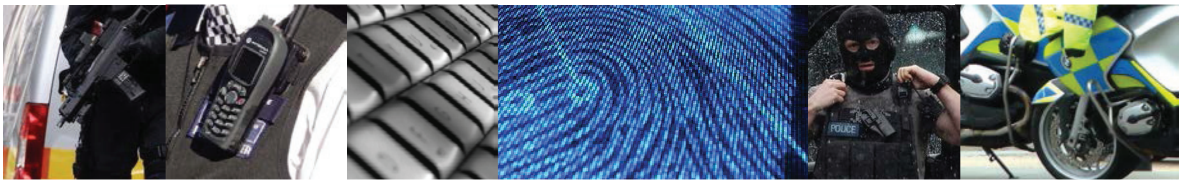
London First

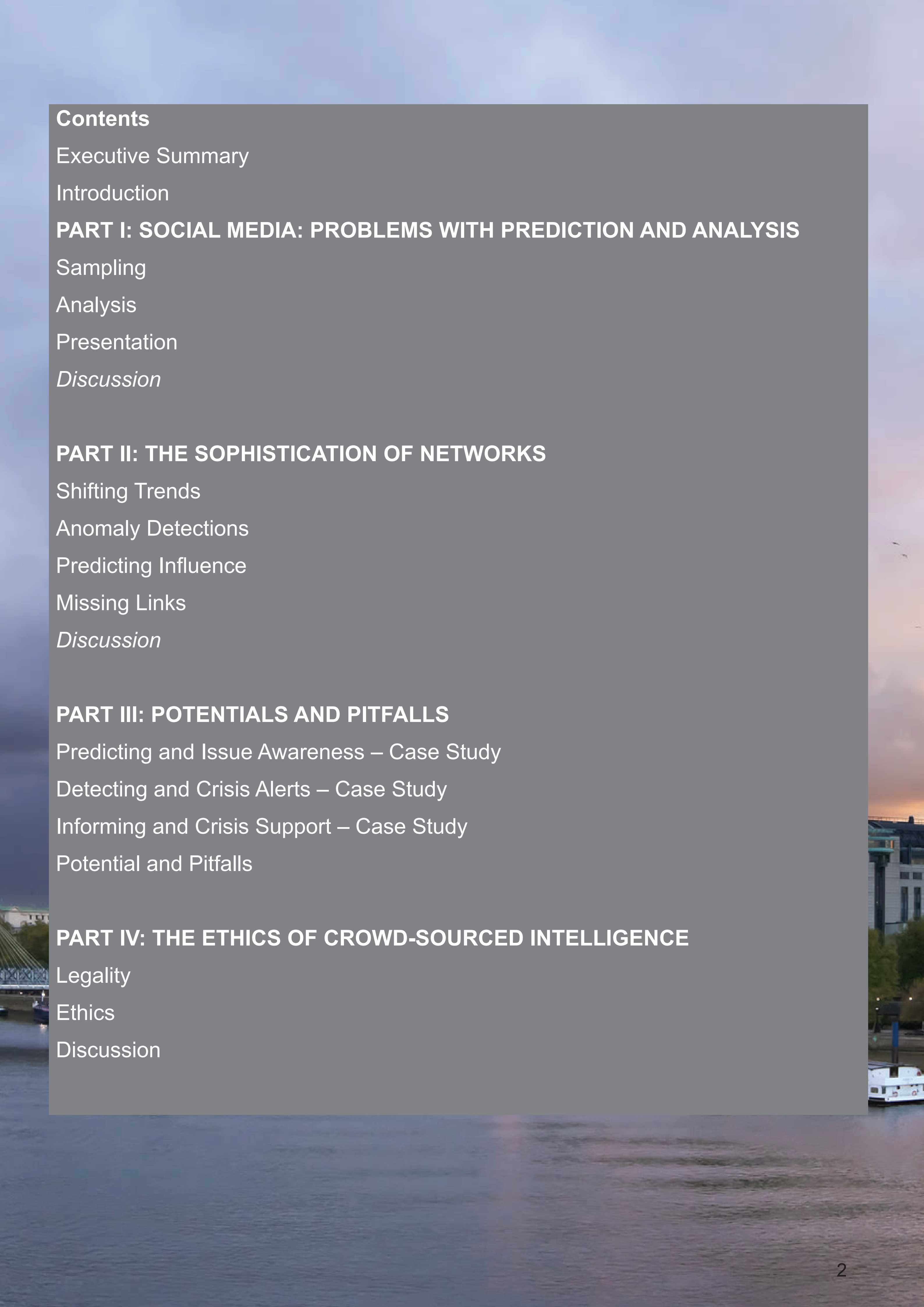
‘Crowd-sourced Intelligence: Potential and Pitfalls’

Roundtable – 26 September 2013

Sponsored and Hosted by Siemens and Trufflenet



London First



Contents

Executive Summary

Introduction

PART I: SOCIAL MEDIA: PROBLEMS WITH PREDICTION AND ANALYSIS

Sampling

Analysis

Presentation

Discussion

PART II: THE SOPHISTICATION OF NETWORKS

Shifting Trends

Anomaly Detections

Predicting Influence

Missing Links

Discussion

PART III: POTENTIALS AND PITFALLS

Predicting and Issue Awareness – Case Study

Detecting and Crisis Alerts – Case Study

Informing and Crisis Support – Case Study

Potential and Pitfalls

PART IV: THE ETHICS OF CROWD-SOURCED INTELLIGENCE

Legality

Ethics

Discussion

EXECUTIVE SUMMARY

- As the revolutionary era of social-media activity has taken hold, traditional rules relating to organisation, protocol, procedures and restrictions, have become a thing of the past. Every minute, 72 hours of video are uploaded on to Youtube, Instagram users share 3,600 new photos, Twitter users send over 170,000 tweets, Facebook users share nearly 700,000 pieces of content, and Google receives over three and a quarter million search queries.

- While the attitude of law-enforcement organisations towards crowd-sourced intelligence has been typically apprehensive, recent innovations in social science research which have made it possible to identify influential figures, and construct missing links within a network, now mean that the intelligence and engagement potential of social-media platforms is so vast that security organisations can no longer afford to ignore them.

- From an industry perspective, crowd-sourced intelligence has a number of useful applications and properties within a corporate environment. It can be used to determine corporate risk and act as an early warning system regarding long-term future risks, in addition to immediate crisis detection and support.

- However, while the potential of crowd-sourced intelligence holds a great deal of promise, concerns regarding the robustness and reliability of the data have grown. Departing from the traditional method of random probability population level polls, which have long since been regarded as an established and trusted method of data collection, the reliability of crowd-sourced intelligence is often met with apprehension.

- In addition to being easily manipulated and misread, it remains difficult to determine the demographic biases within crowd-sourced data and so the ability to make important security decisions based on the integrity of the data is undermined by a lack of rigour and certitude.

- More importantly, however, the context of privacy has been a subject of constant scrutiny and organisations need to consider the ethicality surrounding mission requirement, proportionality and legality of crowd-sourcing intelligence.

- Surveillance should correspond to a legitimate requirement and must be able to fulfil the specific need identified. Additionally, the need for surveillance must be weighed against any potential harm and organisations should always act in accordance with the provision of the law.

- Ultimately, organisations should strive for transparency, be as open as possible with the public about potential uses of data and, wherever possible, should seek their consent.

INTRODUCTION

On 26 September 2013 a roundtable was held by London First on the topic of ‘Crowd-sourced Intelligence: Potential & Pitfalls’. The event was kindly sponsored and hosted by Siemens and Trufflenet.

The aim of the event was to review the latest thinking and capabilities of social media to facilitate predicative analysis ahead of an event, detection at the start of an incident, and situational awareness immediately after an event. The roundtable also examined the potentials and pitfalls of use of social media in emergency response as well as the ethics and legality of the using social media.

The event was programmed around a series of short presentations from:

- **Jamie Bartlett**, Head, Violence and Extremist Programme, and Director, Centre for the Analysis of Social Media, Demos.
- **Professor Chris Hankin**, Director, Institute for Security Science and Technology, Imperial College London.
- **Kevin Savage**, Business Director, Trufflenet.
- **Dr Harvey Lewis**, Research Director, Data and Analytics, Deloitte.

The chairmen for the event, Robert Hall, Director of the Security & Resilience Network at London First, offered a welcome and introduction.

The following text is a non-verbatim recording of the proceedings and no attribution is or should be given to the remarks.

EMBRACING THE REVOLUTION

In the last decade, the advent of online social-media platforms has produced an unprecedented level of data and transformed the way in which information is accessed and exchanged. As this revolutionary era of social-media activity has taken hold, traditional rules relating to organisation, protocol, procedures and restrictions, have become a thing of the past.

While traditional attitudes towards crowd-sourced information from law-enforcement organisations have been typically apprehensive, as the number of Facebook subscribers reaches 1.1 billion and with over 400 million tweets being posted on Twitter every day, the intelligence and engagement potential of these social-media platforms is so vast that security organisations can no longer afford to ignore them. However, given the almost insurmountable quantities of information available through these communication mediums, the task of how to utilize these untapped resources remains a key challenge.