Intelligence and Big Data: What intelligence personnel believe and why it matters?

Michael Mulqueen, University of Central Lancashire.[1]

Big Data and Law Enforcement Intelligence – a decade later:

Almost ten years ago, in 2013 to be exact, it was my happy duty to bring together and lead a most talented if motley crew of academics, law enforcement personnel, and artists. Among us were British police chief constables, Covert Human Intelligence Source (CHIS) handlers, historians, ethicists, lawyers, technologists and computational scientists. We hailed mainly from the United Kingdom, United States, the Netherlands and Ireland.

Displaying a characteristic yearning to be taken seriously, we academics often list the states in which our work is occurring to create an impressive sense of scale. But in point of fact what this multi-national but small and very colourful group sought to deal with exceeded the measure of any state or, indeed, the measure of anything we had ever measured on this earth before.

For this was in the immediate aftermath of data leaks to the media by the US National Security Agency (NSA) contractor, Edward Snowden. And amid the various waves of shock, dismay, praise and congratulations which surrounded Snowden's decision, emerged into public and governmental gaze, a troubling although wondrous realisation.

Big Data, the manifestation of remarkable advances in superfast computer processing power, data storage technologies and clever software programmes, seemed to constitute whatever was going to come after the nuclear age, or, at least, claim stature alongside it. Scholars typically took Big Data to mean vast digital data sets, often including very personalised information about anyone who interacted with any kind of online device (Bunnik et al, 2016, p.1). Big Data's unimaginable potential generated mind-bending examples to help us begin to

[1] Please note that this is a conference address and its content as well as the views of the author herein are liable to alter in the course of receiving feedback and undertaking further research. I would like to extend my sincere thanks to Dr Bill Merrill, Chair of the National Crime Agency's HUMINT Academic Hub (HAH), for his invitation to speak to its conference. Of immense benefit to this paper, and to my thinking, are the fresh and lucid insights into securitisation provided by my recent MSc Counter Terrorism student Ben Burnett.

comprehend its scale: for example, undersea fibreoptic cables, generating most of the world's information, were carrying data at a rate of 10 gigabytes per second or to a theoretical maximum of 21 petabytes a day (Mulqueen 2016, p. 64). In an attempt to make this, somehow, understandable, one newspaper estimated maritime fibreoptic capability to be the equivalent of sending all of the information in all of the books in the British Library, 192 times every 24 hours (MacAskill et al. 2013 cited in Mulqueen, 2016).

Back then we – the Intelligence Futures Group as we were known – were most exercised not only by Big Data's game changing possibilities, such as radically improved medical diagnostics, but also the terrible trouble it could get us all into.

Our concern spanned the design of algorithms written to distil patterns from the data on which outcomes would be based. What, for example, of accidental or intentional racial bias built into the programming of the algorithm? How might this impact upon distribution of healthcare, employment, food, or water? Snowden himself had witnessed the NSA's use of algorithmic data outputs. And he demonstrated how, when those working within the intelligence community found repugnant their employers' use of data, they could cause catastrophic damage to the wider intelligence enterprise - politically, financially and reputationally.

A theme we will return to later in the paper is that Snowden believed himself to be acting virtuously to defend democracy against what he perceived to be profoundly undemocratic practices.

The response of the Intelligence Futures Group to the Snowden fallout was to sound an urgent call, to all who would listen, of the pressing need to combine scientific progress with digital ethics and to do so in ways visible to the workforce and client base. We coined a phrase for this future-facing business model: we called it "sustainable innovation" and we put flesh on its bones by deriving practical models whereby unfamiliar partners, their business thinking rooted deep in sophisticated ethics, could innovate their way through unprecedented challenges.

Today I believe the evidence is that sustainable innovation still has its place. But I must also acknowledge what we, in our research, did not fully grasp at the time. This learning positions me to make a recommendation to intelligence organisations concerning workforce practice that their personnel and their managers may find rather uncomfortable, if not unacceptable. It is on that which this paper, in a short while, will conclude.

But first, and scrolling on from 2013 to 2022: where are we up to and what do I believe you need to know?

In explaining that for you, I wish to take us through a short journey through some political theory. I promise to do this in a way that is as relevant to your concerns as I can make it. But you are going to need to bear with me if I appear to stray away from the daily business of Human Intelligence (HUMINT). Because for the next while, I will focus us more on how states and their peoples act. However, thereafter, I hope you will agree that thinking in this way matters to resolving a key challenge facing your business area.

By way of context, please allow me to bring you back to what we considered to be stable about our world between 2013 and 2015, when the Intelligence Futures Group did its work. Firstly, of course, there was peace in Europe. Globalisation was inevitable. International law was protected as an arbiter of states' disputes. And, institutionally, the utility of the European Union was apparent to all but a fringe minority.

In July 2014 – and so two years before the US presidential election of Donald Trump, the passing of the UK's Brexit Referendum, and, indeed, as an exponential rise in what we now loosely call fake news was cranking up, NATO General Philip Breedlove stated that Russia was employing hybrid war techniques. Or as the general put it – and I quote – the most 'amazing information warfare blitzkrieg we have ever seen in the history of information warfare' (Vandiver 2014). This led to NATO recognising the threat of hybrid actors in their 2015 strategic review (Sperling and Webber, 2016, cited in Burnett, 2022).

Before I lose your attention to musing whether we can join dots between 2014 warnings and 2016 occurrences, I will proceed to theory.

Securitisation in an age of Big Data:

Securitisation, as many of you will know, is an influential theory within the field of security studies that conceptualises threat as a social construction (Buzan *et al*. 1998, p. 19). To explain that idea of threat as a social construction, a good example is of tanks massed at the border: the tanks are not the threat. They are, after all, only pieces of metal. Rather, it is the process of creating mass support for the intent to invade using the tanks that ought to catch our attention. To put it more technically, we must consider how a securitising actor of sufficient influence can present a referent object – or that which must be protected – as subject to an existential threat and, thus, requiring a security response proportionate to an existential threat. In this case that would be the use of tanks to invade a country now successfully cast as posting cataclysmic danger (ibid).

Burnett (2022) and Oskanian (2021) contend that state and societal security, together, constitute a referent object. Burnett, in a 2022 study of official Russian Federation and Ukrainian documentation since the 2014 annexation of Crimea, identifies each side presenting the other as posing an existential threat to the integrity of the border *and* security of society (Burnett 2022). It is striking how, within a similar timeframe, other governments, including the UK's, have extended to securitising migrants as posing an existential threat to border integrity and societal safety (Parker 2022).

Recent thinking in securitisation further warns of the polarisation of society through the creation of in and out groups, cast as such because of identity, belief, or other grounds and presented as a grave threat to state and society alike. Karyotis and Patrikios (2010) identify the use of strong, offensive, symbolic language that can contain metaphors, hyperbole, misdirection and attempts to criminalise the 'out' group to construct a threat.

Emergence of what the journalist Michael Grunwald describes as a new politics of perpetual culture war, associated with former US president Donald Trump may, perhaps, be better understood in this context (Grunwald 2018). Critics of UK Governments since the passing of the 2016 Brexit Referendum may perhaps diagnose similar traits therein. Contemporaneously we might well consider whether, from the very top of government, tribalism has been encouraged around morally infused constructions of freedom, nationalism, migration, climate, sin, gender, and sexuality (Ramsay 2021).

Finally, but importantly, on securitisation is a contested assumption that a security response must occur fairly quickly after a securitising act. Multiple scholars posit the likelihood of sedimentary, or gradual, securitisation (Karyotis and Patrikios, 2010; Austin and Beaulieu-Brossard, 2017; Sperling and Webber, 2017; Ciuta 2009; Williams, 2003). Think here, in the language of intelligence, to sleeper agents cultivating the ground for the right time to act. Sedimented securitisation suggests discourse fermenting in and out group tribalism and sustained over a long period until it reaches the pitch necessary for the security response against the out group to be proportionate to an existential threat. But in the meantime, growing division within society destabilises and does untold other harms. This only stops if the discourse can be turned around; that is, de-securitised.

So let us pull all that together. Hybrid warfare surrounds us. Information is a weapon as never before. When information, including fake information, is deployed persuasively to securitize, the result is in and out groups and, ultimately, competing identities and ideas being cast as existential threats.

But threats to what?

To answer that – and why I think it matters so much to how intelligence organisations need to manage their people – I would like us to consider fascinating research published late last month in the American Political Science Review by Suthan Krishnaharajan of Aarhus University, Denmark (Krishnaharajan 2022).

Sampling across 28,000 respondents in 22 democracies, Krishnaharajan finds the following: 'In today's politics, we are seemingly so adamant in our political convictions that we tend to delegitimize (sic) opposing views by perceiving them as undemocratic—even when they are not' (ibid, p.21). It is within our algorithm-driven data bubbles that those political convictions are being shaped.

The research clearly suggests that citizens no longer define the democratic order in terms of the laws, rules and norms that make up it up. Instead, democracy is being defined as being what the public (or their tribe) think is good for the country. The data is remarkably suggestive concerning what happens when citizens encounter unlawful undemocratic behaviour that aligns with their political convictions: they do not perceive this rule-breaking to be undemocratic.

Bizarrely, when, say, right wing respondents were confronted with regular right-wing behaviour, they instinctively considered it to be much more democratic than identical left-wing behaviour. When confronted with undemocratic right-wing behaviour they did not acknowledge it as undemocratic. But identical left-wing behaviour was seen as highly undemocratic. And right-wing respondents considered anti-democratic right-wing behaviour as more democratic than left-wing democratic behaviour that did not violate laws, rules and norms.

Such behaviour is termed democratic rationalisation. The research suggests that its manifestation in this datafied age it is equally strong among right-wing and left-wing citizens.

It persists across individual characteristics such as age, gender, education, income, and vote choice (ibid, p. 2). The question then is how much this kind of worrying democratic rationalisation goes on. Krishnaharajan’s data suggests it is much more prevalent in troubled democracies whose citizens have undergone recent experiences of ‘backsliding’ or, as might term it, governmental dishonesty and fake news (*ibid*, p.2).

Discussion: Workforce and beliefs - an increasingly justifiable management intrusion?

After all that theory, let us come up for some air.

In 2014, I made the following predictions in a chapter for a book we published on Big Data’s challenges to security and society: I said that Big Data threatened to accelerate a return to great power rivalry in international politics (Mulqueen 2016, p.64). I think we are witnessing key elements of that unfolding notwithstanding international institutional cohesion. Secondly, I argued that those who owned the data and algorithms could cut into the very DNA of the ideas we would think to be our own (ibid, p.66). I think that has come to pass too.

What I did not envisage with sufficient clarity was the extent to which corporates and political parties, working together, would proceed to use Big Data to spot societal weak spots – that is fears, anxieties and resentments (Conoscenti 2018). And I did not fully foresee how they would play on these strategically, through tactics including microtargeting and hyper-nudging, allied to threat-laden speech acts to unravel settled politics, legal and institutional norms, markets and other established certainties (Christiano 2021). Considerable scholarship has since investigated Russian Federation use of Twitter bots and other digital information tactics to favourably influence polling outcomes in other states (McGaughey 2018; Llewellyn *et al* 2019; Hatch, 2019). Use of such tools seems to have lined up with the electoral goals of those political parties and corporates seemingly persuaded as to the value of populist disruption. This is notwithstanding whether suspicion characterised wider political and diplomatic relations between the Russian Federation and these states before the invasion of Ukraine.

All this can now be seen in the context of securitisation, which has been with us for some time, and newer research, which opens the vista of democracy being on course to buckle under the pressure of being pulled apart by bitterly opposed in and out groups seeking to stand up for democracy. (Krishnarajan 2022). Those political convictions are, inevitably, a reflection to some degree of the information we access in our now heavily datafied lives (Christiano 2021). Indeed, it is not preposterous to ask whether – with our lenses on reality increasingly reflecting the data-informed worlds we are sealed within – each of us risk impacting harmfully on democracy? Are we, without realising it, the sleeper agents of influential securitising actors who are already deploying data to convince us as to necessity for a security response that is proportionate to the existential threat? Are we all, potentially, enemies of the state, its laws and order, hidden in plain sight, even from ourselves? Because, surely, we must ask honestly and openly whether we are being drawn into beliefs that democracy should mirror the convictions that our data shapes in us? If this is the case, and, as the evidence suggests, it is happening across society at scale, then hybrid warfare is indeed a devilishly clever enterprise.

Let us consider these points by starting from the proposition of intelligence managers and personnel reflecting, to a greater or lesser degree, the communities from which they have all come. Those communities are experiencing the impacts of destabilised information.

Consider the Covid-19 restrictions and those people on your street, or in your supermarket, who perhaps loudly urged you to stand up for your democratic right by rejecting the great globalist plot to poison us all through vaccination.

It is easy to dismiss whoever we disagree with – be they anti-vaxxers, Capitol Hill conspiracists, or anyone else - as stupid or evil. Thanks to social media insulting at an industrial scale is now, observably, commonplace.

But then explain perhaps Ireland’s most prominent anti-vaxxer Dolores Cahill? She is previously of Germany’s prestigious Max Planck Institute and a recent Professor of Medicine at my Alma Mater, University College Dublin (O’Brien and Power 2021). What too of the ‘messianic’ Canadian professor, Jordan Peterson, and his zealous warnings to us that wokeness and liberalism threaten to capsize our society? (White 2022) His mission to safeguard against informational threats to democratic society, having gone viral online, has since metastasised into the real world: he’s currently selling out major venues all around Europe (ibid).

With clear evidence of such shifts in rationalisation going on in our communities, what is going on in our intelligence organisations, which, after all, comprise people from those communities? Intelligence personnel are among those in service careers we encourage to courageously do the right thing by their society and their democratic state (Souhali 2021). Do intelligence managers really understand what their people believe democracy to be and what they would do, or not do, to defend their notions of what it actually is? Do intelligence personnel really reflect on what, as a consequence of their datafied private lives, they themselves have come to believe?

If you are a manager, have you considered whether there are members of your team who may be finding your organisation's practices and procedures repugnant? Is it repugnant to the democratic society they seek to serve? How will you find out? If you do not and decide to ignore the risk, will they, in their sincerity to uphold democracy, do a Snowden on you?

What if it is not a data leak they believe is needed to do good? What if it were higher tolerance or ambiguity concerning crimes, including organised crimes, or even treachery, if that is what is needed?

And on the day-to-day level, what about behaviours towards each other within the workplace and, externally, with respect to, say, a CHIS? What about the product you generate, receive or circulate? Bias, of course, is not a new problem, nor is a logic of appropriateness whereby especially the ambitious shy away from taking risks by naming destabilising problems and solutions. But how will you detect some subtle gap, a skewing phrase or an underplay because someone is turned off by wokeness or intolerance? Will your organisational culture allow you to take apart and scrutinise how self-assured you are about yourselves and about what just seems ridiculous?

Because, increasingly, we can confirm that how Big Data is manipulated works on us like an invisible virus and our lives online are akin to mass spreading events. Services expected to generate good intelligence are, arguably, especially vulnerable from a phenomenon which exponentially expands and pollutes information and the minds that consumes it.

So how can we safeguard the intelligence enterprise from its own human resources in ways that reflect Big Data's invisible but seemingly pervasive conditioning? I offer two principles to guide management behaviours towards intelligence personnel and each other, moving forward. Both, to be candid, offer immense challenges.

- 1. We need to know what you believe?
- 2. We need to know that all of the time.

Putting these principles into workplace practice implies a revised business model, a people management framework which, reflecting our datafied lives, is unprecedentedly intrusive. Questions arise over how this can be done, given the right to freedom of thought, widely accepted HR norms and financial exposure? There is too, at a more abstract level, a knotty dilemma: in a Big Data age, is it acceptable within a democracy to maintain a veil over the private beliefs of intelligence personnel, in the absence of evidence to the contrary? Or should we protect democracy by intrusively searching for the presence of beliefs that may equate with a rationale for harmful or unlawful acts in its defence? What is the appropriate response when risk is uncovered?

Beyond raising these challenges, I offer you at this point no design for such a people management framework. But I stand ready to assist any organisation that may comprehend the need to explore how it may be safely and effectively achieved. I cannot conclude, however, that 'doing nothing' is a sensible option.

References

Austin, J. L. and Beaulieu-Brossard, P. (2017) '(De)securitisation dilemmas: Theorising the simultaneous enaction of securitisation and desecuritisation', Review of International Studies, 44(2), 301–32 available: doi: 10.1017/S0260210517000511.

Bunnik, A., Cawley, A., Mulqueen, M. and Zwitter, A. (2016) 'Introduction to Big Data Challenges', in Bunnik, A., Cawley, C., Mulqueen, M. and A. Zwitter, eds., *Big Data Challenges: Society, Security, Innovation and Ethics*, London: Palgrave Macmillan, 1-7.

Burnett, B. (2022) *Securitisation, Terrorism and Hybrid Warfare in the Ukrainian Conflict*, unpublished thesis (M.Sc.), University of Central Lancashire.

Buzan, B, Wæver, O, and de Wilde, J. (1998) *Security: A New Framework for Analysis*, London: Lynne Rienner.

Christiano, T. (2022) 'Algorithms, Manipulation, and Democracy', *Canadian Journal of Philosophy*, *52*(1), 109-124, available: doi:10.1017/can.2021.29.

Ciuta, F. (2009) ‘Security and the problem of context: a hermeneutical critique of securitisation theory’, *Review of International Studies*, 35(2), 301–326, available: doi: 10.1017/S0260210509008535.

Conoscenti, M. (2018) ‘Big Data, Small Data, Broken Windows and Fear Discourse: Brexit, the EU and the Majority Illusion’. *De Europa*, Vol 1(2), pp. 65-82, available: doi.org/10.13135/2611-853X/2914.

Grunwald, M. (2018). ‘How Everything Became the Culture War’, *Politico*, November/December, available How Everything Became the Culture War" [accessed 24 Sept 2022].

Hatch, B. (2019). ‘The Future of Strategic Information and Cyber-Enabled Information Operations’ *Journal of Strategic Security*, 12(4), 69–89, available https://www.jstor.org/stable/26851261.

Karyotis, G. and Patrikios, S. (2010) ‘Religion, securitization and anti-immigration attitudes: The case of Greece’, *Journal of Peace Research*, 47(1), 43–57, available: doi: 10.1177/0022343309350021.

Krishnarajan, S. (2022) ‘Rationalizing Democracy: The Perceptual Bias and (Un)Democratic Behavior’, *American Political Science Review*, First View, 1-23, available: doi:10.1017/S0003055422000806.

Llewellyn, C., Cram, L., Hill, R. L., and Favero, A. (2019) ‘For Whom the Bell Trolls: Shifting Troll Behaviour in the Twitter Brexit Debate’, *JCMS: Journal of Common Market Studies*, 57, 1148– 1164, available https://doi.org/10.1111/jcms.12882.

McGaughey, E. (2018) ’Could Brexit be Void?’, *King's Law Journal*, 29(3), 331-343, available doi: 10.1080/09615768.2018.1555881.

Mulqueen, M. (2016) ‘Sustainable Innovation: Placing Ethics and at the Core of Security in a Big Data Age’, in Bunnik, A., Cawley, C., Mulqueen, M. and Zwitter, A. eds., *Big Data Challenges: Society, Security, Innovation and Ethics*, London: Palgrave Macmillan.

O’Brien, C. and Power, J. (2021) ‘Anti-vaccination campaigner Dolores Cahill no longer employed by UCD’, *Irish Times*, 19 Sept 2021, available at: Anti-vaccination campaigner Dolores Cahill no longer employed by UCD – The Irish Times [accessed 24 Sept 2022].

Oskanian, K. (2021) ‘Securitisation gaps: Towards ideational understandings of state weakness’. *European Journal of International Security*, 6(4), 439–458, available doi: 10.1017/eis.2021.13.

Parker, O. (2022) ‘The Politics of Free Movement of People in the United Kingdom: Beyond Securitization and De-securitization?’, *Journal of common market studies*. [Preprint], available https://doi.org/10.1111/jcms.13410.

Ramsay, A. (2021) ‘Culture wars aren't a distraction, they're a battle over everything’, *Opendemocracy.org*, 11 Dec 2021, available at Culture wars aren't a distraction, they're a battle over everything | openDemocracy (accessed on 25 Sept 2022)

Souhali, H. (2021) ‘The Snowden Affair: The Self-Fulfilling Prophecy of an Idealist’, *Afak Ilmia Journal*, 13(2).34-50.

Sperling, J. and Webber, M (2017) ‘NATO and the Ukraine crisis: Collective securitisation’, *European Journal of International Security*, 2(1), 19–46, available doi: 10.1017/eis.2016.17.

Vandiver, J. (2014) ‘SACEUR: Allies must prepare for Russia ‘hybrid war’, *Stars and Stripes*, 4 Sept 2014, available: SACEUR: Allies must prepare for Russia ‘hybrid war’ | Stars and Stripes [accessed 25 Sept 2022].

Whyte, B.J. (2022), ‘Philosopher or pretender? How Jordan Peterson became a culture warrior on a mission’, *The Sunday Business* Post, 16 Sept 2022, available at Philosopher or pretender?: How Jordan Peterson became a culture war warrior on a mission | Business Post [accessed 24 Sept 2022].

Williams, M. (2003) ‘Words, Images, Enemies: Securitization in International Politics’, *International Studies Quarterly*, 47 (4) 511–31.