'Hello, world'[1]: GCHQ, Twitter and social media engagement

Liam McLoughlin, Stephen Ward and Daniel W. B. Lomas

School of Arts and Media, The University of Salford, Salford, Greater Manchester, M5 4WT

Twitter: @SourceMerlin @Leelum @SalfordUni_PCH

Liam McLoughlin is a doctoral student at the University of Salford, and has recently submitted his PhD on political representation and social media in the UK. His research interests centre on political social media engagement and participation. He is also communications officer for the Political Studies Association Early Career Network (@psa_ecn).

Dr Stephen Ward is a Reader in Politics at the University of Salford. His research interests centre on the use of internet and social media by political organisations notably around political campaigning, participation and mobilisation. He has over 60 publications focused on parties, MPs and public participation online.

Dr. Dan Lomas is author of *Intelligence, Security and the Attlee Governments, 1945 – 1951* published by Manchester University Press (2016) and nominated for the 2018 Royal Historical Society's Whitfield Prize, teaching on intelligence and security issues at the University of Salford. His research looks at intelligence, security and policymaking in Britain.

Word count: 9624

Disclosure Statement: The authors have nothing to declare.

Acknowledgements

We would like to thank colleagues and anonymous friends who helped inspire research in this field.

Key words: Twitter, social media, GCHQ, BAME, MI6, MI5

[1] "'Hello, world": GCHQ has officially joined Twitter' < https://www.gchq.gov.uk/news-article/hello-world-gchq-has-officially-joined-twitter > (accessed 12 December 2018).

Research Note:

'Hello, world'[i]: GCHQ, Twitter and social media engagement

ABSTRACT: In May 2016, Britain's signals intelligence agency the Government Communications Headquarters (GCHQ) joined the social media platform Twitter with the message 'Hello, world'. For an agency once seen as the UK's 'most secret', GCHQ's moved to social media received significant attention from the press and other social media, often resulting in ridicule or clichés around the 'Big Brother' state. But why the move and what has been the impact? Can GCHQ's use of Twitter provide lessons for other agencies considering adopting this method? The article suggests that, while certainly welcome, and allowing the agency to reach out to a new tech-savvy generation of potential recruits, while questioning stereotypes of what GCHQ does, efforts towards openness can only go so far and sometimes stoke and amplify conspiracy theories affecting issues such as brand identity.

Introduction

In May 2016, GCHQ announced its social media presence to the public with the simple tweet "hello world" – a traditional phrase beloved of computer programmers when introducing new programmes to public view. In the following few days the tweet attracted significant coverage, (and ridicule), in the mainstream media – with many commenting on the apparent disjuncture of supposedly highly secretive agencies on public networks. Whilst other parts of government, and even the intelligence and security agencies, have had a long-established online presence with open job advertising and websites, the arrival of intelligence agencies on social media symbolically suggested a new more open era. Did it signify an acknowledgement in the post-Snowden era of the need to engage and rebuild public trust or, as cynics commented, a more superficial PR driven exercise? In fact, in the case of GCHQ, the social media account has more specific aims in terms of recruitment and a geographical restructuring of GCHQ.[ii] However, as we will also note, there are perhaps unintended consequences in types of audience that have been attracted – notably as the focal point for conspiracy theorists and opponents of state intelligence agencies.

Whilst there has been considerable focus on the private uses of internet surveillance and big data to achieve intelligence objectives, the public presence of security agencies has attracted minimal academic attention. Hence, in this research, we explore this public presence via GCHQ's Twitter platform, concentrating on three particular aspects: Strategy – in particular we review some of the reasons why they have public presence i.e. what they are seeking to achieve? Content – how GCHQ attempt to achieve this i.e. what sort of content are they delivering online and to what ends? Audience – how successful are they in engaging with either wider public audiences or specific targeted groups and who are trying to engage with them? To do this, we reviewed public documents linked to Intelligence agencies social media activities

to understand their stated objectives. Then in order to see whether such objectives might be met, we gathered Twitter output from, and audience response to, the GCHQ platform. In short, what does GCHQ tweet about and why and who makes up the audience? The results indicate a somewhat mixed picture. At one level, there has been a relatively smooth transition into the social media public world with a platform providing regular GCHQ related content. However, exploration of the Twitter audience and their response to GCHQ is illustrative of difficulties of such government agencies operating in a highly public sphere which is often seen as intensely polarised and where demands for constant authenticity and openness are often met with scepticism, cynicism and hostility.

Government Organisations and Social Media Presence: Why Bother?

The social media presence of government departments and agencies is part of longer history of gradual adaptation to the internet. E-government programmes, created in the 1990s, often initially led to criticisms that governments were merely replicating their offline activities online, or just dumping information online with little thought as to its purpose.[iii] Latterly, however, and especially with the growth of social media, we have seen more consideration of how social media might reshape, or reconnect, the relationship between the public and governments.[iv] Because of the unique role and position of intelligence and security agencies, it difficult to find a clear counterpart in other parts of government in terms of social media strategy and usage. They provide public service, but unlike other government agencies these services are not really individualised or publically measurable. Nevertheless, it is worth acknowledging the broad reasons why Government organisations engage with social media because, in doing so, it underlines the rather unique challenges that GCHQ faces in a very public social sphere. In essence, government social media presence tends to revolve around key functions:

- Providing information on policy: At a basic level, government seeks to use social media to inform the public of what they are doing, how they are implementing policy and changes to the operation in how they work.
- Delivering services online: clearly much of government is involved in service provision. Over the past two decades many government services have moved online to provide ease of access for citizens and increase their efficiency and lower the costs of service delivery.[v]
- Interacting and engaging with the public: the interactive possibilities of technology provide opportunities for government to gather feedback and respond to public questions and criticism. This even goes as far as to suggest that the public can reshape or co-produce policy through regular interaction online.[vi]
- Impression management: Social media arguably allows organisations to communicate their message more directly to audiences without relying on the potentially distorting prism of mainstream media. Hence, there is the ability for organisations and institutions to shape their

messages, control their image, market themselves, and ultimate to create a brand image with the public.[vii]

- Building consent and legitimacy? The four factors outlined above could be argued to serve a further benefit – strengthening trust, or, at least, consent from the public.[viii] Hence, the online presence of government departments could also be seen as humanising bureaucracies notably through the personalisation of interactions and storytelling for audiences. Transparency, the use of humour, presenting the dilemmas of governmental activity and acknowledging criticism are all part of this process.[ix]

All of these basic functions, however, present some obvious, (and some less obvious), difficulties for intelligence agencies. Whilst they can provide information about their broad function, it is clearly difficult for them to detail much of their work. Equally, while they could be seen as providing public service, (public protection), in a general sense, again the covert nature of work means this is not individualised or, easily, publically measurable. Interaction, conversation and dialogue are also problematic, since staff cannot be identified. Moreover, such organisations have never engaged in direct relationships with the public. Yet, the move into social media could be seen as a partial response to rebuilding trust in the wake of Snowden revelations, at least by allowing a public face to the organisation [see below]. However, the basic difficulties outlined above, mean that intelligence agencies are always likely to be circumscribed in what they can achieve. As we shall see, therefore, the focus of social media accounts becomes more limited and, arguably, less well defined.

Intelligence Community and Social Media Strategies: From Private to Public?

Of course, the use of social media by intelligence-security agencies is not new. In the UK, social media has presented the 'intelligence family' with new opportunities to understand, and respond to, security issues, with social media spaces 'significantly relevant to security and public safety'.[x] Social media intelligence or 'SOCMINT' joins human intelligence (HUMINT), signals intelligence (SIGINT) and imagery intelligence (IMINT) as an important tool for agencies, even if it could be argued that SOCMINT is an off-shoot of traditional open source information, rather than a separate entity.[xi] While the use of social media as a surveillance tool requires a sound statutory footing, with clarity and transparency needed over its use, Sir David Omand, former GCHQ Director and the UK's first Security & Intelligence Coordinator, argues that SOCMINT is important for 'identifying criminal activity; giving early warning of disorder and threats to the public; or building situational awareness in rapidly changing situations'.[xii] Social media has also become the frontline in the so-called 'Post-Truth' or 'Fake News' era, with algorithms used to tailor news and propaganda to individuals, with the digital world used to 'shift popular mood without recourse to the clunkier tools of old-fashioned propaganda'.[xiii] But social media is more than just a tool to monitor and

shape public understanding; it allows intelligence agencies to engage, rather than traditionally hide from public debate, while also offering avenues to target and recruit a new, much younger, and tech-savvy generation of entrants. In the UK, both the London-based National Cyber Security Centre (NCSC), the part of GCHQ charged with protecting public and private networks, developing academic and private cyber capability, and disseminating online security knowledge[xiv], and GCHQ use Twitter, respectively joining in November 2015 and January 2016. Understandably, given their different remits, both use social media in different ways, although they acknowledge the importance of having a social media presence. NCSC also uses the business and employment-ordinated LinkedIn platform, while GCHQ uses the Facebook owned picture and video-sharing service, Instagram, even if Twitter is the largest social media platform for both NCSC and GCHQ. In October 2019, NCSC joined GCHQ on Instagram, announcing 'It's time to get a new generation excited about cyber security. If we want to speak to a younger, more female and more diverse demographic we have to be where they are, so we are delighted to announce that from today we are now on Instagram! #ThreeYearsOn'.[xv]

In the case of GCHQ, the use of Twitter provoked media attention after the agency shared its first post 'Hello, world' in May 2016. 'Given its remit to monitor electronic communications, you would imagine the intelligence agency was already on the social media site. But now it's tweeting', reported *BBC News*, while *The Guardian* reported that the feed, having come after months of discussion, was 'part of an effort to make the secretive Cheltenham listening post slightly more transparent and improve its public image', even if initial reaction to the account was 'mockery'.[xvi] Former Deputy Prime Minister John Prescott tweeted, 'After years of following us, we can now follow them!' – a theme reflected across social media reaction, with BBC Security Correspondent Gordon Corera tweeting, 'In a reversal, lots of people on Twitter are now wondering why they are NOT being followed by @GCHQ -although it is following James Bond'.[xvii] *The Financial Times* ran with the habitual Le Carré reference, 'Tinker, tailor, tweeter, spy'[xviii], while satire site *Daily Mash* shared an article claiming the agency was on Twitter to ask 'if anyone has any terrorist stuff going on this weekend'.[xix] The media surprise at GCHQ's new online 'openness' was perhaps a response to the traditional secrecy that surrounded the organisation's work. GCHQ was long considered to be the most secret of Britain's agencies, only begrudgingly avowed in 1982 following the case of KGB spy Geoffrey Prime, and officially placed on the statute books (alongside Britain's foreign intelligence agency the Secret Intelligence Service) by the Intelligence Services Act in 1994, starting an increasing trajectory of public engagement and avowal.[xx] But why use social media, and why now?

The use of social media by intelligence agencies was not actually new, especially in the United States. Indeed, the use of social media generally in government had already been firmly established on the other side of the Atlantic, especially following the announcement of Barack Obama's Open Government Initiative and Directive.[xxi] Social media allowed federal agencies, Michael Landon-Murray writes, to effectively 'meet people "where they are", with the frequently posited benefits of public education, engagement and participation, service provision, collaborative efforts and co-production, openness, transparency and accountability, trust building, and communication efficiency'.[xxii] In December 2013, the

US signals intelligence organisation, the National Security Agency (NSA), joined Twitter. By June 2014, the Central Intelligence Agency (CIA) had also joined Twitter, sending it's first-ever message: 'We can neither confirm nor deny that this is our first tweet'. Within hours, it had been retweeted more than 85,000 times, attracting over 100,000 new followers, and, as of October 2019, had 2.7 million followers.[xxiii] While widely reported, both were following the precedent set by other members of the US intelligence and security community.[xxiv] The Federal Bureau of Investigation, largely because of its role as the leading federal law enforcement agency, launched into social media in November 2008, with more than seventy separate pages or sites across Twitter, YouTube, Instagram, and Flickr, representing field offices across the US. The FBI was followed shortly afterwards by the first US intelligence-related Twitter account for the Office of the Director of National Intelligence, the effective head of the multi-agency US intelligence community, directing and overseeing the US intelligence effort, which joined in July 2009, and which now has over 112,000 followers. The Defence Intelligence Agency (DIA) created a Twitter profile in February 2010, and the National Geospatial-Intelligence Agency joined in August 2011.[xxv] Today, the US intelligence community has a total of over 3.6 million Twitter followers, with many more on other social media platforms.[xxvi] While admitting there was still much to be done, a survey of US intelligence social media found that America's agencies were making positive strides to educate, engage, and provide some limited transparency of the intelligence community's activities.[xxvii] In the UK, social media can be seen as part of the wider strategy of openness on intelligence matters that started in the 1990s, seeing ever-increasing engagement with journalists and the public.[xxviii] As in the US, it can be argued that social media offers a similar avenue to engage, educate and give insight into intelligence activities, while giving new modes of outreach at a time when Britain's agencies are looking for greater personnel diversity, following criticism from the Parliamentary Intelligence & Security Committee. As such social media is important for two reasons: education and diversity.

It is no surprise that the organisations using social media are signals intelligence agencies looking for new recruits plugged into the 'internet of things'. As society becomes more integrated and networked, there has been an increased requirement to protect society from actors who wish to use the internet, and computer-controlled systems as an attack vector. Technological innovations have made it cheaper, and easier, to place more data and critical national infrastructure (CNI) on computer-based systems that may also be connected in some way to global internet networks. These developments have drastically increased the threat of cyber-security attacks that intelligence and security agencies must identify and combat. A failure to protect against such attacks by both state and non-state actors could be catastrophic. For instance, Stuxnet, a computer worm used to attack components of Iran's nuclear weapons program, destroyed 984 uranium enriching centrifuges and set the program back significantly.[xxix] In 2015, the world's first successful cyberattack on a national power grid left 225,000 people without power in Ukraine.[xxx] While no attack has yet successfully knocked-out UK CNI, there is growing pressure on GCHQ and NCSC to protect an increasing number of potential targets from a growing threat.[xxxi] However, CNI is only one area in which a state may be vulnerable. There have also been information warfare attacks by other states, primarily through

social media, and there is also the ever-present danger of serious organised criminal groups utilising the internet for nefarious activities. As a result, organisations such as GCHQ and NSA have been required to significantly increase their capacity to combat digital threats to match the pace of change that comes with each technological innovation. To build this capacity, intelligence agencies not only need the finances for expensive technical infrastructure; they, more importantly, need the staff with the necessary skills to undertake cyber-security activity. Yet in recent years there have been multiple reports that intelligence agencies have struggled to recruit and retain much needed digital talent. In the US, the Comprehensive National Cyber Security Initiative of 2008 (later declassified in 2010), highlighted that 'there are not enough cybersecurity experts within Federal Government or private sector to implement the CNCI [*Comprehensive National Cyber Security Initiative]*'[xxxii]. In the same way, British intelligence is facing similar issues. One report by the UK's Intelligence and Security Committee (ISC)[xxxiii] stated that competition from the private sector is a contributing factor to a 22% shortfall in recruitment within GCHQ.[xxxiv] The agency said it was 'getting value' out of apprentices and other staff brought in at a young age, but the biggest challenge was, officials admitted to the ISC, 'retaining them obviously and developing them and giving them a sort of rounded career'.[xxxv] The same report also stated that the agency 'struggles to attract and retain a suitable cadre of in-house technical specialists because it inevitably has to compete with big technology companies which are able to pay significantly more'.[xxxvi] The drain of specialist staff in GCHQ has been a long running issue; in the ISC's 2011-12 report, it was highlighted that GCHQ was losing 'critical staff with high end cyber technology skills at up to three times the rate of the corporate average (3.4%)', a situation blamed, Director Ian Lobban to the committee, on the 'growing market for cyber security experts … government could not match the salaries that industry was offering. As a result GCHQ was training staff who were then recruited by the private sector, attracted by higher salaries and greater benefits'.[xxxvii] In January 2012, it was reported that GCHQ was giving 'retention payments' to prevent staff leaving for high-tech companies such as Google and Microsoft.[xxxviii] This suggests that a range of skills shortages and competition from the higher-paying private sector is reducing cybersecurity capacity, in an area where there is already a significant skills gap in the UK.[xxxix]

A culture mismatch is also hampering recruitment efforts, as revealed by the ISC's July 2018 report on 'Diversity and Inclusion in the UK Intelligence Community'.[xl] British intelligence has the perception of being predominantly white, male and middle-class. Lingering perceptions that recruitment is conducted through a tap on the shoulder during an Oxbridge education go some way to suggest that a job is inaccessible to those outside this demographic, though the reality is that the situation today – with online and print media advertising and other channels for advertisement – is largely different from the recruitment practices of the past. Of course, the UK is not alone in seeking to diversify the make-up of the agencies. In the US, the Director of National Intelligence has launched an Office of Diversity and Inclusion to promote a more diverse workforce[xli], ending what one former CIA operations officer called a 'white-as-rice culture'[xlii] which saw US intelligence staffed by 'white, male, Anglo-Saxon, Protestant Americans'.[xliii] In 2017, the Australian Secret Intelligence Service (ASIS) launched its Diversity and Inclusion Strategy, to increase

diversity amongst its workforce, with a focus on representation from Aboriginal and Torres Strait Islander people.[xliv] Australia's foreign intelligence agency was joined in this new diversity strategy by the domestic Australian Security Intelligence Organisation (ASIO) the following year.[xlv] In 2019, ASIO launched its own Mudyi – Aboriginal and Torres Strait Islander Staff Network committed to 'promoting an inclusive workplace culture that values and celebrates' Aboriginal and Torres staff, and a separate network developing greater gender diversity.[xlvi] Britain's agencies also recognise the need for change, having been criticised heavily for their lack of minority representation. Figures from 2004 showed that just 9% of MI5's recruits came from BAME backgrounds.[xlvii] By 2007, MI5 had a BAME workforce of 6.5%.[xlviii] In 2010 *The Sunday Times* published extracts from a leaked report, first commissioned by the Cabinet Office, which found there was a 'very small pool' of BAME staff in GCHQ with several interviewed suggesting workplace prejudice. Among the complaints recorded were: 'I wasn't born here, and although I have been security cleared I am constantly challenged about my loyalty to Britain by my colleagues', while another said, 'The security officers ask questions which are culturally inappropriate, insensitive and offensive'.[xlix] In March 2015, the ISC called for more women in the agencies[l], while the July 2018 ISC report criticised the lack of representation amongst minority BAME, LGBT and disability groups, with the agencies still 'not gender balanced' or fully reflecting 'the ethnic make-up of modern Britain' finding that only one of the agencies – GCHQ, had 'any staff at Senior Civil Service level who declared as BAME'.[li] While the committee blamed organisational cultures and security vetting, recruitment and engagement was also a problem area even if agency campaigns were 'increasingly innovative as the Agencies seek to promote "brand awareness" and attract a more diverse range of applicants from under-represented groups'.[lii] For MPs, existing recruitment campaigns, despite attracting significant attention, failed to 'receive enough applications from people from across a sufficiently wide range of backgrounds', with individuals from diverse backgrounds having a 'stereotypical image of these organisations'. As an earlier ISC report into the role of women in the UK's agencies suggested, 'Recruitment campaigns have to evolve to challenge the norms, particularly those surrounding the seemingly male-dominated intelligence world. We should encourage the use of more positive role models to break down the stereotypes that have been established and reinforced by the entertainment industry'.[liii] For the agencies and MPs, recruitment needed to 'reach out to under-represented groups in new ways, and to move away from the more traditional mechanisms', targeting 'lifestyle magazines and … social media' rather than just newspapers and websites.[liv] Responding to the ISC's report, the government acknowledged that aspects of the agency recruitment campaigns had started to work: 'MI5 has seen an increase in BAME and female applications across campaigns in Q1 2018 compared with Q4 2017/18. Since February 2017, female applicants to GCHQ increased considerably from 2016/17. This illustrates the impact that recruitment campaigns are having on applications'.[lv]

Intelligence agencies have long tried to move away from the traditional 'tap on the shoulder' approach to recruitment. In 2009, GCHQ ran a recruitment campaign through Microsoft's Xbox Live for 'quick thinking 18- to 34- year olds'[lvi], following its first-ever game targeted ad campaign in 2007, running the strapline 'Careers in British Intelligence' in games including Tom Clancey's *Rainbow Six: Vegas*, and

Splinter Cell Double Agent, as part of a general drive by Britain's agencies to attract new talent.[lvii] Recruitment through online gaming is just one example of GCHQ's efforts to diversity and innovate in recruitment. In November 2015, it used reverse graffiti – creating an advert by cleaning pavements using a stencil and pressure washer – to create the cryptic message, 'GCH-Who? Technical Opportunities gchq-careers.co.uk', appearing in Manchester, Birmingham, Wolverhampton, Leeds and Shoreditch, East London, especially targeting tech start-ups and 'hipsters' – a campaign that led Hackney Council to threaten enforcement action for graffitiing.[lviii] GCHQ also took out an advert in the Pride Issue of LGBT magazine *Fyne Times*, including the line: 'Alternative perspectives spark the innovative thinking needed to achieve our mission. You can see things differently. So we can flourish'.[lix] In May 2018, SIS also launched its first TV advert in a bid to ditch the traditional James Bond image and attract more female and ethnic minority applications. The advert, which opened with the image of a shark, featured a mother comforting her child with the tagline 'Secretly, we're just like you', was followed by another 'Barbershop Advert' in January 2019 as part of a wider '#secretlywerejustlikeyou' ad campaign on YouTube and Google Display.[lx] In October 2019, it was reported that SIS had been recognised as one of the UK's best organisations for social mobility having run a campaign to attract 'working class spies'.[lxi] Despite ISC concerns about BAME recruitment, the Security Service (MI5) was listed as one of the leading 'employers for race'[lxii], while GCHQ now targets BAME and female candidates through 'GCHQ – Decoded' and all-female cyber-training workshops.[lxiii] In October 2019, working with the government's in-house design agency, Design102, GCHQ won an award – coming top out of 6,000 applications – at the annual Digital Communications Awards, for the 'Journey to GCHQ' campaign aiming to attract 'women and young people' by following the careers of existing members of staff, a campaign that attracted increasing interest in online adverts and resulted in media attention.[lxiv]

Social media is also an important part of GCHQ's educational strategy. As GCHQ Director of Communications Andrew Pike suggested: the feed would allow his agency to 'use its own voice to talk directly about the important work we do to keep Britain safe', explaining, 'We want GCHQ to be more accessible and to help the public understand more about our work. We also want to reach out to the technical community and add our voice to social media conversations about technology, maths, cyber security, and other topics where we have a view'. Topics covered would include 'history, mission outcomes, languages, maths, cyber security, technology and innovation, job opportunities and as a way of signposting events, publications, news, blogs, and opinion pieces'.[lxv] Following their entry to Instagram, GCHQ officials explained 'People generally know we're working 24/7 to help keep the country safe, but they don't get the chance to see behind the scenes. Hopefully this will help dispel some myths and show who we are as individuals … You'll not only learn about our work to stay one step ahead of those wishing to do us harm, but also get a glimpse at our hobbies, clubs, and coffee shops'.[lxvi] But beyond just education, the feed could also, as *The Telegraph* pointed out, 'win back public confidence' that had been dented by some of the more lurid claims of mass surveillance after Snowden's leaks.[lxvii] As was noted in 2014, following the appointment of Director Robert Hannigan, GCHQ had to cope with new demands for 'greater transparency' with the traditional stand-off stance to media and public attention 'no longer a realistic option'. As *The Telegraph's*

editorial explained, 'the intelligence agencies need to be better at explaining what they do to keep us safe and why it is important that they continue to do it. They have a good story to tell and from the little we know of Mr Hannigan, a former communications chief in Northern Ireland, he is considered the person best able to tell it – and to lead GCHQ out of the shadows'.[lxviii] In the 21st Century, the UK's intelligence agencies need to maintain an online presence, with social media being just part of the strategy, even if SIS and MI5 do not use these platforms yet. However, what effect has GCHQ's use of social media had, and has the organisation reached the target audience it wants? Who now follows GCHQ's Twitter account, and are they speaking to the right people?

Content & Audience: Methods & Data

To understand the nature of GCHQ on social media, its' audience, and the comparison with the wider social media activity of the ten other agencies in the UK, US, Canada, Australia and New Zealand, this research used two separate data collections from the Twitter platform. Twitter was chosen for this research as the Application Programming Interface is much more accessible to researchers. The first of which was a collection of a sample of tweets sent on Twitter by these agencies alongside any tweet containing, mentioning, tweeting to, replying, or retweeting eleven separate intelligence agencies over the month of February 2019. In total, this project collected 203,019 tweets. The second data collection gathered follower data on 482,302 different Twitter accounts (or roughly 7% of the total follower network of the agencies identified here). Overall, we are confident that this data represents a good sample of the overall networks that engage with the Five-eyes agencies on Twitter. Two sets of analysis were then undertaken. The first was a content analysis of the types of posts created by GCHQ. Content analysis is a method of deriving qualitative data from quantitative sources. This analysis was used to understand the strategy in place by GCHQ when it comes to Twitter. This second set of analyses was through social network analysis using SNA analysis software Gephi (Bastian *et al.* 2009). This was used as a visual and numerical method of understanding the groupings which formed within the surrounding the 5-eyes, and around the social presence of GCHQ communication. Furthermore, we were also able to use Gephi to find which intelligence agencies had the most importance in the networks and the online discussions.

Results: GCHQ in the Twittersphere

In February 2019, the GCHQ Twitter account posted 76 times, much higher than other accounts from the 5-eyes agencies (see table 1). Through content analysis it was found that nine tweets (11.8%) were directly related to recruitment. These posts are directly advertising vacancies such as software developers, linguists, and intelligence analysts, suggesting that vacancy posts were only a small proportion of the messages they posted using the social media website. However, we also found an increased number of posts related to building its employer brand with underrepresented groups within its workforce (women, LGBT+, BAME,

disability/mental health, and faith). Analysis found a total of 12 (15.8%) posts celebrating the agencies history, or culture in regard to either of these demographics. In addition, there were two further posts (2.6%) communicating messages to so-called 'future codebreakers' encouraging young people to develop the skills needed for the work the agency does. From the perspective of employer branding, these posts can be considered indirect recruitment messages that attempt to make the agency more attractive to these groups. Four additional posts (5.2%) could be considered employer branding, but instead to a general audience, such as posts from behind the scenes, or what it is like to work at the agency. This suggests a two-pronged approach to recruiting staff for GCHQ – firstly, to display that the workplace culture is favourable and accepting of people from the desired underrepresented demographics within its workforce, correcting perceptions of the agency, and secondly, to display active vacancies as they arise to a general audience. However, this still only accounts for 27 (35.5%) of the messages posted by the agency.

When compared to the other agencies included in this study, it seems a pattern can be seen within the types of intelligence agencies and how they approach the use of Twitter. Through all the accounts, an average of 30.5% (SD. 18.7) of all tweets are related to recruitment. However, those agencies with a requirement for harder to recruit roles also had a higher number of recruitment related messages. Agencies whose operations lends itself to cybersecurity or STEM-related activities[lxix], particularly the Australian Signals Directorate, NSA, the Canadian CSE, GCHQ, and NGA had more recruitment messages with a total 42.5% being recruitment related. This is compared to 22.4% for all other agencies such as the CIA. Providing some evidence that amongst those agencies in the study, a common theme is the use of social media for recruitment. However, where the platform is arguably filled with certain demographics (such as 'techies') and the agencies are activity seeking these types of candidates to fill much needed cybersecurity and other STEM roles, there will be an increase in the overall number of recruitment posts, though the success of this strategy needs to be measured in future reports by the UK ISC.

Image 1: Tweet from GCHQ celebrating their LGBT+ credentials by lighting communication dishes in rainbow pride colours. An example of employer branding.

The other 64.4% of posts by GCHQ consisted of news, such as covering the celebration of the agencies 100th year and visit by the Queen, puzzles, historical facts or statements by the agency director, Jeremy Fleming. In effect, much of this content falls within the advice of the Government Digital Service's recommendations on the use of social media, and the educational remit of GCHQ's social media.[lxx] That is content related to raising awareness of the organisation's activities and role, promoting a particular type of culture, and promoting trust in their functions. For instance, linking the current day organisation to its famous Second World War past at Bletchley Park, or by highlighting positive news stories and officially backed GCHQ media content. Stories included the avowal of GCHQ's former Palmer Street site in central London[lxxi], historical blogs on SIGINT for the First World War centenary, and the forthcoming GCHQ exhibition at the London Science Museum. From this, it is evident that the agency is not just using Twitter as a recruitment tool and has other visible communicative purposes. While in comparison, it seems that the Twitter account for the NCSC is much more targeted, with content specifically aiming to reduce the levels of cybercrime and improve cyber security within the UK, with practical advice aimed at businesses and everyday uses with tips on how to stay safe online, and notifications of security vulnerabilities within commonly used software.

Table1. Comparison of 5-eyes agencies in the number & type of recruitment posts on Twitter

Twitter account	Tweets referencing direct recruitment messages	Tweets highlighting diversity (specific and general)	Tweets referencing future codebreakers	General employer branding	Total N of tweets	Total *n* of recruitment tweets	% of tweets related to recruitment
GCHQ	9	12	2	4	76	27	35.5
NSAgov	1	5	4	4	20	14	70.0
FBI	6	5	0	1	50	12	24.0
CIA	2	2	0	4	36	8	22.2
Defenseintel	0	0	0	0	15	0	0.0
ODNIgov	1	2	0	0	19	3	15.8
NGA_GEOINT	7	3	0	5	42	15	35.7
NCSC	0	12	11	2	132	25	18.9
csiscanada	7	2	2	4	29	15	51.7
ASDGovAu	2	3	0	0	11	5	45.5
cse_cst	9	3	2	5	39	19	48.7

TOTAL	44	49	21	29	469	143	30.5

Table2. Comparison of 5-eyes agencies in the number of specific diversity recruitment messages

	Targeted demographic					
Twitter account	LGBT+	Women	BAME	Disability	Mental Health	Faith
GCHQ	6	2	2	0	1	1
NSAgov	0	4	1	0	0	0
FBI	0	0	5	0	0	0
CIA	0	2	0	0	0	0
Defenseintel	0	0	0	0	0	0
ODNIgov	0	1	1	0	0	0
NGA_GEOINT	0	0	2	0	0	0
NCSC	0	11	0	0	0	0
Csiscanada	0	0	1	0	1	0
ASDGovAu	0	3	1	0	0	0
cse_cst	0	2	1	0	0	0
TOTAL	6	24	14	0	2	1

Table: How effective is this communication strategy for communicating with diverse groups?

Out of all the agencies, it seems that the GCHQ had attempted to attract a more diverse range of candidates, being the only account to seek to significantly attract LGBT+ applicants, and overall creating messages for five of the six demographics tested against, while most other agencies only accounted for two or under of these same groups within their tweets. In addition, GCHQ had the highest number of tweets aimed at encouraging candidates from diverse groups to apply, matched only by the NCSC (who was live tweeting an event for female coders, inflating their overall figures). It could, therefore, be argued that when compared to other agencies, it was GCHQ who has been seeking to attract a more diverse workforce. However, this does not provide any evidence to suggest they are successful at reaching these audiences – a topic in need of future research.

To find out to what extent GCHQ was able to connect with a more diverse audience, network analysis was used to test which groups they communicated with on Twitter. Network graph 1 (see Appendix I) shows the network for all tweets that contain GCHQ or mention the agencies Twitter account. While this does not show who had seen tweets by GCHQ, it acts as an indicator for who has been talking about them. This graph shows that the agency's recruitment activity is, indeed, connecting with some of their intended audience. For instance, small networks can be found related to recruitment events, such as a 36-node network surrounding an event based focussed on women coders in Manchester; a 31-node network surrounding the activity of a collaboration between the *Made By Dyslexia* charity and GCHQ advertising the

agencies hiring policies of people with Dyslexia. There was also a further 29-node network surrounding the work of GCHQ staff collaborating with *Code Club* to teach schoolchildren coding, suggesting the collaboration with relevant partners is giving GCHQ access to a segment of their target audience (Women, potential future candidates, and people with dyslexia). However, it should be remembered that this type of activity is small compared to the overall network (96 nodes out of a total of 2,752), and there were no observable networks relating to people from BAME or LGBT+ backgrounds. More significant activity within the network can be found in relation to news. For instance, the Queen's visit to GCHQ's Cheltenham offices to celebrate 100 years of the organisation[lxxii], takes up much of the overall network. Other areas relating to news can be seen occupying large areas of the network, such as tweets relating to a VPN news story amongst other loosely bound groups of political news. Suggesting that much of the Twitter communication is outside of the agency's control and is dictated by news events rather than attempts to draw attention to their recruitment activity or to build trust in the agency generally. Other tightly bound clusters of the network were also found to be dedicated to conspiracy theories, or contain anti-GCHQ sentiment. The nonsensical mentions found within the graph are often filled with users tagging in the GCHQ twitter account for no apparent reason, or to use it as a debating tactic. In one example, a user mentioned the GCHQ account while calling another user a paid shill or troll after expressing disagreement with current policy in Saudi Arabia. Another larger cluster saw GCHQ as part of wider 'deep state' and included its Twitter handle, connecting it to theories regarding the use of so-called 'chemtrails' – a bizzare belief that the condensation trails produced by high-flying aircraft are actually chemical or biological agents spread by government as a means of mind control[lxxiii], or the apparent involvement of GCHQ in 'pizzagate' – a story of a fictitious child trafficking ring involving US Democratic Party officials shared by the alt-right and other opponents of Hillary Clinton's 2016 campaign. Many other mentions related to supposed coverups or 'hiding the truth'. Another popular conspiracy shared online using the GCHQ hashtag is the claim that the agency helped spy on the Trump campaign in 2016. The claims, popularised by White House Press Secretary Sean Spicer in early 2017, led to an unprecedented rebuke from GCHQ, but have continued to be shared online, especially allegations that GCHQ Director Robert Hannigan was part of the conspiracy, 'to surveil' Trump promoted by users of 4chan, popular with the alt-right and conspiracy theorists.[lxxiv]

When compared to the overall follower network (network graph 2, Appendix II), it seems that the majority of followers are localised to specific national contexts. For instance, while many followers of the FBI will also follow CIA and NSA, they will not also follow other intelligence agencies within the 5-eyes. This is represented on the graph by the significant clusters around each agency, and the relative closeness of agencies from the same nation. In comparison to the overall network of tweets that mention one of the 5-eyes (network graph 3), a similar pattern can be found, except that the network is more dominated by agencies with a larger international name recognition (FBI, CIA & NSA). This suggests that just having an agency Twitter account will not automatically raise the profile of the agency, and other external factors such as news, or statements by high ranking political figures (such as Donald Trump), have a great influence.

CONCLUSIONS

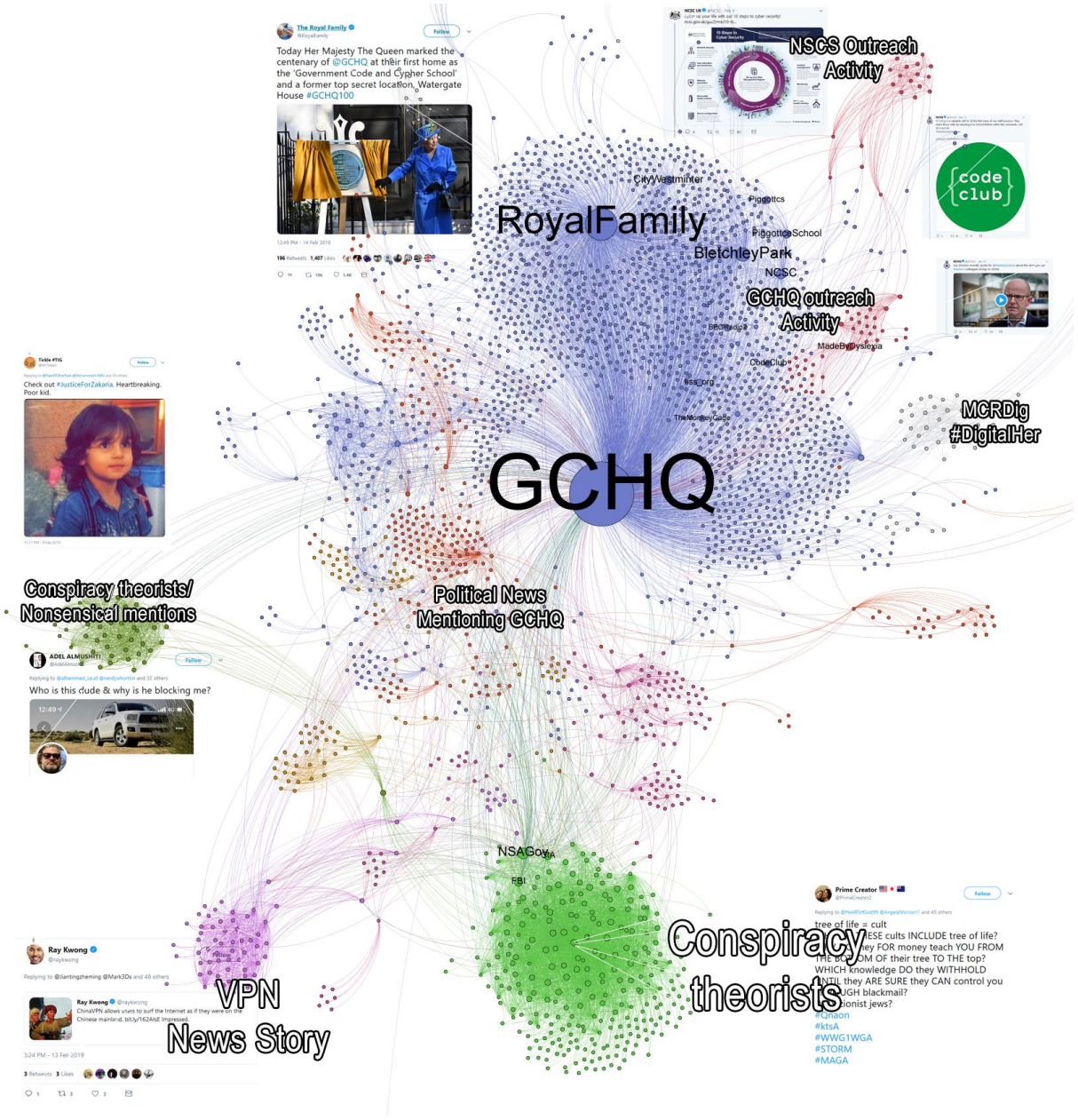
The initial findings here suggest that social media carries with it advantages and disadvantages for intelligence agencies. As we noted at the outset, these organisation's experience of social media is always likely to be more circumscribed than the majority of government departments and agencies. Excited PR chatter about building interactive client relationships or dialogues and personalising and humanising services are always going to be more difficult where you cannot talk back, and staff cannot be identified. Arguably, then trying to benchmark GCHQ against standard lessons from e-government approaches is always likely to be difficult. Such agencies are in a rather unique position. Hence, it makes more sense to examine their current social media communication in the context of their historical evolution and their intelligence counterparts elsewhere. Indeed, GCHQ's example reflects the US experience that Twitter and other forms of social media can engage, educate and give some insights into intelligence activities. For instance, GCHQ's feed has been useful in promoting its organisational history in its centenary year, in highlighting important cultural events and sending the general message that inclusivity and diversity are now integral for GCHQ as it looks to develop in the 21st Century. The feed also shows a sense of humour; one of the most popular tweets shared was a response to the 2019 Dr Who New Year special when Dalek were shown attacking GCHQ. The next day, GCHQ Tweeted: 'We've just about finished cleaning up the mess … but we're happy to confirm GCHQ is at full operational capacity'.[lxxv] By November 2019, GCHQ reached 100,000 followers, celebrating by offering followers the opportunity to win a copy of *The GCHQ Puzzle Book II*, signed by Director Jeremy Fleming. 'Reaching 100,000 followers in our centenary year is a great achievement, and shows the growing understanding the public has of our mission to help to keep the country safe', said 'Chris', GCHQ's head of external relations.[lxxvi] The US experience also shows that agencies can have significant outreach, a lesson that can be applied to the UK example where GCHQ is currently leading. Although use of Twitter and other platforms by the UK's other agencies remains to be seen – and there is no suggestion that SIS or MI5 will join GCHQ and NCSC it the Twittersphere, there could be advantages to MI5, for example, which already has an established programme of historical engagement, recruitment outreach and speeches by the service's Director General which could be used as the basis for online content to be shared with new audiences through social media.[lxxvii] In 2009 MI5's then Director General Jonathan Evans also suggested that with the growing threat of domestic terrorism, it was vital to be 'as open and transparent as possible … because that openness, by supporting public confidence in us, helps us do our job of protecting national security' – something social media can help with.[lxxviii] Even SIS, an organisation that has traditionally avoided publicity, had a link to its first TV advert shared through GCHQ's feed. Being on Twitter would potentially allow agencies the ability to connect and reach out to external audiences they may not otherwise talk to. As seen by GCHQ, partnerships with groups such as Code Club brings with it access to their audience, helping meet recruitment goals and hit particular target groups for diversity and inclusion.

But there are also significant warnings. Simply having an account on Twitter that attracts thousands of tweets and notifications relating to news and recruitment often acts as a focus for anyone wanting to send hostile messages – a phenomenon not just experienced by intelligence agencies. In a general sense, it underlines some of the limitations to any impression management strategy via social media. While in the past, believers in the 'deep state' and hidden hand were restricted to sending malicious letters, writing in unscrupulous journals or ranting while standing on a box at Hyde Park's Speakers Corner, the very public nature of NCSC and GCHQ's social media means it quickly becomes a target for abuse, potentially damaging the brand identity and attracting adverse reactions that the online publicity was designed to deflect in the first place. Going back to the initial aim of allowing GCHQ to use its own voice to 'talk directly' to social media uses, it is clear that the agency policy of not engaging in a two-way dialogue often limits the overall ability to interact with their audience. In practice, while GCHQ may want to add its voice to social media conversations about technology, maths, cyber security, and history, such messages are drowned out by the wider noise generated by other Twitter users, bots and believers in the 'deep state'. It should be also pointed out that even if GCHQ responded to the more hard-core conspiracies online, it would probably have little effect as many are created in an echo-chamber of like-minded believers and, when formed, are unlikely to finish, having, as observed by David Aaronovitch in his history of conspiracies, flexibility where 'any new and inconvenient truth can be accommodated within the theory itself'.[lxxix] Equally, GCHQ's message that their actions are proportionate, and able to discriminate between the activities of everyday citizens and suspected targets is unlikely to alter opinion, shaped heavily by the Snowden revelations, amongst civil liberties groups that modern-day SIGINT agencies have the capability to and regularly do – to quote former NSA Director General Keith Alexander – 'Collect everything' on individuals.[lxxx] Adding to the these external pressures can be in-house opposition to agencies going too far in the direction of openness, especially being seen to normalise use of social media – a long-held concern for staff in the UK's agencies – and the possible dangers of sharing images of staff and facilities. GCHQ's head of external communications acknowledged that 'Generating fresh social media content which protects our staff identities but provides a peek inside GCHQ was always going to be a challenge'.[lxxxi] Even just launching the Twitter feed was a 'tortuous process', explained *The Financial Times* Defence and Security Editor in May 2016, 'GCHQ and all of its staff are subject to draconian security procedures that restrict contact with the outside digital world beyond the agency's operational channels. Setting up a presence on social media has taken months of wrangling'.[lxxxii] Today, there are still significant concerns that social media usage can encourage employees to lessen their guard, exposing them to intelligence rivals or non-state actors. In August 2019, western officials warned that LinkedIn is used extensively by China's foreign intelligence agency to cultivate new sources.[lxxxiii]

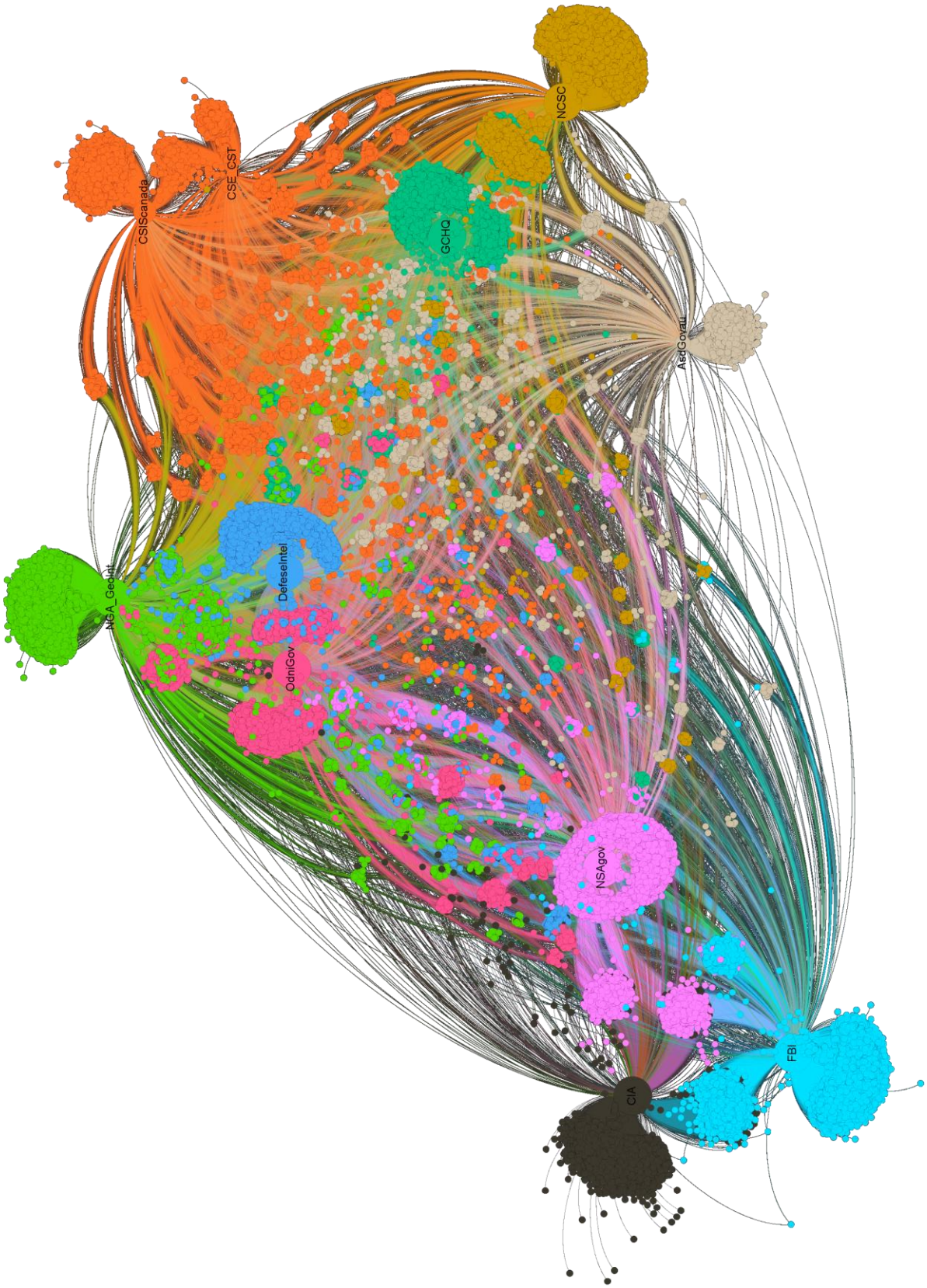
While the analysis presented above provides an overarching image of the communicative landscape for GCHQ and other intelligence agencies, there is certainly scope for additional research in terms of understanding the audience. This research shows that a comprehensive understanding of the types of people who are following intelligence agencies online is needed. A profile analysis alongside a more

comprehensive dataset of Twitter followers of each agency would help better understand the groups and types and numbers of followers. For example, are they academics, cybersecurity professionals, heavy news consumers, or bots and trolls attempting to distort online debate? While GCHQ's use of Twitter is to be applauded, the impact and outreach has to be questioned. The evidence from the above suggests that the conversation about GCHQ is very much outside the hands of the agency, with the conversational agenda being set by current affairs, a clear contrast with NCSC's social media activity. In contrast to GCHQ, much of NCSC's content is practical e-security advice and threat warnings. A browse of tweets sent out in late-November 2019 showed that topics included practical advice on two-factor authentication, email security and anti-spoofing, safety in election campaigns, dealing with common online threats, and how to enjoy online gaming safely and protecting personal and financial data. In the same period, GCHQ tweeted about recruitment, the regular brainteasers building on the success of *The GCHQ Puzzle Book* parts one and two[lxxxiv], a CBBC cyber competition and links to older news items. To some extent, the content reflects the different aims of both organisation's social media presence and the differing levels of 'transparency' that both can provide. For NCSC, with its growing public and business-facing remit, the feed is an excellent way to disseminate expert advice. By contrast, GCHQ as a SIGINT organisation can only briefly talk about support for the military and counter-terrorism effort in public, not the wider focus on foreign communications, even if, alongside NCSC, it shared details of 'Equities Process' and the decision to reveal flaws in software.[lxxxv] Both accounts also show that post-Snowden transparency and public engagement can only go so far. As NCSC CEO Ciaran Martin writes, 'A significant proportion of our work has continued to take the form of defending against hostile state actors. We can say that Russia, China, Iran and North Korea continue to pose strategic national security threats to the UK, but we can't often talk about the operational successes and the full range of the NCSC, GCHQ and wider state capabilities that are deployed against them'.[lxxxvi] To talk about successes often undermines techniques and tradecraft and most officials would agree with the often-quoted CIA saying that 'the secret of our success is the secret of our success'.[lxxxvii] In concluding, this study suggests that GCHQ and NCSC use of social media is a welcome step-change from traditional engagement activity, but there needs to be an objective discussion of the pros and cons of public-facing online activity to improve public understanding and knowledge of intelligence and security in the UK.

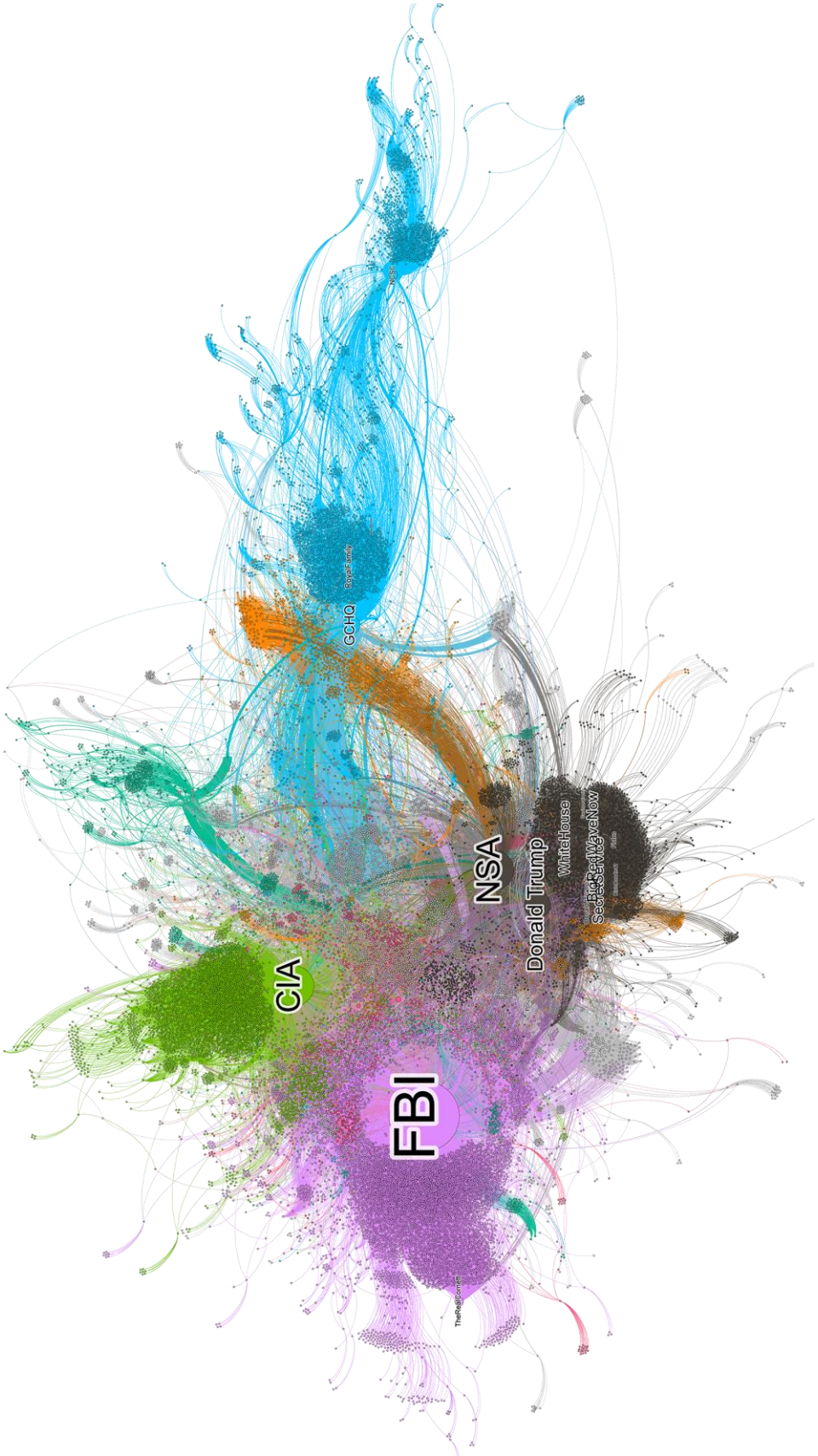
Appendices



Appendix I: Network Graph 1. Network of Tweets sent during February that contain 'GCHQ'



Appendix II: Network Graph 2. – Network of Twitter followers of the Five Eyes



Appendix III: Network Graph 3. Network of Tweets sent during February.

References

Secondary sources

Aaronovitch, David (2010), *Voodoo Histories: How Conspiracy Theory Has Shaped Modern History*. London: Vintage Books.

Aldrich, Richard J. (2019), *GCHQ: Centenary Edition*. London: William Collins.

Allen, Ben. 'GCHQ had a brilliant response to that Dalek attack in Doctor Who's New Year's special', *Radio Times*, 3 January 2019.

Andrew, Christopher (2009). *Defence of the Realm: The Authorised History of MI5*. London: Penguin.

'Asian MI5 and MI6 officers speak', *BBC News*, 26 November 2007 < http://news.bbc.co.uk/1/hi/uk/7112190.stm >

Benedictus, Leo. 'Shoreditch spies: why does GCHQ want to hire hipsters?', *The Guardian*, 23 November 2015.

Broad, W.J., Markoff, J., & Sanger, D.E. (Jan 15, 2011). 'Israeli Test on Worm Called Crucial in Iranian Nuclear Delay'. *New York Times*.

Bullock, K., (2018). '(Re) presenting 'order' online: the construction of police presentational strategies on social media". *Policing and society*, *28*(3), pp.345-359.

d'Ancona, M. (2017), *Post Truth: The New War on Truth and How to Fight Back*. London: Ebury Press.

Coughlan, Sean. 'GCHQ sets up all-female cyber-training classes', *BBC News*, 17 January 2019.

Corera, Gordon (2016). *Intercept: The Secret History of Computers and Spies*. London: Weidenfeld & Nicholson. 350-381.

Dahlgreen, Will (2017). 'Broad support for increased surveillance powers', *YouGov* < https://yougov.co.uk/topics/politics/articles-reports/2015/01/18/more-surveillance-please-were-british >

DePaula, N., Dincelli, E. and Harrison, T.M., (2018). 'Toward a typology of government social media communication: Democratic goals, symbolic acts and self-presentation.' *Government Information Quarterly*, *35*(1), pp.98-108.

Dover, Rob (2019). 'SOCMINT: a shifting balance of opportunity', *Intelligence & National Security* < https://www.tandfonline.com/doi/full/10.1080/02684527.2019.1694132?instName=University+of+Salford+%28Network+Username%29 >

Dunleavy, P., Margetts, H., Tinkler, J., & Bastow, S. *Digital era governance: IT corporations, the state, and e-government*. (Oxford: Oxford University Press, 2006).

Dunleavy, P., Margetts, H. 'The second wave of digital-era governance: a quasi-paradigm for government on the Web'. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *371*(1987).

'GCHQ: Minority Report', *BBC Radio 4*, November 2016 < https://www.bbc.co.uk/programmes/b0832fq3 >

'GCHQ must open up', *The Telegraph*, 16 April 2014.

'GCHQ reveals secret London site', 5 April 2019 < https://www.gchq.gov.uk/news/gchq-reveals-secret-site-for-the-first-time >

'GCHQ spy agency advertises jobs for gay codebreakers', *PinkNews*, 18 June 2018 < https://www.pinknews.co.uk/2018/06/18/gchq-spy-jobs-gay-codebreakers/ >

Griggs, Brandon. 'The CIA sends its first tweet (or not)', *CNN*, 6 June 2014.

Griggs, Ian. '"Hello World": GCHQ reaches Twitter landmark three years after emerging from the shadows', PR Week, 1 December 2019.

Griffin, Andrew. 'GCHQ joins Twitter and is immediately met with jokes about following people online', *The Independent*, 16 May 2016.

Hadley, James. 'How can we solve the UK's cyber skills shortage', *New Statesmen Tech*, 28 September 2019.

Hallemann, Victoria. 'Queens Makes Her First Official Public Appearance of 2019'. *Town and Country Magazine*, 14 February 2019 < https://www.townandcountrymag.com/society/tradition/a26312291/queen-elizabeth-gchq-bletchley-park-veterans-photos/ >

Hannigan, Robert. 'Organising a government for cyber: The creation of the UK's National Cyber Security Centre'. *RUSI Occasional Papers*, 27 February 2019 < https://rusi.org/publication/occasional-papers/organising-government-cyber-creation-uks-national-cyber-security >

'"Hello, world": GCHQ has officially joined Twitter' < https://www.gchq.gov.uk/news-article/hello-world-gchq-has-officially-joined-twitter >

'Intelligence agency GCHQ uses Xbox Live to attract new recruits', *The Telegraph*, 23 November 2009.

Jackson, N. and Lilleker, D., (2011). "Microblogging, constituency service and impression management: UK MPs and the use of Twitter." *The Journal of Legislative Studies*, *17*(1), pp.86-105.

Janssen, M., & Estevez, E. (2013). 'Lean government and platform-based governance—Doing more with less'. *Government Information Quarterly*, *30*, S1-S8.

Jeffreys-Jones, Rhodri (2017). *We Know All About You: The Story of Surveillance in Britain and America*. Oxford: Oxford University Press.

Jones, Sam. 'Tinker, tailor, tweeter, spy – GCHQ joins Twitter', *Financial Times*, 16 May 2016.

'Journey to GCHQ', Design102 < https://www.design102.co.uk/work/journey-to-gchq/ >

Lambert, Chloe. 'Midlife guide to … @GCHQ', *The Telegraph*, 17 May 2016 < https://www.telegraph.co.uk/technology/2016/05/17/midlife-guide-togchq/

Landon-Murray, Michael (2015). 'Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?' *Journal of Strategic Security*, 8(5).

Lawless, Jill. 'Spy agency goes recruiting – in video games', *NBC News*, 18 October 2007.

Laja, Sade. 'GCHQ offers "retention payments" to keep technology experts'. *The Guardian*, 4 January 2012 < https://www.theguardian.com/government-computing-network/2012/jan/04/gchq-bonus-payments-technology-experts >

Leppard, David (2010). "'Racism" at GCHQ is undermining fight against terror', *The Times* < https://www.thetimes.co.uk/article/racism-at-gchq-is-undermining-fight-against-terror-zh3gn9swx6w >

Lilleker, D.G., (2015). 'Interactivity and branding: Public political communication as a marketing tool". *Journal of Political Marketing*, *14*(1-2), pp.111-128.

Linders, D. (2012). 'From e-government to we-government: Defining a typology for citizen coproduction in the age of social media'. *Government Information Quarterly*, 29(4), 446-454.

Lomas, Daniel W.B. (2019). "'Crocodiles in the Corridors": Security Vetting, Race and Whitehall, 1945 – 1968', *Journal of Imperial & Commonwealth History*.

Lomas, Daniel W.B. and Christopher J. Murphy (2019). *Intelligence and Espionage: Secrets and Spies*. Oxon: Routledge.

Margetts, H. (2006). 'E-government in Britain—A decade on'. *Parliamentary Affairs*, 59(2), 250-265.

Marland, A., Lewis, J.P. and Flanagan, T., (2017). 'Governance in the age of digital media and branding". *Governance*, *30*(1), pp.125-141.

'MI5 named as a best employer for race', < https://www.mi5.gov.uk/fa/node/549 >

Moran, C. (2013). *Classified: Secrecy and the state in modern Britain*. Cambridge: Cambridge University Press.

Moran, C. (2011). The Pursuit of Intelligence History: Methods, Sources, and Trajectories in the United Kingdom'. *Studies in Intelligence*, 55(2), 33-55.

Lee, R.M., Assante, M.J.M. & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid. [pdf]*. E-ISAC: Washington, D.C. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Omand, D., Bartlett, J and C. Miller (2012), 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence & National Security*, 27(6).

Omand, D., Bartlett, J., and C. Miller (2012). #*Intelligence*. London: Demos.

Omand, D. and Mark Phythian (2018). *Principled Intelligence: The Ethics of Spying*. Georgetown: Georgetown University Press.

'Online Lies About Spies: How a fake letter revived a claim the UK bugged Donald Trump', 2 February 2018 < https://medium.com/dfrlab/online-lies-about-spies-b1f5fb86aed4 >

Plait, Phil. 'Chemtrails conspiracy theory gets put to the ultimate test'. *New Scientist*, 18 August 2016.

Richelson, J. T. (2012).*The US Intelligence Community, Sixth Edition*. Boulder, Colorado: Westview Press.

Sengupta, Kim. 'MI5 recruitment drive will focus on Asians'. *The Independent*, 24 February 2004.

Song, C., & Lee, J. (2016). 'Citizens' use of social media in government, perceived transparency, and trust in government'. *Public Performance & Management Review*, 39(2), 430-453.

'Spy agency GCHQ facing fines for "hipster" job adverts on London streets', *BBC Newsbeat* < http://www.bbc.co.uk/newsbeat/article/34941261/spy-agency-gchq-facing-fines-for-hipster-job-adverts-on-london-streets >

Stoddart, K. (2016). UK Cyber security and critical national infrastructure protection. *International Affairs,* 92(5), pp. 1079-1105; JCNSS.

Sweney, M. "'Become a Spy" ads target gamers', *The Guardian*, 18 October 2007

Swerling, G. 'MI6 drive to recruit working class spies sees it named as one of the UK's best employers for social mobility', *The Telegraph*, 8 October 2019.

Syed, Matthew (2019). *Rebel Ideas: The Power of Diverse Thinking*. London: John Murray.

Tamplin, H. 'GCHQ join Twitter so people got a bit paranoid', *The Metro*, 16 May 2016.

'The Digital Communications Awards results are in. But did we win?', Design102 Blog, 9 October 2019 < https://design102.blog.gov.uk/2019/10/09/the-digital-communications-awards-results-are-in/ >

The GCHQ Puzzle Book (London: Michael Joseph, 2016).

The GCHQ Puzzle Book II (London: Michael Joseph, 2018).

'The Equities Process', November 2019 < https://www.gchq.gov.uk/information/equities-process >

Van- Puyvelde, D. and A. F. Brantly (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Polity Press.

'Viewpoint: Was CIA "too white" to spot 9/11 clues', *BBC News*, 10 September 2019 < https://www.bbc.co.uk/news/world-us-canada-49582852 >

Weaver, M. "'Hello, world": GCHQ joins Twitter', *The Guardian*, 16 May 2016.

Wong, Edward. 'How China Uses LinkedIn to Recruit Spies Abroad', *The New York Times*, 27 August 2019 < https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html >

Endnotes

[i] "'Hello, world": GCHQ has officially joined Twitter' < https://www.gchq.gov.uk/news-article/hello-world-gchq-has-officially-joined-twitter > (accessed 12 December 2018).

[ii] In addition to sites at Cheltenham, Scarborough, Bude, Harrogate and London, GCHQ announced the location of a new Manchester facility in October 2019. Located in an inner-city location, GCHQ Director Jeremy Fleming said the Manchester hub was a 'unique and exciting opportunity to draw on the talents of one of the most diverse cities in the UK … This is a major event for GCHQ and I am particularly delighted to be able to announce it in our Centenary year' ('Location of new GCHQ site in Manchester revealed', < https://www.gchq.gov.uk/news/location-of-new-gchq-site-in-manchester-revealed >)

[iii] Margetts, H. 'E-government in Britain—A decade on', 250-265.

[iv] Dunleavy, P., Margetts, H., Tinkler, J., & Bastow, S., *Digital era governance: IT corporations, the state, and e-government*. And Margetts, H., & Dunleavy, P., 'The second wave of digital-era governance: a quasi-paradigm for government on the Web'.

[v] Janssen, M., & Estevez, E., 'Lean government and platform-based governance—Doing more with less', S1-S8.

[vi] See for example Linders, 'From e-government to we-government: Defining a typology for citizen coproduction in the age of social media', 446-454.

[vii] Social media impression management and branding have been widely applied across range of government and political sphere. See, for example: Bullock, K., (Re) presenting 'order' online: the construction of police

presentational strategies on social media.345-359; DePaula, N., Dincelli, E. and Harrison, T.M., Toward a typology of government social media communication: Democratic goals, symbolic acts and self-presentation. .98-108; Jackson, N. and Lilleker, D. 'Microblogging, constituency service and impression management: UK MPs and the use of Twitter'. 86-105; Lilleker, D.G. 'Interactivity and branding: Public political communication as a marketing tool.', 111-128;; Marland, A., Lewis, J.P. and Flanagan, T. 'Governance in the age of digital media and branding'.125-141.

[viii] Song, C., & Lee, J., 'Citizens' use of social media in government, perceived transparency, and trust in government', 430-453.
[ix] Government Digital Service (2018) Social Media Playbook. Available at https://www.gov.uk/guidance/social-media-playbook.
[x] Omand, D., Bartlett, J and C. Miller, 'Introducing Social Media Intelligence (SOCMINT)', 803. See also Dover, 'SOCMINT: a shifting balance of opportunity'.
[xi] See also Omand, D., Bartlett, J., and C. Miller, *#Intelligence*. For a wider study of OSINT, read Anthony Olcott, *Open Source Intelligence in a Networked World*.
[xii] Omand, et. al., *#Intelligence*, 11.
[xiii] d'Ancona, *Post Truth: The New War on Truth and How to Fight Back*, 121.
[xiv] On NCSC read Hannigan, 'Organising a Government for Cyber: The creation of the UK's National Cyber Security Centre' and the annual reports available from https://www.ncsc.gov.uk/news/annual-review-2019.
[xv] < https://twitter.com/NCSC/status/1188542989137825793 >
[xvi] '"Hello, world": GCHQ joins Twitter' and Weaver, '"Hello, world": GCHQ joins Twitter'.
[xvii] https://twitter.com/johnprescott/status/732154481501192192 and Griffin, 'GCHQ joins Twitter and is immediately met with jokes about following people online', Tamplin, 'GCHQ join Twitter so people got a bit paranoid'.
[xviii] Jones, 'Tinker, tailor, tweeter, spy'.
[xix] Griffin, 'GCHQ joins Twitter'.
[xx] On the general history of GCHQ, read Aldrich, *GCHQ: Centenary Edition* and the forthcoming authorised history by Prof. John Ferris, *Behind the Enigma: The authorised history of GCHQ, Britain's secret cyber-intelligence agency* (London: Bloomsbury, 2020). For a brief overview of the post-1989 changes, read Moran, 'The Pursuit of Intelligence History', 41-3.
[xxi] See 'Open Government Initiative' < https://obamawhitehouse.archives.gov/open >
[xxii] See Landon-Murray, 'Social Media and U.S. Intelligence Agencies: Just Trending or a Real Tool to Engage and Educate?'
[xxiii] Griggs, 'The CIA sends its first tweet (or not)'.
[xxiv] For an overview of the US intelligence community, read Richelson, *The US Intelligence Community*.
[xxv] The DIA account has 160,000 followers. The NGA has over 70,000.
[xxvi] The combined total of the DNI, CIA, NSA, NGA and DI accounts. Figures accurate as of October 2019.
[xxvii] See Landon-Murray, 'Social Media and U.S. Intelligence Agencies'.
[xxviii] On Britain's changing approach read Moran, *Classified: Secrecy and the state in modern Britain*, 329-349.
[xxix] Broad, Markoff & Sanger, D.E., 'Israeli Test on Worm Called Crucial in Iranian Nuclear Delay'.
[xxx] Lee, Assante & Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid.*
[xxxi] Stoddart, 'UK Cyber security and critical national infrastructure protection', 1079-1105; JCNSS, *Cyber Security of the UK's Critical National Infrastructure: Third Report of Session 2017-19* of Commons/House of Lords: London. Available at: < https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf > On the general threat read Puyvelde and Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*.
[xxxii] 'The Comprehensive National Cybersecurity Initiative' < https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative >
[xxxiii] For more information, see http://isc.independent.gov.uk/
[xxxiv] ISC. (2017). *Intelligence and Security Committee of Parliament: Annual Report 2016-2017*, 86.
[xxxv] Ibid.
[xxxvi] Ibid., 40.
[xxxvii] ISC. (2012). *Intelligence and Security Committee of Parliament: Annual Report 2011-2012*, 67.
[xxxviii] Laja, 'GCHQ offers "retention payments" to keep technology experts'.
[xxxix] On the cyber skills gap, read Hadley 'How can we solve the UK's cyber skills shortage'.
[xl] HC. 1297, 'Intelligence and Security Committee of Parliament: Diversity and Inclusion in the UK Intelligence Community', Open Government Licence, 18 July 2018.
[xli] 'Diversity and Inclusion' < https://www.dni.gov/index.php/how-we-work/diversity >
[xlii] 'Viewpoint: Was CIA "too white" to spot 9/11 clues?'
[xliii] On diversity, or lack of it, in the CIA read Syed, *Rebel Ideas*.
[xliv] See 'Diversity and Inclusion' < https://www.asis.gov.au/About-Us/Diversity-and-Inclusion.html >
[xlv] Launching the strategy, ASIO says that it is 'committed to creating a diverse and inclusive professional environment, where all staff are valued and respected, in order to build a highly capable, innovative and adaptive

workforce to achieve our purpose'. Details of the strategy can be found at 'Diversity and Inclusion Strategy' < https://www.asio.gov.au/diversity-and-inclusion-strategy.html >

ASIO's annual report for 2017-18 stated it was 'committed to creating a diverse and inclusive environment where differences are valued and staff are respected and supported to be highly capable, innovative and adaptive. Creating this workforce and culture will ensure we are best placed to achieve our purpose' including the launch of an inclusion strategy, internal diversity networks, a recruitment drive targeted at minority groups and cultural awareness initiatives (ASIO submission to the Parliamentary Joint Committee on Intelligence and Security: Review of Administration and Expenditure, No. 17 (2017-18), 34).

[xlvi] ASIO Annual Report, 2018-9, 76-77 < https://www.asio.gov.au/sites/default/files/2018-19%20Annual%20Report%20WEB.pdf >

[xlvii] Sengupta, 'MI5 recruitment drive will focus on Asians'.

[xlviii] 'Asian MI5 and MI6 officers speak'. The article also includes the experiences of two officers – one from MI5 and the other MI6 – and their views interviews with BBC Asian Network.

[xlix] Read Leppard, '"Racism' at GCHQ is Undermining the Fight Against Terror". The claims were later discussed on BBC Radio 4's 'Minority Report: GCHQ' in November 2016.

[l] See, HC 970, 'Women in the UK intelligence community: A report by the Intelligence and Security Committee', 5 March 2015.

[li] HC. 1297, 1.

[lii] Ibid., 5.

[liii] HC 970, 18, 19.

[liv] HC. 1297, 25-6.

[lv] Cm 9696, 'Government response to the Intelligence and Security Committee of Parliament Report on Diversity and Inclusion in the Intelligence Community', 3.

[lvi] 'Intelligence agency GCHQ uses Xbox Live to attract new recruits'.

[lvii] Sweeney, '"Become a Spy" ads target gamers' and Lawless, 'Spy agency goes recruiting – in video games'.

[lviii] Benedictus, 'Shoreditch spies' and 'Spy agency facing fines'.

[lix] 'GCHQ spy agency advertises jobs for gay codebreakers'.

[lx] 'MI6 first ever recruitment video for Intelligence Officers', *YouTube* < https://www.youtube.com/watch?v=IOViUQwOgdU > See also 'New "Barbershop Advert"' < https://www.sis.gov.uk/news/barbers-shop-advert.html >

[lxi] Swerling, 'MI6 drive to recruit working class spies sees it named as one of the UK's best employers for social mobility'.

[lxii] 'MI5 named as a best employer for race', < https://www.mi5.gov.uk/fa/node/549 >

[lxiii] 'Recruiting Diverse Talent to Protect Modern Britain' < https://www.gchq.gov.uk/information/recruiting-diverse-talent-protect-modern-britain > and Coughlan, 'GCHQ sets up all-female cyber-training classes'. For background information on the history of BAME inclusion in the intelligence services, read Lomas, '"Crocodiles in the Corridors": Security Vetting, Race and Whitehall, 1945 – 1968'.

[lxiv] On the campaign see, 'Journey to GCHQ' and 'The Digital Communications Awards results are in. But did we win?'

[lxv] Weaver, '"Hello, world": GCHQ joins Twitter'.

[lxvi] 'GCHQ joins Instagram', < https://www.gchq.gov.uk/news/gchq-joins-instagram >

[lxvii] Lambert, 'Midlife guide to … @GCHQ'. Despite the backlash, Snowden's leaks had limited impact in the UK. In a TNS poll conducted following Snowden's claims, 71% of those responding said that government should prioritise security even if this 'erodes peoples' right to privacy' (Jeffreys-Jones, *We Know All About You*, 222). In 2015 YouGov found 53% of those sampled supported retention of data – voice calls, emails, texts, social media posts, and others – for 12 months, opposed by 31% (don't know 16) (see Dahlgreen, 'Broad support for increased surveillance powers'). By 2017 another YouGov poll found 38% supported government laws store data, opposed by 25% and 24% 'neither support nor oppose' and 13 'don't know' (https://d25d2506sfb94s.cloudfront.net/cumulus_uploads/document/guozfocn1q/YGC%2C%20GB%20Surveillance%202017.pdf). On Snowden's claims and impact, read Corera, *Intercept*, 350-81.

[lxviii] 'GCHQ must open up'.

[lxix] NCSC was not included in this list, as it is primarily a discrete part of GCHQ intended to provide cyber security to the public and the private sector and government.

[lxx] Government Digital Service (2018) Social Media Playbook. Available at https://www.gov.uk/guidance/social-media-playbook.

[lxxi] 'GCHQ reveals secret London site', 5 April 2019 < https://www.gchq.gov.uk/news/gchq-reveals-secret-site-for-the-first-time >

[lxxii] On the visit, see Hallemann, 'Queen Elizabeth Makes Her First Official Public Appearance of 2019'.

[lxxiii] See Plait, 'Chemtrails conspiracy theory gets put to the ultimate test'.

[lxxiv] On the claims and the rebuke see 'Online Lies About Spies: How a fake letter revived a claim the UK bugged Donald Trump'.

[lxxv] Allen, 'GCHQ had a brilliant response'.
[lxxvi] Griggs, 'GCHQ reaches Twitter landmark'.
[lxxvii] See 'Latest MI5 files released' https://www.nationalarchives.gov.uk/about/news/latest-mi5-files-released/
[lxxviii] 'Foreword by the Director General of the Security Service' in Andrew, *Defence of the Realm*, xvi.
[lxxix] Aaronovitch, *Voodoo Histories*, 13.
[lxxx] For a sympathetic discussion of the issues surrounding online surveillance and bulk data collection, read Omand and Phythian, *Principled Spying*, 142-169.
[lxxxi] Griggs, 'GCHQ reaches Twitter landmark'.
[lxxxii] Jones, 'Tinker, tailor, tweeter, spy'.
[lxxxiii] Wong, 'How China Uses LinkedIn'.
[lxxxiv] *The GCHQ Puzzle Book* and *The GCHQ Puzzle Book II*.
[lxxxv] See 'The Equities Process', November 2019.
[lxxxvi] National Cyber Security Centre: Annual Review 2019, 6.
[lxxxvii] Lomas and Murphy, *Intelligence and Espionage: Secrets and Spies*, 94.