IT Interdependence and the Economic Fairness of Cyber-security Regulations for Civil Aviation

Martina De Gramatica, Fabio Massacci *(Member, IEEE)*, Woohyun Shim, Alessandra Tedeschi, and Julian Williams

Abstract—Physical security is well understood in Civil Aviation and its rules are mandated across the board from small airports with few flights to hubs aggregating thousands of flights and millions of passengers. To finance security procedures diverse mechanisms from government subsidies to per-passenger taxes and charges have been implemented. A popular scheme is the flat security tax per passenger of €5-7 in Europe and $5.6 in the US. A key question is whether the same regulatory and financial measures should apply to cyber-security. We present the results of interviews with key stakeholders (European and National Regulators, IATA and Eurocontrol Experts, Airport Directors, and Security Managers) on this emerging threat and a cyber-security public policy economic model for Civil Aviation. We illustrate how interdependency issues impacting the probability of a successful attack can make regulation significantly unfair for small or medium airports.

1 Introduction

Recent ICT incidents caused by accidental failures of air traffic management systems show that the risk of a successful cyber-attack in civil aviation is an increasingly emerging threat. A notable example is the failure of a UK National Air Traffic Services server in 2013 that kept the communications network in 'night-time mode' with severely reduced capacity resulting in 300 canceled flights and 1400 delayed ones.

Prior research on terrorism and reports from national and international government agencies have warned that the next generation of terrorist attack could take place by exploiting cyber-security vulnerabilities, [1], [2]. By perpetrating an attack through electronic communications networks, a terrorist does not need to have physical access to an airport but can have the same as or even a bigger impact than a traditional terrorist attack on civil aviation facilities.

Whilst cyber-security is an evolving discipline, physical security in aviation is well understood and heavily regulated [3]. In comparison with other sectors (e.g. PCI DSS for the payment industry), these regulations are very detailed and many measures are applied across the board: the security experience of a passenger boarding in a small airport is essentially the same of a passenger in a large hub.

A key question is *should cyber-security regulation follow the same financing approach used for physical security?*

In the framework of the SECONOMICS project (www.seconomics.org) we have tried to answer it by combining qualitative and quantitative research methods. We first present the results of semi-structured interviews with key stakeholders (European and National Regulators, IATA and Eurocontrol Experts, Airport Directors, and Security Managers) on this emerging threat. Then, we provide a game-theoretic model of the interaction among airports, attackers and a policy-maker, as decisions made by each agent affect decisions of the other agents. The model also considers the interconnectivity among airports to capture partial non-excludability of security investments, since the security level of one airport can contribute toward the reduction of security risks in other airports.

Our calibrated simulation analysis from the model, and the evidence from the interviews, show that simply extending the security regulatory and financial instruments (e.g. mandating the same expenditure and a flat security tax per passenger) from the physical to the cyber domain may lead to an unfair economic treatment of small and medium airports.

2 Cyber-Security for Aviation

The aviation industry is one of the industries heavily relying on ICT in managing its daily critical operations. Fig.1 illustrates how Terminal 5 in Heathrow Airport depends on an extensive ICT infrastructure [4]. The introduction of IT-enabled aircrafts Airbus A380 and Boeing B777 also increases the potential impact of cyber-security incidents (e.g. Aircraft takeover).

The NextGEN program in the US and the SESAR program in the EU will further introduce additional ICT technologies to boost capacity and decrease costs of aviation. Isolated system will migrate to an IP-based infrastructure, the System Wide Information Management (SWIM). It will allow better decision making by giving all actors more accurate and timely information but it may potentially lead to larger data breaches.

Manuscript submitted to IEEE Security and Privacy, for reviewing purposes only.
1. M. De Gramatica, F. Massacci, W. Shim are with DISI, University of Trento, IT.
2. A. Tedeschi is with Deep Blue Srl, IT
3. J. Williams is with Business School, Durham University, UK.
Email: name.surname@[unitn.it, dblue.it, durham.ac.uk]

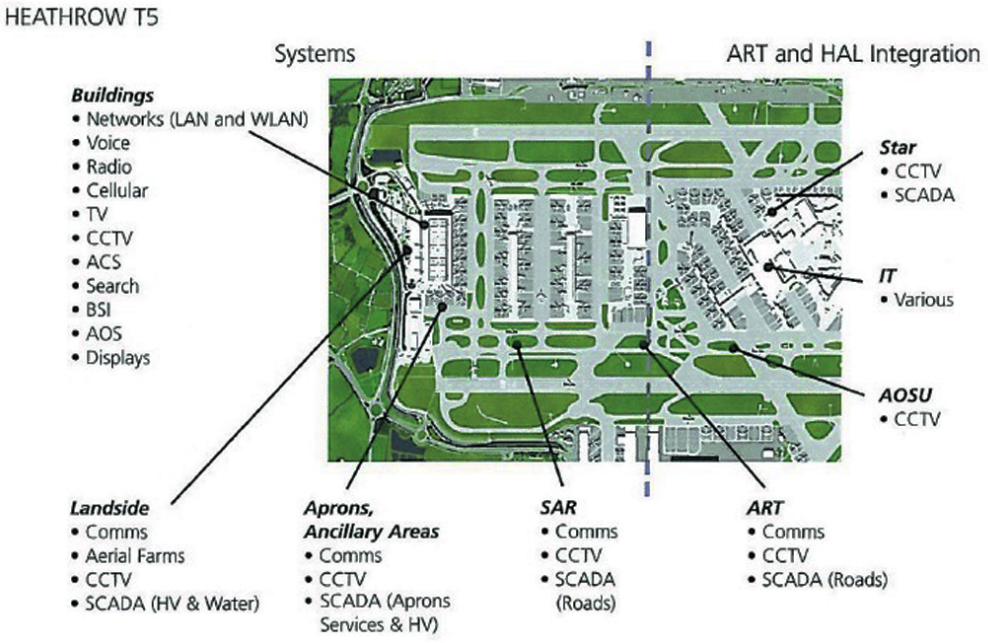


Fig. 1. ICT services and devices used in Terminal 5 of Heathrow airport, U.K. It involves 1,500 camera CCTV systems, 1,100 secure access control points, a wireless LAN with 750 access points, and 2,800 analogue, digital and IP telephones. From [4] with permission from the publisher.

Another innovative concept is the Remote and Virtual Tower (RVT): landing and departure operations at airports are controlled by a central, remotely operated site and the physical view of the airport, originally available from the physical tower, is replaced by virtual reality and remote sensors. The first RVT was announced in November 2014 for Örnsköldsvik Airport in Sweden. RTVs bring significant cost saving but sci-fi scenarios of cyber-criminals replacing sensor feeds with fake ones becomes concrete threats. The USA FAA Administrator M. Huerta already acknowledged in 2011 that *"With that evolution [NextGen] the cyber-security risks will increase."*

The Association of Airport Directors [5] has classified cyber-threats into three groups: subvertible IT systems; theft and fraud causing direct financial losses to airlines, airports and passengers; and terrorism. Cyber-attacks in conjunction with physical attacks may be used to increase potency or be the core focus to exploit cyber to physical effect (e.g. by malicious attacks on SCADA or other critical equipment) or to embarrass commercial entities and act as a conduit for a political message.

The aviation sector has started to set new policies to address some of these threats and to promote common cyber-security standard. In 2013, the European Commission issued a document aiming at defying a shared cyber-security strategy of the cyberspace, encouraging industry to cooperate at the national level and to agree on a set of cyber- security measures among all the EU airports. In 2013, IATA, the international umbrella of airlines, started to develop a toolkit to support airlines in setting up a cyber-security management system.

Yet, few airports have cyber-security measures in place: the main airport of Birmingham (UK's second largest city by population) implemented cyber-security measures through a Corporate Risk Assessment program; Asheville airport (NC, US, with over 700,000 passengers in 2010) recently adopted its own cyber-security policy to evaluate and handle cyber-incidents [5].

Cyber-security does not come for free, and financing cyber-security will likely use the same mechanisms of traditional security. The US uses a centralized model where security activities are primarily the responsibility of the Transportation Security Administration (TSA). TSA is funded partially through direct taxes, and partly on a general subsidy model: a flat rate tax of $5.6 per passenger is raised per each flight segment to cover around 40% of the budget. The remaining part is funded by the general budget of the Federal Government [6].

In Europe, there is no common rule for who should pay for security [7], [8]. Some countries (Austria, Finland, Germany, Iceland, Italy, Luxembourg, Norway, Portugal, Spain, Sweden and Switzerland) follow a centralized financing model (states collect taxes and redistribute them to airports for funding security costs), other countries (Belgium, Denmark, France, Greece, Ireland, Netherlands, and the UK) follow a decentralized model (security is the responsibility of the airport under a central authority supervision) and make airports directly pay for security through charges imposed on passengers. Yet, the final emerging outcome is a flat rate levied on a per-passenger basis [7] ranging between €5 and €7. It is often hardly enough to cover the costs: *"In*

12 of the 13 [European] States with operating deficits [...], the airports fund the major proportion of the deficit." [7, pag.48]. Different considerations are true for the US where essentially the Federal Government is funding the deficit and thus subsidizes unprofitable airports.

Would this financing mechanism be equally adequate for cyber-security regulations?

3 Stakeholders' Views

The empirical evidence behind our study has been collected through several interviews with airport stakeholders along the qualitative study design suggested by [9]. We have organized several meetings with over 60 stakeholders, on different topics such as optimal expenditures allocation, effectiveness of security training programs, attack scenarios, etc. Not all interactions could be recorded or transcribed for security reasons (e.g. attacks to the tower). For 19 stakeholders, who agreed to be formally interviewed, we conducted in-depth 30-40 minute semi-structured interviews which were recorded with permission and transcribed in anonymous form.

The final 6 interviewees reported in Table 1 have been selected by a purposive sampling method to represent a variety of roles specifically involved in the regulatory aspects of emerging threats in the aviation domain. The aim of these semi-structured interviews was to discuss the main issues related to the emerging threats in the aviation domain, and the effectiveness of security regulation to mitigate these upcoming risks. Opinions and findings from other interviews underlay this study, and clarified security issues and the economic model.

All interviewees agreed that risks from cyber-threats are particularly hard to quantify in terms of features, boundaries and potential consequences, and it is mostly regarded as "unknown" threats. They revealed that the main hurdle towards strategies for effective countermeasures lies in the intrinsic uncertainty of cyber-threats: *"We are aware of the cyber-attack, but so far it is not easy to say what the emerging risks are and what their consequences may be"* [#2], commented an European regulator.

This feature increases the complexity and the limits of the risk assessment and management, and is mentioned together with the high interconnectivity within the sector and among sectors as the factors that may expose the aviation domain to additional vulnerabilities [#1]. The consequences of cyber-attack could therefore be more severe than those of traditional attacks.

Cyber-threats therefore are perceived differently from traditional threats and pose additional challenges in the identification of aviation security regulations that could appropriately cover and address these new risks: *"The issue is that we already envisage a fast and quick change in a lot of processes, like the Air Traffic Management and we have to adapt very quickly to respond to the new threat scenarios. This is becoming more and more challenging. I am not sure that we will be able with the current regulatory framework and the current management of security to move at the same pace than the threats"* [#1].

Due to the international and trans-sectorial nature of cyber-threats, a more trans-border and inter-sectoral collaborative security regulation would be required: "[The problem here is] *the lack of a global framework for cyber-security in aviation. We need to address cyber-security in aviation in a more holistic way, meaning all security actors and all aviation players have to be encompassed under the same framework. The regulation has to consider all these aspects"* [#1]. This statement reflects lack or delay of a common policy addressing cyber-security issues: ICAO reported that five major international aviation organizations signed a roadmap towards aviation cyber-security agreement only in Dec. 2014.

The request for broader security regulation is combined with the need for more flexibility, allowing airports to apply it consistently with their specific structure and needs. The prescriptive and static nature of the current normative corpus is strongly criticized mainly by airport managers interviewed [#4, #6], in favor of a more risk-based approach that should consider: "[Additional] *plug-ins to the normal baseline regulation"* [#3], fitting the specificity of different airports. The preference accorded by the interviewees to a risk-based approach is supported by the need of a contextual, shared and complete risk assessment to be done in collaboration with international regulatory bodies and national aviation authorities: "*There should be evaluations done [... by...] ICAO or EU Commission and at a national level by each Government, according to the threats that are expected by those Governments. This is very important to say: threats could vary, there could be high risk in some areas and low risk in other areas"* [#3].

Regulation should be based on the real risk, in order to be effective [#1], a direction toward which EU regulators are trying to move: *"What we are trying to do is to give airports different options to deliver the same outcomes. The small airport may choose to invest more in people than in technology but the big airports may invest more in technology because it is more efficient"* [#2].

A unified but more flexible regulation seems to be a more appropriate policy to cover the current and future threats addressing the aviation domain, mostly in relation to the economic means available by small airports. The current regulation, however, as it is perceived also by ATM experts, seems to favor mainly big airports in the directives: *"If there are regulators which are part of the government authority, and they are consulting with airports for a new decision, big airports have bigger chances than do small airports"* [#3]. The prescriptive application of security requirements mandated by a regulator causes harsh problems of investments for small airports relying on smaller budget [#1, #4, #5, #6], though they must face similar problems tackled by bigger airports and provide the same level of security [#2]. To meet these strict directives, small airports must either claim exceptions and dispensations from the mandated regulation or risk financial losses [#4, #5].

TABLE 1
Participants to the Interviews

ID	Role	Institution	Interview Date
1	Head of ATM Security Unit	European Authority for Air Navigation	Nov. 2014
2	EU Aviation Regulator	EU Directorate for Transport	Nov. 2014
3	Responsible of Security Training programs	IATA	Nov. 2014
4	Security Manager and Training Instructor	Airport and Civil Aviation Authority	Dec. 2014
5	Security Manager	Airport	Dec. 2014
6	Security Manager	Airport	Dec. 2014

4 A Review of Regulatory Models for Cyber-security

While the previous literature has made contributions in the field of economics of cyber-security, there has been no application that particularly studies an issue on fair cost allocation for cyber-security in civil aviation. In other research domains, many authors have studied the issues of fair cost allocation (e.g., [10], [11], [12]). They mainly argue that, since large-scale networks consist jointly of many agents and complex traffic flows, the design of networks should consider not only the minimization of total costs but also the fair allocation of these costs in order to achieve a high level of efficiency. For example, in the field of civil aviation, O'Kelly [11] and Thomson [12] investigate an efficient solution for fair cost allocation in airport networks.

In the cyber-security domain, research using a game-theoretical model has recently started to receive huge interest by the research community. Since the pioneering contributions by scholars, such as Varian [13] and Anderson [14] several scholars have employed game-theoretic approaches to illustrate issues related to cyber-security. In particular, a new focus on attacker and target strategic interactions in game-theoretic model has been recently proposed. For example, Ioannidis et al. [15] pay their attention to externalities and the interactions between attackers and defenders in a security environment. They analyze the incentives of defenders to make investments in security, and identify a role of a policy-maker for structuring socially optimal security investments.

Another point that has recently drawn attention of researchers and practitioners in cyber-security [16], is a policy design principle for establishing and maintaining a sound cyber-ecosystem. The growing role of the governments in cyber-security has been recognized, but there has been little agreement on which policy design should be employed. In a companion paper in SECONOMICS Deliverable 6.4 we discuss the implications for policy-makers behind the choice between risk-based and rule-based regulations.

In this study, we try to link the above-mentioned fields together. Specifically, building on [15], our model considers various airports operating and making security investments jointly in the network, and includes the interaction between and among airports, attackers and a policy-maker, and the role of attacker behavior in analyzing airports' strategic investment decisions. Using a simulation technique, we then explore whether current security regulation can apply to cyber-security from the perspective of economic fairness.

Traditional cyber-security models make a reasonable assumption that permits mathematical tractability: the absence of interdependence. In the economic jargon they assume no direct positive externalities. The only externalities are those manifested by the strategic interactions of the agent in the game.

This is definitely *not* true in Civil Aviation. Airports are definitely independent legal entities, but are interconnected by construction and such interdependence can be approximately measured by traffic volumes among airports. In the physical domain this is part of the day-by-day experience of passengers: a security check in a spook airport makes it possible to land in a hub airport and continue to a connecting flight without going through security again. The regulation mandating a security checkpoint at all airports creates *positive* externalities for the connecting hub airport.

When a policy coordinator is present, airports can exploit potentially positive security externalities, such as common frontiers and standards. Traditional studies assume that financing follows regulations but, as indicated in both interviews [#1, #4, #5, #6] and domain studies [7], state-mandated security requirements and global financial mechanisms can be inconsistent and cause a cost allocation problem among airports. By employing a game theoretic model we provide a quantitative evidence that the extension of the current policy to cyber-security might undermine the fairness in the network.

5 A Cyber-security Economics Model for Civil Aviation

We assume that airports are divided in categories, indexed by i. For tractability we assume that airports within each category are identical and when faced with the same set of information make identical choices. A natural classification of airports is to use traffic volume of the airport: large airports ($i = 1$) are hubs with highest traffic; medium airports ($i = 2$) are airports feeding large hubs and working also as "small-scale" hubs for small airports; and small airports ($i = 3$) as outlying airports with very low traffics. From observation of the clustering of traffic, we believe that three types are sufficient to capture the cross sectional variation in airport. From the traffic data of 509 European airports [17], around

TABLE 2
Traffic information on sample airports

	#pass/year	Average Traffic/day		#pass/day coming from		
		#flights	#pass	Large Airports	Medium	Small
Large (e.g. Munich, DE)	37.7M	680	101.370	18.182	48.205	34.983
Medium (e.g. Verona, IT)	2.7M	222	7.397	3.226	1.467	2.704
Small (e.g. Ancona, IT)	0.5M	20	1.479	565	652	262

Munich is the second hub of Lufthansa in Germany, the 7th European Airport and 27th worldwide; Verona, in a touristic/industrial region in Northern Italy, is a "feeder airport" for the Lufthansa's hubs and other national carriers (e.g. British Airways) and some low-cost airlines; Ancona's airport, in a touristic region on the Adriatic Sea, is only served by Lufthansa, the national carrier Alitalia and three low cost airlines (e.g. Ryanair).

3% of the airports are large airports (15 airports), 10% are medium airports (50 airports) and the rest are small airports (444 airports). The difference in scale among them is illustrated in Table 2.

Each airport would like to minimize its expected loss:

$$U(i) = \sigma_i(X, n_i)L_i + x_i. \tag{1}$$

where $X = \langle x_1, \ldots, x_i, \ldots \rangle$ represents the investments of all airports, n_i the number of attackers per airport of type i, L_i the loss of the airport and σ_i the probability of a successful attack.

Rational attackers will participate in an attack as long as the deterministic cost of entering the market for attacks is lower than the expected profit. At the equilibrium, the entry/exit condition should be:

$$\sum_{i=1}^{N_{types}} \sigma_i(X, n_i)R_i \cdot n_i = C. \tag{2}$$

where $\sigma_i R_i$ is the expected reward for the fraction of n_i attackers on the airport of type i, and C is the cost of mounting an attack to the airport network. The Nash equilibrium is determined by solving simultaneously the equations above for all x_i and n_i.

The key issue is to identify an appropriate functional form for σ_i, the probability of successful attacks. Our proposal contains four factors capturing some important socio-economical features.

$$\sigma_i(X, n_i) = A_i \cdot n_i^{\beta} \cdot e^{-\alpha_i x_i} \cdot e^{-\sum_{j=1}^{n} \tau_{ij}\delta_{ij}x_j}. \tag{3}$$

The first three factors have been already used in the economics of cyber-security literature. The factor A_i is the probability that an attack made against type i airport is successful when there is no additional cyber-security expenditure. It essentially captures the preferences of the attacker for some type of airports over another. In general $\sum_i A_i \leq 1$ as an attacker might prefer other alternatives (e.g. hack a power station). The factor n_i^{β} tells how an increase in the marginal number of attackers multiplies the chances of success. For σ to be a probability, the fraction of attackers across airports has to be less than unity, on which all stakeholders agreed.

The factor $e^{-\alpha_i x_i}$ captures the effectiveness of security investments such that i) increasing x_i diminishes σ_i but ii) the marginal benefit of additional x_i decreases with the investment. All stakeholders agreed that investments do not scale linearly: after investing a million euro, any additional euro yields a negligible benefit; only a very large additional investment brings visible changes.

The fourth term is our innovative contribution. It has the same shape of the third factor (so property i) and ii) holds), and captures the security externalities: δ_{ij} shows the extent to which the security level of a target airport type depends on the security level of other types of airports; τ_{ij} represents an actual structural characteristic of the relationships between different types of airports in the aviation ecosystem.

Notice that $\sigma_i L_i$ decreases as x_i rises, and increases as n_i rises, yet at the same time the "loss" due to x_i increases. So airport i seeks a sweet spot where the security expenditure is not so high, but still high enough to discourage attacker (low n_i) and minimize expected losses (low $\sigma_i L_i$). Furthermore, the investments of other airports x_j may have beneficial effects and thus airport i might decide to lower its investment x_i by reaping the beneficial effects of those who invest. The parameters are summarized in Table 3.

To analyze the game we first consider a case without a policy-maker: type i airports choose x_i based only on their private incentives and do not consider ecosystem externalities ($\delta_{ij} = 0$). The corresponding Nash equilibrium might not be socially optimal as each airport makes an investment decision non-cooperatively to minimize its own expected loss.

Next, we then introduce a policy-maker in the game. Since he prioritizes building socially desirable security conditions, he will consider externalities ($\delta_{ij} \neq 0$). The policy-maker has a single composite objective function consisting of all airports' expected loss functions $\sum_i W_i U(i)$, and shapes a policy to drive all airports' decisions toward the Pareto optimum.

A "political" problem here is that security financing may not follow the mandated security measures and thus the chosen levels of security investments might not be allocated fairly: a policy regulating security investments is Pareto-efficient but some airports might be imposed to carry a significantly heavier burden than they would bear by acting on their private incentives. This might need to be addressed by redistributive measures.

TABLE 3
Description of model parameters

Airports and Attackers		Policy-maker and environment	
L_i	Airport's losses for successful attack	W_i	Social planner's weight for Type i airport
R_i/C	Attacker's reward/cost ratio for successful attacks	f_i	Fraction of type i airports
A_i	Airport's baseline risk	τ_{ij}	Fraction of traffic volume between types i and j airports
α_i	Airport's marginal risk reduction by additional x_i	δ_{ij}	Interdependence coefficient between type i and j airports
β	Elasticity of success when num. of attackers increases	σ_i	Prob. of successful attack on target i given $x_1 \dots x_n$ and n_i
x_i	Airport's security investment	n_i	Number of attackers per target i

6 Simulation of Policy Impact

The Nash equilibrium in the absence of interdependence can be analytically solved whilst the equation for the social optimum combines transcendental and linear terms and is not analytically solvable. The socially optimal solution must be found numerically by simulation.

For the simulation, various parameters are inputed from the airport information (e.g. Table 2). L_i is estimated from the number of days of potential airport shutdown and canceled flights. From studies on natural disasters [18], [19], we assume that a successful attack results in €50K loss per canceled flight for at least seven days. By multiplying for the number of daily flights, L_i is €238M for a large airport, €77.7M for a medium airport, and €7M for a small airport. Some losses can be transferred to airlines. Yet, airlines will eventually abandon an airport and move elsewhere if the cost transfer from the airport is considered financially unviable. A policy makers would also include loss of life as well as damage on society as a whole, yet those losses would be immaterial to the particular airport where the incident takes place, and could be treaded as constants

We calculate τ_{ij} as the ratio $(I_{ij}+I_{ji})/\sum_i \sum_j I_{ij}$ where I_{ij} denotes total number of inbound traffic from type i airports to type j airports. In rough terms 10% of the ongoing traffic of a large airport goes to other large airports and 27% goes to medium airports (confirming the business model of hub-and-spook). However, this 10% is shared among only 15 airports whereas the remaining 63% is shared among over 350 airports. The bulk of the traffic goes to medium and small airports in aggregate but each airport only benefits for a small fraction of it.

Some parameters cannot be directly estimated and must be calibrated from other data. For the baseline risk A_i, most stakeholders agreed that attackers would simply chose a well known, nearby airport. Thus, we assume the chances of selecting an airport to be inversely proportional to the number of airports of that type as the more "identical" airports there are, the less likely is an airport to be selected: $A_i = (1/N_i)/(\sum_1^n 1/N_i)$. As a result, we get $A_1 = 0.750$, $A_2 = 0.225$ and $A_3 = 0.025$. This is a worst case scenario because $\sum_i A_i = 1$: in absence of additional protection measures some airport will be *surely* cyber-attacked. This is not necessarily true and lower values for A_i might be used if some information about the intrinsic preference for airports over other targets is available.

To identify α_i, recall that it captures the effectiveness of security countermeasures mandated by the policy makers. They are unwilling to have a serious incident before d_i days and will likely require technologies such that the probability of accidents is below the threshold

$$\sigma_i \cdot I_i \leq \frac{1}{d_i} \tag{4}$$

where I_i is the number of inbound flights per day. We can then use Eq.(**??**) to rewrite Eq. (3) as

$$\alpha_i = \frac{\log d_i + \log I_i + \log A_i}{x_i} \tag{5}$$

Eq.(**??**) makes it clear that α_i, as mandated by the policy maker, depends from the policy makers acceptable d_i and its expectation on the attractiveness A_i of airports as targets. All interviewees stated their ideal target as "never", so d_i should be at least a decade: $d_i = 10 \times 365$.

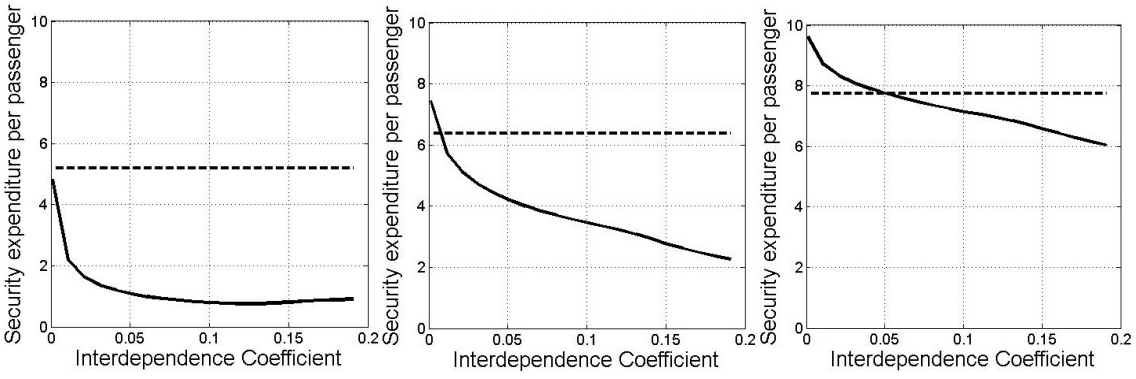
To identify x_i, we use directly the average value of the security tax per passenger €6. Hence $\alpha_1 = 0.071$, $\alpha_2 = 0.766$ and $\alpha_3 = 2.786$. The interviewed regulators indicated that they regard all airports equally. We therefore set $W_1 = W_2 = W_3$.

Lastly, we must calibrate parameter values for attackers. As for a point estimate of R_i/C, since a cyber-attack on an airport can draw nationwide, or even worldwide attention, we assume that such reward is 10-fold the cost.

Using a similar assumption in [15], β is considered to have the value of 0.1 as cyber-attackers' efficiency is relatively high due to the characteristics of cyber-attack. To investigate whether the security expenditures imposed by the policy-maker are fair we run the following experiment:

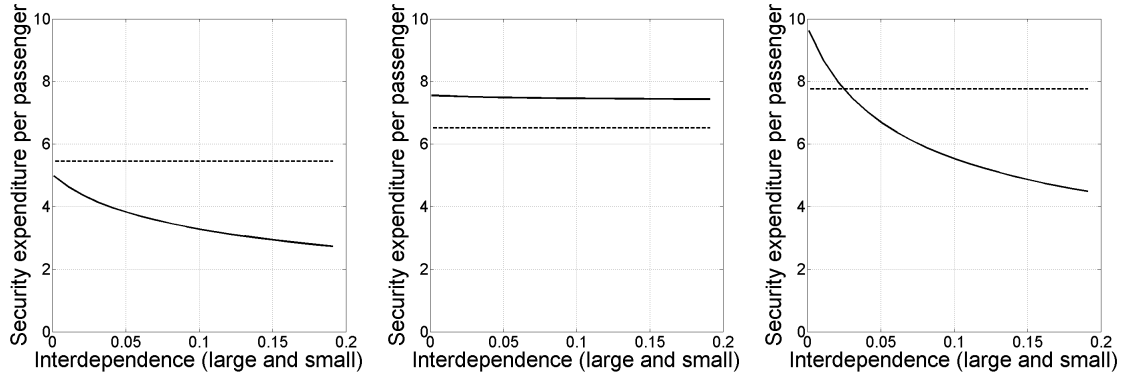
1) We start from a small interdependence coefficient $\delta_{ij} = 0.1\%$ because the SESAR/NextGen envisaged interconnection has yet to be fully operational.
2) We progressively increase the interdependence coefficient up to 20%.
3) For each value of δ_{ij}, we calculate the optimal investment per passenger that a policy-maker could fix by accounting for positive externalities.
4) We compare this investment with the investment that airports would make without social intervention (Nash Equilibrium).

Figure 2 (a,b,c) illustrates what happens if δ_{ij} increase simultaneously for all airports. As δ_{ij} increases, for example by implementing IT-based interconnected networks such as SWIM (i.e., $\delta_{ij} = 20\%$), the social optimal



(a) Large Airports (b) Medium airports (c) Small airports

Solid line represent the optimal expenses calculated by a policy-maker accounting for interdependency, dashed line is Nash equilibrium. The interdependence increases equally among all airport types. Smaller airports have the unfairest treatment they have to pay more than the €6 received from taxes. Big airports make a large profit from a fixed €6 security charge.



(d) Large airports (e) Medium airports (f) Small airports

The interdependence increases only among small and large airports (e.g. by deploying a remotely operated tower). The medium airport ends up with an unfair burden. They can't recover their costs from the €6 flat charge. After 8% increase in interdependency small airports start making a profit over the €6 charge. Big airports make a profit anytime but smaller than above.

Fig. 2. Effects of Changes in Interdependence Coefficient.

expenditures make medium and large airports invest much less in security than small airports, comparing to Nash equilibrium security expenditures. Medium and large airports get greater benefits from the rule than small airports. With limited interconnection they will be forced by the policy-maker to spend more (€10) than they would spend if let on their own (€8 at the Nash equilibrium) and well *above* the €6 current tax they are receiving from the government. So, they are actually paying more than they would. Only at 15% of δ_{ij}, they break even with the government tax. In contrast, big airports security investments are globally high but, per passenger, are well below the €6 government tax. They are profiting from security charges.

The degree of δ_{ij} may also change unevenly between airports of different types. For example, (d), (e) and (f) in Figure 2 show a case where the policy-maker enacts a regulation that increases interdependence between large and small airports, δ_{13}. A paradigmatic case is the deployment of RTVs whereby small airports are controlled by a remote control center which is likely to be located at a large airport. In this case, the unfairness in security expenditures becomes severe since a cost burden on small and large airports gets much less than Nash equilibrium while medium airports are not affected by the regulation and are made to invest more than Nash equilibrium. Large airports and to some extent small airports benefit from the RTV deployment.

To check the robustness of our findings we conducted additional simulations by varying several parameter values, for example, changes in α_i by decreasing d_i to 5×365, by making A_2 or A_3 higher than A_1, and by having R_i to be between 1-fold to 20-fold the cost. There was no qualitative change in the findings. The intuition for this result can be seen from the last three columns of Table 2: the massive imbalance in term of traffic between airports cannot be compensated by reasonable variations in the model parameters.

7 Guidance Recommendations

This study offers a contribution to the ongoing discussion on cyber-security in civil aviation.

The simulation analysis shows that a policy-maker might ask smaller airports to spend more on cyber-security per passenger than larger airports do as security IT interdependence increases. Essentially, the power-law distribution of passengers traffic is such that the large airports benefit from IT interdependence and from the cyber-security investments of small airports. Small airports become net contributors to the social good.

This unfairness in cost allocation for cyber-security becomes more severe under the current security financing rule of a flat security fee per passenger. In this situation, the larger airports might actually make profits out of security fees while smaller airports will have to subsidize security costs from other revenues.

In summary, using a current financing mechanism for cyber-security might not be suitable for allocating a joint and fair cost burden among airports as it may over-burden some airports. Cyber-security regulation should identify redistribution mechanisms of either security costs or security taxes. One of such mechanisms could be sharing the security revenues between hubs and their feeder airports.

Similar considerations would apply to the cyber-security costs in other industries where there is interdependence and massive disproportion in interconnectivity such as for internet service providers and aggregators.

ACKNOWLEDGEMENTS

This work has been partly funded by the European Union's 7th Framework Programme under grant agreement no 285223 - SECONOMICS (www.seconomics.org). We would like to thank the anonymous reviewers for their useful comments and the participants to the stakeholders validation activities for their insights.

REFERENCES

[1] H. C. Chu, D. J. Deng, H. C. Chao, and Y. M. Huang, "Next generation of terrorism: Ubiquitous cyber terrorism with the accumulation of all intangible fears." *Journal of Universal Computer Science*, vol. 15, no. 12, pp. 2373–2386, 2009.

[2] G. Ariely, "Knowledge management, terrorism, and cyber terrorism," *Cyber warfare and cyber terrorism*, 2008.

[3] International Civil Aviation Organization, "Security. safeguarding international civil aviation against acts of unlawful interference," ICAO, Montreal, Canada, Tech. Rep. Annex 17 (8ed), 2006.

[4] C. Cook, "Heathrow terminal 5: An it infrastructure success story," *Airports International*, November 2010.

[5] Airport Council International, "Cyber security: Potential impact on EU airports," ACI, 2014.

[6] Gulliver, "Airline taxes in america: Get ready to pay more," *The Economist*, January 2014.

[7] Irish Aviation Authority & Aviasolutions, "Study on civil aviation security financing," Irish Aviation Authority & Aviasolutions, 2004.

[8] R. Falconer, "Revised EU regulatory framework for aviation security agreed," *Airport Business*, 2008.

[9] J. A. Maxwell, "Designing a qualitative study," in *The SAGE Handbook of Applied Social Research Methods (2nd Ed.)*, L. Bockman and D. Rog, Eds. SAGE Publication Inc., CA, 2009, pp. 69–100.

[10] D. Skorin-Kapov and J. Skorin-Kapov, "Threshold based discounting networks: The cost allocation provided by the nucleolus," *European Journal of Operational Research*, vol. 166, no. 1, pp. 154 – 159, 2005.

[11] M. E. O'kelly, "A quadratic integer program for the location of interacting hub facilities," *European Journal of Operational Research*, vol. 32, no. 3, pp. 393 – 404, 1987.

[12] Thomson, William, "Cost allocation and airport problems," Rochester Center for Economic Research, Working Paper, 2007.

[13] H. Varian, "Managing online security risks," *New York Times*, 2000.

[14] R. Anderson, "Why information security is hard - an economic perspective," in *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*. IEEE, 2001, pp. 358–365.

[15] C. Ioannidis, D. Pym, and J. Williams, "Sustainability in information stewardship: Time preferences, externalities, and social coordination," in *The Twelfth Workshop on the Economics of Inforamtion Security (WEIS 2013)*, 2013.

[16] National Institute of Standards and Technology, "Request for information: Developing a framework to improve critical infrastructure cybersecurity, 78 fed. reg. 13,024," 2013.

[17] S. Vitali, M. Cipolla, S. Micciche, R. Mantegna, G. Gurtner, F. Lillo, V. Beato, and S. Pozzi, "Statistical regularities in ATM: network properties, trajectory deviations and delays," in *SESAR Innovation Days*, 2014.

[18] International Air Transport Association, "Iata economic briefing: The impact of hurricane sandy," International Air Transport Association, 2012.

[19] P. Brooker, "Fear in a handful of dust: aviation and the icelandic volcano," *Significance*, vol. 7, no. 3, pp. 112–115, 2010.

Fabio Massacci Fabio Massacci is a full professor at the University of Trento (IT). He has a Ph.D. in Computing from the University of Rome La Sapienza in 1998. He has been in Cambridge (UK), Toulouse (FR) and Siena (IT). He has published more than 250 articles in peer reviewed journals and conferences and his h-index is 35. His current research interest is in empirical methods for cyber security. He was the European Coordinator of the project SECONOMICS (www.seconomics.org) on socio-economic aspects of security. He is now working on the SESAR EMFASE project on empirical validation of security risk assessment in aviation