Review Article **Open Access**

Antonio Magliulo

Cyber Security and Tourism Competitiveness

DOI 10.1515/ejthr-2016-0015
received 10 January, 2016; accepted 5 May, 2016

Abstract: Until a few years ago, markets were basically physical spaces, more or less large, where sellers and buyers could meet. The exchanges happened through physical contacts at the local as well as the international level. Security meant, basically, to protect people against tangible threats (frauds, thefts etc.). Nowadays, we are facing a new challenge. Markets are mainly becoming a cyberspace where sellers, dealers and buyers can meet without the need for physical contact. Security also has to mean protecting people against cyber threats (internet frauds, identity thefts etc.). In this paper, we would like to deal with an issue that, maybe, has not attracted much attention from scholars, that is, the importance of cyber security for the development of tourism destinations.

Keywords: Cyber Security, Safety, Tourism, Destination, Italy

1 Introduction

Since Adam Smith we all know the importance of security for economic development. People wish and are able to exchange goods and services only if they feel themselves protected against violence and abuses of power; only if the State can guarantee their rights of liberty and property.

Without security a market economy cannot flourish. Until a few years ago, markets were basically physical spaces, more or less large, where sellers and buyers could meet. The exchanges happened through physical contacts at the local as well as the international level. Security meant, basically, to protect people against tangible threats (frauds, thefts etc.).

Nowadays, we are facing a new challenge. Markets are mainly becoming a cyberspace where sellers, dealers and buyers can meet without the need for physical contact. Security also has to mean protecting people against cyber threats (internet frauds, identity thefts ...).

This new challenge involves all the users of the cyberspace: public authorities, simple citizens, companies.

The European Union has been pursuing a long-term strategy, called Horizon 2020, aimed at promoting smart, sustainable and inclusive growth. One of the seven flagship initiatives concerns a 'digital agenda for Europe': the purpose is to build a single, secure, digital market for households and firms. All over the world, schools and universities are engaged in educational programmes aimed at raising the awareness (and skills) of citizens, and the organisations more exposed to cyber threats – like public administrations or banks – are implementing new security plans.

In this paper, we would like to deal with an issue that, maybe, has not attracted much attention from scholars, that is, the importance of cyber security for the development of tourism destinations.

The paper is structured as follows. In the next paragraph we will try to offer a quick sketch of security in the cyberspace. In the following one we will describe the relationships between security and tourism competitiveness. In the final one we will focus on the new challenge of cyber security for tourism destinations. The analysis will basically refer to Italy.

2 The Challenge of Cyber Security in Italy

First of all, it is important to make clear the meaning of the words we will use.

We usually distinguish between safety and security. Safety is protection against natural or accidental events while security means protection against intentional damages. For example, a city can be safe because there is

***Corresponding author: Antonio Magliulo,** Rome University of International Studies, Rome, Italy, Tel.: 0039 06 510777241 E-mail: antonio.magliulo@unint.eu.

The author wish to thank Giada Mainolfi and Fabio Masini for their precious comments. The usual disclaimer applies.

no risk of earthquakes and it can be secured because there is enough intelligence to prevent terroristic attacks.

With the term cyberspace we refer to the complex of all interconnected ICT hardware and software infrastructure, starting from the Internet and including data and mobile devices.

We consider cyber threats as the complex of malicious conducts that can be exercised in, throughout or against cyberspace.

There are four kinds of threats:

- Cybercrime: all malicious activities with a criminal intent carried out in cyberspace, such as Internet fraud, identity theft and stealing of data or intellectual property;
- Cyber espionage: undue acquisition of data, not necessarily of commercial value;
- Cyber terrorism: exploitations of systems' vulnerabilities with political aims;
- Cyber warfare: actions performed with the purpose of achieving a military advantage.

Some cyber attacks are economical motivations: they refer basically to cybercrimes. Other attacks are ideologically motivated: they mainly concern the remaining categories. For them we use the term Hacktivism[1].

It is very difficult to measure the size and the cost of the phenomenon, both because the operators are reluctant to give data about the attacks suffered and because experts still adopt different methodologies[2].

However, we are sure it is a growing phenomenon.

We will focus on cybercrime.

In 2012, Italy was globally ranked ninth for the spread of malware and fourth for the number of the infected PCs controlled by hackers (so-called botnets). In the latter category it occupied the first place in Europe (Sapienza Università di Roma, 2013: 11).

The only available statistics on the economic impact come from the private sector.

According to the Norton Cybercrime Report (September 2012), the number of victims in Italy in the previous 12 months was 8.9 million people amounting to about one-third of Internet users in 2012, with an average cost per person of 275 euros, more than the global average cost per person that is estimated to be 197 US dollars. Moreover, approximately 17% of adults have been victims of social or mobile cybercrime in 2012, and about 10% of social network users have had someone hack into their profile (Sapienza, University of Rome, 2013: 14).

Analysing a sample of Italian cyber attacks in 2012, Clusit (2013) shows that the government is still the most attacked sector and that Hacktivism remains the main activity (see Figures 1 and 2, cited by Sapienza, University of Rome, 2013: 11).

However, cybercrime is a growing threat. In 2012, attacks motivated by cybercrime grew more than those pertaining to Hacktivism (see Figure 2), and in future the threat will be stronger. In fact, although the percentage of people connected to the Internet in Italy is smaller than in other European countries (see Figure 3), the number of users has reached the high level of 33 million and the number of people actively connected to the Internet has consistently increased from 12 million in 2011 to 14.8 million in 2012.

According to the Sapienza Report, 'the development of apps and online services will bring more security

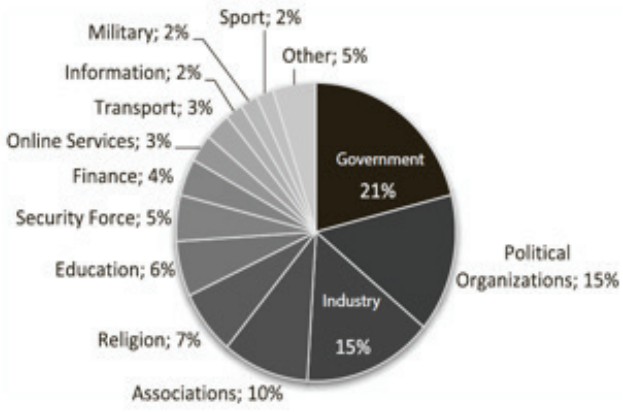

Figure 1: Sectorwise breakdown of number of attacks (percentage on 129 attacks analysed) in Italy

Note: Clusit (2013), Report on ICT security in Italy, Milan.

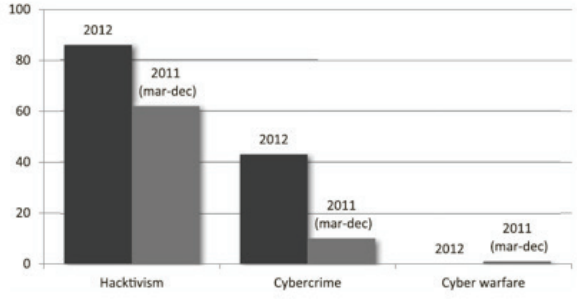

Figure 2: Evolution of cyber threat origins in Italy

Note: Ibidem.

1 See Clusit (2013), Sapienza, University of Rome (2013), Presidency of the Council of Ministers (2013).

2 Our analysis is mainly based on Clusit (2013) and Sapienza Università di Roma (2013).

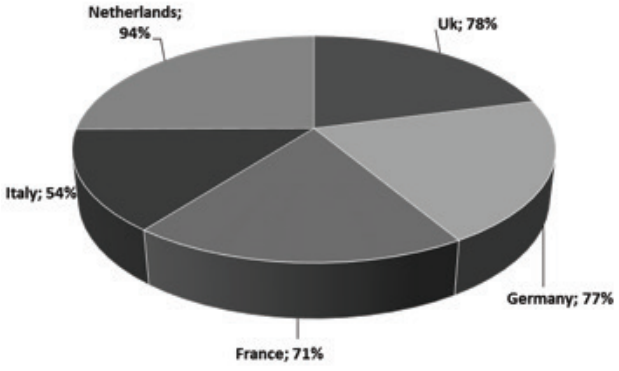

Figure 3: People networked with at least one device
Note: Audiweb (2012), Networking data, Milan, in www.audiweb.it

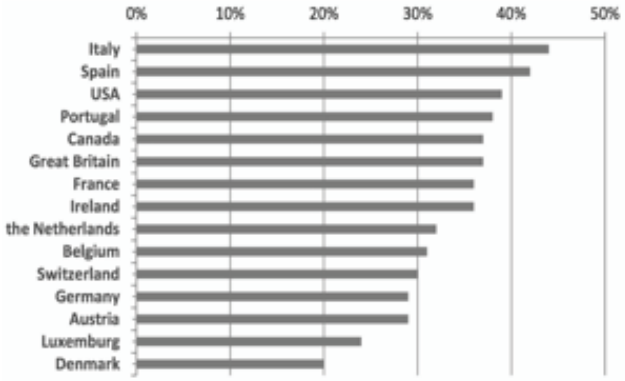

Figure 4: Percentage of personal computers attacked by malware while browsing the Internet
Note: Kasperskylab (2012), Malware attacks, in blog.kaspersky.lab

threats, because, thanks to online services, users perform many more operations directly from their device. Under attack is, therefore, the general public, public services, and business – especially the financial sector' (Sapienza Università di Roma, 2013: 11).

According to the same report, 'the main cause of the spread of attacks is the limited use of threat protection solutions. Only 33% of Italian users (the percentage rises to 44% on a global scale) actually use software able to ensure the necessary security of their data and only 45% of Italian users employ privacy settings to control the information they share with their contacts. In addition, 44% of users in Italy (about 40% in the world) do not use complex passwords or change their keywords frequently' (Sapienza Università di Roma, 2013: 12).

Why do Italians use limited protection solutions? The most shared answer is that there is still a low level of awareness about the risk associated with purchases through the Internet. The main evidence is that in Italy about 44% of PCs are attacked by malware while browsing the Internet, compared with 20% in Denmark (see Figure 4).

In order to analyse the Italian cyber security landscape, Sapienza Center has conducted a research on a sample of organisations that are more exposed to cyber attacks. An anonymous questionnaire was submitted to 68 organisations that were divided into four groups: Public Administrations, Firms of Public Utilities, Financial Organizations and Industrial Companies.

The results of the research have been summarised in a Cyber Security Readiness Index conceived to measure the capacity and willingness of an organisation to tackle cyber threats.

In the Sapienza Center's view, cyber security depends on four main elements measured throughout specific indexes. The four elements are: awareness, defence, policy and external dependency.

In particular:

The 'Awareness Index' assesses the situational awareness related to cyber risks faced by an organisation. It takes into consideration some variables: for example, if the company regularly registers anomalies or if it knows the security policy adopted by providers.

The 'Defence Index' assesses the capacity of an organisation to protect itself from a cyber attack. It considers if the company restricts the use of personal emails and cloud services or if it forbids the use of personal electronic equipments (laptop, smartphone, tablet).

The 'Policy Index' assesses the implementation of security-related policies. It refers to the use of Operator Security Plans or equivalent actions as defined in the Council Directive 2008/114/EC of 8 December 2008.

The 'External Independency Index' assesses the correlation between internal systems and external providers. It focuses on the existence of cloud services in supporting the core business of the organisation.

In general, the awareness declared by respondents is quite high (see Figure 5).

However, sometimes there is a gap between the actual and the perceived awareness. For example, in Public Administration, the actual awareness is measured taking into account some practical actions, which is lower than the declared awareness.

The Sapienza Report lists a series of policy recommendations. Basically, they aim at enhancing the four drivers of the cyber security. In the National Strategic Framework for Cyberspace Security, approved by the Italian Government in December 2013, we find a similar list. Both documents share a common view: the first action must be to raise awareness. According to the Sapienza Report: 'Fostering awareness among the population is a priority. No national strategy for cyber security can be implemented without a plan for dissemination

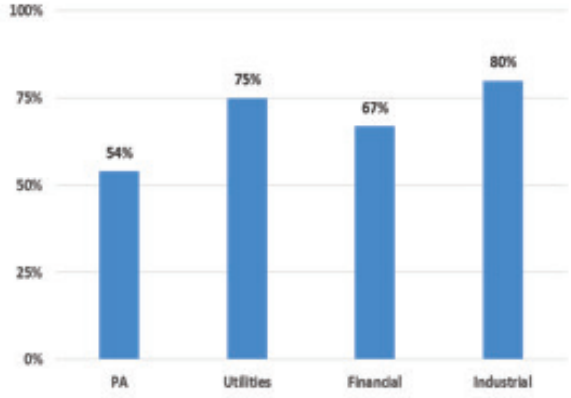

Figure 5: Question 'Do you have situational awareness on the state of cyber threats to your organisation?'

Note: Sapienza, University of Rome (2013), Cyber security awareness inquiry.

activities such as newspaper articles and debates in the mass media to increase awareness of ordinary people not necessarily involved in the protection of critical resources' (Sapienza Università di Roma, 2013: 58). The Italian government stresses the importance of promoting a 'Culture of Security among citizens and institutions, also leveraging the expertise of the academia, so as to raise awareness of the cyber threats among users' (Presidency of the Council of Ministers, 2013: 20).

In brief, cybercrime is an emerging threat for cyberspace and, thereby, for economic development. It requires an active policy primarily based on awareness.

3 The Relationship between Security and Tourism Destinations

The real tourism product is the destination.

A tourism destination is a large or small physical space with attractions. Tourists temporarily leave their usual place of residence and embark on a trip because they are attracted by a destination: natural, cultural, recreational or of another type[3].

Destinations can differ and be analysed in different ways. Perhaps the most important distinction to be drawn is that based on the nature of the product. There are corporate destinations and community destinations. The first are similar to businesses. Theme parks or ski resorts are, for example, corporate destinations: they offer just one (or mainly one) service, they target managers appointed by the owners and they pursue economic growth objectives that may potentially be shared by all those working there.

Community destinations, on the other hand, are territorial communities and have far more complex characteristics.

- They have variable boundaries. St. Moritz is a tourism destination, but so are the Canton of Graubünden, Switzerland and Europe. The borders are marked out by tourists. St. Moritz is mainly a destination for the Germans, French, English and Italians. It is not for the Chinese. No one would travel that far merely to visit St. Moritz and maybe not even to see the Canton of Graubünden and Switzerland. From the far East, people would come to visit Europe. Scholars speak of a 'sense-making phenomenon from a demand perspective'.
- They offer different goods and services. When a tourist spends a week in St. Moritz, he considers, overall, if the climate was pleasant, if there was plenty of snow, if lift services were efficient, if the roads were looked after, if hotels were comfortable and if the locals were welcoming... It is a blend of goods and services that are partly private and partly public and common.
- They are exposed to asymmetrical information. The consumer seeks to have an authentically human experience. He demands and evaluates as a whole the goods and the services offered in that place. Producers, instead, are busy packaging specific services: transport, intermediation or accommodation. No one knows, wants or indeed can package the destination as 'merchandise'.

The destination is therefore the tourism product that consumers demand and evaluate: whether it is a theme park or a ski resort. In corporate destinations, a business strategy can be more easilyidentified, aimed at promoting and marketing the only (or main) product sold. In community destinations, instead, we have a major coordination problem: who can convert a heterogeneous set of goods and services into a homogeneous product to be offered to tourists, and how can they do it?

Community destinations cannot use the visible hand of the private entrepreneur nor the invisible hand of the market. They cannot use the first because, by definition, they are communities in which a great many public and private entrepreneurs operate. There is no mayor or commissioner or hotelier who can force his vision on the rest. And nor can community destinations use the invisible hand of the market, which orders and arranges everything, because, as it has been extensively explained by the economists, the market fails and it is unable to

3 On the concept of tourism destination see Vanhove (2005) and Franch (2010).

allocate resources efficiently when there are public goods, common resources or asymmetries in information. So what then? How can we increase the competitiveness of a destination?[4].

According to the World Economic Forum (2013), the competitiveness of the national tourism systems is related to 14 Pillars: prices, natural resources, cultural resources … Among them, we find 'safety and security' (Pillar 3) and 'ICT infrastructure' (Pillar 9).

Safety and security are measured on the basis of the following parameters (World Economic Forum, 2013: 28):

- Business costs of terrorism
- Reliability of police services
- Business costs of crime and violence
- Road traffic accidents

ICT infrastructure is assessed with reference to the following factors (World Economic Forum, 2013: 29):

- ICT use for business-to-business transactions
- ICT use for business-to-consumer transactions
- Percentage of individuals using the InternetFixed telephone lines/100 pop.
- Broadband Internet subscribers/100 pop.
- Mobile telephone subscriptions/100 pop.
- Mobile broadband subscriptions/100 pop.

In the Travel & Tourism Competitiveness Index 2013, Italy ranks 26th on 140 economies covered. The authors of the Report argue: 'As well as its cultural richness — with many World Heritage Sites, international fairs and exhibitions, and rich creative industries — Italy's strengths lie in its excellent tourism infrastructure (tying with Austria for 1st place) and its relatively good air transport infrastructure (24th). However, it faces a number of challenges that bring its overall rating down. These include policy rules and regulations that are still not sufficiently supportive of the development of the sector (100th) and a lack of price competitiveness (134th)' (World Economic Forum, 2013: XIX).

Italy ranks 44th in safety and security and 31st in ICT infrastructure, performing worse than its direct competitors: France and Spain (World Economic Forum, 2013: 34, 37).

As we can see, there is no reference or stress to the cyber security. The World Economic Forum has chosen a classical idea of security understood as protection against tangible, physical (and intentional) damages. Actually, it is the same idea we find in the most recent and authoritative book on the topic. Tarlow (2014) correctly argues that in tourism it is difficult to distinguish between safety and security and prefers to use the term 'surety' understood as the maximum level of possible protection. He writes: 'although many academic disciplines make a clear distinction between security and safety, tourism scientists and professionals tend not to do so. Security is often seen as protection against a person or thing that seeks to do another harm. Safety is often defined as protecting people against unintended consequences of an involuntary nature. For example, a case of arson is a security issue, while a spontaneous fire is a safety issue. In the case of the travel and tourism industry, both a safety mishap and a security mishap can destroy not only a vacation, but the industry as well. It is for this reason that the two are combined into the term "tourism surety".' (Tarlow, 2014: 12)

Tarlow explores the topic of surety in the different fields of the tourism industry: accommodation, transportation, cruise, aquatic, public meetings. He also outlines an organic policy aimed at preventing and mitigating negative events (risk management and crisis recovery). However, in the book there are just few references to cyber security[5].

In brief, the competitiveness of tourism destinations depends on several factors, including security.

4 The New Challenge of Cyber Security for Tourism Destinations

On October 1st, 2012, for the first time, a European Cyber Security Month took place as a pilot project across Europe launched by ENISA. The slogan was: 'Be Aware, Be Secure'. The aim of the initiative was to promote cyber security awareness among citizens, to modify their perception of threats and to provide updated information through education, good practices and competition[6].

We believe that cyber security is a new challenge for the tourism economy too.

In fact, if the real tourism product is a destination, and if a destination is an amalgam (a basket) of different goods and services, then it is easy to realise that many of those goods and services are exposed to cyber threats. Let us imagine a typical journey. The tourist buys intermediaries, transportation and accommodation services. He

4 There is a huge literature on the concept of tourism competitiveness: see Magliulo (2013).

5 On tourism security see also Hall, Timothy & Duval (2003), Ritchie (2009), Scott, Laws & Prideaux (2010), Mansfeld & Pizam (2011) & Popescu (2011).

6 On the role of awareness in tourism security, see Magliulo & Wright (2014).

or she uses several apps and wi-fi devices. Each of these goods is exposed to a cyber threat.

Let us carefully look at the dynamics of the e-commerce (Clusit, 2013). In the main European countries the sector is growing speedily. In 2010, both Germany and France experienced a growth of 12% compared to 2011 and the United Kingdom of 11%. In Italy, the growth has been higher, 19%, and the first commodity sector has been tourism followed by apparel, insurance and consumer electronics.

According to the Clusit (2013: 91) 'the greater growth in Italy is not due to excellence, but to the significant delay accumulated in the previous times. The e-commerce Italian market value is a little more than 1/6 of the UK value and the half of the French' (see Figure 6).

Clusit lists the main reasons for the Italian delay: less than half of the whole population does Internet shopping compared with the European average; there are law barriers, the electronic payment tools are not commonly used and so on. It also points out the potentiality of growth: Italy 'is the second location for cell phone contracts in Europe, and adapting to the wide growth of the market of smartphones and tablets (respectively 45% and 96% in 2012), is developing a considerable opportunity for a second digital growth linked to the mobile' (Clusit, 2013: 92).

The Report outlines a series of measures for promoting e-commerce. Again, the key factor is the spread of a security culture: 'The missing link in the chain previously described is the culture of information security of the end users, which by the way confirm the success or not of e-commerce in general and of the tools used by it. Most of the frauds do not take advantage of the vulnerabilities of direct instruments but rather of the improper use made by those who have a lower level of security awareness' (Clusit, 2013: 94).

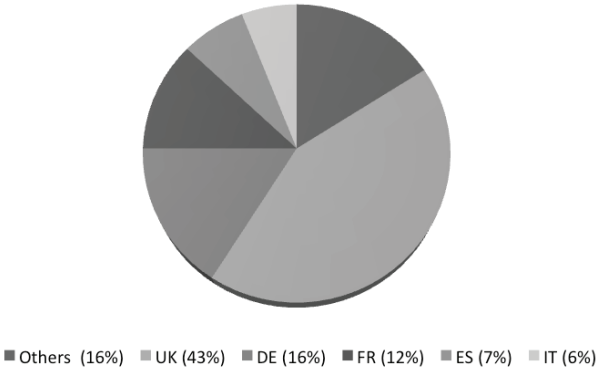

Figure 6: Partition of the e-commerce market in Europe - 2012
Note: Clusit (2013).

In order to assess and monitor the cyber security policy in tourism it could be interesting to elaborate some special tools. For example, the Sapienza inquiry could be extended to the tourism sector selecting a set of core firms and providing a Tourism Cyber Security Index. The core firms should be chosen in the following fields: intermediaries, transportation, accommodation and one type of tourism supply (seaside, mountain, arts etc.).

Moreover, the authors of the World Economic Forum Report could add some indicators that take into account – together with the physical safety and security – also, the cyber security dimension. For example, they could consider the following parameters:

- Percentage of PCs attacked by malware while browsing the Internet (see Sapienza Università di Roma, 2013: 13);
- Cybercrime cost as a percentage of GDP (see Center for Strategic and International Studies, 2014: 21);
- Reliability of cyber security policy (new research).

In brief, tourism destinations are exposed to cyber threats and have to adopt cyber security policies.

5 Conclusion

Now the time has come to offer an answer to our research question: why is cyber security so important for the competitiveness of tourism destinations?

Our answer is: because competitiveness depends on several factors including a concept of safety and security that must be extended to the cyberspace.

In fact, as we have seen: a) the destination, which is the real tourism product, offers a variety of goods and services mostly exposed to cyber threats. It is no more sufficient to protect tourists from physical attacks; b) the cyber threat is expanding over the entire economy including the tourism sector; c) the cyber threats can be tackled only with a new and larger policy built on a higher awareness among all stakeholders.

Tarlow correctly argued that in tourism it is difficult to distinguish between safety and security and it is more appropriate to use the term surety. In this paper, we have tried to show the relevance – close to the physical security – of cyber security. Maybe we should add that, even in this case, it is difficult to mark off the boundaries of the two dimensions as the attackers use also cyber tools in the physical space. Again, the first requirement is awareness: "Be Aware, Be Secure".

References

[1] Audiweb (2012), Networking data, Milan, in www.audiweb.it.
[2] Center for Strategic and International Studies (2014). Net Losses: Estimating the Global Cost of Cybercrime, Santa Clara: Mcafee, http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf
[3] Clusit (2013). 2013 Report on ICT Security in Italy, Milan, http://clusit.it/docs/Rapporto_Clusit%202013_ENG.pdf
[4] Franch, M. (2010). Marketing delle destinazioni turistiche, Milan: McGraw-Hill
[5] Hall, C.M., Timothy D.J. & Duval D.T. (2003) (Eds.). Safety and Security in Tourism: Relationships, Management, and Marketing, New York and London: Routledge
[6] ISDR (2004). Living with risk. A global review of disaster reduction initiatives, Geneva: United Nations
[7] Kasperskylab (2012), Malware attacks, in blog.kaspersky.lab
[8] Magliulo, A. (2013). A Model for the Sustainable Competitiveness of Tourism Destinations. European Journal of Tourism, Hospitality and Recreation, 2, pp. 7-26
[9] Magliulo, A. & Wright A.C. (2014). Cyber Security in Tourism: The Role of Awareness. In M. Sitek, I. Niedziółka, A. Ukleja [Eds.], Consumer Protection, Alcide De Gasperi University, Józefów 2014, pp. 71-96
[10] Mansfeld, Y. & Pizam A. (2011). Tourism, Security and Safety. From Theory to Practice, New York and London: Routledge
[11] Popescu, L. (2011). Safety and Security in Tourism. Case Study: Romania. Forum Geographic, 2, pp. 322-328
[12] Presidency of the Council of Ministers (2013). National Strategic Framework for Cyberspace Security, Rome, http://www.sicurezzanazionale.gov.it
[13] Ritchie, B.W. (2009). Crisis and Disaster Management for Tourism, Bristol: Channel View Publications
[14] Sapienza Università di Roma (2013) – Cyber Intelligence and Information Security Center, Italian Cyber Security Report 2013, Rome, http://www.dis.uniroma1.it/~midlab/articoli/13CIS-Report.pdf
[15] Scott, N., Laws, E. & Prideaux B. (2010). Safety and Security in Tourism. Recovery Marketing after Crises, New York and London: Routledge
[16] Tarlow, P.E. (2014). Tourism Security. Strategies for Effectively Managing Travel Risk and Safety, London: Elsevier
[17] Vanhove, N. (2005). The economics of tourism destinations, Butterworth-Heinemann: Elsevier
[18] World Economic Forum (2013). The Travel & Tourism Competitiveness Report 2013, Geneva

Antonio Magliulo (1962) is full professor of History of Economic Thought at the Rome University of International Studies where he also teaches Economics of Tourism and Culture. He is Dean of the Faculty of Economics and wrote several essays and books on the history of Italian economic thought, the relationships between economics and politics and the economics of tourism.