The need for concerted efforts for COVID-19 Intelligence Gathering: Medical Espionage and Cyber Crime Trends Analysis to Strengthen the UK's Pandemic Response

Professor Vladlena Benson, Aston Business School, UK

Two new cybercrime strands enabled through the Dark Web (DW) threaten the UK Government's fight against the pandemic:

- New cyber-attack strategies are formulated on the DW based around COVID-19 vulnerabilities. The coronavirus pandemic means that an unprecedented number of people are currently working from home. UK businesses are vulnerable to cybersecurity risks such as; IT arrangements for remote working may not be as secure and employees may be anxious about the ongoing pandemic, which could affect their judgment.
- Cybercriminals engaged in the DW sale of illicit drugs have diversified into COVID-19-related medical supplies and widened the espionage activities targeting pharmaceutical companies and policy makers.

Criminals actively exploit anxiety and uncertainty related to the pandemic. Action Fraud (the UK's National Fraud and Cyber Crime Reporting Centre) reported a 400 per cent increase in coronavirus-related fraud reports. A variety of new scams emerged targeting organisations and individuals including:

- Interactive COVID-19 maps and infographics containing spyware and various types of malware
- COVID-19 phishing scams, for example bogus emails appearing to be from a trusted source, requiring entry of login credentials or banking information as well as shopping scams for non-existent products (e.g. vaccines)
- Communications claiming to be from HM Government requesting donations to the NHS or research groups falsely asking for donations to the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO).
- Campaigns offering to take advantage of the economic downturn through investment schemes and trading advice
- Online shopping scams for products which have never been delivered (e.g. protective face-masks, hand-sanitiser).

The technological challenges faced by the UK Government against COVID-19 are significant. The data from the national **Prevent** initiatives confirm that NHS Counter Fraud Authority received 2,450 reports of COVID-19 related fraud, amounting to **£7,396,111** of losses (14/06/20[1]; this

[1] Mersey Internal Audit Agency (MIAA) l NHS Counter Fraud Authority (NHSCFA) l Government Counter Fraud Function l National Cyber Security Centre (NCSC) l Action Fraud (National Fraud Intelligence Bureau) l Metropolitan Police l Financial Conduct Authority (FCA) l Chartered Institute of Public Finance and Accountancy (CIPFA) l Chartered

figure has risen much higher). Fraud remains the most exposed COVID-related crime in the pandemic and the UK Government estimates a loss of up to **£21 billion** or 5% of the COVID stimulus package[2]. NHS requires support at the detection and prevention stages of COVID-related **serious** and **complex** cyber crimes[3], such as medical espionage, foreign-government-sponsored advanced persistent threats (e.g. APT29 July attack on UK organisations involved in developing a coronavirus vaccine) aimed at disruption of key NHS processes, medical trials and UK's efforts to develop a COVID vaccine.

The costs of COVID intellectual property lost to espionage is classified information in the UK, but US prosecution reports a Chinese case which "researched vulnerabilities in the networks of biotech and other firms publicly known for work on COVID-19 vaccines, treatments, and testing technology" and led to "losses of **100s of millions of dollars'** worth of trade secrets, intellectual property"[4]. Reconnaissance, planning, attack strategies and ultimately the spoils of cyber crime appear on the Dark Web (DW). In order for the UK Government to effectively combat serious cybercrime, effective tools are imperative to succeed in the NHS battle against COVID-19. The NHS efforts must be supported by developing advanced detection instruments and providing intelligence on serious COVID-related cyber crimes.

An important knowledge gap that needs bridging is the extent to which current natural language processing (NLP) tools, models and resources can be successfully applied to exploring a specific aspect of dark-web data such as COVID-19-related communication.

It is imperative to support law enforcement in gathering intelligence on the new COVID-19-related cybercrime strategies in the DW. The research gap around the DW search and textual analysis consists in the lack of robust mechanisms for querying, processing and monitoring trends on the DW. The critical data sets and computational solutions need to be made available for **immediate** exploitation and further research to strengthen the UK's pandemic response.

Trading Standards Institute (CTSI) l Citizens Advice Bureau (CAB) l Take Five
https://www.gmmh.nhs.uk/download.cfm?doc=docm93jijm4n7564.pdf&ver=10129

[2] https://www.miaa.nhs.uk/media/Briefings/Corona/Government_Counter_Fraud_Function_COVID-19_Newsletter_-_April_2020.pdf

[3] CPNI (2020) Espionage. https://www.cpni.gov.uk/espionage

[4] US charges Chinese Covid-19 research 'cyber-spies', BBC 21/07/20
https://www.bbc.co.uk/news/world-us-canada-53493028