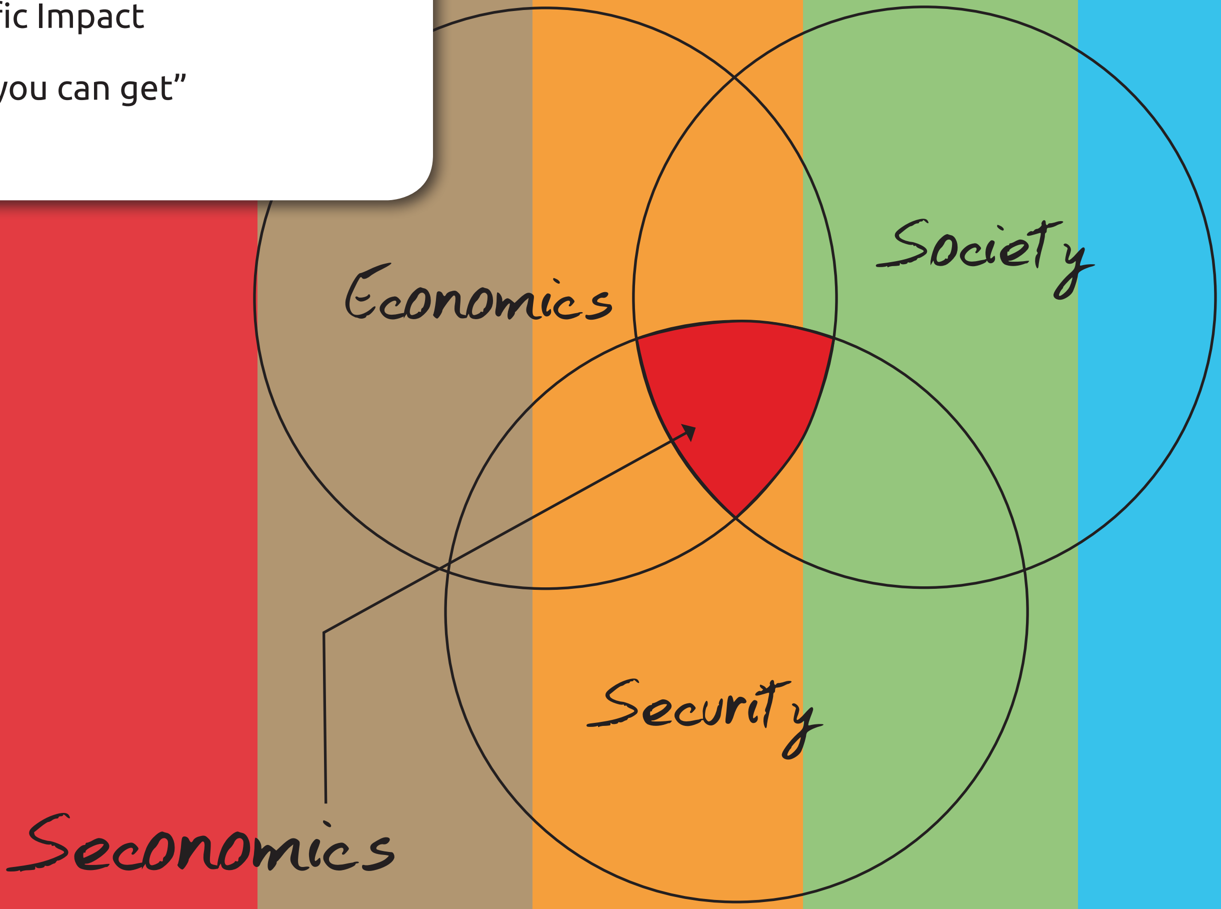
# SECONOMICS

Socio-economics meets Security

SECONOMICS synthesizes sociological, economic and security science into a usable, concrete, actionable knowledge for policy makers and social planners responsible for citizen's security

## White Paper

- What is SECONOMICS
- What we Managed to Produce
- Industrial Impact
- Scientific Impact
- "What you can get"



UNIVERSITÀ DEGLI STUDI DI TRENTO
DEEPBLUE consulting&research
Fraunhofer
Universidad Rey Juan Carlos
UNIVERSITY OF ABERDEEN
Durham University
TMB Transports Metropolitans de Barcelona
AtoS
SECURENOK
SOÚ Institute of Sociology of the Academy of Sciences of the Czech Republic
nationalgrid
ANADOLU UNIVERSITY

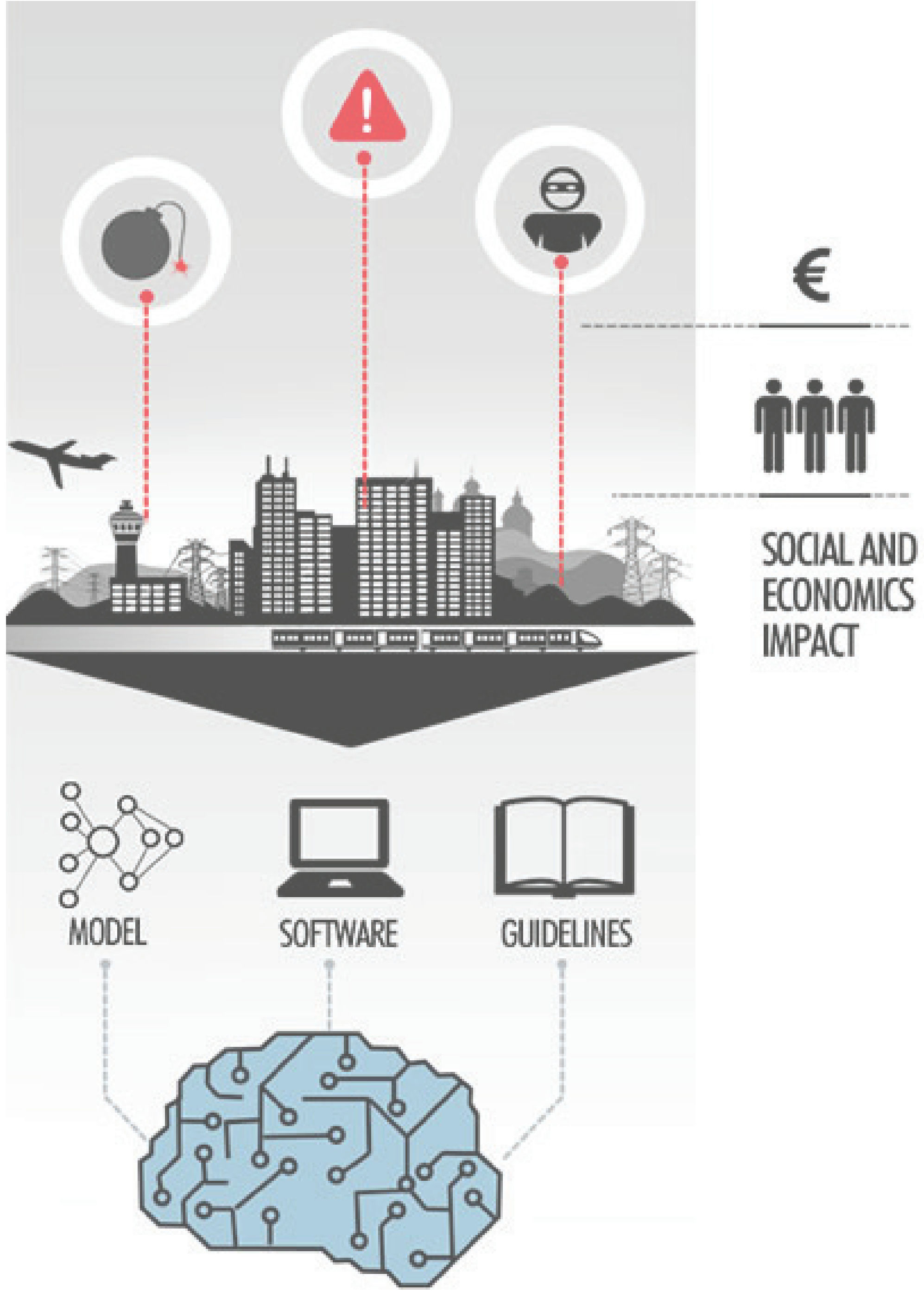
www.seconomicsproject.eu

# What is SECONOMICS

Security is a relatively nebulous concept and hence the quantification of the impact of a security policy at the public or operational level is similarly difficult to identify with any degree of certainty. In the past two decades there has been a movement away from ideologically driven policy approaches to the more nuanced idea of evidence driven policy. For many applications the evidence is often in the form of empirical results from scientific experiments. However, security policy has been resistant to the conventional evidence based policy development mechanisms for several reasons. First, the emotive nature of the subject, security in the broadest sense is a matter of life and death and when stakes are such as these a precautionary approach has prevailed. Second, the very nature of evidence in the security domain is filled with difficulties. Data collected on historical incidents cannot be relied on to paint a fair picture of the underlying drivers. Each security incident, be it in an airport, a train or in the provision of an important public utility has an almost unique set of circumstances under-pinning its realization. Furthermore, it is impossible for us to quantify using an empirical approach all of the incidents that did not happen due to a litany of factors many of which cannot be measured or even identified after the fact.

Into this difficult policy arena comes the SECONOMICs project. We approach the security problem from a foundational viewpoint, looking at the main technological, behavioural and social drivers of security risks and then incorporating this information into a menu of tools (our toolkit) that can be used by policy makers at operational and public policy levels to provide perspective on the potential impacts of their decisions.

SECONOMICS is an EU funded project which deals with issues such as the mitigation of potential security threats and the sustainability of security. The main objective of the project is to provide a direction to policy-makers seeking to understand their policy alternatives and the possible effects of these policies.



The project partners in SECONOMICS have conducted interdisciplinary studies in research areas of media analysis, the public economics of institutions and the quantitative operational research of organizations. In previous years, other projects have studied the security policy problems in an isolated manner which considered only one or two research areas. In SECONOMICS, we use a unique approach which combines the above-mentioned research areas all together. This allows the project to provide policy-makers with broader view and deeper insight in the security policy issues and solutions.

SECONOMICS has three scientific work packages: comparative media analysis of security, public policy and economics of security, and operational research on adversarial risk analysis. While each scientific work package can tackle the security policy issues and solutions separately, our aim in the project has been to generate coordinated and aggregated view on them.

The SECONOMICS approach is based around three industry driver case studies: Aviation, Critical National Infrastructure, and Regional and Urban Transport, these form our user case studies. The scientific work packages observe patterns of risk in the security setting for them and build reality models. These models are rich enough to capture the important effects from the patterns but tractable enough to make predictions.

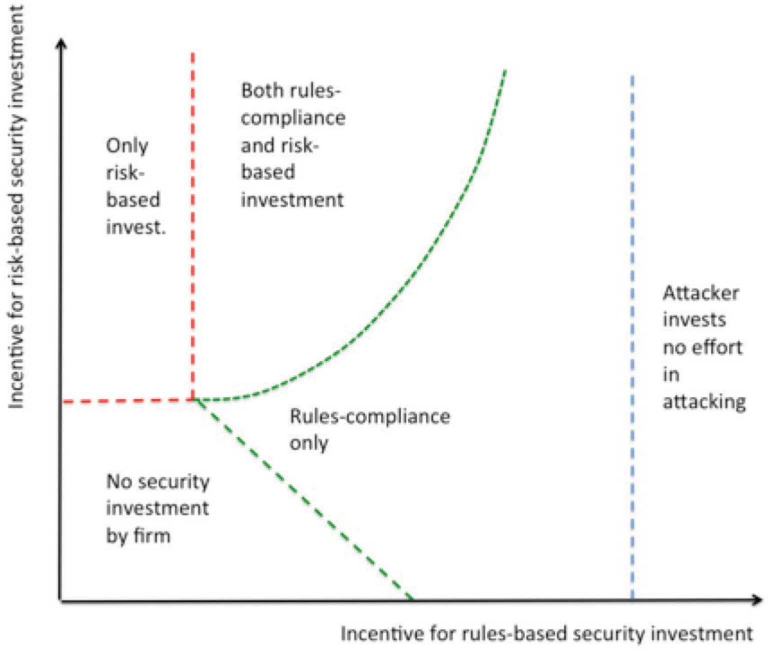
# What we Managed to Produce

## Practice & Methodology to interact with stakeholders

Policy makers are often in the unenviable position of having to make regulatory and investment decisions on security based on incomplete information about the risk structure, and unknown or unknowable preferences of their stakeholders.

The SECONOMICS project has generated various models that can be used in the decision and policy making processes in various critical infrastructure sectors. Although this can be helpful for stakeholders to design appropriate security strategies and policies, relying solely on theoretical approaches might not guarantee the validity of such strategies and policies in practice. The SECONOMICS project teams have therefore attempted to overcome the potential shortcomings in the theoretical models by including practical information and employing a battery of empirical and game theoretic methodologies in the process of the development of our SECONOMICs toolkit. In order to do this, we have used the various quantitative tools including comparative statics, workshops, case-control studies and media analysis. We have also tried to combine these methods together in the project to intensify the advantages and reduce the weaknesses of each method. Furthermore, the project has spared no efforts to interact with stakeholders in getting practical information and capture in-depth meaning of the information. Many meetings, conference calls, workshops and evaluation sessions have helped defining the requirements, validating the models and evaluating the outcomes

As a result, the project has been able to develop an interactive toolkit to provide a visualization of security strategies and policies which can then be validated in a practical setting. With our industrial case studies we have undertaken this task and part of the results of the project are in illustrating the benefits of our approach.


Incentive for risk-based security investment
Only risk-based invest.
Both rules-compliance and risk-based investment
Attacker invests no effort in attacking
Rules-compliance only
No security investment by firm
Incentive for rules-based security investment

## Models

We have produced various models in order to help the policy-makers to achieve their final goals. Those models have been integrated in a Matlab/Java interface that presents the information in a comprehensive and accessible manner.

## Adversarial Risk Analysis (ARA)

Extending and developing the methodology of Adversarial Risk Analysis (ARA) the project has produced a general methodology for security risk models.

Five template models were produced (simultaneous Defend-Attack, sequential Defend-Attack, sequential Defend-Attack-Defend, sequential Attack-Defend and sequential Defend-Attack with private information) which serve as backbone to build more complex and realistic models. Based on this, a number of enhancements were introduced considering different scenarios:

- Multiple attackers (coordinated or not) vs. multiple defenders (coordinated or not).
- Multiple targets to protect (be they independent, or with special configurations which take into account the underlying topology, like a network or a spatial distribution).
- Interactions between attackers and defenders not as streamlined as in the template models.
- Different rationality types expected among the attackers.

The more complex models were also validated considering additional cases oriented towards emergent threats such as terrorism in a railway service (networks), delinquency in cities (spatial distribution) and cybersecurity.

## Public Policy

Moving from the operational policy context provided by the ARA models it is important to utilize these insights for public policy. Simple scaling of operational models has, historically, proven to be almost impossible in most areas of economics. Our approach does mix "micro-foundations" into the policy frame, but we also address the downside of this approach by providing more abstract but policy focused models to help derive the optimal regulatory structures. Our models fall into three main categories:

- Models of multiple attacking agents in a Bayes-Nash equilibrium.
- Representative agent models in a sub-game perfect equilibrium.
- Models of heterogeneous agents that combine elements of the previous two modelling approaches.

We have used, in effect, all of the quantitative models in the economists' armoury. From those that incorporate time dynamics to those that are founded in a static equilibrium, to create counter-factual predictions that can be compared to reality in order to properly calibrate the models. In the main, each of these strategies have yielded materially similar results:

- Public policy is important in ensuring that the cost of security is fairly distributed.

- However, badly informed public policy can result in higher risks than when policy is absent.

- Cost sharing is inherently unfair, but sensible policy can mitigate this with little risk of the issues in the second point occurring (this is a typical mechanism design problem).

- The introduction of strategic attackers does substantively change some of the conventional results in public economics that are often used as a primary motivation for certain regulatory types.

- Mixed evidence from qualitative and empirical sources can be used effectively.

## Coding for salience

LWe have considered citizen's reaction to risks and their acceptance of security measures, interplay between security and risk in public opinion and attitudes, media framing of security and security technologies; examination of salience and acceptance of security measures, the tension between security and privacy, and mutual trade-offs of risks and security for citizens; as well as the identification of effective channels and patterns of communication on security and risk.

In the course of the SECONOMICS project, we have collected and analysed secondary quantitative data on risk perception and security, collected and analysed media debates on three security issues (3D body scanners, Stuxnet and CCTV) in 20 major dailies of 10 countries over a period of 40 months (from January 2010 to April 2013); synthetized media analysis results with customer surveys data (airport, public transport), customer complaints data (public transport), and expert interviews and ethnographic observation (airports), and developed conceptual models combining cost, profit & effects of individual security measures on customer acceptance/salience.

We have developed and applied instruments for qualitative comparative analysis of security issues in the media, in order to conduct in-depth qualitative and quantitative analysis of media coverage; created SECONOMICS media corpus (covering the issues and countries indicated above); constructed salience index and model of public acceptance of security measures and validated these with stakeholders and experts in aviation, urban public transport and critical national infrastructure domains.

## The Toolkit: Matlab/Java implementation of the model

Part of the outcomes of the SECONOMICs project is the toolkit. The toolkit is not simply the graphical interface of the SECONOMICs tool. The toolkit is the combined knowledge base developed throughout the project. However, it is worth reviewing the "front-end" of our work, which we refer to as "the-tool". Due to the high complexity of the threat scenarios and the different mathematical approaches the tool is divided in two major parts; first a powerful numerical engine like Matlab is needed. However, the engine does not provide easy to analyse results and as such we have created a second strand to the tool, a user interface in Java. The toolkit's Java interface hides the models' high complexity to the user and offers a self-explaining form where scenario-specific data can be entered. Finally, the graphical results presented can support a policy-maker taking essential decisions such as "How much money should be invested in security?" or "Which investment distribution will be the most promising one".

The toolkit considers Public Policy Models that incorporate mandatory and risk-based security investments, or also Adversarial Risk Analysis models which simulate the decisions of an attacker and hence compute the most effective defensive strategy.

## Price of Security

### Interdisciplinary Approaches to the Interplay between Security, Economy and Society

Petra Guasti
Zdenka Mansfeldová (eds.)
Price of Security
Interdisciplinary Approaches to the Interplay between Security, Economy and Society
Barbara Budrich Publishers

*Petra Guasti*
*Zdenka Mansfeldová (eds.)*

The dilemma of our times is the question of how much safety and security we want and at what price. The governments are seen as legitimate if they are able to resolve the tension between security and freedom to the general satisfaction of the people.

In this dilemma, the media play a critical role as an arena in which information is made available to the public, multiple claims and justifications are presented and discussed, and essentially opinions are formed.

Therefore, while the balance of security and freedom is the crucial task of contemporary governments, the role of critical media as a platform for public political discourse and as a guardian of freedoms is gaining considerable importance.

# Industrial Impact

## Airport

Aviation security is a strongly regulated domain. Regulations, mandatory procedures and internal rules to ensure Security standards compliance must be respected. The International Civil Aviation Organization (ICAO) specifies minimum standards which every country must satisfy in order to be a member (and, thus, to be permitted to have flights originating, terminating and transiting its own territory). Every Member State is required to build a civil aviation structure, which must satisfy the minimum standards and share it with the rest of the world. Members States can create a different organisation, as European Union Members did with the creation of the European Civil Aviation Conference (ECAC). Each Member State is required to draw up a National civil aviation Security Programme (NSP).

In SECONOMICS, we have involved stakeholders such as European Regulatory bodies (European Commission DG Move and Eurocontrol), International Industrial Associations (IATA and ACI Europe), National Civil Aviation Authorities for Security (ENAC in Italy and AESA in Spain), Airport Management Organisations (AERDORICA, SAGA, etc.), Airlines representatives and Air Navigation Service Providers

The SECONOMICS Toolkit validation was a comprehensive and integrated process evaluating and demonstrating, under realistic conditions, the Software Tool and the Policy Guidelines implemented. The Security Risk Model and the Economics & System Model were applied to the Airport Security domain and evaluated by the stakeholders as a coherent set of instruments with great efficacy and efficiency at security decision making and policy making levels.

## Critical National Infrastructure (CNI)

CNI providers are an example of organisations whose risks have potential impacts beyond the organisation on citizens and society. Governments have the responsibility of ensuring that those organisations identify, understand and appropriately mitigate the security risks.

National Grid, as the electricity transmitter in the UK, was the CNI provider selected; there are numerous risks to electricity transmission that affect everyone connected to it. The landscape of energy delivery is changing with the development and implementation of smart grids and SCADA systems becoming more complex and connected to the internet. As a result the threat landscape would increase in the future. In addition to this, the fast pace of IT innovation will provide future attackers with continually increasing means of attacking CNI. Consequently, an increasing range of threat actors with higher capabilities and motivation to attack CNI can be expected in the future.

Members of Digital Risk & Security (DR&S) Leadership in National Grid, the Centre for the Protection of National Infrastructure (CPNI) in the UK and the European Network of Transmission System Operators for Electricity (ENTSO-E) Cyber group gave robust feedback over a significant number of validation meetings and workshops and agreed that the underlying models of the developed toolkit inherently integrate the security, economic and social perspectives of CNI. The policies presented in the validation meetings, as part of the complete policy landscape covered, were considered applicable and relevant to the CNI industry by the key stakeholders.

## Transport

Regional and public transport is an area where security is closely integrated with the security model of the city. The laws and procedures applied in case of incidents are the same applied to other incidents in the city, but the conditions in a closed space make the risks more severe than in an open place. From the stakeholders' point of view, even though the security incidents have not changed too much in the recent years, the background has evolved significantly. Transnational organizations (e.g. organized fare evasion) are orchestrating criminal activities and the use of new information technologies and the proliferation of anti-social behaviour require a new approach to overcome these new security scenarios. Graffiti and vandalism are also clear concerns as they are becoming not only a regional or national issue but a transnational problem. Transport operators are affected by internationally organized crime networks traveling around Europe to "express their art". Graffiti is a growing trend in the transport sector that creates operational, financial and reputation losses

In SECONOMICS, we focused the case study in the metropolitan transport in Barcelona and involved other public transport operators, security entities such as the regional police of Catalonia and the International Association of Public Transport (UITP).

The SECONOMICS toolkit was introduced to these stakeholders in different phases using the "Good Practice" approach, on how scientific models can be introduced and used by policy makers for evidence-based policy making. Overall, they were very satisfied with the approach of how the best resource allocation for a specific situation was calculated. They agreed that the security risk models can be extended to other types of threats.

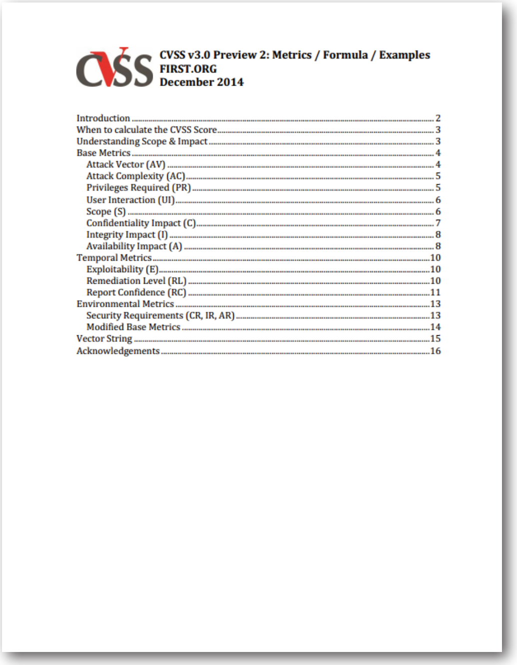
## Beyond the CNI case studies

The field of security needs the ultimate combination of research fields including public administration, economics, and social policy. While we use this combination to conduct the critical infrastructure case studies, the employed approaches in SECONOMICS can be generalized beyond these cases. In the project, we address various aspects of human behavior, such as how citizens perceive risks and how media communicates risk with them. We then implement an array of up-to-date approaches in game-theory, content analysis and adversarial risk analysis to link the evidence from human behavior with theoretical models. Finally, we validate the model outcomes with various stakeholders. This evidence-based approach is critical for security study since there are very few available natural experiments and direct experimentation, and hugely diversified preferences of stakeholders. The approach helps to understand how the previous policies have been built and how we can build policy recommendations in the future.

The security problems of our case studies also appear in other critical infrastructures (e.g., nuclear, financial, oil and gas, water supply, public health), sectors that – by definition – have a direct or indirect impact on citizens as well as a high political relevance. In all of these critical infrastructures, there is also the need for integrating policy and socioeconomic considerations into the security field. The SECONOMICS approach provides an evidence-based and holistic approach that can be applied to address other critical infrastructure security challenges. Through the exploitation of the toolkit with security experts and sector stakeholders, the SECONOMICS approach could customize and calibrate the models and scenarios of these new sectors.

## Security standards

SECONOMICS also contributed in the development of the third version of the Common Vulnerability Scoring System (CVSS v3), the worldwide standard for software vulnerability assessment. CVSS is widely used to manage the security of critical systems such as those managing financial transactions or power transmission. In the context of SECONOMICS we analysed patterns in vulnerability exploitation and developed a model of the "work-averse attacker" that has been instrumental in the development of the new version of the standard. In particular, UNITN was part of the CVSS First.org Special Interest Group and worked with industrial partners such as Intel, CISCO, IBM, Juniper and many others on its definition. Part of the work developed for SECONOMICS has been presented and discussed within the SIG, and the discussion resulted in a revised version of the standard that keeps into account SECONOMICS findings. The University of Trento will be acknowledged as a contributing author of the new standard, when released.



CVSS v3.0 Preview 2: Metrics / Formula / Examples
FIRST.ORG
December 2014

# Scientific Impact

By synthesizing sociological, economic and security science into a usable, concrete, actionable knowledge for citizen's security, SECONOMICS makes it possible for policy makers and social planners to better understand the current and emerging challenges in security and to develop a policy and a strategy from the point of view of pan European coordination.

## URJC

Concerning the academic impact of the ARA aspects of security risk, 11 papers and a monograph have been produced or about to be produced. Some of them have already appeared in major journals like Risk Analysis, Decision Analysis or Annals of Operations Research. Several sessions have been organised at major conferences like EURO-INFORMS or SRA-Europe, as well as invited talks and lectures have been given at major conferences such as ISBA, SRA and research canters like Bocconi, Coimbra or the Royal Academy of Sciences. The new materials developed have been incorporated into courses. Finally, one of the papers has been awarded as best paper by the Society for Risk Analysis; an AXA Cair in adversarial risk analysis has been awarded and invited talks will be delivered soon at major events like the BISP and GDRR conferences. 4 PhD students are working at the moment in problems related with ARA and various security aspects.

## ABDN

A key aspect of the project is is the lack of tractability in using historical data to drive policy in the absence of a theoretical basis. We show this to be a dangerous approach. The main causation factors are the numerous equilibrium states that may have generated the data. Without a very rich quantitative understanding of the various agents involved in generating security threats and hence generating the data, it is almost impossible to discern these mechanisms. What we can do is delineate the potential impact of changes in investment mandated by policy makers given a shift from one equilibrium state to another.

## UNITN

UNITN has conducted various studies for supporting policy makers in designing appropriate security policies. Specifically, in these studies, UNITN in cooperation with other project partners has developed various insights and recommendations for security policies. UNITN showed that the approach used for a security policy might not guarantee the effective of the policy and the economic fairness for market players, and suggested the future direction for an appropriate security policy. UNITN further developed a methodology to assess emerging security threats, particularly vulnerability risks, and identified highly cost-effective risk mitigation policies.

## UDUR

From an economic perspective the SECONOMICS project has provided an unparalleled opportunity to conduct qualitative studies on a variety of behavioral models of security. For instance, the policy modeling for critical infrastructure is an adaptation of models commonly applied to regulated industries with the element of security woven carefully into its structure. By addressing the strategic nature of the interaction with security threats this model illustrates that many of the standard results obtained from classical modeling of regulated industries need to be adjusted to account for the adversarial effect.

As an interesting point of note, we show that even if security expenditure is mandated to be increased, unless the institutional arrangements managing the expenditure are in place, then security outcomes may not necessarily improve, in fact in exceptional cases they may deteriorate. This result is exceptionally interesting and we have empirical examples from each of the case studies that suggest that this is a possibility. On a personal note, we have used extensively the foundational work of Jean Tirole throughout the course of this project, he has had a foundational impact on the theoretical research into regulated industries and the award of a Nobel Prize in Economics for his efforts was well deserved and reflects the contemporary importance of this type of work

## ISASCR

We have developed and applied instrument for qualitative comparative analysis of security issues in the media, in order to conduct in-depth qualitative and quantitative analysis of media coverage; constructed salience index and model of public acceptance of security measures and validated these with stakeholders from each of the case studies. By applying and advancing the methods of qualitative and quantitative research, we are able to fill the gap in the study of security and security risks by presenting a comparison of the unique data (media, survey, macro data) of transnational security issues in three areas of critical infrastructure (air transport, public transport and critical national infrastructures in form of energy provision networks)

# “What you can get”

SECONOMICS has produced a policy framework and toolkit that can effectively assist decision makers at a strategic-tactical level in identifying and reacting to critical infrastructures threats. The project has produced a general methodology that was fed with new research on objectives, risk perceptions and attitudes, budgetary and other constraints, to finally produce the best security resource allocation for an organisation willing to protect multiple targets against multiple threats.

The SECONOMICS service portfolio includes several lines of business: advice on optimal security measures, development of security models, deployment services, and training and maintenance services.

An analysis of the market based on global trends such as increased vulnerability, political concern and projections of new infrastructure investments indicates good prospects for security solutions. Those solutions include the following segments: video surveillance, biometrics, access control technologies, CBRN (chemical, biological, radiological, nuclear) detection and perimeter intrusion detection.

Most of the results will be exploited immediately by the academic community in courses and new research projects. Some models require validation prior to further exploitation, while other results are already adequately developed and are ready for commercialisation, for instance coding techniques for salience analysis in the media, models for public policy with mandatory and risk-based security investments, and model of public acceptance of security measures.

In summary, the results of the project will be of interest to any security manager, public policy-maker or analyst with responsibility for designing, implementing or documenting security policies in most contexts, be they cyber or physical.

➤ Foto by: Guillaume Paumier

# SECONOMICS

Socio-economics
meets Security

## Contact Info

Project Coordinator: Fabio Massacci
Università degli Studi di Trento
fabio.massacci@unitn.it

www.seconomicsproject.eu

@seconomics_eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285223