Discernment: Why information statecraft matters

To speak of "discernment" feels like an appeal to a different era, an earlier time. A somehow old-fashioned call to wisdom, or related values that seem quaintly out of step with modern life. We more typically hear of the rapid changes of technology, the accessibility of information and the need for efficiency and speed in the race to keep up. Yet the flood of material on our news streams via social media and other platforms is so overwhelming, that unless we renew and cultivate afresh skills of critical thinking and discernment we face the real threat of being paralysed and apathetic in the face of the questions that genuinely matter and, paradoxically, manipulated and coerced to respond viscerally to issues that may well be spurious or false. This intentionally divisive manipulation and attack upon our capacity to think critically is arguably a threat to the very foundations of democratic society. As citizens become more disengaged they become more isolated, and more at risk from radicalisation.

The urgency of this situation requires action across the board, with special care and attention given to educating children at school with the core principles and practice of discernment in order to properly prepare and equip our younger citizens and future leaders.

In face-to-face conversation and debate we learn 'cues' for assessing the reliability of someone's argument, though often this knowledge is acquired intuitively through life experience rather than through formal education. If we encounter someone shouting out bizarre accusations or disjointed phrases in our local market square we typically will ignore them and may well draw conclusions as to the mental health of the person in question. Online, however, we don't have the same context of non-verbal clues that are so crucial to the conclusions we draw about the reliability and authenticity of information. Increasingly we find that visual clues provided by photos as well as video footage are also subject to manipulation. Fake imagery, misleading headlines and captions, and distorted reporting can enable disinformation to take root and spread virally. We need a complementary set of tools to help cultivate visual discernment and provide the public with resources to verify stories (especially the most provocative and compelling) before they are shared.

In the case of the attempted murder of Sergei and Julia Skripal by nerve-agent poisoning in Salisbury, there have already been a minimum of 32 different narratives suggested by the Russian state as possible "explanations", most of which are absurd and indeed contradictory. If someone communicated like this to us verbally - directly in conversation - then we would dismiss this out of hand as being an indication of pathological lying or some other disorder. Yet online, when sources are obscured and the "narratives" come at us rapid-fire, we quickly lose track and become confused. Indeed, this state of confusion and disengagement is often the goal of those who actively spread disinformation.

In this context, the call for increased discernment - measured through what we may term as increased 'media literacy' and critical thinking skills - is in part a call to take a step back and observe the wider picture of what's happening in our communities. We believe it is important to acknowledge that our capacity to think critically, understand and respond is being rapidly undermined due to malign disinformation and manipulation. We are facing an unparalleled time of change in the way the we receive, filter and attempt to process information. This level of change has not occurred previously in human history during peacetime, and is rather associated with the stress, upheaval and chaos that accompanies war. Indeed, it is with this observation in mind that we can meaningfully speak of 'information war' as part of the increasingly sophisticated 'hybrid war' that our enemies pursue. We believe we are at a cross-roads and, therefore, need to take the radical steps necessary to prepare and protect our citizens to be equipped to meet this challenge.

A recent <u>US National Security Strategy paper</u> from December 2017 uses the phrase "*Information Statecraft*" to describe the coherent strategy needed if we are to meaningfully address the threat of disinformation. This White House paper describes US efforts to date to counter the exploitation of information by rivals as being "tepid and fragmented", and serve as a warning for our own need in the UK to craft a national strategy. To be meaningful and effective, this needs to include both counter measures to defend information space (examples include restrictions upon known propaganda outlets such as RT and Sputnik, such as changing their status from media outlet to that of a foreign agent), as well as the ongoing exposure and removal of sites/platforms that explicitly promote hate speech, terrorism and recruitment drives through entities such as Daesh. It is critical to understand that the threat from groups historically seen as direct sponsors of terrorism such as ISIS/Daesh and the coordinated state efforts from Russia in recent years are linked.

As Lucas and Pomerantsev write in their 2016 report for CEPA titled "Winning the Information War", the goal of Russian sponsored disinformation is not to persuade, convince, or even to "crudely promote the Kremlin's agenda" as it was during Soviet times. No-one these days rationally argues for communism as an ideological principle or anticipates a world-wide revolution of the proletariat. Indeed, rather than one specific tactical agenda, "Russia aims to erode public support for Euro-Atlantic values in order to increase its own relative power. It exploits ethnic, linguistic, regional, social and historical tensions, and promotes antisystemic causes, extending their reach and giving them a spurious appearance of legitimacy." Nina Jankowicz, in an article titled, "The Disinformation Vaccination" in the Wilson Quarterly, Winter 2018, similarly argues that current Russian disinformation differs from its previous tactics in two critical ways: "...they now rarely promote a strictly pro-Russian narrative, choosing instead to stoke known tensions in a given society, and they are amplified by modern technology and the rapid spread of content on the internet."

We are witnessing a trend where despite the perceived opportunities for the internet to bring people together and bridge divides, in reality the result is often the opposite. 'Echo chambers' - the name for communities online that reflect our natural human tendency to associate with people who share similar ideas to our own - can easily act as a petri dish that accelerates the growth of what previously would have been quite obscure and fringe ideas. The strategies of both radical Islamic groups online and Russian-sponsored disinformation is to embrace extreme conspiracy theories, even ones that are contradictory. As these ideas fester and take hold, they become increasingly plausible and more mainstream and more rational explanations are dismissed as being too boring or conventional.

This divisiveness, if left unchecked, becomes more and more pronounced over time. Those who actively spread disinformation understand the power of "confirmation bias" - our inherent affinity to selectively hear what we want to hear. Within Muslim communities this is a strong factor as deference to religious authorities and family heritage make it especially difficult to challenge disinformation. The more closed the group, the greater the challenge to introduce tools and resources that cultivate discernment. Outside help is needed to break this cycle.

We believe we have a duty and obligation to act to protect the Euro-Atlantic values upon which our democracy stands. Russia and its proxy agents cynically use our own democratic traditions - including the value of free-speech and independent media - as an argument that we are somehow hypocritical if we label them as propaganda, warn citizens about their methods and attempt to restrict access to the material they spread. This distorted view sees freedom of information as an open invitation to spread anything and everything, and from their perspective, the more absurd and contradictory the better.

As an analogy, public health concerns of recent decades have seen a concerted and coordinated effort across government departments to bring about a change in behaviour with a view to critical improvements in individual and community health. For example, efforts against smoking haven't sought to out-right ban cigarettes or take away the freedom of choice for those who remain committed (addicted) to their right to smoke. Yet health warnings, education, changes in advertising regulations, point of sale, access to young people, banning smoking in public places etc. - all these efforts work together to save lives, improve quality of life for individuals and the health of the nation, as well as, critically, reducing the cost and strain on the NHS so it can address other issues of concern.

Arguably, therefore, we need to define the outcome we wish to see in terms of engaged, educated and aware citizens who retain the capacity to make informed choices. This is vital to the health of any democracy. We could call this a strategy for "information health", which in turn requires a concerted, reinvigorated look at the tools of 'information statecraft' at our disposal. Information health requires a robust and relevant level of media literacy. By this we mean the capacity not only to understand content, but also be able to evaluate the reliability and authenticity of material through skills of cross-checking, verification and an awareness of the dangers of confirmation bias. In the valuable and timely resource compiled by 'The Public Data Lab' in 2017 titled, "A Field Guide to 'Fake News' and Other information Disorders", we have to address the dual threat of both malicious content and, crucially, the means and mechanisms by which material is circulated online.

This is a timely and vital discussion, and it seems every day we uncover information about how platforms like Facebook have used our personal data to target us with highly-tailored messaging that merges advertising for goods and services with political messages that reflect our interests and values through our online viewing reinforced by viewpoints we like and follow. This is exacerbated by a financial model that gives financial reward to content that is clicked and shared most widely.

It should be stressed that the focus here isn't primarily about which information with which we should engage, but rather the cultivation of tools and a mindset that encourages critical thinking, discernment and debate across the full spectrum of political viewpoints. It is not about persuading a reader to change from one newspaper to another, or change their TV news station. A healthy democracy needs a diversity of outlook, and needs citizens to be engaged and willing to debate radically divergent views in a manner that doesn't result in violence and aggression. Indeed, this diversity of debate stands in stark contrast to the propaganda models of both the Russian state and Daesh. In their worldview there is no space for dissent and no place to express an idea that runs counter to the view of the authoritarian centre.

In conclusion, a renewed look at media literacy and discernment is a critical element for a robust, 'information statecraft' strategy at the national level. The power of discernment is the power of an individual to regain control at the level of his/her own critical thinking and make informed choices about information and sources that we allow to have a role of authority in our life. To discern is to have the power to say no to disinformation and to make meaningful decisions about whom we chose to trust. If we don't make these choices and help equip our children to do likewise, then we forfeit that responsibility to someone else. As we look at those outside influences (whether Russia-sponsored media or the extremism of Daesh) we see that these malignant agents clearly do not want our democratic societies to flourish. Indeed the opposite is true: our apathy, confusion and collapse is the goal.

Proposed next steps:

- Define and articulate a holistic consensus of "information health" and "information statecraft" that adopts a multi-disciplinary approach and a willingness to absorb best-practice experience from international partners.
- Adapt and apply-media literacy training experience from Ukraine a country at the forefront of Russian disinformation campaigns. The 'Learn 2 Discern' media-literacy programme developed by IREX and StopFake has recently been expanded to address the specific needs of children as part of an integrated school-based programme. These programmes demonstrate changes in understanding and behaviour by measuring criteria such as the ability to verify messages through cross-checking with at least one other source. Of the 15,000 who have completed the 'Learn 2 Discern' programme, over 92% reported checking their sources 3 months after the training event. The tagline for the 'Learn 2 Discern' programme in Ukraine is "care before you share". This is a simple reminder to be wary of a knee-jerk reaction to pass on content simply because it shocks or provokes. Media content and case-studies will be sourced locally and reflect the particular media environment of a region/country. This will be done in conjunction with partners who demonstrate an objective, non-partisan approach.
- Another proposed strategy is to adopt elements of the "Cyber guard" training initiative which utilises retired military personnel as coaches to help young people work through the risks inherent in the cyber domain and the ways these can impact the person and wider society. This training material helps raise awareness of legal risks and criminal liability for content viewed and shared online. In Estonia, a comprehensive curriculum addressing cyber-security and critical thinking is introduced as early as age 9. This model of engagement at a young age helps address gender imbalances when we assess the lower number of girls currently pursuing further studies and professions in cyber security, IT and

programming. Women who are currently active and established in IT and security studies could be vital role-models to encourage more girls to enter and stay in this field.

• We believe it is critical that people are aware of the editorial position and financing of media outlets and the implications of these structures. This is a critical point in understanding why RT is by its very nature a propaganda outlet and how it differs fundamentally from the BBC or other western platforms. Furthermore, we believe it is vital to expose the deception of supposed independent, third-party sites that are in-fact proxies for the Kremlin and whose only purpose is to amplify and spread a particular message. There is a vital, ongoing conversation to be had about privacy, data protection and the vital protection of sources when reporting on issues that place a journalist or whistleblower at risk. However, it is important to distinguish between these appropriate safeguards and the pursuit of anonymity online in order to deceive and distort the origin of material or indeed for the purpose of cyberattacks or other types of subversive action.