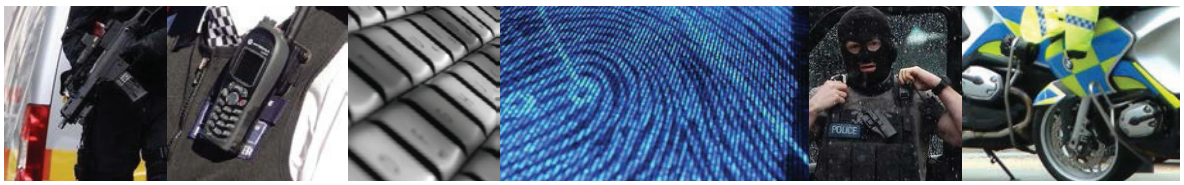
London First

‘Cyber-Intelligence and Cyber-Espionage’

Roundtable – 23 October 2013

Sponsored and Hosted by Avanta



CONTENTS

EXECUTIVE SUMMARY

- Today the biggest emerging threat to economic security and critical infrastructure comes directly from cyber-attacks and cyber-espionage. While state-sponsored cyber-strikes remain a deeply worrying prospect for governments, a larger proportion of cyber-offensives are committed against businesses, the detrimental potential of which should not be underestimated.

- The most serious and demanding scenario that can result from a cyber-attack occurs when one business is primarily targeted by a cyber-offensive but the effects of which are filtered through the supply chain via forward and backward spillages, producing what is known as cascading failure.

- Beyond the immediate logistical concerns of a cyber-attack, however, lies the larger issue of preserving public confidence. It is important that the public remain confident in the ability of business and industry to innovate, create wealth, and sufficiently protect and defend critical infrastructure.

- In order to achieve progress in a climate of mounting cyber-threats a change in approach is required. Conventional thinking, which has tackled cyber-warfare on a grand-scale, has proved to be sub-optimal. Applying strategies on a much smaller scale to terminology, numbers, and offensive capabilities holds considerably greater potential in the fight against cyber-crime.

- Terminology is not just an academic exercise. It shapes the way we think and assign importance as well as the way in which we assign responsibility within both companies and government. Cyber-crime is an incredibly wide-ranging problem and by using expressions such as cyber-war and cyber-security which encompass activities such as spear-phishing, espionage, and crime, the discussion is being held at a level of obstruction which avoids the finer details. This requires considerable attention if the problem of cyber-security is to be effectively tackled.

- Cyber-attacks are not created equal and should, therefore, not be considered as such. Any claims projecting 60,000 attacks per day should be distrusted given the variable nature of these incidents. These larger figures will almost certainly include system scans which are fundamentally different from a successful phishing attack. In order to use figures effectively, therefore, analysts need to alter their approach and look at the small number of incidents which have a high impact.

- When analysing high-impact attacks in terms of offensive capabilities in the most high-impact scenarios, we can operate within a working hypothesis: in order to maximise the impact of a sabotage tool on a specific target, the sabotage tool needs to be built as a bespoke piece of attack software. Therefore, as attackers increase the potential impact of their cyber-weapons, they, in effect, narrow the number of potential targets.

INTRODUCTION

On 23 October 2013 a round-table event was held by London First on the topic of 'Cyber-Intelligence and Cyber-Espionage'. The event was kindly sponsored and hosted by Avanta.

The aim of the event was to understand the world of 'cyber' which is moving at an ever increasing pace. The need to be able to sort rapidly through a mass of data to be able to forecast targeted dangers and attacks, and hence take pre-emptive action, is growing. Such cyber situational awareness depends on an ability to identify pertinent markers as well as to operate data-mining systems so that both the open and dark sides of the web are scanned. This roundtable examined the scale of what can be achieved in a commercial environment, and the practical, legal and regulatory issues that affect businesses. It also considered the threats posed by cyber-espionage from corporate competitors and foreign countries, and made recommendations on how best to minimise the potential losses.

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

- **Sir David Omand GCB**, Visiting Professor at Kings College London, former Security and Intelligence Co-ordinator and Permanent Secretary of the Home Office, and former Director of GCHQ.

- **Len Hynds**, Group CSO at MTG, former Head of UK's National High-Tech Crime Unit.

- **Dr Thomas Rid**, Reader, Department of War Studies, King's College London.

- **Tim Hind**, Director, EMEA Intelligence and Operations, iSIGHT Partners.

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.