15th March 2018

Mr Greg Rowett
Institute of Statecraft

SOCIAL MEDIA INVESTIGATION AND MONITORING PROPOSAL
SUBJECT: POISONING OF SERGEI SKRIPAL

Background

This proposal follows the recent poisoning of Sergei Skripal and his daughter in Salisbury. The requirement is to study social media activity in respect of the events that took place, how news spread and evaluate how the incident is being perceived in the UK, USA, France, Germany and Russia.

Objectives

1. Establish how news of the poisoning was and is being perceived across the UK, USA, France, Germany and Russia.

2. Establish the flow across social media of the messaging, and establish key influencers, friendly and anti, to HMG.

3. Undertake live monitoring of established identifiers and influencers.

4. Seek to provide early warning of identified threat to HMG or the UK.

5. Report on any intelligence that may be useful to the investigation.

The study will take place in two phases:

i. Conduct a retrospective social media study from the date of the poisoning incident. This will cover mainstream social outlets, but not be limited to Facebook, Twitter, Instagram, VK (Russian equivalent of Facebook), including blogs and forums.

ii. Undertake live monitoring of the response and ongoing developments in the investigation.

To undertake this work we will be utilising our state of the art social media monitoring service known as SENTINEL and our investigative platform known as SEEKER. SENTINEL has previously studied Russian issues such as hacking attacks by the known group Fancy Bear. From those attacks we have developed a library of the media outlets and social media accounts that are utilised to

quickly spread news stories that are part of a Russian government media strategy. This background knowledge, gained as recently as January 2018, will greatly assist this project proposal.

Following the imposition of sanctions and earlier perceived media attacks on Russian involvement, it is evident that a Russian State media strategy is brewing. Early deployment of these monitoring tools will greatly assist this study in ascertaining how the Russians seek to influence the countries identified in this proposal.

The output of the work will be provided in written report, infographics and, if necessary, PowerPoint to depict how the messages are spread.

The infographics will include country specific indications of social media activity and indications of the most influential people involved in messaging the story. Although not directly related to hard print media, this study will pick up the electronic involvement of major media outlets such as RT, Sputnik and TASS.

Introduction to Cyber Monitoring

SENTINEL is a state of the art cyber monitoring platform currently in use with US law enforcement agencies, Europol and the German Federal police. We are the only serviced management outlet in the UK. The system is operated by highly knowledgeable intelligence operators with experience in the UK and overseas. Their experience covers virtually every scenario, the key to which is the ability to turn information into actionable activity and analysis. The system can be applied to cover whole countries or regions. A typical investigation involves the analysis of hundreds of thousands of accounts; in this study, probably millions. Whilst the system is language agnostic, our analysts are fluent speakers in Russian, French and German.

What Does SENTINEL Do?

SENTINEL monitors and maps live social media feeds and other digital media inputs. It can be used to reveal, anticipate and analyse real-time reactions to events and to illuminate factors that influence your target audience.

SENTINEL maps out global networks and influencers, such as sympathisers of political ideologies and government media strategies.

SENTINEL automatically identifies key words and atmospherics, and highlights those unique individuals with the ability to influence others and the concepts they use.

SENTINEL legally collects and analyses live data and is a proactive flexible intelligence gathering tool. It should be considered as a standard atmospheric tool for intelligence development.

Timing

The study can commence immediately. Phase One is expected to take up to 5-10 working days. During this period, the second phase will commence as identifiers and influencers are established. Phase Two can be monitored live, or at regular intervals, to keep the target audience updated.

Costs

Phase One
The cost of this historic study dating back to the timing of the incident, establishing identifiers and influencers and preparing a report will be £7,500-£10,000, depending on the volume of activity uncovered.

Please note that the costs are inclusive of monitoring time, targeting, reporting and analysts deployed. It is expected millions of accounts will be examined.

Anticipated time: 75-100 hours.

Phase Two
Regular monitoring:

Daily - £200 per day
Weekly - £1,300 per week
Monthly - £3,000 per month

All prices are in GBP and subject to VAT.