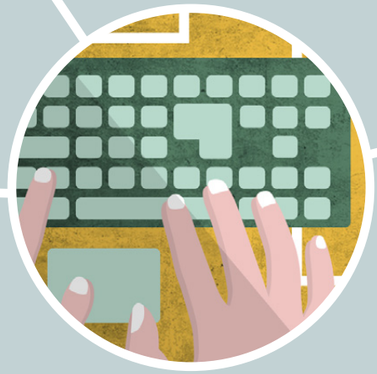

CYBER CRIME AND THE SOCIAL WEB

PETE BURNAP AND MATT WILLIAMS

Many of us spend significant amounts of time on the 'Social Web', the human-centred interactive ecosystem made up of mainstream and social media as well as interactive blogs and websites. However, emerging alongside the innovation that drives these new networks are equally dynamic cyber crime threats that challenge traditional approaches to policing. Criminal activity on the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated. Given the scale, international reach and open nature of the Social Web, law enforcement agencies struggle to meet an expectation of protection from the public.

Cyber crime can be thought of as both cyber dependent – crimes that require information and communications technology in order to be executed and cyber enabled – crimes whose scale or reach is increased by use of computer networks or other internet platforms. In the case of cyber dependent crime, Kaspersky Labs and Symantec anticipate a rise in cyber attacks conducted via social media. Examples of the cyber crimes emanating from this include denial of service attacks, phishing attacks and malware for the commission of network intrusion and cyber fraud. These crimes are an increasing problem for law enforcement agencies. We are seeing social media being increasingly adopted as a dissemination mechanism for hate speech and inciteful content. Both are unlawful in the UK and pose a threat of social unrest within communities, which has been linked to extremism and radicalisation.

For policing purposes, having intelligence on whether cyber threats are escalating or deescalating in frequency is crucial. Research into the quantification of these cyber and human factors has been the core objective of our work over the past 3 years. We have developed algorithms to classify and measure online reactions, and predict emerging threats to cyber (malware attacks) and human security (antagonistic social content) using data mining, machine learning and statistical modelling.

Criminal activity on the Social Web represents a new frontier for national and international security and crime fighting, yet such interactive spaces remain largely unregulated.

Online social networks (OSNs) (e.g., Twitter, Facebook, Tumblr) are inherently vulnerable to the risk of collective contagion and propagation of malicious viral material such as malware and antagonistic content following widely publicised emotive events. Our research on cyber hate following the attack on Drummer Lee Rigby found that it spiked for up to 36 hours on Twitter following the attack, dropping sharply after this period. We also found that it was possible to identify that the longest surviving narratives surrounding the attack were from the police, and far-right political groups. This type of measurement offers significant value to those seeking to observe and monitor levels of cyber hate in the immediate aftermath of a 'trigger' event, such as a terror attack.

We have also studied the behaviour of web links posted to Twitter during the Superbowl, Cricket World Cup, and European Football Championships, with the aim of identifying URLs that perform 'Drive by Downloads'. These occur when the URL endpoint is a server that contains a malicious script which, when executed, attempts to exploit a vulnerability in the browser or a plugin to perform malicious activity on the user's device. A prominent example of the injection of malicious URLs into OSNs is the Koobface worm. Koobface initially spread by using an infected machine to send messages to Facebook 'friends' of the infected user, which included a link to a third-party website that infected the machine of the user visiting it by installing malicious software. The worm was effectively executed on a number of OSNs due to the highly interconnected nature of these network's users. Research identified that current defences flagged only 27% of threats and took 4 days to respond. During this period, 81% of vulnerable users clicked on Koobface links. This highlights the requirement for real-time accurate classification of malicious URLs to limit the infection rate and damage inflicted on global IT infrastructure.

As the Social Web evolves policing authorities will need innovative and automated methods to successfully observe and manage dynamic, large-scale threats emerging from cyber criminals. In the UK, the government have ramped up efforts to tackle cyber crime in a collaborative way through a new National Cyber Security Centre, and the Metropolitan Police force has recently announced that it is to set up an 'Online Hate Crime Hub' to target online Hate Crime. These initiatives offer public and private-sector researchers the opportunity to develop the technological and interpretive techniques necessary to maximize the effectiveness of these national strategic centres. At the same time, ethical observation and the upholding of a fundamental principle of the Web, that 'it is for everyone', is absolutely necessary for the balance between appropriate policing and freedom of expression.

As the Social Web evolves policing authorities will need innovative and automated methods and infrastructure to successfully observe and manage dynamic, large-scale threats emerging from cyber criminals.

Dr Pete Burnap and Professor Matt Williams direct the Social Data Science Lab at Cardiff University. This is an Economic and Social Research Council (ESRC) 'Big Data' programme that brings together social, computer, political, health, statistical and mathematical scientists to study the methodological, theoretical, empirical and technical dimensions of new forms of data in social and policy contexts. Learn more about their research at http://socialdatalab.net