unibz
Fakultät für Wirtschaftswissenschaften
Facoltà di Economia
Faculty of Economics and Management

BEMPS –
Bozen Economics & Management
Paper Series

NO 116/ 2025

Cyber(in)security and Interoperability in Digital Services

Stefano Comino, Alessandro Fedele, Fabio Manenti

Cyber(in)security and Interoperability in Digital Services*

Stefano Comino† Alessandro Fedele‡ Fabio M. Manenti§

October 28, 2025

Abstract

This paper investigates the interplay between interoperability and the incentives to invest in cybersecurity in digital markets. We develop a two-sided symmetric duopoly model in which cyberattacks create a congestion-like externality, and interoperability amplifies hackers' incentives to target connected platforms. We show that interoperability affects cybersecurity investment through multiple channels, potentially producing a non-linear relationship: low interoperability promotes risk-mitigation efforts, whereas high interoperability may discourage investment due to a public good effect. We then compare private and social incentives for interoperability, identifying potential sources of misalignment. Finally, we extend the baseline model to account for additional factors shaping the desirability of interoperability, including platforms' business models, users' awareness of cyber risk, market expansion effects, and asymmetries in user bases.

JEL codes: L13, L15, L51, L86.

Keywords: cybersecurity, interoperability, congestion, hackers, two-sided platforms, investment.

*An earlier version of the paper was circulated under the title "Cyber(in)security in Digital Services: the Unintended Effects of Interoperability". We are grateful for valuable comments and suggestions from Simon Loertshcher, Leonardo Madio, Gonzalo Munilla-Garrido, Martin Peitz, and Rodolfo Alberto Salonia. A special thank to Massimo Motta for repeated interactions and insightful comments on an earlier draft of the manuscript. We also thank the audiences at the ASSET Conference (Rabat, 2025), the Workshop on "The Economics of the DMA" (Bruxelles, 2025), the Workshop "Navigating the Digital Frontier: Cyber-Security, Platforms and Regulation" (Udine, 2025), the CRESSE Conference (Crete, 2025), the EARIE Conference (Valencia, 2025), the "Jornadas de Economia Industrial" (Santander, 2025), the SIEPI Conference (Bologna, 2025), and the Workshop "Cybersecurity and Internet Governance" (Padua, October 2024). Finally, we thank the seminar audiences at the UEA Centre for Competition Policy (2025), the Dept. of Economics - U. of Pretoria (2025) and the Dept. of Economics - U. of Padua (2025). This study is carried out within the project "Cyber resilience: markets, investments and regulation", funded by European Union, Next Generation EU within the PRIN 2022 PNRR program (D.D.1409 del 14/09/2022 Ministero dell'Università e della Ricerca), code: P20229EL9W. This manuscript reflects only the authors' views and opinions, and the Ministry cannot be considered responsible for them.

†University of Udine; email: stefano.comino@uniud.it

‡Free University of Bolzano; email: alessandro.fedele@unibz.it.

§Corresponding author. University of Padua; email: fabio.manenti@unipd.it

1 Introduction

Interoperability—the ability of diverse digital services, platforms, and products to work seamlessly together—is a key enabler of the increasing interconnection of digital systems and is transforming the way businesses and individuals interact, share information, and engage with technology. While delivering substantial benefits, including greater efficiency, productivity, and consumer choice, interoperability also raises concerns about the escalating threat of cyberattacks, which can inflict severe financial, operational, and reputational damage on businesses, public administrations, and individuals alike.[1] In this paper, we investigate the complex interplay between interoperability and cybersecurity with the aim to help bring clarity to the emerging trade-offs.

Whether at the horizontal level (e.g., the ability for different messaging services to exchange data) or at the vertical level (e.g., the ability for apps to run across different operating systems), interoperability fosters the development of more open, flexible, and user-friendly ecosystems (Bourreau et al., 2022), thereby generating benefits for consumers. In may cases, interoperability is also driven by regulatory initiatives aimed at reducing switching costs, enhancing user experience, and promoting network effects. The European Data Act and the Digital Markets Act are two prominent examples of such regulations. The former mandates functional equivalence between cloud service providers, enabling users to easily migrate data and digital assets from one provider to the other. The latter imposes interoperability obligations on platforms offering text messaging services, allowing users of one platform to communicate with users of another. In both cases, the overarching goal is to reduce customer lock-in and foster competition and innovation.

However, the very features that enable interoperability—such as the use of common protocols, standardized interfaces, and open systems—can also introduce new vulnerabilities (Gasser, 2015). Greater interoperability often results in an expanded attack surface: as systems and platforms become more interconnected, the number of potential entry points for malicious actors increases. Moreover, when multiple services rely on similar protocols or communicate through standardized interfaces, an attack on one platform can rapidly compromise others that share the same technological infrastructure. These concerns are particularly salient in sectors where digital infrastructure is critical. In healthcare, for example, the interoperability of electronic health records (EHRs) is designed to improve patient care by providing clinicians with timely and comprehensive information. Yet, as Gates (2024) notes in the context of the U.S. health system, the same interoperability that facilitates access to patient data also exposes sensitive personal information to heightened cybersecurity risks. Similar concerns emerge in the context of Internet of Things (Catuogno and Turchi, 2015; and Rana and Patil, 2023) and communication services where interoperability may undermine end-to-end encryption (Blessing and Anderson, 2023).

In this paper, we develop a two-sided model with two competitive platforms selling digital services to users, on one side of the market, and attracting hackers, on the other. Hackers are assumed to be motivated by the size of a platform's user base, which serves as a proxy for the volume of data that can potentially be compromised.[2] Interoperability enhances the network externalities enjoyed by users, but it also expands the pool of data hackers can access, thereby stimulating their malicious activities. In this context, we show that interoperability impacts on the platforms' incentives to invest in cybersecurity through different channels.

Our main findings are as follows. We uncover a non-linear relationship between interoperability and

[1] For a recent survey on the economics of cyber risk see Abrardi et al. (2025).

[2] This assumption is based on the cybersecurity literature showing that the larger and more valuable firms are, the higher the likelihood they are targeted by hackers (e.g., Villeneuve, 2011; August et al., 2014; Arce, 2018; Geer et al., 2020).

security investment: at low levels, interoperability encourages platforms to invest in risk mitigation, whereas at high levels, it may discourage investments due to a public good effect (i.e. each platform increasingly benefiting from the competitor's security investment). We then compare private and social incentives for interoperability and highlight two main effects. When the public good effect is mitigated by large breach-related damages suffered by platforms, private incentives to pursue interoperability tend to fall short of the social ones, making mandated interoperability welfare-enhancing. Conversely, when the public good effect of interoperability is more far-reaching, platforms may have excessive incentives to become interoperable, as this reduces the need for aggressive pricing strategies to expand their user base. Finally, we extend our baseline model in four directions to explore other potential determinants of the desirability of interoperability: platforms' business models, users' awareness of cyberrisk, the potential for market expansion, and ex-ante asymmetries in installed user bases.

Related Literature. Our paper contributes to three main different strands of literature. First, we add to a growing body of research that investigates the incentives for firms to invest in cybersecurity. This literature has been recently reviewed by Fedele and Roner (2022) who classify existing contributions into two main streams. The first stream examines the investment decisions of firms that operate within a shared computer network but not competing directly in the product market. In this case, cybersecurity investments exhibit a public good nature, as they enhance the overall security of the network and benefit other firms using the same infrastructure. The second stream focuses on firms that compete in the product market but rely on independent, non-interconnected systems. Here, improving cybersecurity provides a competitive edge over rivals. Our contribution lies in bridging these two perspectives by analyzing a setting where firms compete in the product market and, at the same time, their cybersecurity investments acquire a public good dimension due to interoperability.[3] In addition, we study the incentives for firms to be interoperable.[4]

Second, we contribute to a well-established literature on oligopolistic competition in markets subject to congestion (e.g., De Palma and Leruth, 1989; De Borger and Van Dender, 2006; and Matsumura and Matsushima, 2007). In facilities like seaports, airports or hospitals the quality of the service deteriorates as the number of simultaneous users increases, due to rising time costs associated with access. In our setting, a similar congestion-like effect arises: the larger the mass of users patronizing a platform, the stronger the incentives for malicious activities by hackers. Within this literature, the study most closely related to ours is De Cornière and Taylor (2024) which examines two vendors of digital products investing in security to protect their customers from cyberattacks. We extend this line of research by introducing interoperability across services, a feature that turns security investment into a public good and amplifies the congestion effect by increasing the incentives for hackers.

Finally, our paper relates to the extensive literature on compatibility and standardization in markets characterized by network effects (e.g., Katz and Shapiro, 1985a; Farrell and Saloner, 1986; and Crémer et al., 2000). The high levels of concentration recently achieved in digital markets has led scholars and policymakers to emphasize the importance of interoperability regulations for enhancing market contestability.[5] Mandated interoperability can take various forms, from data portability to the imposition of standardized interfaces that allow consumers to interact across services. Huang et al. (2024) analyze various configurations of network interoperability between platforms and identify the

[3] To the best of our knowledge, only two other papers, Liao and Chen (2014) and Jianqiang et al. (2015), develop similar frameworks. Arce (2022) considers another aspect of security investments, namely how they increase the level of consumer lock-in.

[4] Lam and Seifert (2023) offer a different perspective and highlight the need to consider the interdependence between cybersecurity and data privacy decisions.

[5] The report by Bourreau et al. (2022) extensively discusses the pros and the cons of interoperability in digital markets.

conditions under which increasing interoperability enhances consumer welfare. However, a few recent papers uncover alternative mechanisms through which interoperability may be welfare-reducing. Bourreau et al. (2023) find that interoperability may reduce consumers' incentives to multi-home and use multiple competing services. In addition, a reduction in consumers' multihoming may limit the market share a potential entrant can capture (Bourreau and Krämer, 2022) or may prove detrimental when consumers have heterogeneous concerns for privacy (Dhakar and Yan, 2024). Kretschmer et al. (2025) also examine privacy concerns in a market with direct network effects, focusing on competition between a data-driven incumbent and a privacy-preserving entrant. Their findings show that mandating interoperability can prompt the incumbent to increase data collection, resulting in privacy spillovers that undermine both the entrant's business model and overall user welfare. Our contribution to this literature is to highlight a different potential unintended consequence of interoperability: its implications for cybersecurity.

The remainder of the paper is structured as follows. Section 2 introduces the baseline model and derives the main results. Section 3 compares private and social incentives for interoperability. Section 4 explores four extensions of the baseline model. Section 5 concludes. All mathematical proofs are provided in the appendix.

2 The model

Two platforms—we will sometimes refer to them as providers or firms—are located at the end points of a Hotelling-like unitary segment. The platforms sell their services to a mass one of users, also defined as consumers. The greater the mass of consumers patronizing a platform, the more attractive it becomes for hackers seeking to compromise users' data. This creates a congestion-like effect, diminishing the utility users derive from more popular platforms. We assume that platforms, consumers, and hackers are risk-neutral and we study a model with the following timing:

- t_1: given the degree of interoperability, denoted by $g \in [0,1]$, platforms i and j simultaneously invest in cybersecurity; for simplicity, firms are assumed to invest to choose their degree of security, $\alpha_i \in [0,1]$ and $\alpha_j \in [0,1]$, respectively;
- t_2: the two platforms simultaneously choose the prices of the service offered to users, p_i and p_j;
- t_3: users choose which provider to patronize;
- t_4: hackers decide whether to launch an attack;
- t_5: payoffs materialize.

We solve the model by backward induction and we look for the symmetric equilibrium with full market coverage.

2.1 Stage t_4: hackers' behaviour

There are two groups of hackers, denoted by i and j, each one of mass 1. Type-i hackers are specialized in malicious activities (i.e. data breaches) targeting platform i and aimed at exploiting data stored by users on the platform.

Hackers are assumed to observe the degree of interoperability between the two platforms, the size of their user networks, and their level of security; they then decide how to conduct their hacking

activities. Formally, we assume that hackers operate with the aim of maximizing the probability of successfully breaching the targeted platform; hence, indicating with q_i the probability of a successful attack from type-i hackers, their maximization problem is as follows:

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

where the first term is the hackers' expected revenues, and the second term is the cost of hacking.[6] Expected revenues increase with the amount of data and/or information that can be compromised, i.e. with the proportion of users that can be reached by the attack; in turn, this is given by the mass m_i of users joining platform i and, via the degree of platforms' interoperability g, by the mass of users on the other platform, m_j. The cost of hacking is positively affected both by q_i and α_i: for a given level of security α_i, such cost is higher the larger the probability of breach, and, for a given probability q_i, it is higher the more secure the platform. Our modeling of the hackers' payoff function reflects the idea that interoperability, requiring platforms to operate on a (partially) connected computer network, creates a backdoor for indirect cyberattacks: once firm i is breached, malicious activities can propagate to firm j, bypassing its security protections; in turn, the likelihood of this propagation increases with the degree of interoperability between the two platforms.

The first order condition yields the optimal probability of a breach from type-i hackers:

$$q_i^*(\alpha_i; g) = (1-\alpha_i)(m_i + g\, m_j).$$

This expression underscores the first key implication of interoperability in our model: it intensifies hacker aggressiveness. Formally, this is captured by $dq_i^*/dg > 0$. As a matter of fact, a greater degree of interoperability enlarges the mass of consumers that can be compromised and this induces hackers to exert greater efforts in their malicious activities.

Note that $q_i^*(\alpha_i; g)$ is the probability of platform i being breached by a direct attack, that is attacks to platform i from type-i hackers. The overall probability of platform i suffering a successful attack must also account for indirect attacks, namely attacks launched by type-j hackers who, due to interoperability, are capable of compromising platform i too. In symbols, the overall probability of platform i being breached is $prob_i(\alpha_i, \alpha_j; g) = q_i^*(\alpha_i; g) + g q_j^*(\alpha_j; g)$, that is:[7]

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

Expression (1) highlights the second key consequence of interoperability in our model: it turns cybersecurity investment into a public good. Expression (1) shows that platform i benefits from platform j investment: the higher α_j, the lower the probability of platform i suffering an indirect attack and, overall, the lower the probability of being breached. The public good effect strengthens as interoperability between the two platforms increases.[8]

[6] The assumption that hackers are fully informed about firms' security levels is made for the sake of simplicity; however, it is realistic to assume that hackers, as informed agents, have a correct perception of how secure a network infrastructure is and/or its vulnerabilities.

[7] All through the paper, we assume that the values of parameters are such that the equilibrium probabilities of breaching platforms are between 0 and 1. We later provide simulations showing that the set of such values is non-empty.

[8] Note we exclude the (sensible) possibility that an increase in security by firm i causes some type-i hackers to divert their (direct) attacks toward firm j. As pointed out by De Cornière and Taylor (2024), this effect is indeed likely negligible because hackers are not constrained to target a firm within the specific product market under consideration. As a result, type-i hackers can divert attacks to any other target in different markets.

2.2 Stage t_3: consumers' choices

Consumers of mass 1 are uniformly distributed over the Hotelling-like unitary segment $[0,1]$; they choose to purchase the service from either platform i, located at 0, or platform j, located at 1. The utility of a consumer located at x when buying the service from platform i is:

$$U_i(x) = v - \delta\, prob_i(\alpha_i, \alpha_j; g) + \theta\,(m_i + g\, m_j) - t\, d(x,i) - p_i. \tag{2}$$

Parameter $v > 0$ denotes the baseline utility enjoyed by consumers when joining platform i and is assumed to be large enough to ensure full market coverage; $\delta \geq 0$ is the loss suffered by the consumer in case of a security breach; $t\, d(x,i)$ is the transportation cost incurred by the consumer located in x when patronizing platform i and p_i is the price. Finally, the term $\theta\,(m_i + g\, m_j)$, with $\theta \geq 0$, indicates the benefit enjoyed by users when the size of platform i's network is $m_i + g\, m_j$; this is the classic network or feedback effect à la Katz and Shapiro (1985a) and suggests that interoperability may positively influence users' utility. As a matter of fact, in many digital services and products (i.e. software, text messaging services, etc.), interoperability allows users of one network to "communicate" with those of other interoperable/compatible networks, thus generating a positive effect on users.

In our setting, the two providers offer services that are both horizontally and vertically differentiated. Abstracting from network effects, the degree of vertical differentiation between platforms i and j is related to the difference in their levels of cybersecurity and is defined as follows: $\Delta_i(\cdot) = \delta\,(prob_j(\cdot) - prob_i(\cdot))$. Using (1), this expression can be rewritten as:

$$\Delta_i(\alpha_i, \alpha_j; g) \quad = \delta(1-g)\left[(1-\alpha_j)(m_j + g\, m_i) - (1-\alpha_i)(m_i + g\, m_j)\right].$$

For later reference, it is useful to look at how platform i's investment affects this quality differential and how this effect is mediated by the degree of interoperability. Differentiating $\Delta_i(\cdot)$ with respect to α_i it follows that:

$$\frac{\partial \Delta_i(\alpha_i, \alpha_j; g)}{\partial \alpha_i} = \delta \underbrace{(1-g)}_{(i)} \underbrace{(m_i + g m_j)}_{(ii)} > 0. \tag{3}$$

This expression is positive – α_i increases the quality differential $\Delta_i(\cdot)$ – and, interestingly, it is affected by the degree of interoperability in two opposite ways. On the one hand, term (i) suggests that a higher g reduces the impact of α_i on $\Delta_i(\cdot)$. This is related to the public good nature of the investment in security: the higher g, the more platform j benefits from i's investment; therefore, α_i has a weaker effect on the quality differential. Other things equal, this public good effect lowers a platform's incentives to invest in protection. On the other hand, interoperability enhances the impact of α_i on the quality differential, as implied by term (ii) in expression (3). As discussed above, a larger g makes hackers more aggressive, raising the likelihood that platform i will suffer a direct attack; since direct attacks are more effective than indirect ones as long as $g < 1$, the quality differential becomes more sensitive to α_i. Other things equal, this second effect of interoperability strengthens platforms' incentives to invest in security.

Consumers observe platforms' prices and security levels and choose which one to patronize. Condition $U_i(x) = U_j(x)$ yields the location of the indifferent consumer; letting $m_j = 1 - m_i$, the demand function faced by firm i, given any α_i and α_j and any p_i and p_j, is:

$$m_i(p_i, p_j, \alpha_i, \alpha_j; g) = \frac{p_j - p_i + (1-g)\left[(1-\alpha_j - (1-\alpha_i)g)\ \delta - \theta\right] + t}{2t - 2(1-g)\theta + (1-g)^2\,(2-\alpha_i-\alpha_j)\ \delta}. \tag{4}$$

Notice that with full interoperability – i.e. $g = 1$ – firm i's demand boils down to $(p_j - p_i + t)/2t$, i.e., the demand function in a standard Hotelling model. This is because the probability of suffering a successful attack and the benefits from network effects are the same across the two platforms when $g = 1$. In other words, the two providers are no longer vertically differentiated in terms of security and the purchasing decisions of consumers do not depend on each provider's level of protection.

2.3 Stage t_2: firms' pricing decisions

Platform i offers its services to consumers at a price p_i. For simplicity, we let the cost of providing the service be 0. However, we assume that the platform incurs a damage cost ℓ in the event of a successful attack; ℓ could represent the expenses required to repair the IT infrastructure, the reputation losses following a security breach, or the legal liabilities.[9] In the remainder of the paper, we refer to ℓ simply as the damage cost for the platforms. Platform i's profit function is:

$$\pi_i(\alpha_i, p_i) = p_i\, m_i(p_i, p_j, \alpha_i, \alpha_j; g) - \ell\, prob_i(\alpha_i, \alpha_j; g) - c\,\frac{\alpha_i^2}{2}, \tag{5}$$

where the first term denotes revenues, the second is the expected cost of damage, and the third one is the convex cost of investing in cybersecurity.

In stage t_2, platforms simultaneously choose the price to maximize profits; from the platforms' first order condition, we get the reaction functions:[10]

$$p_i(p_j) = \delta\,\frac{[1-\alpha_j-(1-\alpha_i)\,g]\,(1-g)}{2} + \ell\,\frac{(1-g)\,[(1-\alpha_i)-g\,(1-\alpha_j)]}{2} + \frac{t}{2} - \frac{(1-g)\theta}{2} + \frac{p_j}{2},$$

and

$$p_i(p_j) = \frac{1-g}{2}\big((\delta-\ell g)(1-\alpha_j) + (\ell-\delta g)(1-\alpha_i) - \theta\big) + \frac{t}{2} + \frac{p_j}{2}.$$

The analysis of firm j's reaction function allows us to highlight the strategic effect that the investment in security has on pricing. Differentiating it with respect to α_i yields

$$\frac{\partial p_j(p_i)}{\partial \alpha_i} = -\,\delta\frac{1-g}{2} + \ell\,\frac{(1-g)g}{2}. \tag{6}$$

The strategic effect is related to the (negative) first term of this expression: the higher α_i, the more aggressively firm j behaves at the pricing stage. Indeed, a larger α_i comparatively increases the quality of firm i's service and this induces firm j to reduce its price. As suggested by the theoretical literature on congestion, in order to lessen the intensity of price competition, the strategic effect reduces the incentives to invest (Matsumura and Matsushima, 2007; and De Cornière and Taylor, 2024).

[9] Two aspects related to how we model platforms' damages deserve further discussion. First, for the sake of simplicity, we assume that damages take the form of a fixed cost rather than being proportional to the number of users. Nonetheless, in expected terms, total damages still increase with the user base because a larger number of users raises the probability of a successful breach. It is also worth noting that, for low degrees of interoperability, our results on the optimal investment level (Proposition 1 and Corollary 2) are qualitatively consistent with those in De Cornière and Taylor (2024), who study non-interoperable platforms facing user-proportional damages. This correspondence supports our claim that modeling damages as fixed costs involves no significant loss of generality. Second, we assume that platforms incur the same level of damages regardless of whether the attack is direct or indirect. This assumption is natural when ℓ represents the cost of repairing the IT infrastructure. In other cases—where ℓ reflects reputation or liability costs—the assumption is justified on practical grounds, as platforms may find it difficult to prove that an attack was indirect and thus avoid or limit responsibility. Our framework could nonetheless accommodate heterogeneous damage levels across attack types. In such a case, investment in security would remain increasing in both types of damages, albeit less responsive to those arising from indirect attacks.

[10] The second-order condition is $-2/[(1-g)^2\,(2-\alpha_i-\alpha_j)\,\delta + 2(t-\theta\,(1-g))] < 0$ which is clearly satisfied for $\theta < t$.

Interestingly, interoperability has an impact on this effect. A larger g makes the term $-\delta(1-g)/2$ less negative, i.e., it mitigates the strategic effect: greater interoperability makes platforms more similar in terms of security, therefore reducing the relevance of the investment in protection and the competitor's need to lower its price. Through its impact on the strategic effect, g increases the incentives to invest in security (or, more precisely, it reduces the platforms' incentives to lower the investment in order to mitigate price competition).

Solving the system of reaction functions, we can derive the second stage equilibrium prices for any given levels of protection:

$$p_i^*(\alpha_i, \alpha_j; g) = t - (1-g)\,\theta + \delta\,\frac{(1-g)\,[(2\alpha_i + \alpha_j - 3)\,g - \alpha_i - 2\alpha_j + 3]}{3} \\ -\ell\,\frac{(1-g)\,[(1-g)\,(\alpha_i + \alpha_j - 3) + \alpha_i - g\alpha_j]}{3}. \tag{7}$$

2.4 Stage t_1: firms' investment

We are now ready to compute the equilibrium levels of investment. Plugging the second stage equilibrium prices into $\pi_i(\alpha_i, p_i)$, we derive the profit function at the investment stage. Differentiating it with respect to α_i and solving for the symmetric equilibrium, we obtain the optimal security level chosen by the two platforms.

Proposition 1. *Given a certain degree of interoperability, the platforms' equilibrium level of investment in cybersecurity is:*

$$\alpha^*(g) = -\frac{\delta}{12c}(1-g) + \frac{5\,\delta}{12c}g(1-g) + \frac{\ell(1+3g-g^2)}{3c}. \tag{8}$$

Expression (8) highlights the three terms that make up the optimal investment. The first two terms are demand-related, as they are proportional to δ, the damage suffered by consumers in the event of a breach. The last term is cost-related and proportional to the damages incurred by platforms, ℓ. To better grasp the intuition behind this expression, let us first consider the case of no interoperability, i.e. $g = 0$.

Remark 1. *Without interoperability, platforms' equilibrium level of investment in cybersecurity is:*

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

Absent interoperability, our setting reduces to a standard oligopoly with congestion where platforms trade-off the incentive to lower the investment to strategically reduce the intensity of price competition – the first term of $\alpha^*(0)$ –, with the need of increasing α_i to lower expected damages – the second term of $\alpha^*(0)$ – (see Matsumura and Matsushima, 2007; and De Cornière and Taylor, 2024). Interoperability alters this trade-off in various ways. First, as we know from (6), interoperability reduces the impact of α_i on the rival's price, thus lowering the magnitude of the strategic effect of the investment. The first term of expression (8) incorporates this effect: as the ability to reduce the intensity of competition lowers with g, interoperability increases the incentives to invest. Consider now the second term in (8). Its interpretation relies on how interoperability impacts the effect of α_i on the quality differential $\Delta_i(\cdot)$. On the one hand, interoperability increases firms' incentives to invest to enhance the quality differential $\Delta_i(\cdot)$. On the other hand, the larger g the more the rival benefits from the investment; this public good effect reduces firms' incentives to invest. Notice that the second term of expression (8) is increasing in g for $g < 1/2$ and decreasing otherwise: when g is large, the public good effect is severe

and a further increase in interoperability reduces the incentives to invest. Finally, interoperability enlarges the expected damages suffered by platforms because hackers become more aggressive and, also, indirect attacks are more salient. The last term of expression (8) incorporates these effects; this term is increasing in g, implying that interoperability provides greater incentives to invest in cybersecurity.

The next corollary characterizes the impact of interoperability on the level of investment in equilibrium.

Corollary 1. *When $\ell > \delta$, the equilibrium investment level $\alpha^*(g)$ monotnically increases with $g \in [0,1]$; when $\ell < \delta$, it increases with g iff $g < \frac{3(\delta+2\ell)}{5\delta+4\ell} (< 1)$.*

When firms' potential losses in the event of a breach are significant — i.e. when the value of the loss, ℓ, exceeds the value of the penalty, δ — the cost-related determinant of investment dominates. A higher degree of interoperability provides greater incentives to invest in order to reduce expected losses. By contrast, when $\delta < \ell$, the demand-related determinants become comparatively more important, implying a non-monotonic effect of interoperability on the incentives to invest in security. In particular, when the degree of interoperability is already high, investment decreases with g due to the greater salience of the public good nature of firms' investment.

The following corollary provides further comparative statistics useful to understand the properties of firms' optimal investment.[11]

Corollary 2. *The equilibrium investment in security: i) increases with the damage cost ℓ, ii) reduces with the investment cost parameter c, and iii) increases with δ, the loss incurred by consumers in the event of a breach, when $g > 1/5$ and decreases otherwise.*

Points i) and ii) are intuitive. Platforms are induced to invest more the larger ℓ, the cost for the damage incurred in the event of a security breach; instead, they invest less the higher the cost c of enhancing protection against cyberattacks. Point iii) is related to the demand-driven determinants of the investment. A larger δ intensifies the impact of α_i on the quality differential $\Delta_i(\cdot)$, thus providing greater incentives to invest. However, a larger δ also strengthens the incentives to reduce the investment in order to soften price competition. This latter effect is strong when g is small, explaining why the investment decreases with δ for low levels of interoperability.[12]

Finally, substituting the equilibrium investment $\alpha^*(g)$ into the second stage prices $p_i^*(\alpha_i, \alpha_j)$ shown in (7) and rearranging gives the symmetric equilibrium price:

$$p^*(g) = t - (1-g)\theta + (\delta + \ell)(1-g)^2(1-\alpha^*(g)). \tag{9}$$

A simple inspection of expression (9) leads to the following remark:

[11] The equilibrium level of investment depends neither on t nor on θ. This finding aligns with De Cornière and Taylor (2024) and stems from two offsetting effects. On one hand, one can show that a higher t reduces the sensitivity of firm i's demand to α_i, thereby weakening its incentive to invest. On the other hand, greater transportation costs raise the equilibrium price p^*, making each consumer more valuable and thus strengthening the incentive to invest. In our framework, these opposite forces cancel each other out. A similar logic applies to the parameter θ.

[12] Our comparative statics are qualitatively consistent with those in De Cornière and Taylor (2024), where platforms are assumed to be non-interoperable (i.e., $g = 0$). The only exception concerns the effect of δ. While De Cornière and Taylor (2024) show that security investment decreases with δ, we generalize this result and demonstrate that such a negative relationship holds only for low levels of interoperability. By contrast, when $g > 1/5$, investment increases with consumers' damages. This divergence arises from differences in the price elasticity of demand: in De Cornière and Taylor (2024), elasticity is independent of α_i, whereas under interoperability it decreases with security investment, thereby strengthening firms' incentives to enhance protection. Formally, the price elasticity of demand is

$$\eta_i = \frac{p_i}{\delta\left[(1-\alpha_j)(1-g) - (1-\alpha_i)g(1-g)\right] + t - p_i + p_j},$$

which reduces with α_i only when $g > 0$.

Remark 2. *The equilibrium price is lower the stronger the network externalities (i.e. the larger θ); the negative effect of θ on $p^*(g)$ reduces with g.*

As the intensity of network effects, θ, gets stronger, firms have greater incentives to lower prices in order to attract users and generate greater externalities. Remark 2 shows that these incentives are reduced by g, as interoperability allows users to interact also across platforms, thus mitigating the need to enlarge the installed base of users. As we well see below, this implies that, other things equal, interoperability is beneficial to firms as it reduces the incentives to price aggressively.

2.5 Socially optimal investment

Once the privately optimal level of investment in security has been determined, it is useful to move on to a social welfare analysis by calculating the socially optimal investment. Social welfare is defined as the sum of consumer surplus and producer surplus; formally:

$$W(\alpha_i, \alpha_j; g) = \int_0^{m_i} (v - tx - \delta\, prob_i + \theta\,(m_i + g\, m_j))\, dx + \int_{m_i}^1 (v - t(1-x) - \delta\, prob_j + \theta\,(m_j + g\, m_i))\, dx - \ell(prob_i + prob_j) - \frac{c(\alpha_i^2 + \alpha_j^2)}{2}, \tag{10}$$

where, omitting the arguments for simplicity, m_i, $prob_i$ and $prob_j$ denote the second stage equilibrium values. The first two terms are the gross surplus of users patronizing platform i and j, respectively, while the latter two represent the expected damage cost and the security investment costs, respectively, incurred by firms. Note that prices factor out as they are transferred from users to the firms. From the maximization of $W(\alpha_i, \alpha_j; g)$, the following proposition holds.

Proposition 2. *The socially optimal investment in security is*

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

The comparative statics for $\alpha^w(g)$ is intuitive. First, the socially optimal investment increases with the costs incurred both by users, δ, and firms, 2ℓ, following a breach. Second, $\alpha^w(g)$ gets larger with g as a higher degree of interoperability makes hackers more aggressive therefore calling for more protection against cyberattacks. Finally, the security investment cost c has a negative impact on $\alpha^w(g)$.

The next corollary compares the socially efficient investment with the equilibrium one.

Corollary 3. *The socially optimal investment is larger than the equilibrium one, $\alpha^w(g) > \alpha^*(g)$.*

Two key factors drive the underinvestment in security. First, firms fail to internalize the positive externality that their own investment exerts on the competitor's breach probability – reflecting the public good nature of cybersecurity. Second, firms strategically reduce their investment levels to soften price competition.

3 Private and social incentives toward interoperability

In the analysis presented so far, we have derived the equilibrium conditions for any level of interoperability, $g \in [0, 1]$. We now turn to assessing the desirability of interoperability from both private

and social perspectives. Specifically, when evaluating firms' private incentives to adopt interoperability, we compare industry profits in a scenario without interoperability ($g = 0$) to those in a scenario with a given, exogenously determined, degree of interoperability ($g > 0$). This approach has a clear practical rationale: in most digital ecosystems, the degree of interoperability is largely dictated by the characteristics of the underlying technology or by pre-existing technical standards. Service providers – whether offering messaging, cloud computing, or payment services – typically face a binary strategic choice: whether to adopt interoperability at the prevailing technological standard, rather than selecting its intensity. For instance, the interoperability achievable across messaging platforms (e.g., through the RCS or Signal protocols[13] or among cloud providers (via APIs or container standards such as Kubernetes or OpenStack[14]) is determined exogenously by the protocol's design. Firms can therefore decide whether to interconnect within a given framework, but they cannot continuously adjust the degree of interoperability. Our modeling strategy reflects this technological constraint, focusing on firms' adoption incentives rather than on the endogenous determination of interoperability intensity.It is also worth noting that this framework can be viewed as an extension of our baseline setting, in which firms, prior to the investment stage, cooperatively decide whether to become interoperable at the exogenously specified level $g > 0$.

Similarly, when assessing the social incentives toward interoperability, we evaluate the change in welfare when moving from $g = 0$ to a given $g > 0$, knowing that the symmetric equilibrium described in Section 2 follows. The comparison between private and social incentives will allow us to assess possible market failures and to determine the desirability of a regulatory intervention.

Based on expression (5), industry profits in a symmetric equilibrium can be written as a function of the degree of interoperability g:

$$p^*(g) - 2\,\ell\, prob^*(g) - c\,\alpha^*(g)^2,$$

where $\alpha^*(g)$ and $p^*(g)$ are given in (8) and (9), respectively, and using (1), $prob^*(g) = (1-\alpha^*(g))(1+g)^2/2$.

Omitting the equilibrium asterisk * for simplicity, we can use the above expression to indicate the difference in industry profits with and without interoperability: $\Delta\Pi = \Pi(g) - \Pi(0)$. A degree $g > 0$ of interoperability is preferred from the industrial perspective to the absence of interoperability when

$$\Delta\Pi = \underbrace{p(g) - p(0)}_{\substack{\Delta \text{ Industrial} \\ \text{revenues}}} - \underbrace{2\ell[prob(g) - prob(0)]}_{\substack{\Delta \text{ Expected} \\ \text{cost of breach}}} - \underbrace{c[\alpha(g)^2 - \alpha(0)^2]}_{\substack{\Delta \text{ Investment} \\ \text{costs}}} > 0, \tag{11}$$

that is, when the variation in total revenues is greater than the overall variation in total costs (expected damages plus investment expenses).

In turn, social welfare in any symmetric equilibrium is:

$$v - \frac{t}{4} + \frac{\theta}{2}(1+g) - \delta\, prob(g) - 2\,\ell\, prob(g) - c\,\alpha(g)^2;$$

[13] In text messaging, interoperability is governed by communication protocols such as the Rich Communication Services (RCS) standard and the Signal Protocol which define how end-to-end messages are formatted, encrypted, and transmitted: see GSMA (2020); and Marlinspike and Perrin (2016)).

[14] Application Programming Interfaces (APIs) and container standards such as Kubernetes or OpenStack define common technical specifications that enable software components and cloud services to communicate and operate seamlessly across different infrastructures: see Bernstein (2014).

hence, a given degree of interoperability $g > 0$ is socially preferable to no interoperability if:

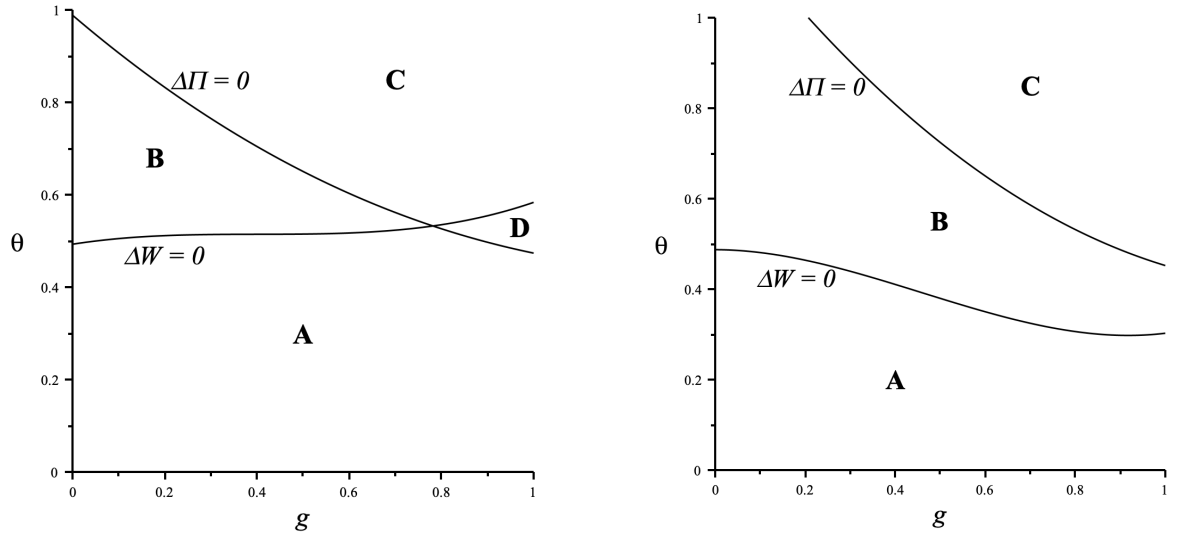
$$\Delta W = \underbrace{\frac{\theta g}{2}}_{\substack{\text{Greater net-}\\ \text{work effects}}} - \underbrace{(\delta + 2\ell)[prob(g) - prob(0)]}_{\substack{\Delta \text{ Expected social}\\ \text{damages of breach}}} - \underbrace{c[\alpha(g)^2 - \alpha(0)^2]}_{\Delta \text{ Investment cost}} > 0. \tag{12}$$

In the Appendix, we derive the analytical conditions under which $\Delta\Pi > 0$ and $\Delta W > 0$. Specifically, we determine the thresholds for the intensity of network effects above which interoperability is privately and socially desirable. Intuitively, a large θ makes interoperability welfare enhancing as it amplifies the magnitude of the impact of the network externalities it generates; this effect is highlighted in the first term of expression (12) above. The reason why also private benefits from interoperability increase with θ lies in what is highlighted in Remark 2: interoperability reduces the incentives to price aggressively in order to enlarge the installed base of users, and this benefit is greatest when both g and θ are large. In the Appendix, we also identify the conditions under which social and private incentives for interoperability diverge. The explanation for this misalignment becomes evident when examining expressions (11) and (12). On the one hand, only social welfare accounts for the damages δ users suffer in the case of breach; therefore, ΔW is more sensitive than $\Delta\Pi$ to changes in the probability of breach, $prob(g) - prob(0)$. On the other hand, $\Delta\Pi$ is affected by changes in prices which are instead neutral when welfare is considered.

In order to illustrate more effectively the analysis presented in the Appendix, we complement the analytical results with numerical simulations. Figure 1 plots the thresholds that determine the social and private desirability of interoperability that we derive in the Appendix. We indicate with $\Delta\Pi = 0$ and $\Delta W = 0$ these thresholds and we refer to them as the *isoprofit* and *isowelfare* frontiers, respectively. In the region above the isoprofit (resp. isowelfare) frontier interoperability is privately (resp. socially) beneficial, that is $\Delta\Pi > 0$ (resp. $\Delta W > 0$); the opposite occurs in the region below the frontier. Figure 1 is generated using the following parameter values: $v = 2$, $c = 0.25$, $t = 1$, and $\delta = 0.18$. In addition, we consider two different scenarios: panel (a) is drawn for a relatively low value of ℓ, $\ell = 0.13 < \delta$, while panel (b) for a relatively high value, $\ell = 0.2 > \delta$.[15] Indeed, as established in Corollary 1, $\alpha(g)$ varies non-monotonically with g in the former case, whereas it monotonically increases with g in the latter. In other words, when ℓ is relatively low, firms have less incentives to protect themselves, while they are encouraged to invest more when ℓ is relatively high.

Consider panel (b) first. The isoprofit and isowelfare frontiers segment the space (g, θ) into three distinct areas. In area C, characterized by large values of both g and θ, it turns out that interoperability is desirable both from the social as well as from the firms' point of view. By contrast, in area A, network effects are rather weak and interoperability is desirable neither socially nor privately. Both in C and in A, private and social incentives are aligned and the reason for this is mainly related to the role of θ discussed above. In area B, the values of g and θ are such that interoperability is socially beneficial but privately undesirable, $\Delta W > 0$ and $\Delta\Pi < 0$. This misalignment arises under two distinct sets of conditions: (i) relatively high θ and low g (western portion of area B), and (ii) lower θ and larger g (eastern portion). Although both situations lead to the same qualitative outcome, the underlying mechanisms differ. In case (i), interoperability yields substantial network benefits for users, thereby enhancing welfare and making $\Delta W > 0$. However, since g is low, firms are unable to capture these benefits through higher prices, leading to $\Delta\Pi < 0$. In case (ii), welfare is again higher

[15] We use these parameter values in all the simulations that we present in the paper. Different values can be used, but the qualitative results will not change. Notice that in all the simulations, we control that the conditions for the existence of an interior solution of the model are satisfied: investments and probabilities of breach are between 0 and 1, firms' profits and consumers' utility are positive, second order conditions for profit maximization are satisfied.



(*a*) $\ell = 0.13$ (*b*) $\ell = 0.2$

Figure 1: $\Delta\Pi$ and ΔW

under interoperability because, the probability of a breach turns out to be substantially lower at larger values of g, which is socially valuable. Yet, with lower θ, the corresponding increase in prices is limited, so firms do not gain from interoperability, which results in $\Delta\Pi < 0$.

Consider now panel (a), which corresponds to the case where ℓ is smaller than δ. When firms' damages are limited, incentives to invest are weaker, the public good component of security investment becomes more pronounced, and – according to Corollary 1 – the condition $\ell < \delta$ implies that $\alpha(g)$ has an inverted-U shape. In this case, high interoperability increases the probability of breach; formally, $prob(g) > prob(0)$.

Interestingly, panel (a) shows that for intermediate values of θ, there can be two forms of misalignment: $\Delta W > 0 > \Delta\Pi$ in area B, as before, and $\Delta\Pi > 0 > \Delta W$ in area D. In area B, g is relatively low, and interoperability has only a moderate impact on both the probability of breach and the equilibrium price; hence, it is socially desirable but privately unprofitable. Conversely, when g is large, interoperability substantially increases the probability of breach while benefiting firms through higher equilibrium prices. In this case, interoperability becomes privately profitable but socially harmful. Finally, consistent with panel (b), when θ is either high or low, private and social incentives are aligned, making interoperability either desirable (area C) or undesirable (area A).

Our analysis has interesting implications regarding the desirability of regulatory policies mandating interoperability. When network effects are either strong or weak, the incentives of firms and society align, allowing interoperability (or the lack thereof) to emerge voluntarily without the need for policy interventions. By contrast, when network effects are of intermediate strength, private and social incentives for interoperability may diverge. In this case, mandating interoperability enhances welfare—provided that the public good component of security investment does not significantly distort firms' incentives to invest in protection. Overall, the impact of interoperability on social welfare depends on sector-specific characteristics, including the strength of network effects, the degree of interoperability that can be technically achieved, and how this affects firms' incentives to invest in cybersecurity.

4 Extensions

4.1 Sophisticated/unsophisticated consumers

Our previous analysis assumed that all consumers are fully capable of assessing the likelihood of hackers' attacks on platforms. It is now interesting to explore how our conclusions change when some users lack this level of sophistication. In this extension, we generalize the previous setting and we posit that only a fraction $\lambda \leq 1$ of consumers are aware of cyber risk. These "sophisticated" consumers factor this risk into their platform choices and behave as described in the prior sections; hence, when $\lambda = 1$ we are back to the baseline setting of Sections 2 and 3. The remaining $1 - \lambda$ share of consumers are "unsophisticated" as they disregard the risk of a cyber attack when acquiring the digital service; formally, for this type of users $prob_i(\cdot) = 0$ and the utility they receive when patronizing firm i is $U(x) = v - p_i - t\, d(x,i) + \theta(m_i + g\, m_j)$. This setting also allows to discuss the consequences of regulations requiring platforms to certify their level of security or of campaigns raising public awareness of cyber risks.

Solving for the indifferent sophisticated and unsophisticated customers, under the assumption that both types of users are uniformly distributed on the unitary segment, it is possible to derive the demand function faced by firm i:

$$m_{\lambda,i}(p_i, p_j, \alpha_i, \alpha_j; g) = \frac{(1-g)\,(1-(1-\alpha_i)\,g-\alpha_j)\,\delta\lambda - (1-g)\,\theta + p_j + t - p_i}{(1-g)^2\,(2-\alpha_i-\alpha_j)\,\delta\lambda + 2t - 2\,(1-g)\,\theta}, \tag{13}$$

where the subscript λ is a mnemonic for the setting with both sophisticated and unsophisticated customers. Using this expression, it is possible to obtain from firms' profit maximization the second stage equilibrium prices, given α_i and α_j:

$$p_{\lambda,i}(\alpha_i, \alpha_j) = t + \frac{(1-g)\,((g\,(2\alpha_i+\alpha_j-3) - \alpha_i - 2\alpha_j + 3)\,\delta\lambda + (g\,(\alpha_i + 2\alpha_j - 3) - 2\alpha_i - \alpha_j + 3)\,l - 3\theta)}{3}. \tag{14}$$

Plugging this expressions into the platforms' profit functions, we can derive the equilibrium investment in security. Plugging this expressions into the platforms' profit functions, we can derive the symmetric equilibrium investment in security.

Proposition 3. *In the presence of both sophisticated and unsophisticated consumers, the platforms' equilibrium level of investment in cybersecurity is:*

$$\alpha^*_\lambda(g) = \lambda\left[-\frac{\delta}{12c}(1-g) + \frac{5\delta}{12c}g(1-g)\right] + \frac{\ell(1+3g-g^2)}{3c}. \tag{15}$$

As λ enlarges, $\alpha^*_\lambda(g)$ increases if $g > 1/5$, and it decreases otherwise.

Expression (15) closely resembles (8) and corresponds to it when $\lambda = 1$. The demand-related component is now weighted by λ, the mass of sophisticated consumers. The comparative statics concerning λ mirrors the effect that δ – the damage suffered by users in the event of a breach – has on $\alpha^*(g)$, as highlighted in Corollary 2. This is because δ exclusively influences the decisions of sophisticated consumers. An increase in λ generates two opposing effects on the incentives to invest in cybersecurity. On one hand, firms are better off by reducing investment, as this mitigates the intensity of price competition. On the other hand, firms are induced to invest more to counteract hackers' threats. As observed in Corollary 2, the former effect dominates when $g < 1/5$ (i.e., when hackers are less aggressive), whereas the latter dominates for higher levels of interoperability; this applies to $\alpha^*_\lambda(g)$

too.[16]

The analysis with sophisticated and unsophisticated users lends itself to discuss interesting implications from a social welfare perspective. We characterize these implications by considering a "paternalistic" regulator, i.e. a social planner that takes possible damage from hackers' attacks into account, even against unsophisticated users, when regulating; in other words, we consider a social welfare function which incorporates the damages δ in the case of a breach also for unsophisticated users. Formally, the paternalistic welfare function corresponds to (10), that is, to the welfare function of the baseline model where all consumers are aware of cyber risks.

Proposition 4. *In the presence of both sophisticated and unsophisticated consumers:*

i) the investment in cybersecurity chosen by a "paternalistic" regulator is $\alpha^w(g)$, which is a) the same as in the baseline setting, and b) larger than $\alpha^*_\lambda(g)$;

ii) social welfare increases with the mass of sophisticated consumers if $g > 1/5$ and it decreases for lower degrees of interoperability.

Part *i*) of Proposition 4 shows that the presence of unsophisticated users does not affect the socially optimal level of investment, and that firms still underinvest in equilibrium. Part *ii*) instead proves that social welfare increases with the proportion of sophisticated consumers only when $g > 1/5$, a condition that implies that the equilibrium investment increases with λ (see Proposition 3). This result has an interesting policy implication, as it identifies the conditions under which public policies aimed at raising users' awareness of cyber risks are more (or less) likely to enhance welfare.

Turning to the analysis of the desirability of interoperability, we proceed as in Section 3. Figure 2 illustrates the social and private incentives for interoperability for the same parameter values employed previously. The figure plots the isowelfare and the isoprofit frontiers for two values of λ: $\lambda = 1$ (which corresponds to the baseline model) and $\lambda = 0.4$. Figure 2 show that, compared to the baseline, the presence of unsophisticated users decreases the social desirability of interoperability (the isowelfare frontier moves upwards) while increasing the private one (the isoprofit frontier moves downwards): this holds true both for relatively low (left panel) and relatively high (right panel) levels of ℓ.

The reduction in social benefits from making services interoperable stems from how firms adjust their optimal cybersecurity investments when transitioning from no interoperability to a positive level. While interoperability generally leads to increased investment in cybersecurity, the extent of this increase grows with λ.[17] This implies that the largest investment increase due to interoperability occurs in the baseline scenario ($\lambda = 1$). When the market includes unsophisticated users ($\lambda < 1$), firms invest less in cybersecurity, leading to a smaller reduction in breach probability compared to the no-interoperability case. As a result, interoperability becomes less socially desirable when unsophisticated users are present.

By contrast the greater private desirability of interoperability is related to the strategic role of cybersecurity investment in mitigating price competition. In the baseline case ($\lambda = 1$), interoperability

[16] In a setting where platforms are not interoperable, De Cornière and Taylor (2024) show that the equilibrium investment level reduces with λ. We generalize this result and prove that this occurs only at low degrees of interoperability; by contrast, when $g > 1/5$, platforms increase their protection as the mass of sophisticated consumers increases. The reason for this findings is related to how α_i impacts on the price-elasticity of demand, as discussed when commenting Corollary 2.

[17] Formally, using expression (15), it follows that

$$\alpha^*_\lambda(g) - \alpha^*_\lambda(0) = g\,\frac{\delta\lambda(6-5g) + 4\ell(3-g)}{12c},$$

which is increasing in λ. Intuitively, relative to the baseline case with $\lambda = 1$, $\alpha^*_\lambda(g)$ becomes less responsive to changes in g because the demand-related component of the investment incentive is proportional to the share of sophisticated users.

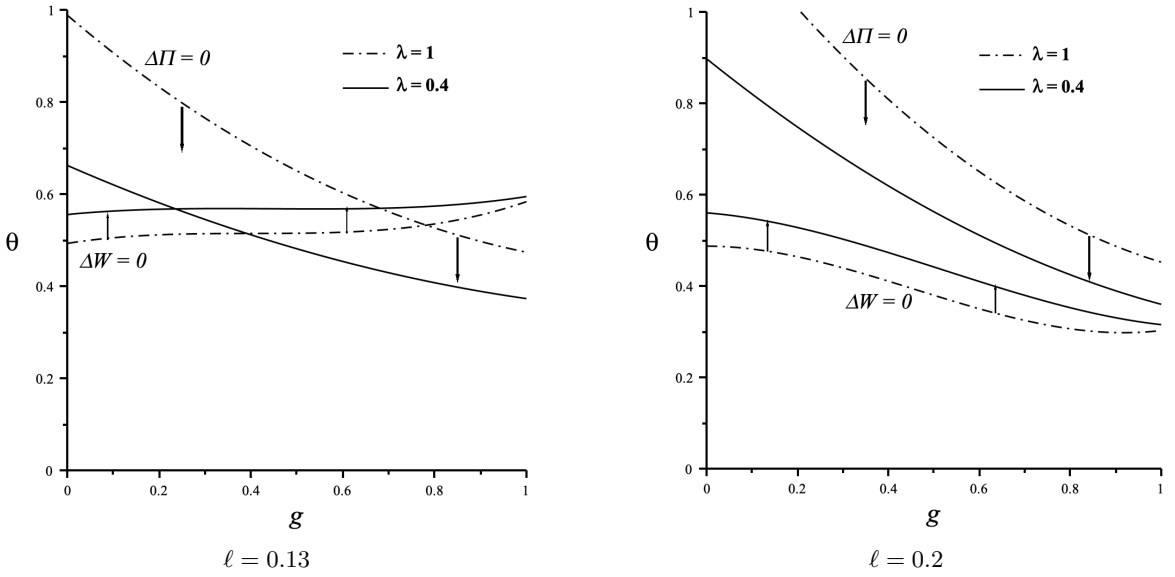


Figure 2: $\Delta\Pi$ and ΔW: baseline vs. unsophisticated users models

reduces the scope for strategic investment, thereby weakening firms' ability to use security as an anti-competitive instrument. When unsophisticated users are present, however, cybersecurity investment loses part of its strategic relevance.[18] As a result, interoperability becomes less harmful to firms, since the reduction in the strategic component of investment mitigates its competition-enhancing effect. Overall, in markets with a larger share of unsophisticated users, firms exhibit stronger private incentives to adopt interoperability.

4.2 Ad-funded platforms

In the analysis presented so far, we have considered firms that monetize through pricing. However, when it comes to the production and distribution of digital services, firms often adopt different business models based on alternative monetization strategies. One of the most prevalent business models in the digital economy is based on monetization through advertising, whereby firms offer their services for free and generate revenues by selling advertising space on their platforms. In this section, we adapt our baseline model to this "Ad-funded" scenario; our aim is to analyze how firms' cybersecurity investment strategies change in this context, as well as the impact on the desirability of interoperability.

Hackers' payoffs, are the same as in the baseline setting. Consumers, instead, do not pay a price for the service, hence the utility of the individual located in x when patronizing firm i is:[19]

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

where the probability of platform i being attacked is still given by expression (1). Similarly, the impact of α_i on the quality differential $\Delta_i(\cdot)$ is characterized by (3). The degree of interoperability gives rise

[18] Formally, differentiating firm j's price–reaction function with respect to α_i yields

$$\frac{\partial p_j(p_i)}{\partial \alpha_i} = -\,\delta\,\frac{1-g}{2}\lambda + \ell\,\frac{(1-g)g}{2},$$

where the first term is proportional to λ. In the baseline case, expression (6) applies with $\lambda = 1$.

[19] We assume, for simplicity, that advertising has no direct effect—either positive or negative—on consumers. Note, however, that our results would be unaffected if advertising entailed a small and symmetric disutility across users and platforms.

to the same trade-off discussed in the previous section: a higher g weakens the impact of α_i on $\Delta(\cdot)$ through a public good effect, yet at the same time it increases the responsiveness of $\Delta_i(\cdot)$ to investment, as greater interoperability makes hackers more aggressive.

The demand faced by platform i for given investment levels of α_i and α_j is:

$$m_i(\alpha_i, \alpha_j; g) = \frac{(1-g)\left[(1-\alpha_j-(1-\alpha_i)g)\ \delta - \theta\right] + t}{2t - 2(1-g)\theta + (1-g)^2\left(2-\alpha_i-\alpha_j\right)\ \delta}. \tag{16}$$

As for the profits, indicating with $A > 0$ the per-user revenue collected by each platform through advertising, platform i's profits are:

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

Solving the profit maximization problem with respect to α_i and focusing on the symmetric equilibrium yields the following result.

Proposition 5. *When firms adopt an Ad-funded business model, the equilibrium level of investment in cybersecurity is:*

$$\alpha^*_{Ad}(g) = \frac{1}{2} + \frac{\theta(g-1)+t}{2(1-g)^2\delta} + \frac{\ell(1+g)^2}{8c} - \frac{\sqrt{N(g)}}{8c\delta(1-g)^2}, \tag{17}$$

where

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

A close inspection of the above expression reveals that $\alpha^*_{Ad}(g)$ increases with the level of advertising revenues, A. By contrast, the socially optimal investment remains $\alpha^w(g)$, as defined in Proposition 2, and therefore unaffected by A. As a result, firms will underinvest in cybersecurity when A is sufficiently small, and overinvest when A is relatively large. This is consistent with De Cornière and Taylor (2024), which shows that overinvestment may occur in the Ad-funded setting, where raising security investment is the only means to attract users.

To conclude this section, we compare the social and private incentives to adopt interoperability. From a social perspective, incentives do not differ from the baseline model and are still captured by ΔW, with the equilibrium investment given by $\alpha^*_{Ad}(g)$. By contrast, in the Ad-funded case, industry profits in any symmetric equilibrium are:

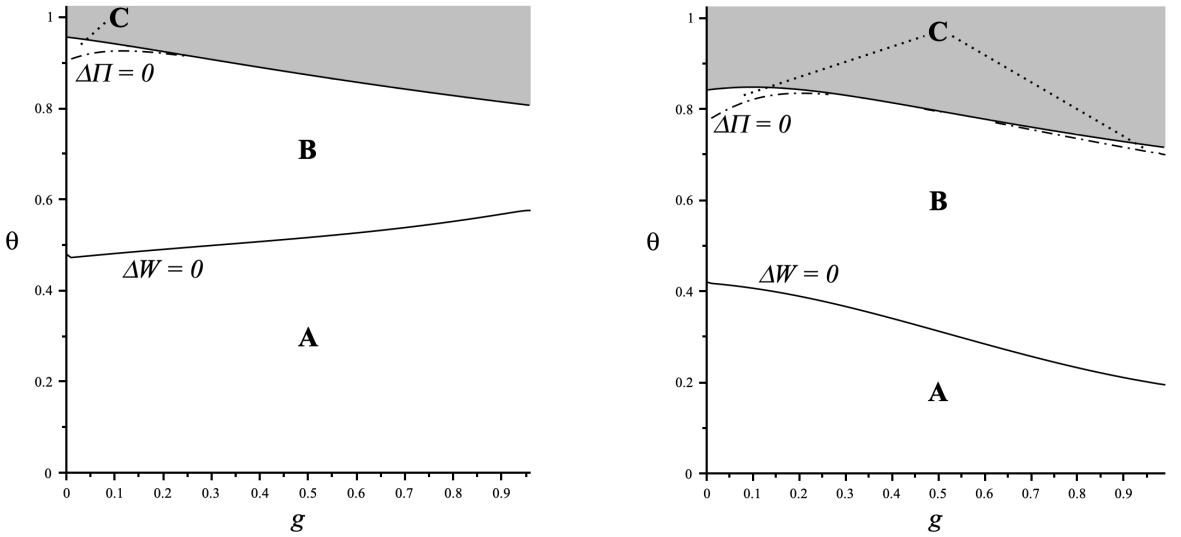
$$2A - 2\ell\, prob(g) - c\,\alpha(g)^2.$$

Accordingly, interoperability ($g > 0$) is privately preferred to no interoperability if

$$\Delta\Pi = -2\ell\left[prob(g) - prob(0)\right] - c\left[\alpha(g)^2 - \alpha(0)^2\right] > 0.$$

This condition indicates that when revenues derive from advertising, firms' incentives to adopt interoperability are generally weaker than in the baseline case. As discussed in Section 3, interoperability reduces the need to compete aggressively on prices to expand the user base. This competition-softening effect, which strengthens the private incentives to make services interoperable in the price-based setting, is absent when firms monetize through advertising. Consequently, relative to the baseline, the private return from interoperability is substantially lower.

The simulations summarized in Figure 3 confirm this intuition. The figure is based on the same parameter values used in the baseline case; in order to make the analysis comparable with Figure 1, the per-user advertising revenues are set equal to the equilibrium price from expression (7), that is, $A = p^*(g)$. Both when $\ell = 0.13$ and when $\ell = 0.2$, interoperability is privately desirable only for a very limited range of parameters (area C).[20] Overall, these findings indicate that, under advertising-based monetization, firms' private incentives to pursue interoperability are likely to be inefficiently low.



(a) $\ell = 0.13$ (b) $\ell = 0.2$

Figure 3: $\Delta\Pi$ and ΔW: Ad-funded model with $A = p^*(g)$

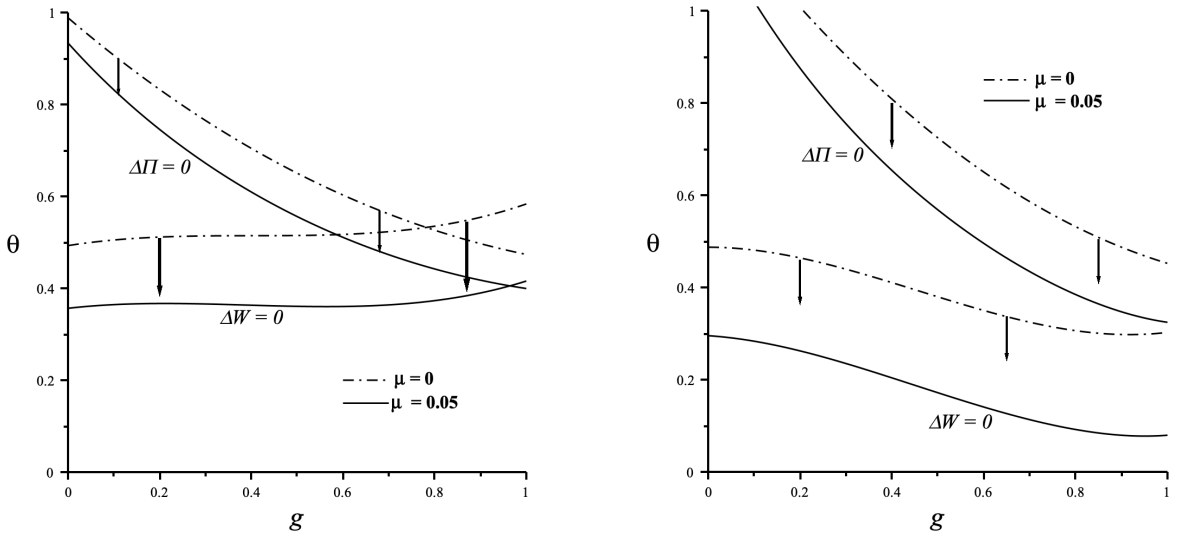
4.3 Market not fully covered

Thus far, we have characterized the equilibrium of the game under the assumption of full market coverage. In this scenario, the total demand is fixed, implying that our analysis overlooks a potential benefit of interoperability – namely, its ability to expand the pool of users who purchase the service. We now generalize the model by introducing two distinct user groups. The first group consists of non-captive consumers, identical in characteristics to those described in the previous sections: they are uniformly distributed over the interval $[0, 1]$ with density 1 and choose between the two platforms when purchasing the service. The second group of consumers consists of captive users who only consider purchasing from the focal platform and never switch to the rival one. We assume that each platform has a mass $\mu \geq 0$ of captive consumers, uniformly distributed over the interval $[0, \infty)$ according to their distance from their focal platform. Clearly, when $\mu = 0$ we are back to the baseline setting.

The model cannot be solved analytically and we need to resort to numerical simulations to determine the equilibrium levels of investments. As in the baseline setting, we look for the symmetric equilibrium. At the equilibrium, all non-captive users purchase the service, while only a fraction of captive users are served; hence, overall sales vary depending on the mass of captive users that purchase the service.[21] Formally, in order to determine the mass of users patronizing each platform, we need to identify three indifferent consumers. The non-captive consumer who is indifferent between the two platforms – i.e. for whom $U_i(x) = U_j(x)$ – and, for each platform, the captive consumer who is indifferent between

[20] The gray area in the figures indicates a parameter region in which the function $\Delta\Pi$ is not defined.

[21] Notice that if the market for non-captive users was not fully covered, then platforms would behave as local monopolies, with no interaction between them.



(a) $\ell = 0.13$ (b) $\ell = 0.2$

Figure 4: $\Delta\Pi$ and ΔW: baseline vs. not fully covered market models

purchasing or not – i.e. for whom $U_i(x) = 0$ and $U_j(x) = 0$, respectively. Denoting with x, y and z the location of the three indifferent consumers, the mass of users patronizing each platform is $m_i = x + \mu y$ and $m_j = (1 - x) + \mu z$, respectively.

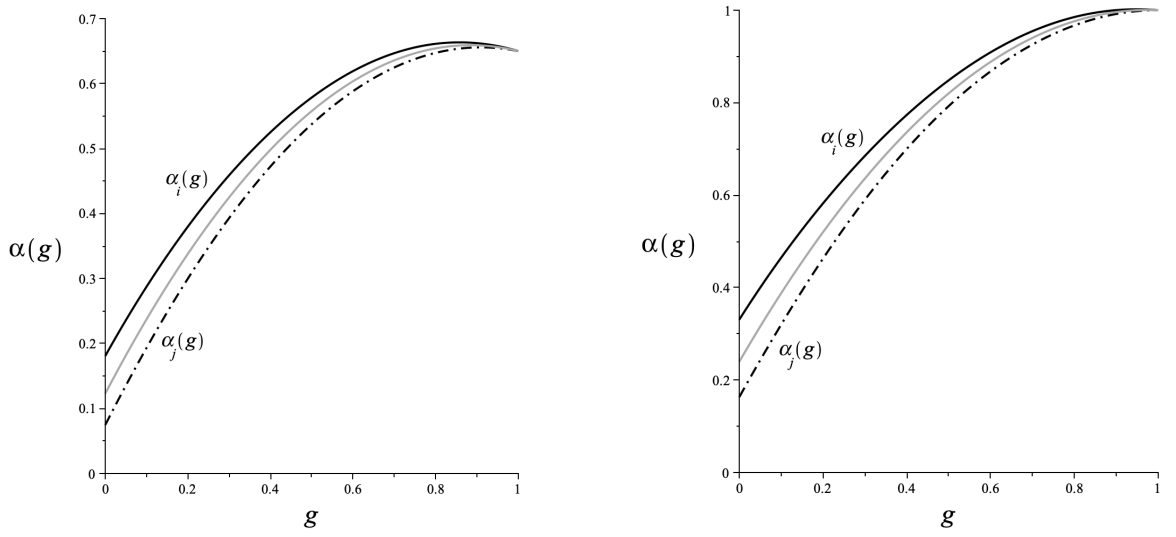
One can show that firms invest more in security than in the baseline model; this result is intuitive: the (additional) presence of captive consumers increases hackers' expected returns from attacks, making them more aggressive.[22] Most interestingly, Figure 4 shows our usual isoprofit and isowelfare frontiers for a mass of captive users $\mu = 0.05$ – the solid curves in the figures—and contrasts them with those obtained in the baseline scenario ($\mu = 0$) – the dashdotted curves in the figures. The simulations clearly show that the demand-expansion effect generated by the presence of captive consumers increases the desirability of interoperability. Graphically, irrespectively of the value of ℓ, both $\Delta W = 0$ and $\Delta\Pi = 0$ shift downwards with μ: recalling that $\Delta\Pi > 0$ when θ is relatively high for any given g, this means that the region where interoperability is both socially and privately desirable gets bigger. This result is unsurprising, as the benefits of interoperability are largely driven by network effects, which intensify with the size of the user base.

4.4 Private incentives for interoperability with an incumbent firm

In our baseline framework, the two platforms attract the same share of users at equilibrium. In digital markets, however, firms are often characterized by heterogeneity in the size of their installed user bases. This may result from market dynamics through which incumbent firms build a critical mass of users and subsequently leverage strong network effects to consolidate their market positions against new entrants.

In this context, it is well established in the literature (Katz and Shapiro, 1985b; Crémer et al., 2000) that firms of different sizes may have divergent incentives regarding the interoperability of their networks. Smaller firms often seek interoperability with larger incumbents to capitalize on the network effects arising from the latter's large installed user base. Conversely, larger firms, aiming to protect their dominant position, have weaker incentives to enable interoperability with new entrants.

[22] We leave the simulations concerning firms' investment levels with captive users available upon request from the authors.



(a) $\ell = 0.13$ (b) $\ell = 0.2$

Figure 5: Firms investments with asymmetric "attached" users ($\theta = 0.8$)

To account for this potential tension, we extend the baseline model and examine how different user bases affect firms' (private) incentives both for cybersecurity and for interoperability. We borrow from Crémer et al. (2000) and assume that platforms i and j have "attached" users of mass β_i and β_j, respectively. The two masses are exogenous—derived from previous sales that we do not model—and produce no revenue. We let $\beta_i > \beta_j$, meaning that platform i plays the role of the incumbent. The two platforms compete for a new cohort of users of mass 1: competition occurs under the same conditions as in our baseline model, except for the presence of the installed user bases β_i and β_j.

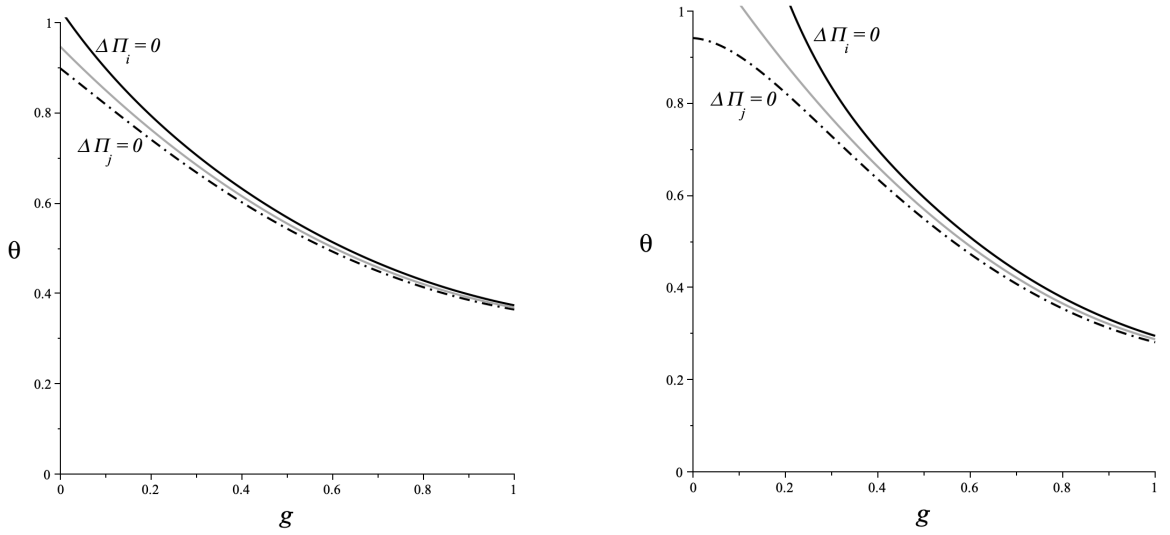
We solve this model under two scenarios: the asymmetric case where $\beta_i > \beta_j$ and the symmetric one where $\beta_i = \beta_j$. Our goal is to examine whether and how the larger platform i's incentives to invest in cybersecurity and to enable interoperability differ from those of the smaller platform j, and to analyze how the incentives of the two firms change relative to the symmetric user base case.

The masses of users patronizing the two platforms are $m_i = x + \beta_i$ and $m_j = 1 - x + \beta_j$ respectively, where x is the location of the indifferent consumer, determined by the usual condition $U_i(x) = U_j(x)$. As argued above, β_i and β_j generate no revenues for firms, but they influence the location of the indifferent consumer through network effects and the impact on hackers' malicious activities.

As in the previous sections, we need to resort to numerical simulations to solve the model. Figure 5 reports the investment levels of the two firms (solid and dashdotted curves) under the usual two cases, $\ell = 0.13$ and $\ell = 0.2$, assuming $\beta_i = 0.2$ and $\beta_j = 0.05$.[23] The gray curve indicates the same investment level chose by platforms when the overall mass of attached users is equally distributed across the two firms, $\beta_i = \beta_j = 0.125$. The figure refers to the case $\theta = 0.8$, although qualitatively identical results are obtained for different values of the network externality parameter.

What immediately emerges is the difference in investment levels between the two firms, with the incumbent consistently investing more than its rival for all values of $g < 1$. When $g = 1$, the two investment levels converge: with full interoperability, the installed user bases of the two firms are perfectly interconnected, and the asymmetry between them effectively disappears. Compared to the symmetric case, the incumbent invests more while the entrant invests less. The incumbent therefore

[23] Again, different values for the installed user base can be chosen; the results do not change qualitatively. Even in this case, we check that the conditions for the existence of the model are satisfied.



(a) $\ell = 0.13$ (b) $\ell = 0.2$

Figure 6: $\Delta\Pi$: asymmetric and symmetric "attached" users

has stronger incentives to invest in cybersecurity—not only because it benefits from greater network effects, but also because its larger size attracts more attention from hackers, thereby increasing its incentive to strengthen its protection level.

The effects on the private incentives for interoperability are illustrated in Figure 6, which reports the isoprofit frontiers for the two firms, $\Delta\Pi_i = 0$ and $\Delta\Pi_j = 0$. For comparison, the figure also shows the common frontier that would obtain under symmetry (gray curve).[24] It is immediately evident that the incumbent's frontier lies not only above the one with symmetry, but also entirely above that of its rival, which in turn lies below the symmetric frontier. Recalling that $\Delta\Pi > 0$ when θ is relatively high for any given g, we can infer that the incentives for interoperability diverge: the incumbent has weaker incentives in that the region where $\Delta\Pi_i > 0$ becomes smaller, while the opposite holds for the rival; these findings align with Bourreau et al. (2023). Intuitively, the incumbent contributes more to cybersecurity in terms of larger investment α and it is, therefore, less willing to make services interoperable. This difference in incentives for interoperability decreases with g—the two frontiers approach each other—since the two levels of security investment tend to converge. It is worth noting that the presence of asymmetry opens the door to potential conflicts between firms: in the region between the two frontiers, the incumbent firm prefers not to enable interoperability, whereas the rival does.

All this highlights that smaller firms have not only weaker incentives to invest in cybersecurity than an incumbent firm, but also greater potential gains from interoperability. In other words, entrants have an incentive to free-ride, while the incumbent has an incentive to protect itself from such behavior by denying interoperability. It is interesting to note that these considerations also underpin Article 7 of the Digital Markets Act (DMA) which requires that third parties interoperating with a gatekeeper maintain the same level of cybersecurity as the gatekeeper itself, and conversely, that the gatekeeper preserve its existing level of security. In this regulatory setting, if a third party fails to meet the mandated security standards, the gatekeeper may lawfully restrict interoperability.

[24] Notice that the $\Delta\Pi_i$ frontier here represents the difference in profits for firm i with and without interoperability and not the difference in industry profits; the same holds for $\Delta\Pi_j$.

5 Concluding remarks

This paper studies how interoperability interacts with cybersecurity in digital services markets. We build a symmetric duopoly model in which cyberattacks create a congestion-like effect, and interoperability simultaneously (i) amplifies user-side network benefits and (ii) enlarges the effective attack surface by enabling indirect breaches across interconnected services. We use this framework to analyze how interoperability shapes firms' investments in protection and to compare the private and social incentives to make services interoperable.

Our main results are threefold. First, we show that interoperability affects cybersecurity investments through multiple channels, yielding either a positive or an inverted U-shaped relationship with the protection efforts. At low levels, interoperability encourages investment in cybersecurity; at high levels, however, security increasingly behaves like a public good across interconnected services, reducing the incentives to exert protection efforts. Second, relative to the social optimum, firms underinvest in security for two reasons: (i) they do not internalize the positive externality of their counterpart's reduced breach probability; (ii) they use investment strategically to soften price competition. Third, while strong user-side network effects increase the desirability of interoperability, private and social incentives to make services interoperable can be misaligned. Our analysis suggests that when firms face significant breach-related damages—such as large legal liabilities—the public good nature of security investments becomes less problematic, thus making interoperability more likely to be welfare enhancing.

Extending the baseline model in several directions allows us to investigate, mainly through numerical simulations, the relevance of different determinants of the desirability of interoperability. First, the level of user awareness regarding cyberrisk is an important factor: the presence of (unsophisticated) users who ignore such risks reduces the social desirability of interoperability, while increasing the private one. Second, the business model adopted by firms affects their private attitude toward interoperability. We find that Ad-funded firms are comparatively less willing to become interoperable, as they can no longer benefit from the strategic role of security investments in mitigating price competition. Third, both private and social desirability of interoperability increase when interoperability entails a significant market expansion effect. Finally, assuming that firms start off with asymmetric installed bases, we replicate insights similar to those emerging in the literature on network compatibility. In our framework, the large firm is more committed to investing in security and has weaker incentives to become interoperable, while the smaller one invests less in security and is more willing to make services interoperable. This latter finding underpins the importance of policy provisions—such as those included in Art. 7 of the Digital Markets Act—requiring a reciprocal minimum level of security when services become interoperable.

While providing interesting insights regarding the complex relationship between interoperability and cybersecurity, our analysis has limitations that may highlight directions for future research. Our model is static and therefore ignores the following potential benefit of making services interoperable: interoperability reduces the costs users incur when switching from one provider to another, thus making the market more contestable. In addition to that, our analysis focuses on the case of horizontal interoperability between firms selling differentiated services. Different insights may emerge when investigating the consequences of vertical interoperability between firms operating at different levels of the value chain. Finally, our model also abstracts from multihoming (i.e. the case of users patronizing more than one platform). Although multihoming and interoperability are typically viewed as substitutes—when consumers multi-home, the benefits of interoperability are lower—things may change once cyberrisks are taken into account. Interoperability amplifies the effectiveness of indirect attacks, a fact which is

likely to harm single-homed users more intensively. If this is the case, a higher degree of interoperability comparatively reduces the utility of single-homing, stimulates users to purchase services from more than one provider, and thus leads to complementarity between interoperability and multihoming.

6 Mathematical Appendix

Proof of Propositions 1 and 3. The baseline model is a special case of the more general setting with sophisticated and unsophisticated consumers presented in Section 4.1; it corresponds to the case in which the mass of sophisticated consumers is $\lambda = 1$. In this proof, we consider the more general setting which holds for any $\lambda \in [0,1]$.

At stage t_1, platform i's profits are:

$$p_{\lambda,i}(\alpha_i,\alpha_j)\, m_{\lambda,i}(p_i,p_j,\alpha_i,\alpha_j;g) - l\, prob_i(\alpha_i,\alpha_j,g) - c\frac{\alpha_i^2}{2},$$

where $p_{\lambda,i}(\alpha_i,\alpha_j)$ is the second-stage i's equilibrium price shown in (14) and $m_{\lambda,i}(p_i,p_j,\alpha_i,\alpha_j;g)$ is obtained plugging $p_{\lambda,i}(\alpha_i,\alpha_j)$ and $p_{\lambda,j}(\alpha_j,\alpha_i)$ into expression (13). Differentiating this expression with respect to α_i and then imposing the symmetry condition $\alpha_i = \alpha_j = \alpha$, the first order condition becomes:

$$\left(-\frac{\delta}{12}(1-g) + \frac{5\delta}{12}g(1-g)\right)\lambda + \frac{\ell(1+3g-g^2)}{3} - c\alpha = 0.$$

Solving this equation for α gives $\alpha^*_\lambda(g)$ shown in expression (15). In the numerical simulations presented in Sections 3 and 4, we verify that the second order conditions are satisfied. Finally, differentiating $\alpha^*_\lambda(g)$ with respect to λ, it is immediate to verify that the derivative is positive if and only if $g > 1/5$. □

Proof of Corollary 1. The derivative $\frac{d\alpha^*(g)}{dg}$ is positive if and only if $g < \frac{3(\delta+2\ell)}{5\delta+4\ell}$; in turn, the latter fraction is larger than 1 if $\ell > \delta$ and smaller than 1 otherwise. □

Proof of Corollary 2. The derivative $\frac{d\alpha^*(g)}{d\ell} = \frac{1+3g-g^2}{3c}$ is positive for any $g \in [0,1]$. The derivative $\frac{d\alpha^*(g)}{d\delta} = \frac{(1-g)(5g-1)}{12c}$ is positive for $g > 1/5$. The derivative $\frac{d\alpha^*(g)}{dc} = -\frac{\alpha^*(g)}{c}$ is negative. □

Proof of Proposition 2 and Corollary 3. Expanding the integrals of the social welfare function (10), we have:

$$\begin{aligned} W \;=\; & v - \delta - \frac{t}{2} + m_i\,(1-m_i)\,t \\ & + \delta\left((1-g)^2\,(\alpha_i+\alpha_j-2)\,{m_i}^2 + 2\,(1-\alpha_j - g\,(1-\alpha_i))\,(1-g)\,m_i + (\alpha_i-1)\,g^2 + \alpha_j\right) \\ & - l\,(g+1)\,((\alpha_i-\alpha_j)\,(g-1)\,m_i + g\,(1-\alpha_i) - \alpha_j + 1) - \frac{c\left(\alpha_i^2+\alpha_j^2\right)}{2}. \end{aligned}$$

Plugging m_i as from (4) and using the second period prices given in (7), we obtain the total welfare, given α_i and α_j. Taking the derivative with respect to firms' investments, the first order condition for welfare maximization under the symmetry condition $\alpha_i = \alpha_j = \alpha$ is (the second order condition is assumed to hold)

$$\frac{(g+1)^2\,(2l+\delta)}{4} - c\alpha = 0.$$

Solving this equation for α yields the socially optimal investment $\alpha^w(g)$ shown in Proposition 2.

Computing the difference between the socially optimal and the equilibrium investment levels, we have:

$$\alpha^w(g) - \alpha^*(g) = \frac{(5l+4\delta)g^2 + l + 2\delta}{6c} > 0,$$

and this proves Corollary 3. □

Analytical conditions for the private and social desirability of interoperability. Condition $\Delta W > 0$ is

satisfied if and only if:

$$\theta > \frac{(\delta + 2\ell)\left[(1-\alpha(g))(1+g)^2 - (1-\alpha(0))\right] + 2c\left(\alpha(g)^2 - \alpha(0)^2\right)}{g} \equiv \overline{\theta}_w(g),$$

where $\alpha(g)$ and $\alpha(0)$ are the equilibrium investment levels defined in Proposition 1. Condition $\Delta\Pi > 0$ is satisfied if and only if:

$$\theta > \frac{(\delta + \ell)\left[1 - \alpha(0) - (1-g)^2(1-\alpha(g))\right] + \ell[(1-\alpha(g))(1+g)^2 - (1-\alpha(0))] + c\left(\alpha(g)^2 - \alpha(0)^2\right)}{g} \equiv \overline{\theta}_\Pi(g).$$

Comparing the two thresholds, it follows that $\overline{\theta}_\Pi(g) > \overline{\theta}_w(g)$ if:

$$2(\delta + \ell)\left[(1-\alpha(0)) - (1-\alpha(g))(1+g^2)\right] - c\left(\alpha(g)^2 - \alpha(0)^2\right) > 0. \tag{18}$$

When this condition is satisfied:

- interoperability is neither privately nor socially desirable if $\theta < \overline{\theta}_w(g)$ (area A in Figure 1);
- interoperability is socially desirable but privately harmful if $\overline{\theta}_w(g) < \theta < \overline{\theta}_\Pi(g)$ (area B in Figure 1);
- interoperability is both privately and socially desirable if $\theta > \overline{\theta}_\Pi(g)$ (area C in Figure 1).

When this condition is instead not met:

- interoperability is neither privately nor socially desirable if $\theta < \overline{\theta}_\Pi(g)$ (area A in Figure 1);
- interoperability is privately desirable but socially harmful if $\overline{\theta}_\Pi(g) < \theta < \overline{\theta}_w(g)$ (area D in Figure 1);
- interoperability is both privately and socially desirable if $\theta > \overline{\theta}_w(g)$ (area C in Figure 1).

Notice that, in Figure 1, the isoprofit frontier $\Delta\Pi = 0$ corresponds to the threshold $\overline{\theta}_\Pi(g)$ while the isowelfare frontier $\Delta W = 0$ corresponds to the thresold $\overline{\theta}_w(g)$. □

Proof of Proposition 4. Under the assumption of paternalistic regulator, the social welfare function is still given by expression (10); therefore, the socially optimal investment level is the same as in the baseline model, that is $\alpha^w(g)$ as shown in Proposition 2. Computing the difference $\alpha^w(g) - \alpha^*_\lambda(g)$, it follows that:

$$\alpha^w(g) - \alpha^*_\lambda(g) = \frac{\left((5\lambda+3)\,g^2 + 6\,(1-\lambda)\,g + \lambda + 3\right)\delta + 2l\left(5g^2+1\right)}{12c} > 0,$$

which implies that there is underinvestment and completes the proof or part i) of the proposition.

Consider now part ii) of the proposition; at the symmetric equilibrium, $m_i = 1/2$ and $\alpha_i = \alpha_j = \alpha$, and social welfare is:

$$W(\alpha) = v - \frac{t}{4} + \frac{\theta\,(1+g)}{2} - \frac{(1-\alpha)\,(\delta+2l)\,(1+g)^2}{2} - c\,\alpha^2.$$

Evaluating this expression at α^*_λ and calculating the derivative with respect to λ gives

$$\frac{dW(\alpha^*_\lambda)}{d\lambda} = \underbrace{\frac{dW(\alpha^*_\lambda)}{d\alpha^*_\lambda}}_{(a)}\underbrace{\frac{d\alpha^*_\lambda}{d\lambda}}_{(b)},$$

where the sign of (b) is determined in Proposition 3, and (a) is positive since (a) expression $W(\alpha)$ is concave in α and (b) we know from part $i)$ that $\alpha^*_\lambda(g) < \alpha^w(g)$. □

Proof of Proposition 5. At stage t_1, platform i's profits are:

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

where $m_i(\alpha_i, \alpha_j; g)$ is given by expression (16). Differentiating this expression with respect to α_i and then imposing the symmetry condition $\alpha_i = \alpha_j = \alpha$, the first order condition becomes:

$$\frac{(1-g)\left(A\,(1+g) + (1-g)\,(1-\alpha)\left(\ell\,(1+g)^2 - 4c\alpha\right)\right)\delta + 2\,(\theta\,(1-g) - t)\,(2c\alpha - \ell\,(1+g))}{(1-g)\,(4\,(1-g)\,(1-\alpha)\,\delta - 4\theta) + 4t} = 0$$

Solving this equation for α gives $\alpha^*_{Ad}(g)$ shown in expression (17). In the numerical simulations presented in Section 4.2, we verify that the second order conditions are satisfied. □

References

Abrardi, L., Comino, S., and Grassini, S. (2025). The economics of cyber risk: A survey of the literature. *Journal of Industrial and Business Economics*, forthcoming.

Arce, D. (2022). Security-induced lock-in in the cloud. *Business & Information Systems Engineering*, 64(4):501–513.

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity*, 4(1):tyy010.

August, T., Niculescu, M. F., and Shin, H. (2014). Cloud implications on software network structure and security risks. *Information Systems Research*, 25(3):489–510.

Bernstein, D. (2014). Containers and cloud: From lxc to docker to kubernetes. *IEEE Cloud Computing*, 1(3):81–84.

Blessing, J. and Anderson, R. (2023). One protocol to rule them all? on securing interoperable messaging. In *Cambridge International Workshop on Security Protocols*, pages 174–192. Springer.

Bourreau, M. and Krämer, J. (2022). Interoperability in digital markets: boon or bane for market contestability? *Available at SSRN: https://ssrn.com/abstract=4172255*.

Bourreau, M., Krämer, J., and Buiten, M. (2022). Interoperability in digital markets. *CERRE Report*.

Bourreau, M., Raizonville, A., and Thébaudin, G. (2023). Interoperability between ad-financed platforms with endogenous multi-homing. *CESifo Working Paper No. 10332*.

Catuogno, L. and Turchi, S. (2015). The dark side of the interconnection: security and privacy in the web of things. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 205–212.

Crémer, J., Rey, P., and Tirole, J. (2000). Connectivity in the commercial internet. *Journal of Industrial Economics*, 48(4):433–472.

De Borger, B. and Van Dender, K. (2006). Prices, capacities and service levels in a congestible bertrand duopoly. *Journal of Urban Economics*, 60(2):264–283.

De Cornière, A. and Taylor, G. (2024). A model of information security and competition. *Marketing Science*, forthcoming.

De Palma, A. and Leruth, L. (1989). Congestion and game in capacity: a duopoly analysis in the presence of network externalities. *Annales d'Economie et de Statistique*, 15/16:389–407.

Dhakar, M. and Yan, J. (2024). Interoperability & privacy: A case of messaging apps. *Available at: https://www.cresse.info/wp-content/uploads/2024/09/2024_ps11_pa3_DHAKAR.pdf*.

Farrell, J. and Saloner, G. (1986). Installed base and compatibility: Innovation, product preannouncements, and predation. *American Economic Review*, 76(5):940–955.

Fedele, A. and Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, 36(1):157–187.

Gasser, U. (2015). Interoperability in the digital ecosystem. *Available at SSRN: https://ssrn.com/abstract=2639210*.

Gates, L. (2024). Cyber attacks on interoperable electronic health records: A clear and present danger. *Missouri Medicine*, 121(1):6.

Geer, D., Jardine, E., and Leverett, E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5(1):9–29.

GSMA (2020). Universal profile for advanced messaging (rcs): Technical specification. `GSMA Technical Document`. Available at https://www.gsma.com/futurenetworks/rcs/.

Huang, J., Tan, G., Teh, T.-H., and Zhou, J. (2024). Network interoperability and platform competition. *Working Paper 24-03, NET Institute*.

Jianqiang, G., Shue, M., and Weijun, Z. (2015). Analyzing information security investment in networked supply chains. In *2015 International Conference on Logistics, Informatics and Service Sciences (LISS)*, pages 1–5. IEEE.

Katz, M. L. and Shapiro, C. (1985a). Network externalities, competition, and compatibility. *American Economic Review*, 75(3):424–440.

Katz, M. L. and Shapiro, C. (1985b). Network externalities, competition, and compatibility. *American Economic Review*, 75(3):424–440.

Kretschmer, T., Rasch, A., Shekhar, S., and Wenzel, T. (2025). Strategic response to mandated interoperability: Privacy spillovers in network markets. *Available at SSRN: https://ssrn.com/abstract=5516420*.

Lam, W. M. W. and Seifert, J. (2023). Regulating data privacy and cybersecurity. *Journal of Industrial Economics*, 71(1):143–175.

Liao, C.-H. and Chen, C.-W. (2014). Network externality and incentive to invest in network security. *Economic Modelling*, 36:398–404.

Marlinspike, M. and Perrin, T. (2016). The signal protocol: Building the modern asynchronous end-to-end encrypted messaging system. *Open Whisper Systems Technical Report*. Available at https://signal.org/docs/.

Matsumura, T. and Matsushima, N. (2007). Congestion-reducing investments and economic welfare in a hotelling model. *Economics Letters*, 96(2):161–167.

Rana, P. and Patil, B. (2023). Cyber security threats in iot: A review. *Journal of High Speed Networks*, 29(2):105–120.

Villeneuve, N. (2011). Trends in targeted attacks. *Trend Micro*, (October).