**PROJECT DETAILS**

**Project Title**

**Malware-oriented Detection Evasive Techniques for Terrorist Activity Recognition on the Web**

**Project Summary**

Nowadays, Law Enforcement Agencies face important challenges in how they identify and gather terrorist generated content online (i.e. on the web as social media). One of the main difficulties monitoring such content faces is the defensive methods used by the suspicious sites for crawlers, bots and other systems that automate the process of recognising Terrorists’ relevant material. These mechanisms include Intrusion Detection and Prevention Systems (IDPS).

In order to bridge this gap, the purpose of this research project will be to study and adopt techniques that are commonly used by malware but for bypassing the existing security technologies for the purpose of facilitating the process of terrorist activity recognition on the web and social media. In particular, the techniques that will be examined are the ones that are currently being used by well-known malware families in combination with recent related academic work. Bearing in mind the state of the art technology, new techniques that may be of use for detection evasion will be proposed. A human centric behaviour for crawlers, bots, and other Terrorist recognition systems will be introduced in order to avoid detection. Novel methods for evading botnet detection will be proposed, resulting in more evasive/robust systems capable of efficiently recognising terrorism-related activity. Low-bandwidth network traffic techniques will be applied so as not to alert the respective mechanisms. Novel methods using fuzzy techniques, machine learning, probabilistic models, semantic reasoning and game theory will be created to assess the nature of the defensive mechanisms in use and adapt the behaviour of the botnet to avoid detection specifically from these mechanisms. As a plethora of Security Systems nowadays use machine learning to respond to adaptive malware, solutions to this problem will be proposed. Specifically, the systems used for Activity Recognition on the Web will adapt to evolving and auto-learning security mechanisms, thus obfuscating the respective security mechanisms. Finally, these bypassing systems will be evaluated in real-environment settings and improved accordingly.

In conclusion, this research can be used as a valuable asset in the fight against terrorism. Security Agencies can use these techniques to increase accuracy towards actionable threat intelligence. At the same time, it will prove very meaningful from an academic perspective, as it approaches detection evasion from a different angle.

This research will be done in cooperation with the Multimedia Knowledge and Social Media Analytics Lab of ITI-CERTH.

**Academic Impact**

This research will examine detection evasion from the opposite angle. It will combine various techniques such as machine learning and game theory with the concepts of malware detection evasion in order to fight terrorism. In this process, entirely new methods for detection evasion will be proposed, that can be further developed and used in other projects that are related to surveillance as well, such as the de-anonymisation and attribution of terrorists (identity and/or location), or the simulation of terrorist behaviour in controlled forums or websites. Moreover, it can be used in projects related to the improvement of computer security against malware and/or botnets. The resulting techniques will be tested and evaluated in real environment applications by a team of scientists, which will further contribute to its academic impact by demonstrating their potential. Moreover, the fact that this project will combine academic aspects with a real application challenge (i.e. recognizing terrorist activity in the web and social media) will definitely add a new prospect to it.
**Societal Impact**

The results of the PhD will be techniques for detection evasion that can be used for supporting LEAs in identifying and revealing terrorist activity in the web and social media. Given the latest incidents of terrorism in Europe (e.g. Paris 2015), the benefits for the society from such technologies are very important since they can contribute in revealing on time terrorist activities and planning attacks. At the same time, Internet users' fundamental rights, such as freedom of expression and privacy will be protected through various measures.

Aside from its intended outcomes, however, the technologies presented in this project will provide insight on the vulnerabilities that attackers or organised crime could use against companies. This aspect may help maintain economic prosperity.

In short, it is envisaged that this project will have a positive societal impact, through the enhanced measures, tools and concepts to assist Law Enforcement Agencies to identify, gather and process terrorist information on the internet, leading to safer and more secure societal environments.

**Training Opportunities**

The student will be provided with a variety of research training opportunities. Being jointly supervised by Computing and MKLab of the ITI research institute, he/she will have significant opportunities to develop a broad range of transferable, interdisciplinary as well as research project management skills, as he/she will have the opportunity to participate in grant applications.

During the project the PhD student will be considered as a member of the Multimedia Knowledge and Social Media Analytics Lab (MKLab) (https://mklab.iti.gr) (i.e. having a double affiliation with the University of Bournemouth and ITI-CERTH). This means that he will have direct access to all the state of the art knowledge developed in MKLab through the close cooperation with other researchers, reuse of resources and tools, participation to common projects and preparation of publications. She/he will be involved in running FP7 and Horizon 2020 research projects in the area of cyber-security, such as HOMER and TENSOR in which he can develop research, management and IPR skills.

After the PhD is completed she/he will have the opportunity to continue working in MKLab as a post-doc researcher in relevant projects in order to further develop her/his career.

**SUPERVISORY TEAM**

<table>
<thead>
<tr>
<th>First Supervisor</th>
<th>Prof Vasilis Katos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Supervisors</td>
<td>Dr Ioannis Kompatsiaris, Dr Paul Yoo</td>
</tr>
</tbody>
</table>
| Recent publications by supervisors relevant to this project | K. Taha, P. D. Yoo, SIIMCO: A Forensic Investigation Tool for Identifying the Influential Members of a Criminal Organization, IEEE Trans. on Information Forensics & Security, 2016


### INFORMAL ENQUIRIES

To discuss this opportunity further, please contact Vasilis Katos via email: vkatos@bournemouth.ac.uk

### ELIGIBILITY CRITERIA

All candidates must satisfy the University’s minimum doctoral entry criteria for studentships of an honours degree at Upper Second Class (2:1) and/or an appropriate Masters degree. An IELTS (Academic) score of 6.5 minimum (or equivalent) is essential for candidates for whom English is not their first language.

### HOW TO APPLY

Please complete the online application form by **31/10/2016**. Further information on the application process can be found at: [www.bournemouth.ac.uk/studentships](http://www.bournemouth.ac.uk/studentships)