
CALL FOR PAPERS

Come and share your research at the

WEB SCIENCE CYBERCRIME/CYBERWARFARE WORKSHOP 2014

'Research Methodologies for analyzing Cybercrime and Cyberwarfare'

http://webscience-cybercrime-workshop.net

June 23rd, 2014

ACM Web Science Conference 2014
Indiana University, Bloomington, IN. USA – June 23-26 2014

Research Methodologies for analyzing Cybercrime and Cyberwarfare

Since the early days of Web Science, Cybercrime, Cyberwar and Darknet activities have proven to be great topics for innovative and relevant research. Criminal activities on the Web reflect deeply the violent aspects of modern society. Most of the risks of the offline world (aside from physical harm) are replicated on the Web. What is illegal offline is illegal online.

The Web enables us to transact and share globally; such activities are not confined to national borders, and so are not subject to clear national jurisdiction. Due to the large scale nature of the Web, illegal activities can be identified in many online human interactions, from money laundering to illegal surveillance, from drug dealing to the sale of weapons, from hacking to Cyberwar. Today, it is also possible to detect conjunctions between criminal activities online. For example, within the recent events in Syria, Cyberwarfare was conducted by an electronic army which is mainly composed of sub-networks of criminal hackers, organized crime groups and mercenaries, using crypto-currencies to obfuscate their funding sources.

A recent paper in the printed edition of The Economist claimed that 'big numbers and online crime go together, but few cybercrime surveys cite the methodology they used'. This detracts from the scientific method, reducing validity, reliability and repeatability of research. In the UK, Cybercrime has been recognized as a Tier 1 Threat, making it more important than ever to ensure that research into this area is thorough and accurate. However, given the diverse and transformative nature of cybercrime, quantifying such behavior can be truly challenging. Previous research into social structures of groups engaged in Cybercrime is suggesting that qualitative analysis might be more efficient than a data oriented quantitative approach.

The motivation behind this workshop is to gather together researchers from different disciplines and ask them to share and evaluate their methodologies. How do we measure the impact of Cybercrime? How do we identify Cyberattacks? What data regarding an attack needs to be collected, and how should that be done? What methods are relevant to detect influence or efficiency of people and technologies who work hard to avoid detection?

Here, it is important to mention that the workshop is not intended to focus on types of Cybercrime or Cybersecurity technologies. The Web Science researcher is interested in understanding the impact of the Web on society, and in observing how humans from around the World, in various contexts, use the Web to produce transformations on a large scale. This workshop will not be about fighting Cybercrime or fraudulent activities online, but about how the Web Science researcher should proceed, with an interdisciplinary approach, to identify, to understand, to measure and to reflect the reality of Cybercrime. What do we know for certain about Cybercrime & Cyberwarfare? Are we working towards designing methodologies that will help us gain a better understanding of the true situation?

Useful information:

This workshop will allow participants to present research experiences, good practices and ideas for analyzing Cybercrime and Cyberwarfare on the Web.

Papers will be peer reviewed by a select program committee.

Research papers are to be kept short, limited in length to 2 pages (in ACM template) and can be position papers or primary studies presenting methods used to study Cybercrime and Cyberwarfare.

At least one author of each paper is expected to register for the workshop and attend to present the paper.

Accepted proposal and papers will be given a 15-minute slot of which no more than 10 minutes will be used for presentation, the rest of the time will be available for questions and discussion.

Presentation material and research papers will be made available online on the Web Science Cybercrime / Cyberwar Workshop's website after the workshop.

We are expecting to receive up to 30 paper submissions, and plan to accept up to 8 papers.

- The submission deadline is April 20th, 2014
- Notification of acceptance is May 20th, 2014

The Call for Papers

Researchers wishing to present at the workshop should submit short research papers presenting finalized or ongoing research activities on the following topics:

- Cybercrime
- Darknet activities
- Cyberwarfare
- Cyberhacktivism

Research papers are to be kept short, limited in length to 2 pages (in ACM template) and can be position papers or primary studies presenting methods used to study cybercrime and cyberwarfare.

How to Submit?

Submission format:

- English Language
- Maximum 2 pages – 1000 words
- Word or PDF document

Paper submissions should be formatted according to the official ACM SIG proceedings template (http://www.acm.org/sigs/publications/proceedings-templates). Please make use of the ACM 1998 classification scheme (http://www.acm.org/about/class/1998/), and submit papers using EasyChair at

https://www.easychair.org/conferences/?conf=wscybercrime2014

Important dates

The submission deadline is April 20th
Notification of acceptance is May 20th

For more information and contact

http://webscience-cybercrime-workshop.net