PRESS RELEASE

CYBECO: A project which will help to prevent cyber- attacks like WannaCry.

The project will analyse cybersecurity risks to advise major organisations in the selection of security countermeasures and cyber insurance.

The project is a collaboration between seven European institutions, and it is funded by the EU's H2020 RIA programme with two million Euros for two years.

Cybersecurity has become one of the most, yet still unresolved, critical issues for many businesses, institutions and public administrations dealing with a vast amount of information and increasingly interconnected. One example is the recent WannaCry ransomware, with which its creators hijacked more than 360.000 computers in 180 countries to later ask for a ransom price for their release, as reported by the Spanish National Cybersecurity Institute (INCIBE). With the objective of preventing this kind of attacks, emerges CYBECO (Supporting Cyberinsurance from a Behavioural Choice Perspective), a European research project.

The main objective is developing new mathematical models that provide tools and products, specifically insurance premiums, that help the deployment of more secure communication systems and networks. The need for implementing innovative solutions responds to a disturbing reality: cybernetic offensives against critical infrastructures – like hospitals, nuclear plants or airports – are more frequent, points out INCIBE. The number of attacks has increased from 63 in 2014 to 479 in 2016; and, only in the first quarter of 2017, it raised to 247 incidents.

The goal is to transfer the mathematical models that have been successfully applied in physical security into the cybersecurity field. To do so, the European Union, through the Horizon 2020 program, has granted them 2 million Euros for two years.

New risks of the digital society

Attacks like WannaCry can push business out of the market for a while, since many of their activities depend on information systems; furthermore, attackers can steal compromising information and, as a consequence, business could lose their reputation and, with that, customers or business opportunities. On the other hand, for systems support critical infrastructures, a power blackout throughout a part of the country or a contamination of the water supply in a certain area could be possible, a series of catastrophic risks related to the fact that the systems controlling these infrastructures have a strong digital component.

Mathematics enable the construction of models for risk analysis and adversarial risk analysis, which can be used for anticipating the types of attacks and their consequences in the virtual world. Specifically,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740920

models can determine the best countermeasures in each organisation for protecting against the attacks. To do so, the project applies techniques for anticipating the behaviour of individual decision-makers, for either the attackers – to determine the potential risks – or the owners of digital infrastructures and insurance – for improving their choice and their service offerings.

CYBECO started on the 1st of May, 2017. Project partners are institutions like Instituto de Ciencias Matemáticas (ICMAT – CSIC) from Spain, Intrasoft International S.A. (INTRASOFT) from Luxembourg, Devstat Servicios de Consultoría Estadística S.L. (DEVSTAT) from Spain, AXA Technology Services (AXA) from France, Technische Universiteit Delft (TU DELFT) from Netherlands, the University of Northumbria at Newcastle (UNN) from the United Kingdom. The project is coordinated by TREK Development S.A. (TREK) from Greece.

Each of the project partners has a specialised role. INTRASOFT will develop the software tool; DEVSTAT and UNN will conduct the behavioural and economic experiments; AXA will bring all their insurance expertise; TU DELFT will incorporate the 'cyber' aspects to the risk analysis model; ICMAT will develop the risk analysis models; and TREK will coordinate, manage the project, disseminate project results and define the exploitation strategy and plan of CYBECO.

Economics of Cybersecurity

This project is under the societal challenges pillar of Horizon 2020, the current macro program of the European Union for funding research and innovation activities. This plan aims to provide answers to seven challenges of the European society that have been identified as a priority. Among them, the digital security area and, more specifically, the economics of cybersecurity topic. Under this topic, the program encourages projects that take into account cybersecurity and its cost-benefit, as well as new business and incentive models.

Currently, there are three projects funded under this topic: CYBECO, SAINT (Systemic Analyzer in Network Threats) and HERMENEUT (Enterprises intangible Risks Management via Economic models based on Simulation of Modern Cyberattacks).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740920