Detecting and ANalysing TErrorist-related online contents and financing activities

Sprawozdania

Informacje na temat projektu

DANTE

Identyfikator umowy o grant: 700367

Strona internetowa projektu

DOI
10.3030/700367

Projekt został zamknięty

Data podpisania przez KE
19 Kwietnia 2016

Data rozpoczęcia
1 Września 2016

Data zakończenia
28 Lutego 2019

Finansowanie w ramach
Secure societies - Protecting freedom and security of Europe and its citizens

Koszt całkowity
€ 6 206 216,25

Wkład UE
€ 4 998 527,88

Koordynowany przez
ENGINEERING - INGEGNERIA INFORMATICA SPA
Italy

Periodic Reporting for period 2 - DANTE (Detecting and ANalysing TErrorist-related online contents and financing activities)

Okres sprawozdawczy: 2018-03-01 do 2019-02-28

Podsumowanie kontekstu i ogólnych celów projektu

DANTE project aims to deliver more effective, efficient, automated data mining and analytics solutions and an integrated system to detect, retrieve, collect and analyse huge amounts of heterogeneous and complex multimedia and multi-language terrorist-related contents, from the surface, deep web and dark nets. DANTE is also implementing a flexible and extensible framework able to support Intelligence for combating terrorist activities. DANTE is developing capabilities for gathering, tracking and analysing resources, messages, files and other relevant data exchanged online among terrorists for organise capillary propaganda campaigns, radicalisation activities and terrorist acts.

Main DANTE objectives can be summarised as follow:
O1: Increased knowledge on terrorism and raising funds; guidelines on counter-terrorism and intelligence
O2: Enhanced intelligence on Deep Web and Dark nets
O3: Evolution of automatic analysis and data mining tools for detection and monitoring of terrorist-related online contents and activities
O4: Innovative effective and efficient automated reasoning and knowledge mining tools and services
O5: Innovative TRL-7 collaborative system prototype supporting LEAs in intelligence activities
O6: Evaluation and demonstration in real operational environments
O7: Prepare the business exploitation of DANTE tools and services
O8: Adherence to privacy, ethical and legal requirements
O9: Raising awareness of DANTE results in LEAs

Prace wykonane od początku projektu do końca okresu sprawozdawczego oraz najważniejsze dotychczasowe rezultaty

During the first reporting period DANTE has deepened the phenomenological analysis highlighting trends and threats (WP2). Such study was conducted in close collaboration with the LEAs involved in the project and provided significant input for the overall conceptualisation of the system. In particular some common behaviours and terrorist practices have been identified fostering the user requirements elicitation and formalisation.
Taking care the user needs and requirements the system specifications and the DANTE System Architecture were defined (WP4).
Afterwards all technical work-packages has been addressed starting from the relevant sources discovery and datasets preparation (WP4). The selected sources and datasets have been used for crawlers and analysers training and customisation (WP5, WP6, WP7 and WP8). DANTE is currently analysing the following resource type: audio, image, video and textual contents. For each data type, suitable classifiers have been designed and trained. Textual analysis is performed in six different languages: English, French, Spanish, Portuguese, Italian and Arabic. All partners participated in an accurate video annotation process for enhancing video analysis and analytics LEAs capabilities in terrorist related object identification.
The overall user interfaces and widgets were designed. After the mockups validation (WP9), the development stage of the Collaborative Intelligence Applications was started as planned (WP10) and is still in place according to an iterative improving approach.

Pilot scenarios and pilot plans have been defined (WP11).
To ensure that DANTE system is respectful of European and National legislations on privacy, ethics and data protection, an assessment of all DANTE modules was prepared and performed during the first reporting period (WP3).
Particular attention was paid to the management of the EU-Restricted information. Education materials and guidelines have been prepared and a Security Advisory Board was established.Two educational sessions on EUCI management have been performed and an online EUCI management course was realised. It is available anytime on DANTE collaborative platform.
The dissemination activities (WP12) have been planned and are mainly regarding the active collaboration among the relevant projects funded in the context of H2020 security funded projects. Project results have been disseminated in many conferences, fairs and workshops. Scientific papers and online e-book were also realised.
A preliminary market analysis has been defined and preliminary collection of assets has been prepared by all technological partners.

Innowacyjność oraz oczekiwany potencjalny wpływ (w tym dotychczasowe znaczenie społeczno-gospodarcze i szersze implikacje społeczne projektu)

Progress beyond the state of the art

DANTE project aims to deliver the following main results:
- A set of innovative services for the automated detection and analysis of online multimedia and multi-language contents, relying on existing solutions, frameworks, and prototypes owned by the project partners or available as Open source software;
- A TRL-7 system prototype exploiting and integrating the functionalities and capabilities offered by the above-mentioned services: the system will deliver intelligence and collaboration applications as well analytics services for LEAs.

In particular, following end-users needs and LEAs requirements DANTE is focused on enhancing the state of the art and introducing potential innovation in:
1) Visual-based semantic concept detection
2) Audio analysis
3) Textual analysis
4) Knowledge Mining, Fusion and Intelligence Tools

Potential Impacts

The project is implementing the following automated functionalities able to provide LEAs with performing services for supporting, improving and speed up investigative activities:
1) To promptly find, monitor and manage sources of potentially relevant terrorist-related data in the surface Web;
2) To promptly find, monitor and manage sources of potentially relevant terrorist-related data in the

Deep Web, including the Dark Nets;
3) To accurately and promptly identify, analyse, assess, and filter potential terrorist-generated and terrorist-related multimedia data and contents in multiple languages;
4) To accurately classify, categorize, and group potential terrorist-related and/or terrorist-generated multimedia data and contents in multiple languages (including to group information from several sources that support same history, to isolate potential sources of “disinformation”, etc.);
5) To store and preserve captured “relevant” data in dedicated and secure data management infrastructures and repositories to enable and support further forensic analysis, respecting the chain of custody;
6) To accurately summarize relevant terrorist-related multimedia data and contents;
7) To promptly detect, identify, analyse, and monitor potential terrorist-related activities, with a special focus on raising funds.
8) To detect and identify potential undiscovered terrorists and terrorist-related individuals (including the mapping of digital identity and pseudonyms with physical identity, with the aim of finding the original author of or people mentioned in terrorist-related contents);
9) To accurately detect and identify potential undiscovered terrorism-related groups of people and online communities (i.e. global terrorist organizations, grassroots terrorist cells);
10) To perform large-scale temporal analysis of terrorism trends, by analysing the collected and extracted terrorism-related relevant events to achieve better understanding of terrorism phenomena (including automatic analysis of dissemination contents such as news, papers, reports, etc.).

Such functionalities, aimed at delivering a novel and breakthrough way of detecting, identifying and monitoring terrorist-related contents and activities on the Web, including the less accessible part.

DANTE conceptual view

Ostatnia aktualizacja: 9 Września 2019

Permalink: https://cordis.europa.eu/project/id/700367/reporting/pl