Cyber Observatory: update OCTOBER 2020 - A Résumé of developments since October 2019

In November 2019 the UK launched a National Cyber Deception Laboratory, a joint venture between the UK MOD and Cranfield University. It is based at the UK defence Academy in Oxfordshire. This is an up-dated approach to an old military technique; make the enemy look elsewhere, or make them believe what they are seeing is the true picture. This method enables network defenders to direct intruders away from the 'Crown Jewels', by creating 'honeypots'

Advances in Artificial Intelligence means that automation has the potential to reduce the cost of creating and monitoring defensive deceptions. The focus of defensive deception in the cyber domain is likely to shift towards actions which shape an adversary's understanding of the situation, affecting their subsequent behaviour.

*S*ince the last formal report of WG Cyber, there has been an increase of reporting on the dangers posed to western societies by the proliferation of privately held data. **In January 2020**, *Jane's* reported concern about the breadth and depth of data held by private companies. This concern was sparked by the acquisition of Fitbit by Google. The connection between tech companies and the healthcare sector potentially opens the door to personal electronic health records. This development echoes earlier concerns about personal privacy and individual liberty, as well as raising a more important concern about the accumulation of large amounts of data by 'data controllers'.

The matter of concern in the security arena is the tendency for hostile actors to identify and target dissidents, or people of interest via their personal data. The risk of inadvertent data breaches attracts the civil liberties lobby; the risk of backdoors into technology, or into research facilities is increased. Tech companies themselves risk the kind of insider threat that traditionally faces defence or research establishments. Insiders can use employee credentials to access e-mail addresses, I P addresses and dates of birth.

In June 2020 the European External Action Service (EEAS) stepped up the activities of its Rapid Alert System (RAS) to address disinformation about the Covid 19 pandemic. The RAS was launched in March 2019 by the EEAS, and managed by its Strategic Communications and Information Analysis Division. In February 2020 the WHO Director General Dr Tedros Adhanom Ghebreyseus spoke at the Munich Security Conference, declaring "We're not just fighting an epidemic; we're fighting an infodemic."

Since 2015 the European Council has been concerned at Russian disinformation efforts, and in September 2015 the East StratCom Task Force (ESTF) was stood up. Initially its efforts were designed to counter Russian disinformation aimed at eastern EU Member States. In 2018 the EU published an 'Action Plan against Disinformation'. It is reported that the overall budget for the EU's StratCom effort to address disinformation is EUR 6 Million.

In October 2020, the newly appointed head of the UK Internal Security Agency (MI5) reported to media that the National Cyber Security Centre, part of GCHQ, had identified Russian efforts to penetrate UK institutions linked to Covid 19 vaccine research. This was linked by attempts by Russian based social

media operatives to discredit western efforts to develop a vaccine, labelling it 'monkey medicine' to spark a boycott of any vaccine, when it is eventually developed.

In **October 2020** the former UK national Security Adviser, Mark Sedwill, acknowledged that the UK had taken action directed against associates of Vladimir Putin, using 'discrete methods to disrupt the illicit cash flows of high level associates. It was also announced that GCHQ along with other Allied agencies had blocked Russian plans to disrupt the opening ceremony of the Tokyo Olympics (which were cancelled due to the Covid 19 pandemic). Up until now, GCHQ has only acknowledged attacks directed against Islamic State; blocking access to data and disrupting cash transactions. MMM

Discussion: The 'fusion' of technology and data is not new. What seems to be new is the pace of change. Even before the onset of the Covid 19 pandemic, the connection between data, cyber intrusion and disinformation, was changing the strategic landscape. It is important to remember the Chinese saying; '*the way to win a war is by not having to fight it'* (rough translation!)

At the European level the EU is taking measures to protect civil society, by preventing the exacerbation of economic and social difficulties being used to promote division. The best defence of a free and open society is by constant vigilance supported by transparent governance. For this reason the integrity of the democratic process must be protected, as much as Critical National Infrastructure.

There may yet be legal measures taken in the US against monopolistic behaviour by the major tech giants; on 24th October the FT reported that the Department of Justice had launched an action against Google. The Federal Trade Commission has been investigating Facebook, and several States are considering probes into Amazon and Apple. The European Commission has previously taken action against monopolistic behaviour by big IT companies.

Citizens must be confident about the balance of rights and security. They must also be confident that where there is bad behaviour, there are remedies in either the civil or criminal courts. Likewise, societies must enable Security agencies and their defence forces to act to safeguard their National Interests. The EU and NATO continue to develop their co-operation, in a rapidly changing world.

It is worth remembering the difference between 'hard' power and 'soft' power; hard power compels, soft power attracts. Europe's strength lies in its attraction as an open society, but it must be realistic about the motivation of so-called 'strong men' and disruptors. Often they are seeking to divert attention from failings in their own societies.

Cyber security and Information Operations should now be considered an integral part of the arsenal of western democracies.

NPW 27 10 20