1. INTRODUCTION

1.1 This is a further submission from the Manchester Metropolitan University following the Committee's inquiry on Cybersecurity and Critical National Infrastructure. This further submission arises to address the Committee's inquiries with respect to national security capabilities and threat appraisal in respect of hostile threats to the United Kingdom in the cyber sphere. This submission provides assistance to the Committee in respect of those terms of reference only.

2. CYBERSECURITY AND DEMOCRATIC IMPLICATIONS

2.1 In November 2016 and subsequent months, the world was left in awe when it was discovered that Russian sponsored social engineers had interfered with the election of the US president by hacking into a Democratic Union computer in order to tip the scales of the election. There is no suggestion here on whether Donald Trump or any other US official knew about what was taking place, the incident is cited merely to exemplify how powerful "keyboard warriors" have become. It is possible, for instance, to circulate fake news in order to influence social media users with posts containing false and alarmist information. This did, in 2014, appear to involve the United Kingdom during the EU referendum when fake news and propaganda was circulated not just by political parties seeking certain outcomes, but by other nation states wishing to influence UK voters so that a decision would be taken of benefit to that nation state.

2.2 Events over the past twelve months shows that the ongoing implementation of the National Security Strategy and Strategic Defence and Security Review has inclination to buy down risk in some areas while underrating other areas of risk. We say that little work has been done to address the issues of interference in elections and the increased cyber attacks on businesses by hostile states and criminal groups.

2.3 The year 2017 has seen a series of key European elections. The growing cyber threat to elections from hostile states takes many forms, from propaganda and disinformation to hacking and denial of service attacks. There seems to be a broad consensus from the US to Europe that Russia has attempted to meddle with voters decisions either as a state or through criminal gangs originating from that state. These fears are renewed with every election, e.g., the upcoming
Czech Republic presidential elections [1], which demonstrates the ineffectiveness of provisions taken by governments to combat such threats. As the UK uses paper ballots, a cyber attack on voting systems is highly unlikely to occur. While the GCHQ and NCSC are making efforts to securing voters identification data and personal data assets, there is still concern about leak of internal emails from individuals, constituency offices and pressure groups amongst others [2]. The House of Commons email security breach is one such example.

2.4 The sources of threats to voters are not only from hostile states. As the latest US elections showed, but fake news websites have been traced to teenagers motivated by earning money from advertising [3]. Disinformation and propaganda threats place voters as the most vulnerable target. Despite the prominence of the disinformation fears in Germany, France and elsewhere in the world, the UK government did not take active measures to protecting our democracy from these threats, particularly during the EU referendum. The UK government has not been as particularly explicit as their German peers in addressing propaganda and disinformation that may not only influence voters decisions, but also spread conflict in our society and aggravate divisions on critical issues such as immigration, Brexit and external aid.

3. BUSINESS IMPACT

3.1 Another area where the government security strategy has not been successful is the reduction of cyber attacks on UK businesses. As of April 2017, a survey commissioned by the Department of Culture, Media and Sport revealed that 52% of small businesses and 66% of medium-sized businesses reported identifying at least one cybersecurity breach in the past 12 months [4]. Small businesses accounted for 99.3% of all private sector businesses at the start of 2017 and 99.9% were small or medium-sized (SMEs), and the total employment in SMEs was 16.1 million; 60% of all private sector employment in the UK and the combined annual turnover of SMEs was £1.9 trillion, 51% of all private sector turnover in the UK [5]. Yet, the authors believe that SMEs are likely to have limited resources to devote to cyber security and few personnel to react to threats to critical IT systems. The NCSC is already making a significant contribution to SMEs cyber protection by making threat information readily available to help protect them. The introduction of GDPR will surely help SMEs to establish data security policy and awareness around the importance of cybersecurity. However, we believe that knowing and having cyber defence technologies alone is not enough and this is exactly where help is needed from the government. SMEs need help to adopt and maintain real-time security approach to cover all attack routes.

3.2 Until the UK establishes stronger defences of our cyber space and takes the necessary measures to prevent future external influence campaigns, the UK’s democratic system will remain vulnerable. The UK national security and defence strategy must maintain cyber warfare as a primary security concern in the review of national security capabilities. To support institutions in enhancing their cyber defence capabilities in the presence of skills and resource shortages, the government should establish regional quick reaction units for information security. Government institutions, local authorities and political parties must identify sources of threats and improve their cyber defences as part of, we say, a mandatory strategy in each locality. Moreover, the cyber defence policy should highlight the demand of a new independent information monitoring think tank or organisation should be setup to call out and correct disinformation. Finally, to gain the public confidence and to limit the effectiveness of propaganda and disinformation attacks, political parties should pledge not to use any information obtained through leaks or hacks in election campaigns.
4. SIGNALS INTELLIGENCE AND SECURITY DIFFICULTIES

4.1 The massive increase in uptake of ubiquitous devices means that a twofold problem has emerged. Firstly, ubiquitous devices can be used for signalling by nation states, organised criminals and terrorists. Secondly, ubiquitous devices are by definition very unusual and unique, potentially implementing very complex cryptographic technologies. This creates difficulties for signals intelligence capabilities because, particularly taking into account the rapid development and change cycle in ubiquitous devices, such devices are very difficult to scope and analyse for potential sources of access to intelligence. Much of this is owed to the fact that ubiquitous devices change very quickly and can be both physically and virtually difficult to access.

4.2 We are aware of public statements about increased investment in research and development within MI5 and GCHQ, but we would argue that given the pace of the development of cyberwarfare technologies, this needs to be at a significantly greater level of investment than it currently is. This is not necessarily so that such intelligence services can respond to a specific device, but because they need the resources to react very quickly to the emergence of new technologies and devices that could make it impossible to prevent catastrophic attacks on the United Kingdom as a result of a failure to access vital intelligence.

5. DEVELOPMENT OF NEW TECHNOLOGIES

5.1 In our recent submission to the Committee in our response to its Critical National Infrastructure Inquiry, we pointed out that many current technologies rely on statistical induction, rules and otherwise heuristic analysis. As a mathematical fundamental, these technologies cannot prevent 100% of all threats to infrastructure and likewise this allows intelligence agencies, for example, the capability of penetrating systems through the 1% rule. That is to say, the statistical margin of failure is enlarged and exploited.

5.2 Investment in technology capabilities to protect national security are required in both offensive and defensive technologies. Defensive technologies are now very slowly implementing the zero trust security paradigm, which means systems are being designed on the basis that every user is malicious in order to mitigate the 1% rule. Thus, the United Kingdom needs to invest significantly in defensive technologies to implement zero trust. More importantly, it needs to develop offensive technologies able to meet intelligence needs whilst addressing the fact that in the future, it may not be possible to penetrate distributed computer systems and more conventional means may need to be developed in order to protect UK national security. By way of illustration, in the future, cyberattacks may require a significant degree of coordination on the ground as well as in the cybersphere for virtual intelligence activities to be feasible in any defensive or offensive capacity. This is why major investment is urgently required.

REFERENCES

1 Czech’s Fear Russian Fake News in Presidential Election - Financial Times Link
2 UK Political Parties at Risk of Russian Cyberattacks The Independent Link
3 The City Getting Rich from Fake News – BBC News Link
4 Cybersecurity Breaches Survey, HM Government. Link
5 Federation of Small Businesses - Report Link