IT Interdependence and the Economic Fairness of Cybersecurity Regulations for Civil Aviation

Martina De Gramatica, Fabio Massacci, and Woohyun Shim | University of Trento
Alessandra Tedeschi | Deep Blue SRL
Julian Williams | Durham University

A cybersecurity public policy economic model for civil aviation and several interviews with key stakeholders illustrate how interdependency issues can lead to aviation regulations that put smaller airports at a disadvantage.

Recent information and communications technology (ICT) incidents caused by accidental failures of air traffic management (ATM) systems show cyberattacks in civil aviation are an increasing threat. A notable example is the 2013 failure of a UK National Air Traffic Services server that kept its communications network in nighttime mode with severely reduced capacity, resulting in 300 canceled and 1,400 delayed flights.

Prior research on terrorism and reports from national and international government agencies have warned that the next generation of terrorist attacks could come through cybersecurity vulnerability exploitation.[1,2] By perpetrating an attack through electronic communications networks, a terrorist doesn't need to have physical access to an airport—such an attack could have the same or even a bigger impact than a traditional terrorist attack on civil aviation facilities. Although cybersecurity is an evolving discipline, physical security in aviation is well understood and heavily regulated.[3] In comparison with other sectors (for example, the Payment Card Industry Data Security Standard for the payment industry), civil aviation's regulations are very detailed and apply many measures across the board: the security experience of passengers boarding in a small airport is essentially the same as that of passengers in a large hub.

A key question is: Should cybersecurity regulation employ the same financing approach that is currently used for physical security? In the framework of the Seconomics project (www.seconomics.org), we try to answer this question by combining qualitative and quantitative research methods.

Cybersecurity for Aviation

The aviation industry heavily relies on ICT in managing its daily critical operations. Figure 1 illustrates how Terminal 5 in Heathrow Airport depends on an extensive ICT infrastructure.[4] The introduction of IT-enabled aircraft, including Airbus A380 and variants of Boeing B777, also increases the potential impact of cybersecurity incidents (for example, aircraft takeover).

 Copublished by the IEEE Computer and Reliability Societies

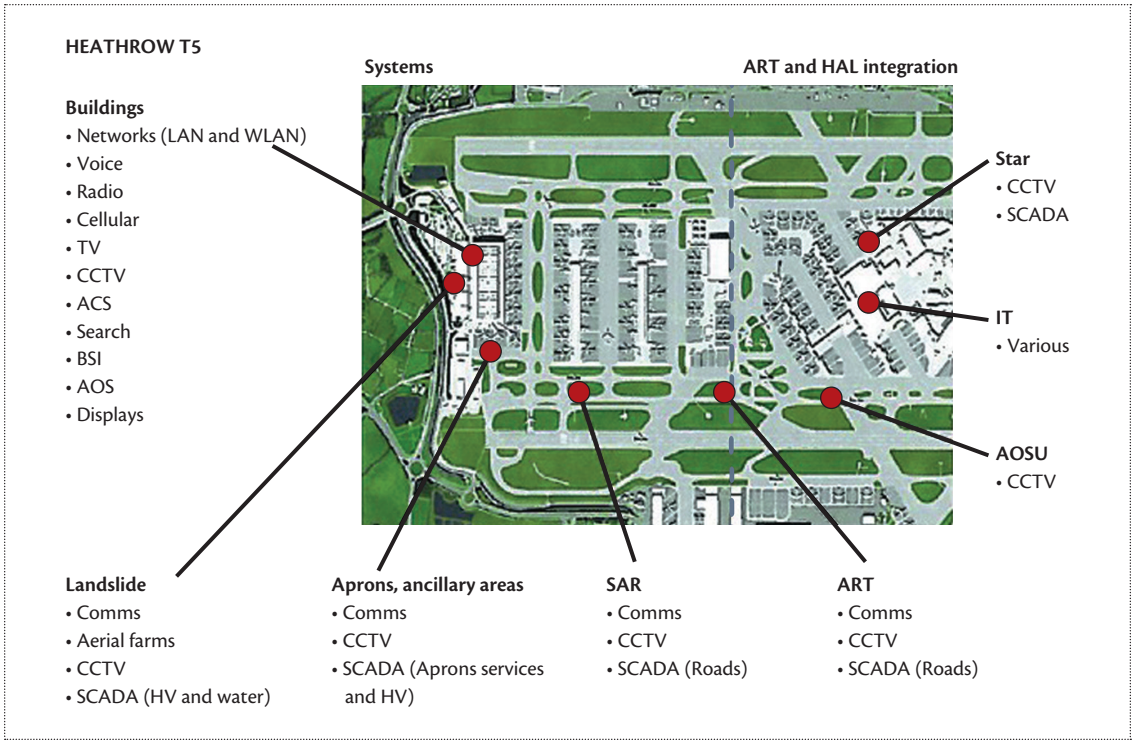

Figure 1. Information and communications technology services and devices used in Terminal 5 of Heathrow Airport. The infrastructure involves 1,500 closed-circuit television (CCTV) systems; 1,100 secure access control points; a wireless LAN with 750 access points; and 2,800 analog, digital, and IP telephones. (Printed with permission from the publisher.[4])

The NextGen program in the US and the Single European Sky ATM Research (SESAR) program in the EU will introduce additional ICT technologies to boost capacity and decrease aviation costs. Isolated systems will migrate to an IP-based infrastructure: systemwide information management (SWIM). This will allow for better decision making, giving all actors more accurate and timely information, but it could also potentially lead to larger data breaches.

Another innovative concept that NextGen and SESAR are developing is the remote and virtual tower (RVT) wherein landing and departure operations at airports are controlled by a central, remotely operated site. 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. RVTs bring significant cost savings, but scenarios in which cybercriminals replace sensor feeds with fake ones are concrete threats. Michael Huerta, the administrator of the US Federal Aviation Administration, already acknowledged in a keynote speech at the 2011 Information Technology/Information Systems Security Conference that "with [NextGen's] evolution the cybersecurity risks will increase."[5]

The Association of Airport Directors has classified cyberthreats into three groups[6]: subvertible IT systems; theft and fraud that cause direct financial losses to airlines, airports, and passengers; and terrorism. Attackers can use cyberattacks in conjunction with physical attacks to increase potency (for example, via malicious attacks on SCADA or other critical equipment) or embarrass commercial entities and act as a conduit for political messages.

The aviation sector has started to set new policies to address some of these threats and promote common cybersecurity standards. In 2013, the European Commission issued the COM(2013) 48 final 7.2.2013 document, aimed at defining a shared cybersecurity strategy for cyberspace and encouraging industry to cooperate at a national level and agree on a set of cybersecurity measures among all EU airports. In 2013, the International Air Transport Association (IATA), the international umbrella of airlines, started to develop a toolkit to support airlines in setting up a cybersecurity management system. However, only a few airports have put cybersecurity measures in place: the main airport in Birmingham (the UK's second-most populous) implemented cybersecurity measures through a corporate risk assessment program; the Asheville airport in North Carolina (which had more than 700,000 passengers in 2010) recently adopted its own cybersecurity policy to evaluate and handle cyberincidents.[6]

Table 1. Interview participants.

ID	Role	Institution	Interview date
1	Head of air traffic management security unit	European Authority for Air Navigation	Nov. 2014
2	EU aviation regulator	EU Directorate for Transport	Nov. 2014
3	Security training program manager	International Air Transport Association	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

Financing Challenges

Although its importance is clear, cybersecurity is not free. Its financing model will likely use the same funding processes as those of traditional security. The US uses a centralized model where security activities are primarily the responsibility of the Transportation Security Administration (TSA). TSA funds come partly from direct taxes and partly from a general subsidy model: a flat rate tax of US$5.60 per passenger for each flight segment covers about 40 percent of the budget. The rest of the funding comes from the federal government's general budget.[7]

In Europe, there's no common rule for who should fund security.[8,9] Some countries (Austria, Finland, Germany, Iceland, Italy, Luxembourg, Norway, Portugal, Spain, Sweden, and Switzerland) follow a centralized financing model wherein 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 airport's responsibility, with a central authority supervising) and make airports directly pay for security through charges imposed on passengers. The final outcome is a flat rate, ranging from €5 and €7, levied on a per-passenger basis.[8] 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."[8]

This is a very different model from that of the US, in which the federal government is essentially funding the deficit and therefore subsidizing unprofitable airports. Would all financing models discussed in this article be equally as adequate for funding cybersecurity regulations?

Stakeholders' Views

The empirical evidence behind our study was collected through several interviews with airport stakeholders (modeled after Joseph Maxwell's qualitative study design[10]). We organized several meetings with more than 60 stakeholders, such as European and national regulators, IATA and Eurocontrol experts, airport directors, and security managers; these meetings covered different topics, such as optimal expenditure allocation, security training programs' effectiveness, and attack scenarios. For security reasons, not all interactions could be recorded or transcribed (for example, interviews regarding the details of attack scenarios to the control tower). For the 19 stakeholders who agreed to be formally interviewed, we conducted in-depth, semi-structured interviews, 30 to 40 minutes long, which we recorded with permission and transcribed in anonymous form.

The six interviewees represented in Table 1 were selected by a purposive sampling method to represent a variety of roles involved in the regulatory aspects of emerging threats in the aviation domain. Interviewers aimed to discuss both the main issues related to these emerging threats and the effectiveness of security regulation to mitigate these upcoming risks. Opinions and findings from other interviews, for example, underlying assumptions and parameter values used in the quantitative analysis, underlie this study and are used to clarify security issues and the economic model.

All interviewees agreed that risks from cyberthreats are particularly hard to quantify in terms of features, boundaries, and potential consequences and that they're mostly regarded as "unknown" threats. The interviews revealed that the main hurdle for strategies for effective countermeasures lies in the intrinsic uncertainty of cyberthreats; a European regulator (participant 2) commented, "We are aware of the cyberattacks, but so far it is not easy to say what the emerging risks are and what their consequences may be." This uncertainty increases complexity and limits risk assessment and management. Participant 1 mentioned that this feature, along with high interconnectivity within and among sectors, could expose the aviation domain to additional vulnerabilities. Thus, the threats of cyberattacks could be more severe than those of traditional attacks.

Stakeholders therefore perceive cyberthreats differently from traditional threats, and they see a challenge in identifying aviation security regulations that could appropriately cover and address these new risks. Participant 1 said: "The issue is that we already envisage a fast and quick change in a lot of processes, like the ATM,

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 to move at the same pace as the threats with the current regulatory framework and the current management of security."

Due to the international and transsectorial nature of cyberthreats, a more transborder and intersectoral collaborative security regulation is needed. Participant 1 said: "[The problem here is] the lack of a global framework for cybersecurity in aviation. We need to address cybersecurity 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." This statement reflects the lack or delay of a common policy addressing cybersecurity issues: the International Civil Aviation Organization (ICAO) reported that five major international aviation organizations signed an agreement for a road map toward aviation cybersecurity, but this didn't happen until December 2014.[11]

The need for broader security regulations also requires more flexibility; airports must be able to apply the regulations consistently within their specific structures and according to their individual needs. Two airport managers we interviewed (participants 4 and 6) strongly criticized the prescriptive and static nature of the current normative corpus. In addition, participant 3 was in favor of a more risk-based approach that would consider "[additional] plug-ins to the normal baseline regulation," fitting the specificity of different airports. The preference accorded by the interviewees to a risk-based approach is supported by the need for a contextual, shared, and complete risk assessment to be done in collaboration with international regulatory bodies and national aviation authorities. Participant 3 said: "There should be evaluations … [by] ICAO or the European Commission, and at a national level by each government, according to the threats that those governments expect. This is very important to say: threats could vary—there could be high risk in some areas and low risk in other areas."

Participant 1 stated that, to be effective, regulation should be based on the real risk—a direction in which EU regulators are trying to move. Participant 2 further noted: "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."

A unified but more flexible regulation seems to be the most appropriate approach to cover the current and future threats to the aviation domain, mostly in relation to small airports' economic means. However, the current regulation's directives, as ATM experts perceive them, seem to favor large airports. Participant 3 said: "If there are regulators that are part of the government authority and they are consulting with airports for a new decision, big airports have a better chance [for influence] than do small airports." Participants 1, 4, 5, and 6 stated that the prescriptive application of security requirements mandated by a regulator causes harsh problems of investments for small airports, which rely on smaller budgets; as participant 2 noted, they face similar problems to those of bigger airports and still must provide the same level of security. To meet these strict directives, participants 4 and 5 stated that small airports must either claim exceptions and dispensations from the mandated regulation or risk financial losses.

Research Considerations

In this article, we try to link studies that cover several research fields (see the "Related Work in Regulatory Models for Cybersecurity" sidebar). Specifically, building on the work of Christos Ioannidis and his colleagues,[12] our model considers various operating airports and their security investments jointly within their networks. This area of study includes the interaction between and among airports, attackers, and policymakers as well as 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 cybersecurity from the perspective of economic fairness.

Traditional cybersecurity models make a reasonable assumption that permits mathematical tractability: the absence of interdependence. In 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 independent legal entities but are interconnected by construction; traffic volumes among airports can provide a measure of such interdependence. In the physical domain, this is part of the passengers' daily experience: a security check in a spoke (versus hub) airport makes it possible for a passenger 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. An example is the presence of standardized security controls for baggage and passengers at the point of entry into an airport. Airports regulated by the same policymaker can assume that controls have been done properly and, when "receiving and forwarding," the passenger or the baggage doesn't need to be rechecked. Traditional

Related Work in Regulatory Models for Cybersecurity

Although previous literature has contributed to cybersecurity economics research, there hasn't been an application that specifically studies the issue of fair cost allocation for cybersecurity in civil aviation. However, many authors have studied the issues of fair cost allocation in other related domains.[1–3] They mainly argue that because large-scale networks consist jointly of many agents and complex traffic flows, network design should consider not only the minimization of total costs but also the fair allocation of these costs to achieve a high level of efficiency. For example, in the field of civil aviation, Morton E. O'Kelly[2] and William Thomson[3] investigate efficient solutions for fair cost allocation in airport networks.

In the cybersecurity domain, the research community has recently started to show great interest in work that uses a game-theoretic model. Since the pioneering contributions of scholars such as Hal R. Varian[4] and Ross Anderson,[5] several other scholars have employed game-theoretic approaches to illustrate issues related to cybersecurity. In particular, in the game-theoretic model, there's a new focus on strategic interactions between attackers and targets. For example, Christos Ioannidis and his colleagues studied externalities and the interactions between attackers and defenders in a security environment.[6] They analyzed defenders' incentives to invest in security and also identified the role of policymakers for structuring socially optimal security investments.

Another point that has recently drawn the attention of cybersecurity researchers and practitioners is a policy design principle for establishing and maintaining a sound cyberecosystem.[7] The growing role of governments in cybersecurity 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 (seconomics.org/content/d064-set-policy-papers-0), we discuss the implications for policymakers regarding the choice between risk- and rule-based regulations.

References

1. D. Skorin-Kapov and J. Skorin-Kapov, "Threshold Based Discounting Networks: The Cost Allocation Provided by the Nucleolus," *European J. Operational Research*, vol. 166, no. 1, 2005, pp. 154–159.
2. M.E. O'Kelly, "A Quadratic Integer Program for the Location of Interacting Hub Facilities," *European J. Operational Research*, vol. 32, no. 3, 1987, pp. 393–404.
3. W. Thomson, "Cost Allocation and Airport Problems," working paper 538, Rochester Center for Economic Research, Univ. Rochester, 2007.
4. H.R. Varian, "Managing Online Security Risks," *New York Times*, 1 June 2000.
5. R. Anderson, "Why Information Security Is Hard—An Economic Perspective," *Proc. 17th Ann. IEEE Computer Security Applications Conf.*, 2001, pp. 358–365.
6. C. Ioannidis, D. Pym, and J. Williams, "Sustainability in Information Stewardship: Time Preferences, Externalities, and Social Co-ordination," *Proc. 12th Workshop Economics of Information Security* (WEIS 13), 2013; www.weis2013.econinfosec.org/papers/IoannidisPymWilliamsWEIS2013.pdf.
7. "Request for Information: Developing a Framework to Improve Critical Infrastructure Cybersecurity," *Federal Register*, Nat'l Inst. Standards and Technology, vol. 78, no. 38, 2013.

studies assume that financing follows regulations, but as indicated in both our interviews (with participants 1, 4, 5, and 6) and other domain studies,[6] 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 quantitative evidence that the extension of the current policy to cybersecurity might undermine the fairness in the network.

A Cybersecurity Economics Model for Civil Aviation

In this model, we assume that airports are divided into 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 by traffic volume: large airports ($i = 1$) are hubs with the highest traffic, medium airports ($i = 2$) feed large hubs and also work as "small-scale" hubs for small airports, and small airports ($i = 3$) are outlying airports with very low traffic. After observing the clustering of traffic, we believe that these three types are sufficient to capture airports' cross-sectional variation. According to the traffic data of 509 European airports, approximately 3 percent of the airports are large (15 airports), 10 percent are medium (50 airports), and the rest are small (444 airports).[13] The difference in scale among them is illustrated in Table 2.

Each airport aims to minimize its expected loss, which can be calculated according to the equation

$$U(i) = \sigma_i(X, n_i)L_i + x_i, \quad (1)$$

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

Table 2. Traffic information for sample airports.

Airport size*	No. of passengers per year (million)	Average traffic per day		No. of passengers per day coming from		
		No. of flights	No. of passengers	Large airports	Medium airports	Small airports
Large (for example, Munich, Germany)	37.7	680	101,370	18,182	48,205	34,983
Medium (for example, Verona, Italy)	2.7	222	7,397	3,226	1,467	2,704
Small (for example, Ancona, Italy)	0.5	20	1,479	565	652	262

** Munich is the second hub of a major European air carrier. In 2014, it was the 32nd largest in the world, in the range of Delhi, Miami, and Toronto. Verona, an industrial and tourist city, is a feeder airport for the same carrier as well as several European carriers to the respective hubs in European capitals and some low-cost airlines. Ancona's airport, in a sea resort on the Adriatic Sea, is served only by the same carrier to Munich, Italy's national carrier, and three low-cost airlines.*

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

$$\sum_{i=1}^{types} N_i \sigma_i(X, n_i) R_i = \sum_{i=1}^{types} n_i N_i C \,, \qquad (2)$$

where $\sigma_i R_i$ is the expected reward for the fraction of n_i attackers on the airports of type i, and C is the cost of mounting an attack to the airport network. The Nash equilibrium is determined by simultaneously solving Equations 1 and 2 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 socioeconomic features:

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

The first three factors have already been used in other studies on cybersecurity economics. The factor A_i is the probability that an attack made against type i airport is successful when there is no additional cybersecurity expenditure. It essentially captures the preferences of the attacker for one type of airport over another. In general, $\sum_i A_i \leq 1$ because an attacker might prefer other alternatives (for example, hacking 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: $\sum_i n_i N_i / \sum_i N_i$, where N_i is the number of type i airports.

The factor $e^{-a_i x_i}$ captures the effectiveness of security investments such that

1. increasing x_i diminishes σ_i, but
2. the marginal benefit of additional x_i decreases with the investment.

All stakeholders from our interviews agreed that investments do not scale linearly: after investments reach €1 million, any additional money yields a negligible benefit; only a very large additional investment brings visible changes.

The fourth term is our own innovative contribution. It has the same shape of the third factor (so properties 1 and 2 hold) 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 attackers (low n_i) and minimize expected losses (low $\sigma_i L_i$). Furthermore, the investments of other airports x_j might have beneficial effects, and thus airport i might decide to lower its investment x_i by reaping the beneficial effects of those who invest. Table 3 summarizes these parameters.

Analysis

To analyze our game-theoretic model, we first consider a case without a policymaker: 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 because each airport makes noncooperative investment decisions to minimize its own expected loss.

Next, we introduce a policymaker into the game.

Table 3. Descriptions of model parameters.

Airports and attackers		Policymaker 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 types i and j airports
β	Elasticity of success when number of attackers increases	σ_i	Probability of successful attack on target i given $x_1 \ldots x_n$ and n_i
x_i	Airport's security investment	n_i	Number of attackers per target i

Because the policymaker prioritizes building socially desirable security conditions, he or she will consider externalities ($\delta_{ij} \neq 0$). The policymaker 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 might 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 required to carry a significantly heavier burden than they would bear when acting on their private incentives. This might need to be addressed by redistributive measures.

Simulation of Policy Impact

The Nash equilibrium in the absence of interdependence can be analytically solved, whereas 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 inputted from the airport information (such as the information from Table 2). L_i is estimated from the number of days of potential airport shutdown and canceled flights. From studies on natural disasters,[14,15] we assume that a successful attack results in airport shutdown for seven days and a €50K loss per day for each canceled flight. 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 policymaker would also look at loss of life as well as the damage on society as a whole, yet those losses would be immaterial to the particular airport where the incident takes place and could therefore be treated as constants.

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

There are some parameters that we cannot directly estimate and must instead calibrate from other data. For the baseline risk A_i, most stakeholders agreed that attackers would simply choose 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, because the greater number of "identical" airports there are, the less likely an attacker is to select those airports: $A_i = \left(1/N_i\right) \Big/ \left(\sum_1^n 1/N_i\right)$. 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 the absence of additional protection measures, some airports will surely be cyberattacked. However, this is not necessarily true because lower values for A_i might be used if some additional 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 policymakers. They are unwilling to have a serious incident before d_i days and will likely require technologies so the probability of accidents is below the following 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 Equation 4 to rewrite Equation 3 as

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

Equation 5 makes it clear that α_i, as mandated by the

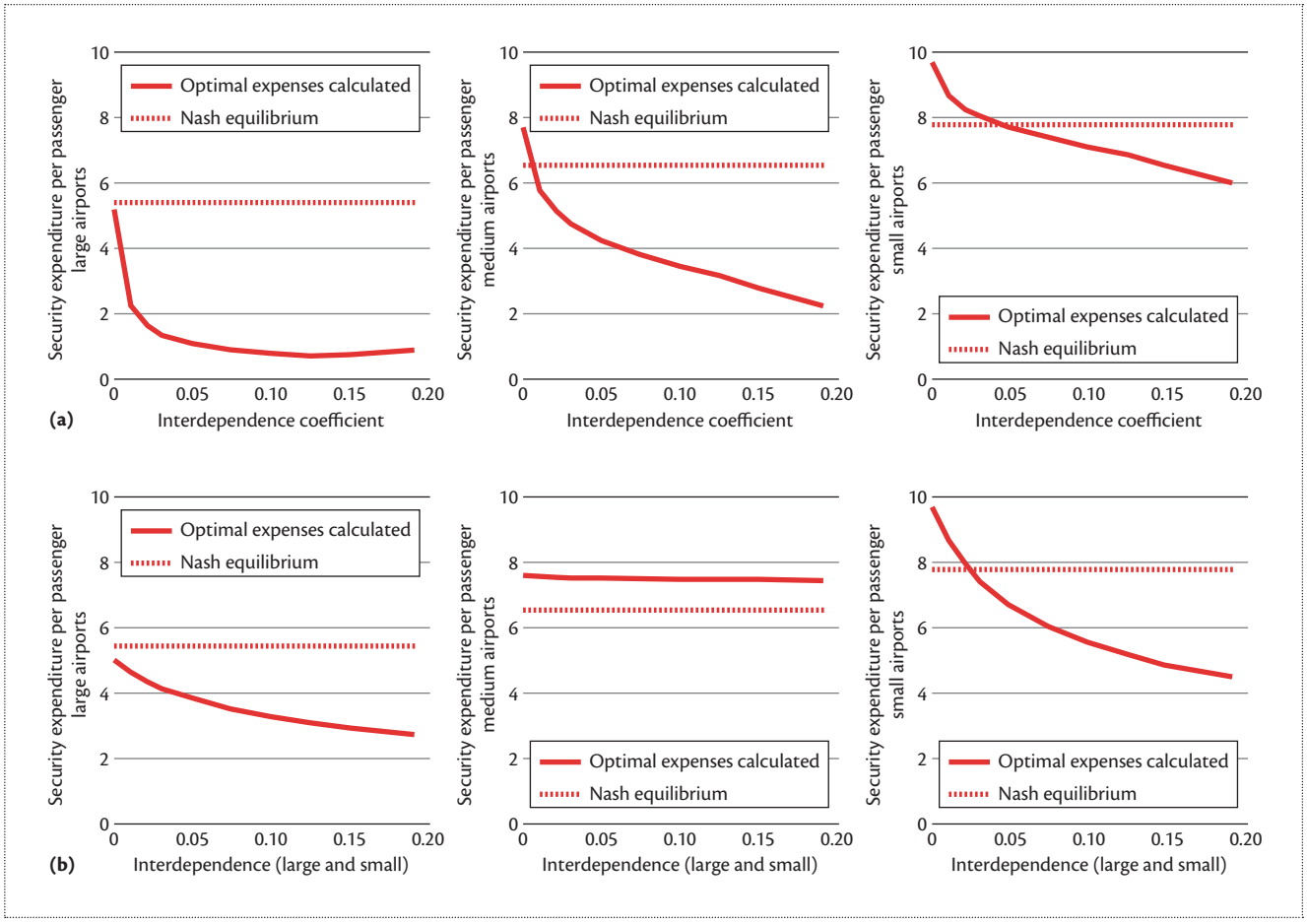

Figure 2. Effects of changes in interdependence coefficient. The solid line represents the optimal expenses calculated by a policymaker accounting for interdependency. The dotted line is the Nash equilibrium. (a) The interdependence increases equally among all airport types. Smaller airports have the least fair treatment, as they must pay more than the €6 received from taxes. Large airports make a large profit from a fixed €6 security charge. (b) The interdependence increases only among small and large airports (for example, by deploying a remotely operated tower). Medium airports end up with an unfair burden. They can't recover their costs from the €6 flat charge. After an 8 percent increase in interdependency, small airports start making a profit over the €6 charge. Large airports always profit.

policymaker, depends on the policymaker's acceptable d_i and its expectation on A_i which can be considered as the attractiveness of airports as targets. All interviewees stated their ideal target for having a serious incident is "never," so we assume that d_i should be reasonably long and at least a decade: $d_i = 10 \times 365$.

To identify x_i, we directly use the average value of the security tax per passenger: €6. Hence, $a_1 = 0.071$, $a_2 = 0.766$, and $a_3 = 2.786$. The interviewed regulators indicated that they regard all airports equally. We therefore set $W_1 = W_2 = W_3$ and $n_1 = n_2 = n_3$.

Last, we must calibrate parameter values for cyberattackers. As for a point estimate of R_i/C, because a cyberattack on an airport can draw national or even worldwide attention, we assume that such reward (for example, international recognition) is tenfold the cost.

Using a similar assumption as Ioannidis and his colleagues,[12] we consider β to have the value of 0.1, because cyberattackers' efficiency is relatively high owing to the characteristics of cyberattacks (for example, availability of various exploit kits and possibility of a remote attack). To investigate whether the security expenditures imposed by the policymaker are fair, we run the following experiment:

- we start from a small interdependence coefficient $\delta_{ij} =$ 0.1 percent because the SESAR/NextGen envisaged interconnection has yet to be fully operational;
- we progressively increase the interdependence coefficient up to 20 percent;
- for each value of δ_{ij}, we calculate the optimal investment per passenger that a policymaker could fix by accounting for positive externalities; and finally,

- we compare this investment with the investment that airports would make without social intervention (Nash equilibrium).

Figure 2a illustrates what would happen if δ_{ij} values for all airports increased simultaneously. As δ_{ij} increases—for example, by implementing IT-based interconnected networks such as SWIM (that is, δ_{ij} = 20 percent)—the social optimal expenditures lead medium and large airports' investments to be proportionally much less in security than small airports, compared to Nash equilibrium security expenditures. Medium and large airports get greater benefits from the rule than small airports do. With limited interconnection, small airports will be forced by the policymaker to spend more (€10) than they would spend if left to their own security systems (€8 at the Nash equilibrium); this is well above the current €6 tax they're receiving from the government. They don't break even with the government tax until δ_{ij} is at 15 percent. In contrast, large airports' total security investments are globally high, but per-passenger investments are well below the €6 government tax. So they're profiting from security charges.

The degree of δ_{ij} might also change unevenly between airports of different types. For example, Figure 2b shows a case in which the policymaker 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 because the cost burden on small and large airports is much less than the Nash equilibrium, whereas medium airports are not affected by the regulation and must invest more than the Nash equilibrium. Large airports, and to some extent small airports, therefore benefit from the RTV deployment.

To check the robustness of our findings, we conducted additional simulations by varying several parameter values—for example, by implementing changes in a_i by decreasing d_i to 5 × 365, by making A_2 or A_3 higher than A_1, and by setting R_i to be between one to 20 times the cost, C. There was no qualitative change in the findings. As seen in the three right columns of Table 2, the massive imbalance in terms of traffic between airports cannot be compensated for by reasonable variations in model parameters.

The current financing mechanisms for cybersecurity might not be suitable for allocating a joint and fair cost burden among airports. Under current conditions, large airports benefit from IT interdependence and from the cybersecurity investments of smaller airports; smaller airports become net contributors to the social good as they are often forced to spend more on their cybersecurity measures than large airports do. In the future, cybersecurity regulation should identify redistribution mechanisms of either security costs or security taxes. One such mechanism could be sharing security revenues between hubs and their feeder airports. Moreover, in the future, these considerations could also be applied in other industries in which there is interdependence and massive disproportion in interconnectivity, such as for Internet service providers and aggregators. ■

Acknowledgments

The EU's 7th Framework Programme partly funded this work under grant agreement 285223—Seconomics (www.seconomics.org). We thank the anonymous reviewers for their useful comments and the participants of the stakeholders' validation activities for their insights.

References

1. H.C. Chu et al., "Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of All Intangible Fears," *J. Universal Computer Science*, vol. 15, no. 12, 2009, pp. 2373–2386.
2. G. Ariely, "Knowledge Management, Terrorism, and Cyber Terrorism," *Cyber Warfare and Cyber Terrorism*, L.J. Janczewski and A.M. Colarik, eds., Information Science Reference, 2008, pp. 7–16.
3. *Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference*, tech. report annex 17 (8th ed.), Int'l Civil Aviation Organization, 2006.
4. C. Cook, "Heathrow Terminal 5: An IT Infrastructure Success Story," *Airports Int'l*, 25 Nov. 2010; www.airportsinternational.com/2010/11/heathrow-terminal-5-an-it-infrastructure-success-story/4563.
5. M. Huerta, "Cybersecurity and NextGen," keynote speech, Information Technology/Information Systems Security Conf., 2011.
6. *Cyber Security: Potential Impact on EU Airports*, tech. report, Airport Council Int'l Europe, 2014.
7. "Airline Taxes in America: Get Ready to Pay More," *Economist*, 1 Jan. 2014; www.economist.com/blogs/gulliver/2014/01/airline-taxes-america.
8. *Study on Civil Aviation Security Financing*, summary report, Irish Aviation Authority, 2004.
9. R. Falconer, "Revised EU Regulatory Framework for Aviation Security Agreed," *Airport Business*, 1 Feb. 2008; www.airport-business.com/2008/02/revised-eu-regulatory-framework-for-aviation-security-agreed.
10. J.A. Maxwell, "Designing a Qualitative Study," *Sage Handbook of Applied Social Research Methods* (2nd ed.), L. Bockman and D.J. Rog, eds., Sage, 2009, pp. 69–100.
11. "Aviation Unites on Cyber Threat," Int'l Civil Aviation

Organization, 2014; www.icao.int/Newsroom/NewsDoc2014/COM.46.14.EN.pdf.
12. C. Ioannidis, D. Pym, and J. Williams, "Sustainability in Information Stewardship: Time Preferences, Externalities, and Social Co-ordination," *Proc. 12th Workshop Economics of Information Security* (WEIS 13), 2013; www.weis2013.econinfosec.org/papers/IoannidisPymWilliamsWEIS2013.pdf.
13. S. Vitali et al., "Statistical Regularities in ATM: Network Properties, Trajectory Deviations and Delays," *Proc. Sesar Innovation Days*, 2012; www.sesarinnovationdays.eu/files/SIDs/2012/SID%202012-21.pdf.
14. "IATA Economic Briefing: The Impact of Hurricane Sandy," Int'l Air Transport Assoc., 2012; www.iata.org/publications/economics/Documents/hurricane-sandy-impact-nov2012.pdf.
15. P. Brooker, "Fear in a Handful of Dust: Aviation and the Icelandic Volcano," *Significance*, vol. 7, no. 3, 2010, pp. 112–115.

Martina De Gramatica is a research associate at the University of Trento. Her research interests include innovation potential and technology transfer of EU projects through ethnographic analysis, research studies on innovation, and information and communications technology (ICT) markets and trends. De Gramatica received an MS in anthropology and social research from Bicocca University. Contact her at martina.degramatica@unitn.it.

Fabio Massacci is a full professor at the University of Trento. His research interests include empirical methods for cybersecurity and security risk assessment in aviation. He coordinated the Seconomics joint industry–academia project on socioeconomic aspects of security under which this research was performed. Massacci received a PhD in computing from the Sapienza University of Rome. He's a member of IEEE. Contact him at fabio.massacci@unitn.it.

Woohyun Shim is a research fellow at the University of Trento. His research interests include security economics and innovation economics for sustainable development in ICT, with an emphasis on public policy and governance issues for utilizing the full benefits of ICT for society. Shim received a PhD in media and information studies from Michigan State University. Contact him at woohyun.shim@unitn.it.

Alessandra Tedeschi is a security and validation expert with Deep Blue SRL. Her research interests include analyzing and modeling complex systems with game theory techniques. Tedeschi received a PhD in applied mathematics from the Sapienza University of Rome. Contact her at alessandra.tedeschi@dblue.it.

Julian Williams is the chair of accounting and finance at the Durham University Business School. His research interests include applying quantitative risk management and capital investment techniques to areas such as the regulation of public utilities, securing critical infrastructure, and assessing techniques in treasury management, such as the issue of execution risk and open market operations by central banks. Williams received a PhD in finance from the University of Bath. Contact him at julian.williams@durham.ac.uk.