$$U_i(x) = v + \theta(m_i + g m_j) - \delta\, prob_i(\alpha_i, \alpha_j, g) - t\, d(x, i) - p_i$$

- v: baseline utility (assume large to ensure full coverage)
- $\theta(m_i + g\, m_j)$: network effects
  - interoperability increases network effects
- δ: the damage from a security breach
- $t\, d(x, i)$: transportation costs
- p_i: price charged by platform i

Firms/Platforms

- Demand functions derived from: $U_i(x) = U_j(x) \;\Rightarrow\; m_i(p_i, p_j, \alpha_i, \alpha_j)$
- Hence, the profit function of platform i

$$\pi_i(\alpha_i, p_i) = p_i\, m_i(p_i, p_j, \alpha_i, \alpha_j) - \ell\, prob_i(\alpha_i, \alpha_j, g) - c\,\frac{\alpha_i^2}{2},$$

  - costs for providing the service normalized to 0
  - ℓ: loss in the event of a breach (damage to the IT infrastructure, reputation loss, etc.)
  - $c\alpha_i^2/2$: cybersecurity investment costs

Pricing stage: the strategic effect of α_i

- Look at how security investment α_i impacts on the competitor's price-reaction function $p_j^*(p_i)$:

$$\frac{\partial p_j^*(p_i)}{\partial \alpha_i} = \underbrace{-\delta \frac{1-g}{2}}_{\text{strategic effect}} + \ell \frac{(1-g)g}{2}$$

- larger α_i induces more aggressive pricing by j
- strategic incentive to reduce α_i to mitigate price competition $\Rightarrow$ standard result in the literature on congestion

Tension between cybersecurity and interoperability (**Driver 3**):

- interoperability, g, reduces the magnitude of the strategic effect
- $\Rightarrow$ interoperability mitigates the platforms' incentives to lower the security investment (platforms more similar in terms of security $\Rightarrow$ investment in protection less relevant)

Investment stage

Zero-interoperability case ($g = 0$):

Remark (1)

With no interoperability, platforms' equilibrium level of investment in cybersecurity is:

$$\alpha^*(0) = \underbrace{-\frac{\delta}{12c}}_{(i)} + \underbrace{\frac{\ell}{3c}}_{(ii)}.$$

- trade-off: mitigate price competition *vs* reduce expected damages

Investment stage

Zero-interoperability case ($g = 0$):

Remark (1)

With no interoperability, platforms' equilibrium level of investment in cybersecurity is:

$$\alpha^*(0) = \underbrace{-\frac{\delta}{12c}}_{(i)} + \underbrace{\frac{\ell}{3c}}_{(ii)}.$$

- trade-off: mitigate price competition *vs* reduce expected damages

Proposition (1)

For a given g, the platforms' equilibrium level of investment in cybersecurity is:

$$\alpha^*(g) = \underbrace{-\frac{\delta}{12c}(1-g)}_{\text{Driver } 3(-)} + \underbrace{\frac{5\,\delta}{12c}g(1-g)}_{\text{Driver } 1(+) > \text{Driver } 2(-)} + \frac{\ell(1+3g-g^2)}{3c}.$$

Equilibrium price

$$p^* = t - (1-g)\theta + (\delta + \ell)(1-g)^2(1-\alpha^*)$$

Remark (2)

The equilibrium price p^* reduces with the intensity of network externalities θ; the negative effect of θ on p^* reduces with g.

- equilibrium price reduces with θ: the stronger the network externalities the lower the price to enlarge the installed base of users
- this effect is moderated by g: the more interoperable the services the less the need to enlarge the installed base of users

Socially optimal investment

Proposition (2)

The socially optimal investment level is

$$\alpha^w = \frac{(1+g)^2(\delta+2\ell)}{4c}.$$

Corollary (3)

The socially optimal investment is larger than the equilibrium one, $\alpha^w > \alpha^*$.

Interoperability: private *vs* social incentives

- Unable to derive analytically the private and social optimal levels of interoperability

- What we do:
  - compare conditions under which a given $g > 0$ is preferred to $g = 0$
  - interoperability g is **privately** preferred iff $\Delta\Pi = \pi(g) - \pi(0) > 0$
  - interoperability g is **socially** preferred iff $\Delta W = W(g) - W(0) > 0$
  - compare private *vs* social desirability

  $\Rightarrow$ NOTE: considering g as given has a practical justification:
    - ★ the degree of interoperability that digital service providers can achieve, whether they offer text messaging, cloud computing, or other services, is largely exogenously determined by the characteristics of the technology under consideration.

Interoperability: private *vs* social incentives

- Private incentives towards interoperability iff

$$\Delta\Pi = \underbrace{p(g) - p(0)}_{\Delta\ Ind.Revenues} - \underbrace{2\ell(prob(g) - prob(0))}_{\Delta\ Exp.cost\ of\ breach} - \underbrace{c(\alpha(g)^2 - \alpha(0)^2)}_{\Delta\ Inv.\ costs} > 0$$

Interoperability: private *vs* social incentives

- Private incentives towards interoperability iff

$$\Delta\Pi = \underbrace{p(g) - p(0)}_{\Delta\ Ind.Revenues} - \underbrace{2\ell(prob(g) - prob(0))}_{\Delta\ Exp.cost\ of\ breach} - \underbrace{c(\alpha(g)^2 - \alpha(0)^2)}_{\Delta\ Inv.\ costs} > 0$$

- Social incentives towards interoperability iff

$$\Delta W = \underbrace{\frac{\theta g}{2}}_{greater\ netext} - \underbrace{(\delta + 2\ell)(prob(g) - prob(0))}_{\Delta\ exp.\ damages\ from\ breach} - \underbrace{c(\alpha(g)^2 - \alpha(0)^2)}_{\Delta\ investment\ cost} > 0$$

Interoperability: private *vs* social incentives

- Private incentives towards interoperability iff

$$\Delta\Pi = \underbrace{p(g) - p(0)}_{\Delta\ Ind.Revenues} - \underbrace{2\ell(prob(g) - prob(0))}_{\Delta\ Exp.cost\ of\ breach} - \underbrace{c(\alpha(g)^2 - \alpha(0)^2)}_{\Delta\ Inv.\ costs} > 0$$

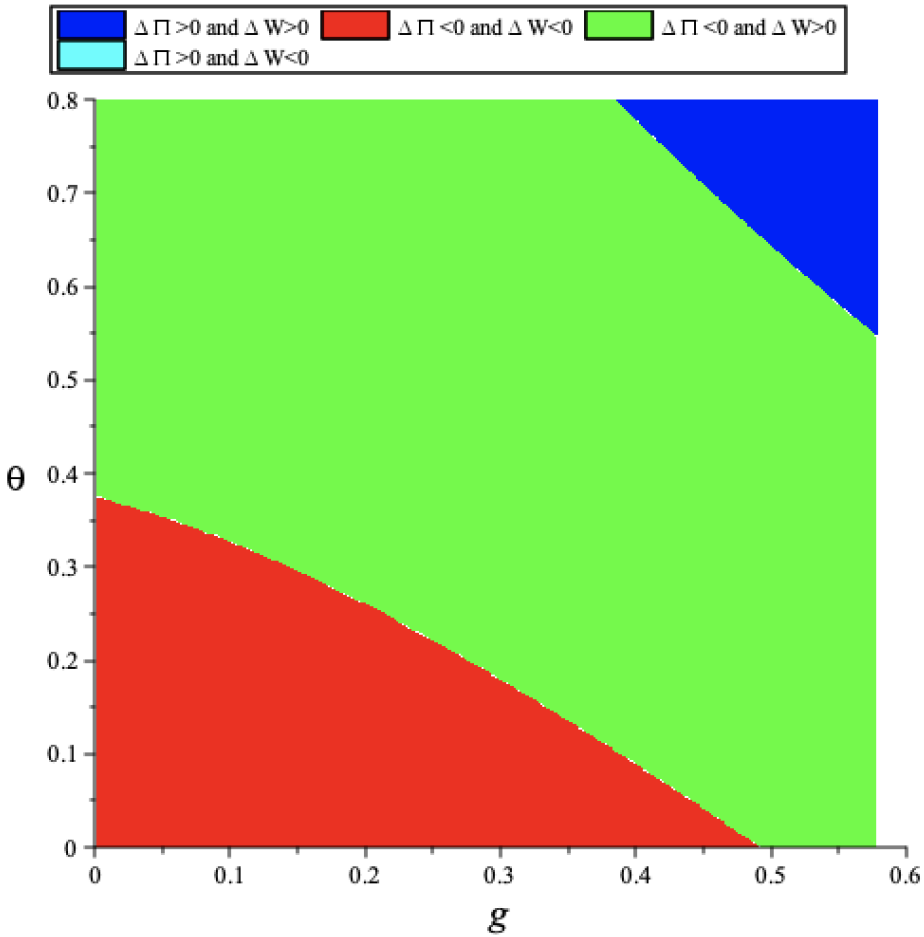
- Social incentives towards interoperability iff

$$\Delta W = \underbrace{\frac{\theta g}{2}}_{greater\ netext} - \underbrace{(\delta + 2\ell)(prob(g) - prob(0))}_{\Delta\ exp.\ damages\ from\ breach} - \underbrace{c(\alpha(g)^2 - \alpha(0)^2)}_{\Delta\ investment\ cost} > 0$$

Notice:

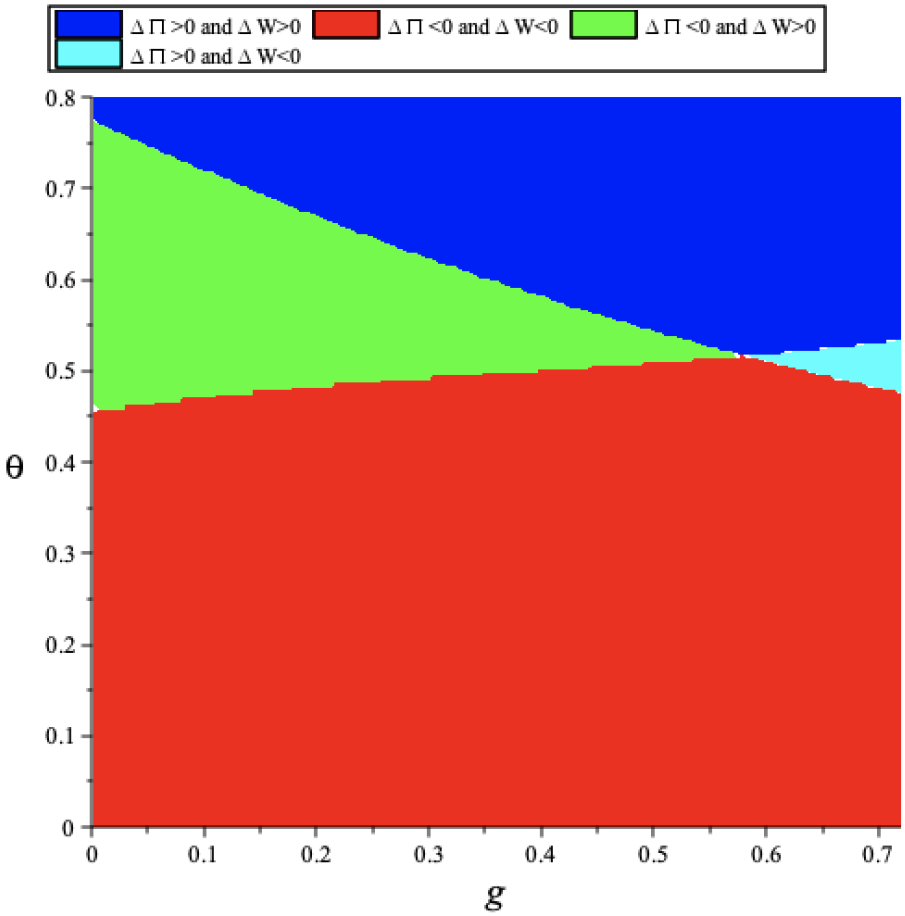
- θ positively affects ΔW (directly) and $\Delta\Pi$ (via the effect on prices)
- $\Delta\Pi$ depends on price difference
- ΔW more sensitive to the difference in the probability of breach

Simulations: ℓ large - strong incentives to invest



- we can show that the probability of breach is lower with interoperability than without
- when θ and g are both large or both small, private and social incentives are aligned
- when *i*) θ is high and g is not too large, or *ii*) when θ is relatively small and g is large interoperability is socially desirable but privately not profitable
  - *i*) high network externalities for users ($\Delta W > 0$), but due to the moderate values of g, they contribute little to firms profits ($\Delta \Pi < 0$)
  - *ii*) when g is large, the probability of breach is substantially lower with interoperability, a fact that is more beneficial for welfare then for firms.

Simulations: ℓ small - lower incentives to invest



- public good effect is more relevant
- firms invest less the higher the degree of interoperability. The probability of breach is larger with $g > 0$ than with $g = 0$
- new misalignment: when θ is sufficiently large and g is large, interoperability is privately desirable but not socially
  - the public good effect is very strong: firms invest very little under interoperability, the probability of breach increases substantially and this damages users

Extension 1: sophisticated and unsophisticated users

Two types of customers:

i) $\lambda \in [0,1]$ users aware of cyber risk, and behave as before:

$$U_i(x) = v + \theta(m_i + gm_j) - \delta\, prob_i(\cdot) - td(x,i) - p_i$$

ii) $1-\lambda$ users **unsophisticated and ignore the risk of cyber attacks**:

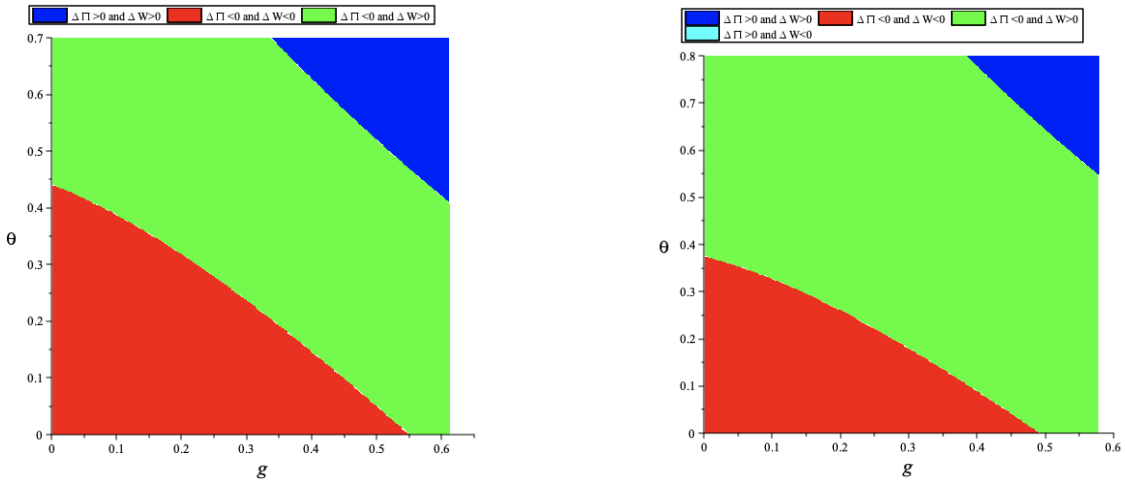
$$U_i(x) = v + \theta(m_i + gm_j) - td(x,i) - p_i$$

Useful to discuss the consequences of

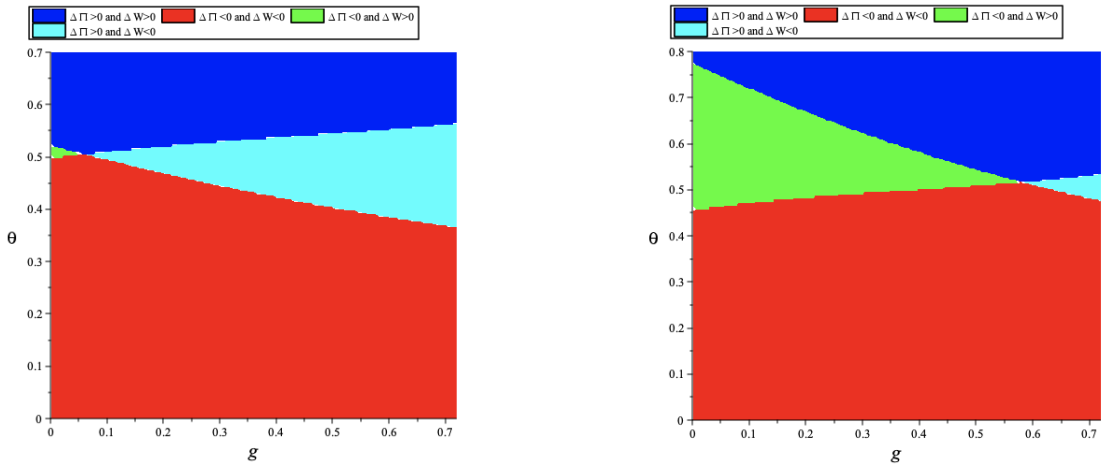
$\Rightarrow$ a regulation requiring platforms to certify their level of security

$\Rightarrow$ campaigns aimed at raising public awareness of cyber risks

Extension 1: Incentives towards interoperability



figureLarge ℓ: left $\lambda = 0.4$, right baseline



figureSmall ℓ: left $\lambda = 0.4$, right baseline

Extension 2: Ad-funded platforms

$$U_i(x) = v + \theta(1-g)m_i - \delta\, prob_i(\alpha_i, \alpha_j, g) - t\, d(x),$$

$$\pi_i(\alpha_i) = A\, m_i(\alpha_i, \alpha_j; g) - \ell\, prob_i(\alpha_i, \alpha_j; g) - c\,\frac{\alpha_i^2}{2}.$$

Proposition (5)

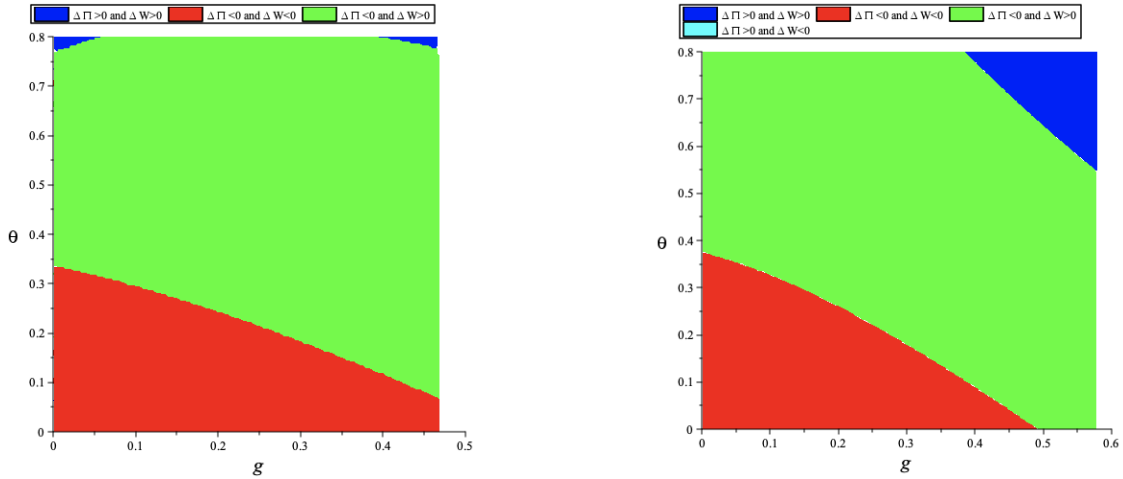
When firms adopt an Ad-funded business model, the equilibrium level of investment in cybersecurity is:

$$\alpha^*_{Ad}(g) = \frac{1}{2} + \frac{\theta(g-1)+t}{2(1-g)^2\delta} + \frac{\ell(1+g)^2}{8c} - \frac{\sqrt{N(g)}}{8c\delta(1-g)^2}, \tag{1}$$

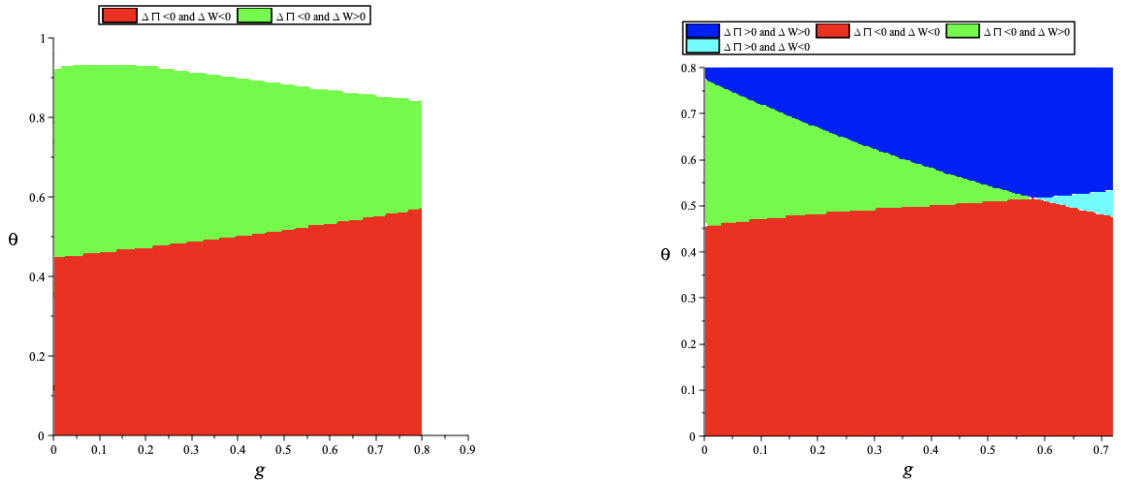
where

$$\begin{aligned} N(g) \;=\; & \left(4((1-g)^2\delta - \theta(1-g) + t)c\right)^2 - \\ & 8\delta(1-g)^2(1+g)\left((1-g)\left(2A + \ell\left(1-g^2\right)\right)\delta - \ell(3-g)(\theta(1-g)-t)\right)c + \delta^2\ell^2(1-g)^4(1+g)^4. \end{aligned}$$

Extension 2: Incentives towards interoperability



figure$A = p^*$ and large ℓ: left $\lambda = 0.4$, right baseline



figure$A = p^*$ and small ℓ: left $\lambda = 0.4$, right baseline

Summary

- **Interoperability** can **stimulate cyberattacks**
- We propose a congestion-like model to study the effect of interoperability
  - different drivers impact on how g affects investment in security
- **Social desirability** of interoperability depends on the interplay between **network externalities** and the **level** of interoperability
- It also depends on other aspects (extensions - *not today*): business model, sophistication of consumers, damages suffered by firms (ℓ)...
  - services characterized by large network effects, regulations imposing interoperability are likely to be welfare enhancing
  - when firms are ad-funded there are likely to be too few incentives to be interoperable

THANK YOU FOR YOUR ATTENTION!