2019 PSA Conference Paper

The Impact of Populism on Government Security and Intelligence Agencies

Robert Dover (University of Leicester) (rob.dover@leicester.ac.uk)

(Work in progress – this version 3 April 2019)

Abstract

The 'age of populism' that the post-industrial world is living through has generated many challenges to existing security and intelligence structures. Some of these challenges are new versions of 'classic' problems: tracking the movement of money and people across borders, attempts to undermine Parliamentary democracy and societal cohesion, internal subversion and counterintelligence are old problems, updated for the 21st century. The magnitude, scale and precise targeting of foreign interventions in the 2016 referendum, for example, provides unique challenges to intelligence agencies, and indeed to the system of laws and law enforcement agencies who have struggled to effectively respond to these foreign interventions, and those willing to engage in norm breaking activity. This paper advances a new understanding of how information campaigns are conducted. There are profound opportunities and challenges to the technological and technical underpinnings of intelligence agencies currently, including a technological arms race and persistent debates around the scope and appropriateness of their actions. There are fundamental questions of politicisation raised by the ceaseless march of populists: we know that one of guiding mantras of intelligence agencies is 'speaking truth to power', but evidence suggests that there is currently a disjuncture in some jurisdictions that hinders this exchange. Indeed, in many populist jurisdictions intelligence agencies have been placed in a 'them or us' dynamic that is the antithesis of effective intelligence gathering, analysis and dissemination. Because much of this populism is premised upon the disruption of existing rules and traditions, its precise nature needs to be more accurately defined to allow intelligence agencies to operate within it.

The modern political era is replete with tropes around this being the 'internet age', 'the social media age', 'the big data age', and the era of populist politics. There is truth in and to all these labels, and to the notion that what impacts upon wider society must also impact upon intelligence officers, agencies and intelligence practice. There are broadly two connected developments at play: 1) the development and growth in terms of usage and use-cases of electronic communication, storage and analytical technologies, and 2) the disruption to established political (and social and economic) cultures in the post-industrial world. These connected developments have – as the paper will expand upon – generated opportunities for intelligence agencies to increase the amount of data they are able to collect and analyse, to increase their capacity for situational awareness, and to conduct inquiries and investigations, even if some of the clearer advantages are in post-hoc investigations. For intelligence agencies and officers, the technological and political disruption has offered great advantages – in terms of collection, retention and analysis – but unwieldy challenges because of the same, and to essential elements of intelligence activity such as human intelligence and the retention of secrets. But these developments have placed great challenges on counterintelligence defences (both of agencies and the infrastructure they are charged with protecting) and in running covert human intelligence operations due to the norms of social media presence and activity[1], on counter-subversion in the manipulation of politics and of public narratives, and in developing technologies

[1] In simple terms, an officer with no social media profiles is as potentially problematic as one with a hearty life on social media over many years. The notion that people who engage in (diplomatically) all the opportunities that are there to be had on social media and internet dating sites have not engaged in activity that they would rather not give further exposure to – and thus present a vetting risk – is difficult to square.

and techniques to collect and analyse useful information, rather than finding the enhanced quantities of collected information a positive hindrance.

In the wider technology, innovation and business studies literature, and particularly mainstream publications there has been a largely uncritical belief that disruptive (non-security related) commercial technology has been and is a good thing, that 'connecting people' and providing 'smarter search' are unquestionable positives. Furthermore, that the disruptors who use technology to change society are at the cutting edge of modernisation, a vanguard of a new industrial revolution. Some of this has been tempered by 'scandals' or 'revelations' like those of Edward Snowden, the insights into how *Google* collects and uses data, or the seemingly never-ending set of revelations around the *Facebook* platform, but whilst these revelations seem sufficient to prompt users to change behaviour, there has been very little in reported drop-off of uptake or use of these platforms, demonstrating the level of dependence that society has developed upon and continues to have on these companion technologies. For those campaigners who complain about the extent of government intelligence surveillance and intrusion, it must surely be the case that the level of intrusion into the privacy of individuals is far more acute from the private sector, because the public sector does not have the range of powers and legal underpinnings to make the full use of the coercive end-use tools available to them and to the private sector.[2] The public have acquiesced to the overwhelming private sector use of these technologies in a social contract concerning the access to services in exchange for private data. They have not acquiesced to the state doing the same in exchange for enhanced security, be it short term security or longer term security. That widespread need for instant gratification has led publics to wilfully ignore the vulnerabilities created by the commercial exchange of data for service provision, whilst the longer term security gain is viewed with far greater scepticism.

So, whilst I leave a critique of the business and finance implications of these technological and economic disruptions to another publication, my argument here is that in the political sphere this disruption has had a mostly negative set of perceived consequences undermining truth, integrity, and placing discourse, identity, and security under tension. Of course, one could argue that this generation of political actors have no more nor less integrity than previous generations, they merely have access to far more effective tools for behaving in an age-old way. For intelligence agencies, the consequences have been a faster moving, and more technically difficult set of propositions to resolve. In terms of collection, many of the mitigations are technical and require research and development effort. In human intelligence collection, some of the mitigations require a reframing of practice. For some practitioners there is a line of thinking that HUMINT and SIGINT are now unified because of the all-pervading nature of our communication technologies, but this is a debate between traditional models of intelligence officer and those who create technologies for these agencies. For analysis, there are profound challenges to the speed of analytical practice, but also to the interpretation of raw intelligence which, in the increasingly digital age, is subject to systematic mis and disinformation campaigns. And latterly the use of intelligence in the policy realm is subject to the prevailing political norms, oversight and regulatory lag, and thus the autocratic tendencies that have become mainstream are as much a challenge to intelligence agencies as the zeal of technology creators who have been more interested in the art of the possible than ethical

[2] Although one might question whether the ability to shape the delivery of all news, search and social information has coercive potential all of its own.

appropriateness. These technologists have been operating with a development curve that is far in excess of where society and legislators' understanding has reached.

The opportunities and threats to intelligence activity from globalization

The Opportunities for Intelligence :

The key opportunities to intelligence agencies and officers within this technological revolution has been in the amount and the depth of raw intelligence that can be collected, stored and computer analysed. This raw intelligence includes telephony records, electronic communication records, location data, social networking data, direct intercept of voice (be it on calls or VOIP, or in the case of PRISM of rooms using telephone microphones (Lee 2015)), transaction data, car and people movement data, CCTV data (Gates 2011) and so on and so forth. The sheer weight of data that these 'always on' feeds generate has created entirely new analytical problems, in terms of processing capacity, sense-making, and signalling false positives and negatives, but it has also spurred new technological insights into voice, gait and facial pattern matching, and of course the rapid sifting of very large-n data sets, and generating notions of 'normal', both in societal terms, and for individuals – it is possible to assess when an individual is doing something differently, and therefore possibly acting suspiciously (Du and Maki 2019). So, there are additional avenues into individual targets that were previously impossible (or more difficult), but there is also a range of tools, techniques and technologies that allow a meta-level analysis of data to provide some generalisable behavioural security rules to be understand patterns of behaviour that give rise to concerns or which might trigger investigations and so on.[3]As was seen with an over-reliance on SIGINT and ELINT at the turn of the century, there is a danger of losing analogue intelligence techniques (eg intuition, forms of corroboration etc) to data, and therefore computer, driven solutions: a false assessment of the financial efficiency and accuracy of data-driven analysis.

Whilst the democratisation of travel and the liberalisation of migration (although now under threat and tension) has led to targets being able to move across the globe easily and cheaply, with some extra-judicial operations being able to be prosecuted without effective counterintelligence (Urban 2018) or longer term sleeper operations also being able to operate covertly for years (Lucas 2012), the truth is that the movement of people, and objects across the globe is recorded and can be monitored in a way that would have been unthinkable only 20years ago. As a response to atrocities such as the Lockerbie aircraft bombing, and indeed the 9/11 attacks too, the US Department of Homeland Security utilised their dominant market position to insist upon a data-sharing scheme across the transatlantic area called Passenger Name Record (PNR), for access to US airspace and

[3] There are unresolved issues around the creation of these 'normal' behaviours, from which outliers can be derived and noted. I was party to a heated exchange between several academic colleagues after the 7/7 attacks in 2005, in which one – who was diagnosed with autism and presented as a-social – strongly remonstrated (including with the memorable accusatory phrase 'normalist') with the other over the sorts of profiling which had resulted in the death of Jean Charles De Menezes, because he was someone who also wore a heavy coat in the summer on the tube and felt more comfortable with his hood up. The problem of creating profiles that only capture 'neural normality' as 'safe', is deeply problematic for those impacted by conditions that render them unable to conform to the neutrally normal norms, and undermines the analytical power of the models.

airports (Argomaniz 2009). This allowed – at the point of booking – the US authorities, and whomever they shared the intelligence with, to cross-reference travel plans with known terrorists or those who had come under suspicion in some way. The PNR is – however – a dragnet, catching all of us who travel, not just targeting on those who might fall under suspicion. The negotiations between the US and EU were protracted and often ill-tempered. European legislators – for good historical and cultural reasons – were deeply uneasy about the data of their citizens being 'hoovered up' in this way, and were particularly exercised about the length of time that data would be retained, and what guarantees would be in place to ensure that the data was not passed onto third countries (and therefore what those countries might do with it) (Di Matteo 2017). PNR data is – however – not restricted to international air travel, it also applied to movements by train, and by sea as well. The PNR initiative was as much about doing something because the technical capability existed to collect, retain and analyse this data, as it was about addressing a real security concern. The n= of this data also allows for meta-level analysis to occur, to create an assessment of 'normal' behaviours and 'outlier' behaviours (at the individual and group level), which can then be flagged and responded to by domestic security agencies, creating any number of false positives. Equally, it has led to other types of traditional transaction to become labelled as suspicious, such as paying for train tickets in cash, rather than by credit or debit card, something that should not necessarily trigger an alert, given that it is a legal means of purchasing a train ticket. The act of using legal tender has been given a value loading because it is more difficult to track, and we can see in the field of general commerce that the use of physical cash is being subject to incentivisations (both positive and negative), with the encouragement for users to use traceable 'contactless' card payment systems (Jones 2019). Uptake of these contactless non-cash methods has seen variable uptake across Europe, with very high-levels of uptake in Sweden (Arvidsson 2019), but correspondingly low levels of uptake in Germany (Korella and Li 2018), with one of the non-technical reasons for this variation being the historic experience of German governments having too much insight into the personal life of individual citizens.

In a similar vein the monitoring of monetary transfers, in part as a response to the terrorist threat, has offered a historically unprecedented set of insights into the transactions and conduct of individuals, within borders and across borders. There is, of course, a reasonable rationale for why international monetary transfers have increased in number in the last twenty years as cheaper and freer movement of labour has allowed migrant workers to send remittances back to family members in countries of origin. Butthose involved in the operational and logistical lines of terrorist activities were adept at using international money transfer services to facilitate their activities. After 9/11 most NATO nations sought to enact laws that allowed them greater levels of lawful intrusion into banking activities. The 2010 SWIFT affair (De Goede 2012) (Suda 2018) (which involved the US acquisition of EU citizen's financial data) demonstrated a level of intelligence capability that at once raises questions around why other sorts of financial malfeasance goes undetected or undealt with, but also moved terrorist logistics lines away from international financial instruments and towards other types of financial transaction, be they via a Hawala system of moving money between intermediaries on promissory notes, or via assets in freeports, making surveillance and detection far more complicated for security agencies (Dover 2016). The improvements to the technologies underpinning financial surveillance has resulted in far greater surveillance of and enforcement against the general citizenry. The UK HMRC's 'Connect' computer system is a good, contemporary example of how data analytics and 'big data' can be used to improve enforcement practice (Petit 2018). Connect draws in feeds from the banking sector, financial services such as loans, credit cards, and spreads into social media to make assessments of whether the declared income matches up to

the spending patterns of the individual. Greater levels of international interconnected in the tax space (which is threatened by a 'no-deal Brexit') has also allowed the tax authorities to detect when individuals have offshore financial interests and to raise a question about whether undeclared earnings exist there for tax purposes (HMRC 2019). The use case for these technologies is to improve the percentage collection rate of revenues, but we should observe that the UK government's 'connect' system does a very similar job to private sector data aggregation and analysis services, such as Experian and Equifax in credit referencing, the supermarket 'club-cards', and major insurance brokers all of whom collect and analyse similar data as the HMRC, but for different use cases, and without some of the political oversight of a government agency, and – as a whole – a track-record of leaks and vulnerabilities that is unenviable (Bloomberg 2019).

The other major line of benefits to intelligence agencies comes in communications technologies. The ability to intercept communications (be they telephony, instant messaging, emails, files), to intercept voice (via the reported mechanism of PRISM, or voice recognition CCTV), and to exploit vulnerabilities in the technologies of the 'internet of things' to track whereabouts, social networks and patterns of behaviour is a significant improvement on the mostly analogue techniques of the Cold War. Where these electronic vulnerabilities can be exploited by domestic agencies, they can of course also be exploited by adversary and friendly, but competitor agencies, and so part of the underlying debate around the Snowden revelations, previous debates around whether China and Russia are able to intercept undersea internet traffic in transit, and also around the somewhat loud and persistent debate about Huawei and their 5G networking infrastructure is the sense that whilst 'friendly' agencies might able to understand their publics in a far more detailed way, so might adversaries and competitors from less open nations, putting them at a clear strategic advantage, particularly in the event of future hostilities, particularly if one considers how little allied nations will know about the publics of Russia, China and North Korea in response due to legislative and technical barriers to prevent information leakage. The extent of the knowledge (be it personalised or meta level) that is capable of being lawfully intercepted is large, but of a comparative (if not reduced scale) to that of the handset manufacturers, data carriers, and app providers, as shown by the recent scandals that have enveloped Facebook, amongst others (Schneble, Elger and Shaw 2018). So, there continue to be questions about what appropriate controls can be placed around the data that is generated by companion devices (smart-phones and internet of things peripherals), and by applications whose business model seems premised upon the collection, aggregation and sale of data, rather than the service they are providing (Zhubov 2019).

The final major class of opportunity for intelligence agencies is located in the management of public narrative and operational spaces. This is an opportunity that seems to have been significantly grasped by the Russian government in what has been variously described as information war or hybrid conflict by observers and analysts (Gioe 2018) (Seely 2018). Where the Russian government and their energetic western supporters are correct is in the observation that the NATO powers engage in a range of activities that are not entirely dissimilar to the Russian modus operandi. This is a clash between regimes who believe strongly in *their* version of *the truth*. Understanding these *truths* and why actors believe in them and act in reliance of them is key to challenging and countering them. In the UK, there is a military doctrinal underpinning for non-violent operations, which include the utilisation of media channels and psychological profiling, known as '77 Brigade' (UK Ministry of Defence 2019). The United States and Israel, amongst many nations, are also highly engaged in this area. In the winter of 2018, there was a hack and public dissemination (albeit via the unindexed web first) of internal documents of a British foreign and defence policy charity, the *Institute for Statecraft*, who had been partly funded by the *UK Foreign and Commonwealth Office* to identify and counter Russian misinformation campaigns, but who were accused by the Russian state

media and a large number of online commentators of carrying out precisely the sort of mis- and dis-information campaign that the Russian state has been accused of, most notably over the previous three years.[4] The particular project to highlight Russian disinformation was called 'the Integrity Initiative' and this phrase has become – on social media platforms – synonymous with 'deep state' activities, in part because of the presence in the core staff of people who activists say have intelligence backgrounds, and because of the activities the initiative is said to have involved (Sputnik 2019) (Sputnik 2018). The incident resulted in urgent questions and a debate in the House of Commons (Thornberry 2018), which conforms to part of the modus operandi of information warfare noted in several paragraphs time. Since November 2018 the phrase has been used to describe any perceived western government media manipulation, on twitter alone the hashtag has been used over 120k times between November 23rd 2018 and 28 February 2019.[5]

Again, there is a partial analytical truth in those who had been most vocal and most critical of the UK Foreign Office for its funding of the Institute, which is that the academic and think-tank research into 'hybrid warfare' (a term that continues to be contested and which is perhaps premised upon a misunderstanding of the Gerasimov doctrine) has focused upon Russian misinformation campaigns (and this was the stated purpose of the Institute), and Chinese and North Korean activities (presumably for the normative reasons of the 'other' being bad whilst 'our' activities are value neutral, and equally for reasons of national allegiance), whilst the counter-efforts of NATO members has yet to be subject to sustained analytical critique. So, we do not currently know whether – in cyber space – the modus operandi of allied or adversary intelligence and security agencies (or their contractors) are similar, or whether there are national ways of war in this area.

At the time of writing there does appear to be a single or prevailing modus operandi for adversary mis and disinformation campaigns that sit within the broader umbrella of hybrid warfare. Previously it was thought that these information operations operated with combined human and 'bot' accounts to generate misinformation and a critical mass of messages to overwhelm or undermine the official narrative, something that would then be amplified by fellow travellers or those inadvertently amplifying these messages, which in turn would be picked up various parts of the legacy media (e.g. broadcast television and online and paper based press outlets). The originating moment was seen, therefore, to emerge on regular social media platforms such as Twitter and Facebook (House of Commons: Digital, Culture, Media and Sport Committee 2019), whilst the Institute for Strategic Dialogue places those originating moments (albeit in the particular context of German elections) as coming from platforms such as *4Chan*[6] and *Reddit*[7] (Institute for Strategic Dialogue 2019). This fits within the conceptual framework of the 'hybrid media system' as framed by Andrew Chadwick (Chadwick 2013). In terms of information warfare, the hybrid media system and earlier researchers have missed that these campaigns actually begin in forums on the unindexed part of the world wide

[4] It should be noted that a number of academics and journalists were erroneously noted on leaked documents as being part of a UK hub of experts taking part in these activities: the vast majority of them have publicly refuted the notion that they participated in these activities, and have noted their surprise at being included on the documents.

[5] As scraped by the author, using an API. The set of scraped tweets may not be complete due to the vagaries of access Twitter provides researchers, and APIs who do not subscribe to 'the full stream', something which I am told costs a six figure sum per annum.

[6] https://www.4chan.org/

[7] https://www.reddit.com/

web, otherwise known as 'the dark web'. These forums share leads, rumours, documents and so on. The challenge for those seeking to counter these attacks is to accurately assess whether they are viewing government sponsored coordination, sophisticated non-government coordination (and the Venn diagram between those two groups might be interestingly close), amateur attempts, or – intriguingly – denial and deception strategies. Far from there being an organic or organically viral quality to the early moments of social media coordination, messages and strategies are developed in unindexed forums and are then brought to the public and indexed level (be it via social media, private messaging, dissemination to journalists). If we extend the 'viral' metaphor slightly, we can find utility in finding and identifying 'patient zero' in a messaging campaign, as this provides more information about the motivations and origins of the campaign, its aims and likely trajectory. But just as in epidemiology, finding this 'patient zero' is technically difficult: when I tried to find patient zero in the messaging around four terrorism incidents, I had confidence that I had managed it once, and my confidence subsided in that instance as well. Working under an understanding of information campaigns that begin in the indexed web, these efforts were also pointless. By the time these campaigns have found their way to the indexed web, they have been rinsed of much of the data that would make the patient zero analysis interesting.[8]

So, my reconceptualization of this modus operandi is that for regime or state-based information campaigns, the originating sources (who push out to non-state-based accelerators) are capable of being found in the unindexed web, mostly in forums. These accelerators then bring these messages to the indexed web, and social media and push these messages out using a combination of familiar channels (accounts) and often new 'bot' accounts to provide the messaging with trending heft. Legacy media which is aligned through ideology or ownership will then pick up these trends and further rinse and legitimise them by reporting on them, in skeleton format to begin with, and then via invited academic and think-tank research experts in interview and talk-show formats, which then spurs further online commentary, and may eventually break these messages out into unaligned legacy media outlets, by which time the message can be considered to be virtually mainstreamed. In parallel, during these campaigns, a significant and active quotient of individuals will be engaged in open source intelligence investigations or activism journalism, to do what they market as being digging further into a story. They do this using a range of internet tools and freedom of information requests and so on that has been labelled as 'lawfare' by some, and the 'instrumentalisation of the law for strategic ends' by others (Dover 2019) (Sari 2019). What these accounts (be they individuals or 'bots') are often doing is picking up fragments of information and narrating around them. By the time these fragments and narration has entered its third reformulation it is has reached beyond the point where it is logically connected to the original fragment of information. As an analytical technique it is perilously close to the logic of conspiracy theories, and indeed the logic of populist politics, where there will always been a tiny kernel of evidence that sparks the narrative, but that the narrative's end point will be significantly removed from where the evidence sits. Having scraped a considerable quantity of social media data[9] it is clear to me that once a disinformation theme takes hold on the large social media channels it is then also used to reposition other narratives the

[8] The use of the term 'rinsing' is to deliberately evoke the term from the practice of money laundering where money is seen to become progressively 'cleaner' when it is moved through a variety of accounts or a variety of asset classes before it emerges at the end as 'clean money'. In a similar way, information campaigns

[9] in two stages: first using the Stream Twitter's Application Programming Interface (API), and second using the Search API which is part of Twitter's REST API. The stream API accepts the filtering of request results, as Twitter maintains limitations in its API to the volume of data that can be retrieved within a given duration (450 requests every 15 minutes).

collective behind the theme find awkward.[10] So, narratives around individuals are reshaped to produce favourable or unfavourable recastings, the narratives around particular episodes are re-historicised in the light of the new, and largely unrelated data to provide 'new insights' as the activists see it. But the extent of the reshaping endeavour, and the standardised way it is produced from a shard of tangential evidence suggests to me that it is a mistake (per Brandolini) to focus on the micro-movements in the narrative, but to home in on the far broader questions of 'what are these campaigns trying to achieve?', and 'what are these campaigns trying to distract us from?' and in the case of Russia both of these questions are pertinent, whilst with China and North Korea it is the former question that might be more productive.

The opportunity and challenge to intelligence agencies from this form of information campaigning sits in the ability to shape the operational environment at one end, and to be unable to wrestle back control of the narrative, at the other. There has been a strong and understandable argument within the literature that by paying these campaigns credence they are given greater influence: the impact of the UK television channel 'RT' (formerly called Russia Today) with its very small viewing figures is undoubtedly overdrawn, but we have seen the impact of disinformation upon election and referendum campaigns both in the UK and wider (Yablokov 2015). The impact of narratives around immigration (in the case of Brexit, elections in Germany, Sweden, Denmark, France, and the United States, and in the 2018 case of the Salisbury chemical poisonings) have been to undermine certainty in the minds of the public: such ground is fertile for competitor agencies to capitalise upon, and to undermine national resilience and the ability to respond and cohere: central tenets of strategy (UK Ministry of Defence 2019). There is currently inadequate understanding of the mechanisms of influence (of 'what works'), and indeed how these campaigns are being prosecuted. This research gap fits between information and computer sciences, political communication, strategic studies, psychology (personal and social), sociology and the practitioner field of counterintelligence and psychological operations and can only satisfactorily be addressed in collaborative forms by these fields.

The Challenges to Intelligence

The main challenge to intelligence activity in this modern era comes from the underpinning and ongoing disruptions to technology, finance, and society. The Snowden revelations demonstrated where technological possibility, coupled with a lack of ethical and legal oversight and control, can lead to curiosity or possibility-led collection of intelligence that is disproportionate to the threat it presents and itself can form a threat to social relationships. Snowden demonstrated – in the main – a pattern of collection for collection's sake. The impact of this – as it rippled out into common understanding – was to undermine the sophisticated tools for situations when they are used for entirely appropriate and proportionate targeting (Walsh and Miller 2016). Overall, though, the interconnectedness of everyday life across the globe, not just in the post-industrial global north, has provided an unprecedented opportunity for intelligence agencies – particularly those engaged in signals and electronic intelligence – to gain access to the inner lives of their own citizens and those of other nations. With this opportunity has come the challenge of making sense of hitherto unimaginably large data sets, and that those who are engaged in subversive activities have constantly iterated their technology and techniques, creating a form of arms race akin to that which was seen during periods of the 20th century in conventional and then nuclear technology. This

[10] I am currently working with data across a range of such cases to distil out useful lessons for political messaging, and consequently I am being slightly coy in what I pre-present here.

analogy holds true for non-state-based actors, who have prosecuted Vietnam-style 'wars of the flea', finding increasingly ingenious ways to gain advantage over state-based intelligence actors. In communication terms, we see relevant evidence in the use of dark-net forums in the early part of this century, the utilisation of in video-game communication platforms as a means by which to pass targeting data to each other as a means by which to avoid detection, without having to go 'toe to toe' with state based agencies in developing high-end technology (Podhradsky, D'Ovidio and Casey 2012). Indeed, as has been commented by others, part of the success of these groups has been in using the high-end technology developed by neo-liberal economies against those countries. In finance terms, the use of international wiring was quickly replaced after 9/11 and improvements to financial tracking by the US and British authorities by a combination of analogue – and ancient – money transfer practices, complemented by the moves into cryptocurrency, which require considerable processing power to de-anonymise. Asymmetric actors have also been at the forefront – and preceding some of the behaviours of populists – of developing effective communication doctrine, in one guise utilising hacking and dark-web propagation as a means to break stories into the indexed-web social and legacy media and effectively crowd-sourcing social media attacks and mobs, whilst in another guise, adopting high-end production values for propaganda videos, and being ahead of western militaries in breaking stories quickly, and thus asserting message control and timeliness: two core facets of effective public communication.

There is an important and ongoing corrective to what has become bracketed under the Snowden revelations, which is the growth of surveillance capitalism (Bellamy-Foster and McChesney 2014) (Zhubov 2019). This form of capitalism is in many respects far more disruptive than anything that government agencies have hitherto attempted to do with electronic surveillance. Thus far, so officials claim, European and North American governments have been more preoccupied with attempting to disrupt and prosecute those involved in threats to people, property and national security and thus have not had the resource to engage in other types of oppressive activity. This claim might be viewed with some healthy scepticism following the Snowden revelations (Bellamy-Foster and McChesney 2014) (Lyon 2015) (Dencik and Cable 2017), the ongoing UK inquiry, headed by Sir John Mitting, into enhanced surveillance into activist groups (the vast majority of which appear to have been law-abiding and peaceful) (Inquiry 2018) (Schlembach 2016) (Casciani 2019), the British government's previous history in these activities, notably the Ministry of Defence's Information Research Department (1948-1977) which operated to counter communist activism and propaganda (Wilford 1998). As an argument, it is also something of a fig-leaf that in effect 'yes, we have the capability, but we're just too busy to use it', particularly in an era where authoritarian inflected populists are coming to power across the globe. In the private sphere, however, there is enough evidence to suggest that this form of surveillance capitalism is having a profound impact upon our social relationships, on how youngsters and young adults are forming their core identity, on commerce and economic relations, and in terms of how well understood we are as citizens by data owners and data analysers, predominantly those in the advertising sphere, sufficient to cause forms of social disruption, and therefore presents an attractive target for manipulation by adversaries.

A technology columnist, Kashmir Hill, did an interesting experiment to test whether it is possible to function in post-industrial society without drawing upon the services (or underpinning architectural services – e.g. data hubs, web-hosting) of Amazon, Apple, Facebook, Google, and Microsoft (Hill 2019). To do this she inserted code into her connected devices to block them communicating with services from any of those five companies, and to do so over a period of 6 weeks, although she only

blocked all five together in the final week. What Hill discovered was that the vast majority of the services she used (essentially all of them), were dependent upon one of these big five companies. Even when she attempted to use work-arounds, such as using the privacy search engine 'duck-duck-go', she discovered that it was underpinned by Amazon's web servers and thus unavailable to her. When Hill wanted to transfer a media file for work, she discovered that the workarounds of *Mozilla*[11] and even *Onionshare*[12] were premised upon Google and Amazon webservices, thus excluding them as well. Consequently, Hill concluded that is technically possible to avoid the big internet companies but the cost in time and expertise to do is considerable, and prohibitive (Hill 2019). From an intelligence and security perspective we should note the concentration of web services, and therefore data capture, for nearly every member of society with access to interconnected technology. The personalised delivery of information to users, based upon preferences, usage and interest, means that the news I read is likely to be very different from the news my students read, or the non-academics I socialise with read (Bakshy, Messing and Adamic 2015). So, one of the inherent powers of these big five internet companies is the ability to shape the political space via the algorithms they are utilising for search and the push for data. The delivery of personalised news, and the absence of cross-cutting news (as per Bakshy et al) may partly account for the starkly polarised news environment we are witnessing currently. There is also a popular misconception of these algorithms being somehow value-neutral or 'objective' because they are utilised by computing technology. They have – of course – been programmed by humans and are therefore a scaled manifestation of the experiences, education, conscious and unconscious biases of the programmers who programmed them. The values of the programmer, and the way that information is distributed and delivered not only is capable of delivering change to the political culture, but to the values and understandings of the citizenry but also the law enforcement and security officials that are drawn from society. In a fascinating article, Landon-Murray and Anderson tie together the increasing prevalence of the internet as a source of information, intelligence and neuroscience to suggest that the internet is having a fundamental impact upon the ability of intelligence analysts to effectively sift, sort and understand evidence (Landon-Murray and Anderson 2013). This argument can now be extended to suggest that actually the big five internet firms have the ability to partially shape intelligence officer's understanding of the world and of events, through the way they sift, sort and deliver information, through the absence of classified material or the need to reach policy makers in a way that aligns to their knowledge base. The types of surveillance society commonly associated with George Orwell's *Big Brother (1949)* dystopia, or the fictionalised account of East Germany's Stasi in the film *The Lives of Others (2006)*, looks somewhat tame compared to the potential held within the main internet and technology companies.

The dominance of so few companies places them in a peculiarly strong position in regard to understanding all strata of society, down to the level of individual granularity. They are so strong in this regard, because it is this data and their understanding of it that they have successfully monetized (Zajc 2015) (Skeggs and Yuill 2016). And they have not been passive in this monetization or improvements to their respective offers to monetize it. There is evidence and commentary on the techniques deployed by some of these companies to ensure that users keep interacting with these services, including – for example – the deployment of techniques to manipulate dopamine responses in individual users (Błachnioa, Przepiorkaa and Pantic 2016). These companies are also technically able to control the flow of information (Schelter and Kunegis 2018), be it to governments or the public, something that could have a significant strategic impact, or less seriously, an ongoing impact upon politics, or unfolding events. As noted previously our understanding of how messages impact

[11] https://send.firefox.com/
[12] https://onionshare.org/

upon citizens is underdeveloped, and our understanding of how citizens would respond to being bombarded with critical messages, or a messaging vacuum is similarly poorly understood. But the literature has now begun to reflect a discussion and growing concern about how internet companies are able to have an impact upon the political views and the voting actions of their users, both in terms of search and in terms of social media aggregation (Robertson, et al. 2018) (Diakopoulos, et al. 2018) (Rose 2017).

State based actors, on the other hand, have engaged in day-to-day cyber-attacks on each other, which amount to a low-intensity conflict, and constant subversion (Betz 2017) (Opara, Mahfouz and Holloway 2017). And it is to subversion and destabilisation that these activities really owe their origins: the micro-impact, or the overt intended outcome seems less important than to create an over-arching culture of subversion and destabilisation. So, whilst there has been considerable Chinese and North Korean activity in stealing intellectual property from western nations, which has enhanced the manufacturing base of China, in particular, the aim is far more meta, than the theft of the particular IP (Beckett 2017). Hacks and attacks against persons of interest (be they politicians, journalists, academics or even film industry workers – as per North Korea's hack and revelations against Sony Pictures in 2014) are again aimed at more general subversion and destabilisation (Inkster 2015). In a similar vein, the active courting of western politicians, journalists, academics and other influencers with money, travel and advantage has had the impact of creating a cadre of fellow-travellers who serve to advance the interests of their patron, in a way that sometimes conflicts with the interests of their own nation (Parton 2019) (Gioe 2018) (David-Fox 2003). So, we can observe an information and influence conflict that has become more structured, better organised and more richly financed than in previous eras. There is also evidence akin to the arms race dynamic of conventional and nuclear weapons in the heavy spending on paradigm shifting technology, such as quantum computing, which would render current cryptography entirely obsolete (Mosca 2018) (Farouk, et al. 2018). Breakthrough technologies such as fifth generation networks (5G) which would accelerate the utility and adoption of the 'internet of things' and with it 'smart home', and 'smart cities' initiatives (Li, Xu and Zhao 2018), whilst the breaking of standard cryptography will be highly disruptive because economic transactions, communications and sensitive and personally identifiable data have become so heavily premised upon these technologies. The evolution of mobile phones into 'companion devices', those which we are constantly interacting with, has reduced our collective capacity to operate in traditional analogue or indeed just ways that do not involve some form of interaction with an electronic or communicating device. The notion of neuroplasticity in this field, of how the brains of individuals are being physically transformed by the collective inability to focus on longer form research, to cope with silence, or boredom, are emerging areas of research that impact upon our understanding of the citizenry and indeed of intelligence analysts (Dongwon 2015) (Montag and Diefenbach 2018). Similarly, we expect intelligence analysts to be able to simultaneously provide well thought through and clear product, but also to be closely following technological developments, something that is undermined by the rate of technological-generational change in information technologies, in terms of hardware, techniques, tools, attack vectors and so on.

Populism and Disruption

Political disruption has been assisted by internet enabled platforms (Krämer 2017) (Gerbaudo 2018). This has commonly been felt to be in the way that they facilitate the creation of shared identities, of 'community', the sharing of core or important information, the coordination of actions and events, and the reporting of actions against the shared identity. These highlighted mechanisms under-report the extent to which these dynamics are impacted by considerations of the hybrid media system (that is the extent to which the legacy media and new media are related and are synergistic), and the extent to which there is influence or even control over narratives by classic or traditional interest groupings. Moreover, the extent to which messages impact upon citizens (and the mechanisms by which they do so) is an area of research that has yet to come to maturity[13] but it an important component of the impact of these disruptive platform and politics have had on the security of nation and the sanctity of our democracy. These dynamics are very similar to the dynamics observed earlier in this paper around state-based information warfare campaigns and their utilisation of private sector communications platforms.

Modern day populists have been demonstrated a strong willingness to break rules. They have also showed a considerable disregard for the truth. They have a facility for the evocation of myth, and to very accurately tap into the illiberal fears of the population (Kelsey 2016) (Groza and Groza 2017). Some of this facility is not through political 'feel' or 'touch' but by the utilisation of data analytical techniques and large-n data sets of personally identifiable data, that is a reapplication of marketing techniques into the political communications sphere (Ward 2018) (Ruppert, Isin and Bigo 2017). Populism is also a response to an established political system that has run ahead – in terms of sentiment on some issues – of its population and these populist actors serve as a particularly stark form of market correction.

Expertise and Illiberalism.

The rise of so-called populists across the globe has been typified by a strong disconnection from verifiable evidence, whilst simultaneously impugning those who make evidence-based claims and refutations of populist claims with evidence. As the computer programmer Alberto Brandolini somewhat caustically – but accurately – claimed: "The amount of energy necessary to refute bullshit is an order of magnitude bigger than it is to produce it." (Brandolini 2013). Brandolini's law – as it is now known – is highly applicable to populist politics and to modern political discourse where it is found both on social media platforms and played out in the legacy media, where it is wrapped into the hybrid media system - where attempts to correct important detail results is loss of momentum and impetus, and is therefore ultimately futile. Furthermore, a recent study provided evidence for the old truism that lies spread more quickly than truths in a study of how stories proliferate online (Vosoughi, Roy and Aral 2018). Some influential contemporary politicians have gone out of their way to compound these effects through discrediting those who have dedicated their professional lives to understand whatever subject it is under discussions. So, for example, the current UK Environment Secretary Michael Gove said in the 'Brexit' referendum campaign that 'the people have had enough of experts', which was a meme that took hold during the campaign, as a means by which to undermine the overwhelming majority of academic economists who assessed a negative impact to the British economy from Brexit (Financial Times 2016). During and since the referendum result, every expert assessment – including those of the Bank of England and the UK's Treasury have been dismissed by leave campaigners with a catch-all term of 'project fear' (Halligan and Lyons 2017). Similarly, there are a vast number of examples of where the settled assessment of the climate change discipline has been challenged, not with science, but with variations of emotional response

[13] But is one I am actively working on.

and revisionist history (Oreskes 2018) (McCright and Dunlap 2011) (Lewandowsky, Oberauer and Gignac 2013). In the US Presidential election (including in the primaries) there was accusations levelled at candidates around their probity, family histories and so on that had literally no basis in evidence at all (but which helped to inform narratives that voters seemed wedded to), and indeed the election has been haunted by the investigations into the alleged involvement of foreign powers seeking to interfere with the election process. But these trends are important to understanding the challenges that face security officials in this modern era, because it is suggestive of the way that our political class is able to instrumentally utilise a rejection of evidence and evidence based assessment in favour of value-based positions, and it is also suggestive of a wider dysfunction in our political and security culture between evidence based and value based decision making, reducing the attractiveness of careers and therefore quality staff in these areas, and the cultural gap that exists between these positions. Such a rejection of evidence-based assessment, not only by the policy sphere but by the publics undermines the work of intelligence agencies and the collective credibility they depend upon.

Value-based voting is not new (Schwartz, Caprara and Vecchione 2010) (Barnea and Schwartz 1998). Part of the explanation for 'champagne socialists' and 'working-class Tories' can be found in value-based voting patterns, rather than those which premise rational maximization of economic interests, for example. We can see the same pattern in why some consumers display brand loyalty when they believe the brand aligns to values they identify strongly with (Gyrd-Jones and Kornumb 2013) (Ross and Harradine 2011). The populists who won the referendum campaign in 2016, and the US Presidential race in the same year understand – far better than their competitors – not only the values of a critical base of support, and how to articulate messages to that base of support. And so, there is an additional critical challenge to intelligence and security in this age of populism, which is that there is a significant gap between 'elite sentiment' and the sentiment of the ordinary citizen. We take for granted – in universities, as well as in policy making circles – that the various equality agendas that have developed over the last century and a half, and which have been variously legislated during that time are universalized norms, or on their way to being so. There is now quite good evidence to suggest that this is not the case, and it is 'populist' discourse that has understood this far more effectively than 'establishment' actors. We can select some emblematic examples to illustrate this point, from across the breadth of experience of 'ordinary' citizens:

Immigration and the attendant freedom of movement (of labour, for lifestyle and for living) was assumed to be a significant positive of the European Union project. The ability to access by 2018 28 different economic markets, without relatively few restrictions, was unprecedented in modern history, and in 2018 20.4million EU citizens were living in different EU countries than they were born in (EUROSTAT 2019). But whilst the political classes, and indeed those placed at the strategic end of business and commerce viewed this as an unalloyed good, the public – particularly under conditions of financial restraint and austerity – did not (Gietel-Basten 2016) (de Vreese and Boomgaarden 2005). Some of this negative view seems to have been informed by the perception of not sharing in the economic benefits of globalization, and – therefore – being on the outside of the globalization of finance and commerce (Colantone and Stanig 2018). And whilst it is not particularly easy or popular to say so, immigration was not an issue that was neatly aggregated in the minds of the electorate between EU immigration, and non-EU immigration, which was and is governed by separate regimes. Indeed, the entanglement in the popular mindset between domestic radicalization, 'foreign fighters', returning fighters and wider population displacement from the Middle Eastern warzones into Europe was repeatedly cited during the referendum campaign and since as the most persuasive reason for casting a vote for leave, even though it had little to do with EU immigration policy (Goodwin and Millazo 2017) (Veltri, et al. 2019). This was further, and deliberately, entangled by

leave campaigners who cited – in poster adverts, and through directly targeted adverts on platforms such as Facebook – that remaining in the EU would open up the prospect of uncontrolled immigration from Turkey, playing on racial and religious sensitivities (Ker-Lindsay 2018). The reality – as experienced through the ballot box – was that 'the establishment' were far more comfortable with immigration than the public, and the referendum represented an opportunity to express that dissatisfaction tangibly. In turn this has left the security establishment with a weight of public expectations to police the perceived security threat of non-EU nationals, as a mirror to the preferences of the public.

We can see similar disjuncture in the establishment and legislated view of protected identity characteristics and religiosity in which the freedom to declare one's own (gender) identity, sexuality or to practice religion, with all associated practices and symbology. The legislated view is clear, but the popular acceptance of these differences from a constructed, perceived or held homogenous norm is not as clear, and forms part of the discourse of discontentment even amongst those who one might characterise as belonging to 'middle England' in all other ways. And this is important in several ways: 1) the official and public understanding of what are and are not acceptable views (and by extension what are extreme views) is currently unaligned; 2) such a misalignment serves to alienate those whose views are now unacceptable (but which had been normatively acceptable, and indeed been largely unchallenged over the previous 50years), and it also serves to alienate those protected from these views because it highlights difference and creates an impetus to seek redress. And it is this that has – in part – driven electoral backlash: the phenomena of 'we are not listened to by the Westminster bubble'; and 3) there is a hitherto underexplored set of impacts around preferences and views of intelligence officers, in absolute terms and in relative terms when norms shift, and how these impact upon their performance.

The key challenge to intelligence activity from populist politics is via forms of politicisation. These might include co-option of officers and agencies or – perhaps more strangely - in the case of the United States currently, alienation, and a wider undermining of the credibility of intelligence activity, the undermining of expertise and a creative tension or malleability of narratives. The structural underpinnings of this populist age creates a second line of challenge that is wider than the populists themselves: the international interconnectedness of transnational interest groups or networks, the sharing of techniques, expertise, and resource across national boundaries, and the arms race in technologies and techniques that requires a great deal of resource and expertise to maintain pace with constantly allows opportunities for competitor groups and states. This has now taken on the dynamics of an arms race, crystallised by the prospect of quantum computing, and the strong (and probably unwarranted) moves against Huawei's 5G networking equipment (Zhang 2018). Perhaps the greatest mistake made, thus far, by agencies, with a strong steer from the political elites has been to avoid calling out the serious damage populism and its structural underpinnings has done to the established systems of governance in the countries effected. The preference for the line that our democracies are not only intact but are robust and flourishing has allowed competitor nations and groupings greater latitude to continue inflicting harm upon our political systems and political culture.

Conclusion:

There is an interesting set of paradoxes in the narrative of the new and populist politics around intelligence and security.

Invasive security is good. Unless it is directed at 'us'.

It is good when it is directed at 'them'. And 'they' would have nothing to fear if they were not doing anything wrong.

Policing and intelligence levels should be reduced because they represent bad value for money, and do not investigate 'the right things', but crime and subversion is going up because the 'peasants are revolting' and that is also intolerable.

Similarly, internationally founded collective defence and security jars with populist disrupters because it is part of an established and self-appointed rules-based system that opposes them. Indeed for the first time in modern history there are potential leaders of post-industrial nations with whom there are said to be serious concerns in various intelligence communities about sharing intelligence with them (Schindler 2017) (Balls 2018). In particular configurations this might serve to undermine established international intelligence liaison, such as the Five Eyes group, or even the NATO alliance. Domestically, the unwillingness to share might hinder the investigation or curtailment of security threats, and furthermore the definition of subversion (and therefore what might qualify as activities requiring curtailment) might be subject to significant change. The preference amongst populists for current and historical world leaders who are described as being 'strong' or 'autocratic', depending on your stance raises the prospects of the advances in surveillance technologies and techniques being used in the internal capture of the apparatuses of state.. So, whilst government intelligence activity has always necessarily been political – despite the widely held view and position that it is not – it may well play a far more significant political role in the medium to long term, in policing the boundaries and curtailing the excesses of populists, albeit still within a position of 'not being political'.

The increased politicization of security and surveillance comes through in the advanced uses of data analytics, which may result in a widening of the scope of investigations, but also in the constant prompting for investigations and prosecution of opponents that follows the modus operandi of information warfare described earlier in this paper. Security is – therefore – not subject to logically consistent narratives. There is a constant set of constitutional questions, around the positioning of intelligence and security actors guarding our democracies and our democratic institutions that are becoming more pressing: for activists this debate would centre on the appropriate role, scope and powers of intelligence agencies to interfere across analogue and digital channels. For those who do not see themselves as activists per se, the debate would focus on the ways in which foreign powers utilise open platforms, our institutions and domestic citizens to advance their strategic ends, and this has become more pressing in the light of populists being more willing to break norms and rules. The disruption of our politics is as much about the hidden wiring of the state (the security and intelligence services) as it about conspiracies around the activities of the 'deep state', which is a pejorative code for the same actors (O'Neil 2017). This paper makes a novel acknowledgment of the political role of the intelligence agencies, an argument that sees evidence for the 'steady' rather than 'deep' state, but one which also recognises their unique political role across post-industrial societies, including our own. In discharging those functions, the rapid development of transnational interconnected technologies, and the near parsimony of those technologies is stretching traditional analogue, analytical and digital functions of intelligence.

Bibliography

Argomaniz, J. 2009. "When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms." *Journal of European Integration* 119-136.

Arvidsson, N. 2019. *Building a Cashless Society: The Swedish Route to the Future of Cash Payments.* Munich: Springer.

Bakshy, E, S Messing, and L Adamic. 2015. "Exposure to ideologically diverse news and opinion on Facebook." *Science* 1130-1132.

Balls, K. 2018. "Should the government share full intelligence with Corbyn?" *The Spectator*, April 2.

Barnea, M, and S Schwartz. 1998. "Values and Voting." *Political Psychology* 17-40.

Beckett, P. 2017. "Data and IP are the new nuclear: facing up to state-sponsored threats." *Network Security* 17-19.

Bellamy-Foster, J, and R McChesney. 2014. "Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age." *Monthly Review: An Independent Socialist Magazin*, July 1: 1-6.

Betz, D. 2017. *Cyberspace and the State: Towards a Strategy for Cyber Power.* London: Routledge.

Błachnioa, A, A Przepiorkaa, and I Pantic. 2016. "Association between Facebook addiction, self-esteem and life satisfaction: A cross-sectional study." *Computers in Human Behavior* 701-705.

Bloomberg. 2019. "The Unfinished Business of the Equifax Hack." *Bloomberg.* January 29. Accessed March 6, 2019. https://www.bloomberg.com/opinion/articles/2019-01-29/equifax-hack-remains-unfinished-business.

Brandolini, Alberto. 2013. "Twitter post." *Twitter.* January 11.

Casciani, D. 2019. "Secret document reveals police 'blacklisting'." *BBC News.* March 6. Accessed March 6, 2019. https://www.bbc.co.uk/news/uk-47457330.

Chadwick, A. 2013. *The Hybrid Media System: Politics and Power.* Oxford: Oxford University Press.

Colantone, I, and P Stanig. 2018. "Global Competition and Brexit." *American Political Science Review* 201-218.

David-Fox, M. 2003. "The Fellow Travelers Revisited: The "Cultured West" through Soviet Eyes." *The Journal of Modern History* 300-335.

De Goede, M. 2012. "The SWIFT Affair and the Global Politics of European Security." *Journal of Common Market Studies* 214-230.

de Vreese, C, and H Boomgaarden. 2005. "Projecting EU Referendums: Fear of Immigration and Support for European Integration." *European Union Politics* 59-82.

Dencik, L, and J Cable. 2017. " (2017) The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks." *International Journal of Communication* 763-781.

Di Matteo, F. 2017. "The Massive and Indiscriminate Collection of Passengers' Data: A Congenital Defect Within the EU PNR Directive?" *Diritti umani e diritto internazionale* 213-236.

Diakopoulos, N, D Trielli, J Stark, and S Mussenden. 2018. "I Vote For—How Search Informs Our Choice of Candidate ." In *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, by M Moore and D Tambini, 22.

Dongwon, C. 2015. "Physical activity level, sleep quality, attention control and self-regulated learning along to smartphone addiction among college students." *Journal of the Korea Academia-Industrial cooperation Society* 429-437.

Dover, R. 2016. "Fixing Financial Plumbing: Tax, Leaks and Base Erosion and Profit Shifting in Europe." *The International Spectator* 40-50.

—. 2019. "UK Response to Hybrid Threats." *UK Defence Select Committee.* January 8 . Accessed March 1, 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/uk-response-to-hybrid-threats/written/94257.pdf.

Du, L, and A Maki. 2019. "These cameras can spot shoplifters even before they steal." *Bloomberg.* March 4. Accessed March 7, 2019. https://www.bloomberg.com/news/articles/2019-03-04/the-ai-cameras-that-can-spot-shoplifters-even-before-they-steal.

EUROSTAT. 2019. "Migration and migrant population statistics." *EUROSTAT.* January 1. Accessed March 5, 2019. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Migration_and_migrant_population_statistics#Migration_flows:_2_million_non-EU_immigrants.

Farouk, A, M Tarawneh, J Elhoseny, B Mosayeb, Aboul, N, E Hassanien, and M Abedl-Aty. 2018. "Quantum Computing and Cryptography: An Overview." In *Quantum Computing:An Environment for Intelligent Large Scale Real Application*, by A Hassanien, M Elhoseny and J Kacprzyk, 63-100. Munich: Springer.

Financial Times. 2016. "Britain has had enough of experts, says Gove ." *Financial Times*, June 4.

Gates, K. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York: New York University Press.

Gerbaudo, P. 2018. "From Cyber-Autonomism to Cyber-Populism: An Ideological Analysis of the Evolution of Digital Activism." *tripleC* 1-13.

Gietel-Basten, S. 2016. "Why Brexit? The Toxic Mix of Immigration and Austerity." *Population and Development Review* 673-680.

Gioe, D. 2018. "Cyber operations and useful fools: the approach of Russian hybrid intelligence." *Intelligence and National Security* 954-973.

Gioe, D. 2018. "Cyber operations and useful fools: the approach of Russian hybrid intelligence." *Intelligence and National Security* 954-973.

Goodwin, M, and C Millazo. 2017. "Taking back control? Investigating the role of immigration in the 2016 vote for Brexit." *British Journal of Politics and International Relations* 450-464.

Groza, T, and E Groza. 2017. "Populism: A Factory of Myths." *Journal for the Study of Religions and Ideologies* 147-152.

Gyrd-Jones, R, and N Kornumb. 2013. "Managing the co-created brand: Value and cultural complementarity in online and offline multi-stakeholder ecosystems." *Journal of Business Research* 1484-1493.

Halligan, Liam, and Gerald Lyons. 2017. *Clean Brexit: Why leaving the EU stillmakes sense - Building a post - Brexit economy for all.* London : Biteback.

Hill, Kashmir. 2019. *I Cut the 'Big Five' Tech Giants From My Life. It Was Hell.* February 7. Accessed February 15, 2019. https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

HMRC. 2019. *Make a Disclosure using the Worldwide Disclosure Facility.* February 8. Accessed March 1, 2019. https://www.gov.uk/guidance/worldwide-disclosure-facility-make-a-disclosure.

House of Commons: Digital, Culture, Media and Sport Committee. 2019. *Disinformation and 'Fake News': Final Report.* Parliamentary Inquiry, London: HMSO.

Inkster, N. 2015. "Cyber Attacks in La-La Land." *Survival* 105-116.

Inquiry, UK Undercover Policing. 2018. *UK Undercover Policing Inquiry.* October 10. Accessed February 15, 2019. https://www.ucpi.org.uk/.

Institute for Strategic Dialogue. 2019. *The Battle for Bavaria: Online information campaigns in the 2018 Bavarian State Election.* Inquiry, London: Institute for Strategic Dialogue.

Jones, R. 2019. "UK cash system 'on the verge of collapse', report finds." *The Guardian*, March 6.

Kelsey, D. 2016. "Hero Mythology and Right-Wing Populism." *Journalism Studies* 971-988.

Ker-Lindsay, J. 2018. "Turkey's EU accession as a factor in the 2016 Brexit referendum." *Turkish Studies* 1-22.

Korella, J, and W Li. 2018. "Retail payment behaviour and the adoption of innovative payments: A comparative study in China and Germany." *Journal of Payments Strategy & Systems* 245-265.

Krämer, B. 2017. "Populist online practices: the function of the Internet in right-wing populism." *Information, Communication & Society* 1293-1309.

Landon-Murray, M, and I Anderson. 2013. "Thinking in 140 Characters: The Internet, Neuroplasticity, and Intelligence Analysis." *Journal of Strategic Security* 73-82.

Lee, N. 2015. "The Afterlife of Total Information Awareness and Edward Snowden's NSA Leaks." In *Counterterrorism and Cybersecurity*, by N Lee, 151-182. Munich: Springer.

Lewandowsky, S, K Oberauer, and G Gignac. 2013. "NASA Faked the Moon Landing—Therefore, (Climate) Science Is a Hoax: An Anatomy of the Motivated Rejection of Science." *Psychological Science* 622-633.

Li, S, L Xu, and S Zhao. 2018. "5G Internet of Things: A survey." *Journal of Industrial Information Integration* 1-9.

Lucas, Edward. 2012. *Deception: The Untold Story of East-West Espionage Today.* New York: Bloomsbury.

Lyon, D. 2015. "The Snowden Stakes: Challenges for Understanding Surveillance Today." *Surveillance and Society* 139-152.

McCright, A, and R Dunlap. 2011. "Cool dudes: The denial of climate change among conservative white males in the United States." *Global Environmental Change* 1163-1172.

Montag, C, and S Diefenbach. 2018. "Towards Homo Digitalis: Important Research Issues for Psychology and the Neurosciences at the Dawn of the Internet of Things and the Digital Society." *Sustainability* 415-436.

Mosca, M. 2018. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security and Privacy* 38-41.

O'Neil, P. 2017. "The Deep State: An Emerging Concept in Comparative Politics ." *SSRN.* November 20. Accessed March 1, 2019. https://ssrn.com/abstract=2313375.

Opara, EU, AY Mahfouz, and RR Holloway. 2017. "(2017) Network Platforms, Advanced Persistence Threat – The Changing Patterns of Cyber-Attacks. J Forensic crime investi 1(1): 104." *Journal of Forensic and Crime Investigation* 104-114.

Oreskes, N. 2018. "The Scientific Consensus on Climate Change: How Do We Know We're Not Wrong?" In *Climate Modelling*, by A, Winsberg, E Lloyd, 31-64. NY: Palgrave Macmillan.

Parton, C. 2019. *UK-China Relations: Where to draw the line between influence and interference? .* Occasional Paper, London: RUSI.

Petit, N. 2018. "Artificial Intelligence and Automated Law Enforcement: A Review Paper ." *SSRN (https://ssrn.com/abstract=3145133)* 1-12.

Podhradsky, A, R D'Ovidio, and C Casey. 2012. "The Xbox 360 and Steganography: How criminals and terrorists could be going dark. ." *Annual ADFSL Conference on Digital Forensics, Security and Law.* Richmond: ADFSL. 33-54.

Robertson, R, S Jiang, K Joseph, L Friedland, D Lazer, and C Wilson. 2018. "Auditing Partisan Audience Bias within Google Search. . 2, CSCW, Article 148." *Proc. ACM Hum.-Comput. Interact.* 22.

Rose, Jonathan. 2017. "Brexit, Trump, and Post-Truth Politics." *Public Integrity* 555-558.

Ross, J, and R Harradine. 2011. "Fashion value brands: the relationship between identity and image ." *Journal of Fashion Marketing and Management: An International Journal* 306-325.

Ruppert, E, E Isin, and D Bigo. 2017. "Data Politics." *Big Data and Society* 1-7.

Sari, A. 2019. "Hybrid Warfare: The Legal Challenges." *UK Defence Select Committee.* January 23. Accessed March 5, 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/uk-response-to-hybrid-threats/written/95802.html.

Schelter, S, and J Kunegis. 2018. "On the Ubiquity of Web Tracking: Insights from a Billion-Page Web Crawl." *Journal of Web Science* 53-66.

Schindler, JR. 2017. "The Spy Revolt Against Trump Begins." *Observer.* February 12. Accessed March 1, 2019. https://observer.com/2017/02/donald-trump-administration-mike-flynn-russian-embassy/.

Schlembach, Raphael. 2016. "The Pitchford inquiry into undercover policing: some lessons from the preliminary hearings." *Papers from the British Criminology Conference.* Nottingham.

Schneble, C, B Elger, and D Shaw. 2018. "The Cambridge Analytica affair and Internet-mediated research." *EMBO Reports.*

Schwartz, S, GV Caprara, and M Vecchione. 2010. "Basic Personal Values, Core Political Values, and Voting: A Longitudinal Analysis." *Political Psychology* 421-452.

Seely, B. 2018. *A Definition of Contemporary Russian Conflict: How Does the Kremlin Wage War? .* London: Henry Jackson Society.

Skeggs, B, and S Yuill. 2016. "Capital experimentation with person/a formation: how Facebook's monetization refigures the relationship between property, personhood and protest." *Information, Communication and Society* 380-396.

Sputnik. 2019. "Anonymous Publishes New Docs on Integrity Initiative's Institute for Statecraft." *Sputnik.* January 25. Accessed March 7, 2019. https://sputniknews.com/europe/201901251071818668-anonymous-integrity-initiative-statecraft/.

—. 2018. *Anoymous Exposes UK Hybrid Warfare.* 12 1. Accessed March 7, 2019. https://sputniknews.com/trend/anonymous_integrity_initiative_2018/.

Suda, Y. (2018). 2018. *The Politics of Data Transfer.* New York: Routledge.

Thornberry, E. 2018. "Institute for Statecraft: Integrity Initiative." *Hansard.* December 12. Accessed March 7, 2019. https://hansard.parliament.uk/commons/2018-12-12/debates/298F9A3C-307A-40ED-9CB1-3B2A98F14165/InstituteForStatecraftIntegrityInitiative.

UK Ministry of Defence . 2019. "UK Response to Hybrid Threats." *UK Select Committee on Defence.* January 28. Accessed March 5, 2019. http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/defence-committee/uk-response-to-hybrid-threats/written/95802.html.

UK Ministry of Defence. 2019. *77 Brigade: Influence and Outreach.* March 5. Accessed March 5, 2019. https://www.army.mod.uk/who-we-are/formations-divisions-brigades/force-troops-command/77-brigade/.

Urban, Mark. 2018. *The Skripal Files.* London: MacMillan.

Veltri, G, R Redd, T Mannarini, and S Salvatore. 2019. "The identity of Brexit: A cultural psychology analysis." *Journal of Community and Applied Social Psychology* 18-31.

Vosoughi, S, D Roy, and S Aral. 2018. "The spread of true and false news online." *Science* 1146-1151.

Walsh, P, and S Miller. 2016. "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden." *Intelligence and National Security,* 345-368.

Ward, K. 2018. "Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting." *Journal of Media Ethics* 133-148.

Wilford, Hugh. 1998. "The Information Research Department: Britain's secret Cold War weapon revealed." *Review of International Studies* 353-369.

Yablokov, I. 2015. "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)." *Politics* 301-315.

Zajc, M. 2015. "The Social Media Dispositive and Monetization of User-Generated Content." *The Information Society* 61-67.

Zhang, D. 2018. "U.S. Push on Huawei Ripples Through Markets." *The Washington Post*, November 23.

Zhubov, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: Profile Books.