Written evidence submitted by Paul Schulte

Mitigating the Coming Infodemics and The Impacts of Information Disorder on the British Body Politic

INTRODUCTION AND SCOPE

I was invited to submit evidence to this enquiry at the suggestion of Prof Michael Clarke. I respond as a private individual, with current academic affiliations to Birmingham Institute for Conflict, Cooperation and Security, as an Honorary Professor and King's College Department of War Studies, as a Senior Visiting Fellow. I am a retired MoD UK civil servant, who was, for several years, the senior non-medically qualified official in the Defence Medical Service, when it was preoccupied by intractable, intangible, but politically transfixing, legacies of Gulf War Syndrome and Post-Traumatic Stress Disorder. Between 1997-2002, I was Director of Proliferation and Arms Control, where potential biological and chemical threats, from hostile states and nonstate actors, were one of my key areas of concern. I shall not refer to the technical and intelligence information which I accessed during those years, which was quite properly highly classified and would in many cases be out of date.

I have since followed the subject as an academic and commentator though very consciously do not wish to comment on the current threat levels from biological attack or accident, or medical or logistical practicalities to deal with it. Others are much better qualified to do that. Nor do I wish to take any position about the politically contentious question of HMG's handling of the Covid 19 Pandemic, including its communication strategy, or its overall comparative performance. This will undoubtedly be assessed in great detail in the years to come.

However, as a citizen, observing and reflecting on the strains and disputes occurring from Covid 19, reported in the US, UK , France, Israel and other democratic states, and as a student of group psychology and political warfare, I have become concerned that there are systemic informational vulnerabilities in relation to biosecurity threats, whose social, political and strategic implications have not, as far as I can tell, sufficiently addressed in public discussions of resilience in the National Security Strategy, and which include indirect impacts on public health and prosperity. I have been in touch with networks of experts in UK, and US academia[1], and participated in recent London and transatlantic online expert workshops on national resilience and biosecurity responses. This has confirmed to me that the informational problem potentially ranges all across all elements of healthcare – from those looking up dietary advice, to parents concerned about vaccinating their children. For wider society, it could, for example, include the sources that specialists from various disciplines, as well as ordinary members of the public, will access to inform themselves about the range and utility

[1] I am exceptionally grateful, for ideas, references and critical suggestions, to Karl Dewey, Ulf Schmidt, Filippa Lentzos, Brett Edwards, John Walker, Greg Koblentz, Brad Roberts and Ariel Levite. But errors, omissions and misinterpretations are entirely my own fault.

of available medical treatments, and medical history, including the history of infectious diseases.

I am so far unable to venture any convincing view on whether these informational vulnerabilities are adequately acknowledged, and are being effectively addressed in the confidential realm. The publicity surrounding the UK Integrated Review and MOD Integrated Operating Concept suggests a strong doctrinal willingness to take them into account, at least from a defence and foreign affairs perspective. But some resultant actions determined by that perspective will be necessarily classified. And a whole of government approach will in any case be needed for an adequate response.

AIM

I shall therefore attempt an unclassified examination of informational vulnerabilities over biosafety and biosecurity, from a principally British perspective, bringing together in one document very recent research, some of it stimulated by the Covid 19 pandemic, and suggesting a range of questions on which the Committee might consequently seek information and guidance. (For ease of access, I have thus tried to provide immediately retrievable web resources wherever possible.)

SUMMARY

National informational vulnerabilities, currently revealed in a Covid 19 Infodemic composed of analytically separable varieties of “Information Disorder”, are shared with other liberal democracies. But they are much less problematic for closed, authoritarian systems. They should be taken seriously - and better understood by Government, Parliament, Media, Academia, and, as far as possible, the British public, to avoid complacency, mass deception or panicked exaggeration. Their implications extend well beyond what the public see as military or intelligence affairs, into public health, economics and politics.

It is no longer disputable that systematic, increasingly sophisticated, efforts are being made to undermine shared public understanding of the Covid 19 pandemic, and public confidence in government decisions over its handling. That risk cannot be completely avoided in free societies and the scale of its impact is not yet openly calculable. Mitigating these vulnerabilities may raise grave political, legal, ethical, and technical dilemmas. They are likely to recur, with variations, in future biosecurity crises. For a full understanding of the biosafety and biosecurity situation, Government should be asked for its assessment of the causes, impacts and implications of the Covid 19 Infodemic, and its plans and organisational arrangements for addressing the future informational dimension of national biosecurity. Some of its diagnosis and proposed solutions may have to be handled in confidence. But non-governmental, experts from numerous disciplines and occupations will also have much to offer

BIOSECURITY AND INFORMATION DISORDER

Infodemics: A Growing 21st-Century Strategic and Public Health Vulnerability

Covid 19 is serving as a painful reminder that, within liberal democracies, epidemics generate social, economic, organisational, legal, and political strains well beyond the health sector. These strains will be intensified, sometimes deliberately, by accompanying "Infodemics". According to a recent statement by the WHO and various other international organisations:

"An infodemic is an overabundance of information, both online and offline. It includes deliberate attempts to disseminate wrong information to undermine the public health response and advance alternative agendas of groups or individuals. Mis- and disinformation can be harmful to people's physical and mental health; increase stigmatization; threaten precious health gains; and lead to poor observance of public health measures, thus reducing their effectiveness and endangering countries' ability to stop the pandemic"[2] .

The statement called on

"Member States to develop and implement action plans to manage the infodemic by promoting the timely dissemination of accurate information, based on science and evidence, to all communities, and in particular high-risk groups; and preventing the spread, and combating, mis- and disinformation while respecting freedom of expression.

We urge Member States to engage and listen to their communities as they develop their national action plans, and to empower communities to develop solutions and resilience against mis- and disinformation.

We further call on all other stakeholders - including the media and social media platforms through which mis- and disinformation are disseminated, researchers and technologists who can design and build effective strategies and tools to respond to the infodemic, civil society leaders and influencers - to collaborate with the UN system, with Member States and with each other, and to further strengthen their actions to disseminate accurate information and prevent the spread of mis- and disinformation."[3][4]

[2] "Managing the COVID-19 Infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation Joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC ", 23 September 2020 Statement https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation

[3] Adam Kucharski, in " The Rules of Contagion: Why Things Spread - and Why They Stop - Welcome Collection ", 2020, explores the possibility that infodemics might obey the same internal logic as the epidemics which trigger them.

[4] But Kucharski's is still only an intriguing supposition in a nascent science of Infodemiology defined by the WHO as the "science of managing Infodemics ". " Eysenbach, G (27 March 2009). "Infodemiology and infoveillance: framework for an emerging set of public health informatics methods to analyze search, communication and publication behavior on the Internet". Journal of Medical Internet Research. 11 (1): e11. doi:10.2196/jmir.1157. PMC 2762766. PMID 19329408.) Eysenbach saw Infodemiology as a" new area of science research that focuses on scanning the Internet for user-contributed health-related content, with the ultimate goal of improving public health".
The World Health Organisation has organised conferences on Infodemiology in June and July 2020. Infodemiology, https://www.who.int/news-room/events/detail/2020/06/30/default-calendar/1st-who-infodemiology-.

National and International Action Plans to Counter Infodemics

Calling for action plans at national level is an entirely understandable suggestion by the WHO. But, given suspicions about undue Chinese influence in the WHO and other international agencies, and fierce Russian and Chinese denials of evidence that they have conducted influence operations connected to Covid 19, it is impossible to believe that such national plans could be constructively shared openly, and in their entirety, within the WHO and wider UN environment. This still leaves opportunities for selective international coordination, some of which would have to occur at the classified level, between like-minded states, as in NATO[5][6], and with the EU, where the EU Disinformation Lab plays a continually useful diagnostic and warning role,[7], and substantive new ideas continue to emerge from the External Action Service [8]. An EU High-Level Level Group delivered an influential and well-received report in 2018 on fighting disinformation[9] . Its key recommendations were

"1. enhance transparency of online news, involving an adequate and privacy-compliant sharing of data about the systems that enable their circulation online;

[5] "NATO's approach to countering disinformation: a focus on COVID-19 "17 July 2020 https://www.nato.int/cps/en/natohq/177273.htm

[6] "**Tackling Russian propaganda** The generalized lack of confidence was made worse by hostile propaganda from Russia which ruthlessly exploited the health crisis in an aggressive strategic communication campaign. At NATO HQ, there was a sense of urgency that this campaign needed to be countered in order to protect NATO's relevance. So, the Public Diplomacy Division and other communication directorates throughout the Alliance began coordinating their response to Russian and Chinese propaganda. The messaging was illustrated by pictures of NATO's concrete actions, thus demonstrating to the world that the organization was not sitting idle, even if dealing with a pandemic was not NATO's core business....[But most NATO efforts were concentrated on logistics and medical stocks and] Some countries did not understand the real need to counter the hostile propaganda with concrete examples, or were so deeply involved in their own national handling of the crisis that they did not take the time"
NATO and the COVID-19 emergency: actions and lessons
By LGEN Olivier RITTIMANNNDC Policy Brief No. 15 - September 2020

[7] "Covid 19 disinformation narratives, trends and strategies in Europe", EU Disinfo Lab, April 2020 and subsequently updated:
https://www.disinfo.eu/publications/covid-19-disinformation-narratives-trends-and-strategies-in-europe

[8] "The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework "James Pamment, Carnegie Endowment and European External Action Service's (EEAS) Strategic
Communications Division, 2020
https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720

[9] "A multi-dimensional approach to disinformation: Report of the independent High-level Group on fake news and online disinformation", EU Directorate-General for Communication Networks, Content and Technology, 2018
https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

2. promote media and information literacy to counter disinformation and help users navigate the digital media environment;[10]

3. develop tools for empowering users and journalists to tackle disinformation and foster a positive engagement with fast-evolving information technologies;

4. safeguard the diversity and sustainability of the European news media ecosystem, and

5. promote continued research on the impact of disinformation in Europe to evaluate the measures taken by different actors and constantly adjust necessary responses."

This was a substantial agenda but since it was written the intensity of malicious information activities has significantly increased.

In addition to wider actions to inoculate society against infodemics by building up informed public scepticism about questionable information, a UK Action Plan would certainly also have to include effective proposals to regulate harmful and misleading information on the Internet and social media. The need for this was recognised in HMG's Online Harms White Paper[11], initially published, to a mixed reception[12] in 2019, updated in February and since delayed. At the time of writing it is not clear how the eventual Bill will be modified against criticisms from various directions, and from the cumulative experience of the Covid 19 biosecurity event and its ramifications. Nor is it evident how cooperation in this area will be sustained with EU states. Yet there are two obvious ways in which international cooperation could help mitigate infodemics: by sharing information on the actors propagating information, and by agreeing shared and therefore more authoritative rebuttals, between like-minded countries.

Analysing Infodemics: Mutating Components and Non-Standardised Taxonomy

Terminology in this field is uncertain and, outside meticulous bureaucracies like NATO, EU and HMG, unsystematic and evolving. A useful multiple approach to analysing the information environment was suggested by Claire Wardle last year in the Scientific

[10] One topical and widely accessible example of teachable heuristic protective methods is given by Will Oremus," The Simplest Way to Spot Coronavirus Misinformation on Social Media - A digital literacy expert shares his method "Medium, 4 March 2020 https://onezero.medium.com/the-simplest-way-to-spot-coronavirus-misinformation-on-social-media-4b7995448071

[11] Online Harms White Paper, Gov.uk updated 12 February 2020 https://www.gov.uk/government/consultations/online-harms-white-paper

[12] ""UK proposals on online harms miss their mark: A more nuanced approach is needed to ensure freedom of speech", Financial Times Editorial Board, this 4 July 2019 https://www.ft.com/content/505865d8-9c23-11e9-b8ce-8b459ed04726

American. (Wardle 2019)[13], proposing a general description of increasing “Information Disorder” [14], composed of:

Misinformation: unintentional mistakes such as inaccurate dates, captions, statistics, and misunderstood, yet all the more passionately espoused scientific theories, believed for sociopsychological reasons. Or ostensible satire, deliberately misrepresented to avoid censorship, and sometimes weaponizing context rather than content, so that originally ironic memes become interpreted seriously, (a process sometimes called “*irony poisoning* “[15]).

Disinformation: fabricated or deliberately manipulated, content, including “fake news” and “fake faces”. Disinformation, including hostile state Information Warfare, often relies upon intentionally created conspiracy theories or rumours, intended to be recirculated in good faith.

Malinformation: deliberate publication of private information for personal or corporate, rather than public interest: such as doxing[16], and revenge porn, often with deliberate but hard to detect changes of context, date or time of genuine content.

Across these categories there may be “many shades of misleading” with varying proportions of genuine error, obsession, deceit and malice. The distinction between misinformation and disinformation may in some cases be impossible to establish, and could shift with the subjective understandings of poorly informed or partisan cultists.

Rapidly Increasing Recognition of the Informational Dimension, and Recent Admissions of UK Government Responses

The notion that, usually undefined, “Information Warfare” poses a threat to British national cohesion and social resilience is now widely accepted in national security planning, but far less so in public debate over health issues. As a very recent article in the RUSI Journal put it:

[13] Claire Wardle "Misinformation Has Created a New World Disorder : Our willingness to share content without thinking is exploited to spread disinformation", Scientific American, September 1, 2019 https://www.scientificamerican.com/article/misinformation-has-created-a-new-world-disorder/

[14] Extending this terminology, Information disorders have also been described as” "*cognitive-emotional conflicts"* or *"Emotion wars"-new forms of political and social engineering, exploiting data and digital technologies."*
Eleonora Pauwels, "The Anatomy of Information Disorders in Africa: Geostrategic Positioning and Multipolar Competition over Converging Technologies" Konrad Adenauer Stiftung October 2020 https://www.kas.de/documents/273004/10032527/Report+-+The+Anatomy+of+Information+Disorders+in+Africa.pdf/787cfd74-db72-670e-29c0-415cd4c13936?version=1.0&t=1599674493990

[15] Piia Varis "On being diagnosed with irony poisoning" Digital Magazine, 14 March 2019, https://www.diggitmagazine.com/column/being-diagnosed-irony-poisoning

[16] *doxing*: "the Internet-based practice of researching and publicly broadcasting private or identifying information (especially personally identifying information) about an individual or organization. The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. It is closely related to Internet vigilantism and hacktivism"

"The information environment is under siege by a mass of domestic and foreign actors whose tools and agendas overlap in ways that blur borders and challenge norms. Capability outpaces both regulation and education." [17]

According to the latest MoD Integrated Operational Concept [18], (IOC), aimed at 2025, but written in the present tense:

"*The old distinction between foreign and domestic defence is increasingly irrelevant. When 'fake news' appears to originate not abroad but at home it gains credibility and reach, stoking confusion, disagreement, division and doubt in our societies. This has been particularly evident with the significant uptick in disinformation and misinformation during the coronavirus crisis……Sub-threshold operations are continuously executed at reach by malign actors who seek to undermine our military readiness, our critical national infrastructure, our economy, our alliances and our way of life."*

Public commentaries on these clandestine activities are accumulating fast. On 14 October the new MI5 Director General, Ken McCallum was explicit. [19]

"*Crucially, on the vaccine, we've been working to protect the integrity of UK research…, our academic research, our infrastructure. And, much discussed, threats to our democracy. In the 2020s, one of the toughest challenges facing MI5 and indeed government is that the differing national security challenges presented by Russian, Chinese, Iranian and other actors are growing in severity and in complexity – while terrorist threats persist at scale."*

This was rapidly followed by linked revelations in The London Times of open Russian efforts on state TV channels to denigrate and so damage international public trust in the Covid vaccine under development in Oxford.[20] The two statements have been seen as unusually pointed counter- disinformation responses.

[17] "How Threat Actors Are Manipulating the British Information Environment" Daniel Dobrowolski, David V Gioe and Alicia Wanless in RUSI Journal Volume 165, Number Three, April 2020, Pages 22-38 https://rusi.org/publication/rusi-journal/how-threat-actors-are-manipulating-british-information-environment

[18] Guidance "The Integrated Operating Concept 2025: Integrated Operating Concept calls into question the traditional approach to war fighting."
UK Ministry of Defence: Published 30 September 2020
https://www.gov.uk/government/publications/the-integrated-operating-concept-2025

[19] Ken McCallum, "Top Priorities And The Current Threat Landscape", UK Security Service 16 October 2020 https://www.mi5.gov.uk/news/director-general-ken-mccallum-makes-first-public-address

[20] TIMES INVESTIGATION "Russians spread fake news over Oxford coronavirus vaccine- Officials suspected of 'contemptible' online ploy " https://www.thetimes.co.uk/article/russians-spread-fake-news-over-oxford-coronavirus-vaccine-2nzpk8vrq

On 9 November The Times was able to publish [21]further information quoting "official sources" to reveal that GCHQ[22], in cooperation with the British Army's 77 Brigade [23]was involved in offensive cyber operations tackling anti-vaccine disinformation, using tactics similar to those used against the Islamic State. A rapid response team has been established in the Cabinet Office to coordinate such action against damaging narratives, including bogus treatments and conspiracy theories about the virus. But the sources stated that disruption would only be permitted against information originating from state adversaries and not online content from ordinary citizens, however misinformed. Nor could UK government specialists attack websites based in the other nations of the "Five Eyes" Intelligence Partnership (US, Canada Australia and New Zealand), which would remain the responsibility of partner agencies.[24] These were major revelations about sensitive and previously highly classified topics.

Biosecurity: Increasing Indicators of Associated Information Disorder

With understandably topical urgency, other authors outside government have been singling out the "*perils from mendacious social media*" arising during the pandemic.

"*Covid 19 disinformation is a sign of a broader trend in geopolitics. In place of military force, authoritarian states are increasingly exploiting the open media environment of democracies to try and shape public opinion and undermine social cohesion, sometimes in surprising ways. For example, disinformation that equates coronavirus restrictions with population control and the curtailment of freedom can help to remould a public health issue as an identity one, weaponizing it for subversion."* (Ignatidou 2020) [25]

A currently obtrusive example of this is the Culture War between "Covidiots versus Face - nappy wearers" - but perhaps soon anti-vaxxers versus doctors and public health officials.

Esam (2020), for the Henry Jackson Society, concludes [26] that extremists, especially from the radical right, have been drawn by public fears of Covid 19 to project their conspiracies into

[21] TIMES INVESTIGATION, Lucy Fisher and Chris Smyth "GCHQ in Cyberwar on anti-VAT propaganda-Spies tackle disinformation linked to Russia" https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2

[22] https://www.gchq.gov.uk/

[23] https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/

"[24]Home Secretary chairs virtual 'Five Eyes' security summit -Key allies met and agreed joint action to tackle emerging security threats during the coronavirus (COVID-19) pandemic. https://www.gov.uk/government/news/home-secretary-chairs-virtual-five-eyes-security-summit

[25] "Covid Lies Go Viral" Sophia Ignatidou "The World Today" October and November 2020, Pages 22-23 https://www.chathamhouse.org/publications/the-world-today/2020-10/covid-lies-go-viral-thanks-unchecked-social-media

[26] Rakib Ehsan "Beyond Covid, the UK must face up to renewed threats ", CAPX 6 October 2020 https://capx.co/beyond-covid-the-uk-must-face-up-to-renewed-threats/

the public mind, in an environment influenced by what he called Russian “Black PR”. State cultivated accusations of connections between Covid and biological weapons have been a trust-destroying feature of the pandemic almost from the date when the Chinese began, after unaccountable delay, to alert the world to the outbreak [27]. It is noteworthy that the subsequently admitted Soviet Active Measure (Operation Infektion) which launched the myth that AIDS stemmed from American bio labs, is still widely believed in the Third World.

Here strategic concepts emerging from disguised sub- conventional interstate conflict infiltrate the normally polite and benign discourse of public health. It will prove uncomfortable for many to accept that infectious disease medicine is now also an undeclared (and routinely denied) field of geostrategic and ideological competition. Yet there is no doubt that the Russian and Chinese governments have been attempting to influence Western publics in their understanding of the origins and effective treatments of Covid 19. The EU Disinformation Lab, for example, has been constantly tracking Covid 19 disinformation messaging in European information ecosystems.[28] All this suggests that wholehearted international cooperation may play a lesser role in resolving the Covid crisis or in future epidemics than many, especially in the WHO, would have hoped.

The important question, pervading this entire subject, is how effective malicious or mistaken information is, or might become. Thomas Rid, in his authoritative recent history of Active Measures[29], emphasised that, although many schemes for covert influence operations can be traced, often apparently launched for personal reputation and advancement within competitive intelligence bureaucracies, there is little evidence that they have so far been effective in changing the behaviour and decisions of targeted states and electorates[30].

[27] Michael S. Goodman and Filippa Lentzos, "Battles of Influence: Deliberate Disinformation and Global Health Security" Centre for International Governance Innovation, August 24, 2020 https://www.cigionline.org/articles/battles-influence-deliberate-disinformation-and-global-health-security

[28] YouTube version of an RT interview with a dissident German physician:
DISINFO: COVID IS NOT A KILLER VIRUS, WEARING MASKS AND TESTING HAS NO SENSE AT ALL
https://euvsdisinfo.eu/report/covid-is-not-a-killer-virus-wearing-masks-and-testing-has-no-sense-at-all/

DISINFO: THOUSANDS OF BELGIAN MEDICS DEMAND TO STOP THE COVID-19 HYSTERIA
This is particularly interesting as it fabricates the claim that Belgian doctors ask their governments to investigate the WHO's role in causing a needless Infodemic over Covid
https://euvsdisinfo.eu/report/thousands-of-belgian-medics-demand-to-stop-the-covid-19-hysteria/

[29] Thomas Rid, “Active Measures: The Secret History of Disinformation and Political Warfare “, Profile Books, 2020

[30] “…..Active measures” (AM) was the term assigned to influence operations in the Soviet Union and its satellites. This is not the term used in the U.S., where information operations, influence operations (IO), psychological warfare and other terms are more common.
Rid elaborates on the definition in the following ways. Active measures:
…are not spontaneous lies by politicians, but the methodical output of large bureaucracies,” usually situated in intelligence agencies
…all contain an element of disinformation: content may be forged, or the source of valid information doctored; agents and intermediaries pretend to be something they are not; the accounts publishing or amplifying messages may be inauthentic

Ignatidou cites evidence that only 10% trusted news on social media, compared with 44% who trusted news organisations. The most recently available surveys from the Pew Research Centre [31]found that 73% of the populations of 14 advanced economies approved of their nation's response to Covid. But the UK and US, were notable exceptions. 54% (UK) and 52 % (US) felt their country had done badly. 77% of Americans felt that their country had become more divided, but only 46% of UK respondents. These polls cannot of course reveal how far such judgements were moulded by social media. They were conducted in summer, before possible Pandemic Fatigue had grown, numbers of infections had rebounded, death tolls had risen, and political disputes over mask wearing, travel restrictions, and circuit breaker or hotspot lockdowns became increasingly highly publicised and embittered. It has also been suggested that, since the US and UK are already so internally divided about Covid, there would be little point (at least yet) in obtrusive and detectable external intervention to create further dissension.

Virtual Societal Warfare and its Potential Motives and Methods

Why is this information disorder happening, and why is it likely to continue and intensify in relation to public health, biosafety and biosecurity? How can it be best understood?

Underlying causes of distrust and disenchantment in advanced contemporary societies are a huge sociological question, far beyond the scope of this submission. But for more precise operational understanding of contemporary choices in the informational field there are important pre-Covid analytical categories, such as

"***Societal Warfare**, that is, warfare conducted by, within, through and against people and societies*", "[32]

or, more exactly, according to a slightly later Rand study,

…are politically instrumental. They intend to weaken an adversary by fomenting divisions, creating friction or mistrust between individuals or organization, or undermine the legitimacy of institutions.
Rid tries to dispel common misconceptions about IO, particularly the notions that disinformation is always well-crafted, that it propagates false news, and that it occurs in the public sphere. In fact, active measures are often messy due to their contradictory status as "covert operations designed to achieve overt influence." Generalizations about "fake news" miss the mark: "some of the most vicious and effective active measures in the history of covert action were designed to deliver entirely accurate information." These truths, however, were often "flanked by little lies" about the provenance of the data or the identity of the publisher. He also shows that many influence operations do not take place in public, a notable example being the 1972 defeat of a no confidence vote in Germany's Parliament, which relied on private lies that swayed two critical votes." Milton Mueller," A Review of Thomas Rid's "Active Measures", Internet Governance Project, Georgia Tech, 26 May 2020.
https://www.internetgovernance.org/2020/05/26/a-review-of-thomas-rids-active-measures/

[31] "Most Approve of National Response to Covid 19 in 14 Advanced Economies". Pew Research Centre https://www.pewresearch.org/global/2020/08/27/most-approve-of-national-response-to-covid-19-in-14-advanced-economies/

[32] Ariel E. Levite & Jonathan (Yoni) Shimshoni, "The Strategic Challenge of Society-centric Warfare," Survival, Volume 60, 2018 - Issue 6 Published Online: 20 Nov 2018 https://www.tandfonline.com/doi/abs/10.1080/00396338.2018.1542806?journalCode=tsur20

Virtual Societal Warfare [33] "*hostile social manipulation…. the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior".*

In the past year, as Ignatidou observes,

"*The virus brought together distinct streams of conspiracy theories, far right extremism, politically motivated propaganda, foreign influence operations and profit driven fakery in an unprecedented torrent* …".

Within such general information disorder, the notion of Virtual Societal Warfare, by the hostile states and organised, generally right wing, extremist groups, identified by Ignatidou, utilising disinformation and malinformation, and attempting to stimulate cascades of misinformation, usefully accommodates the malicious interstate competition and internecine conflict described and predicted in the British IOC. Their underlying purpose would be to confuse, damage and demoralise British society.

This destructive motivation is in principle distinguishable from other groups who can be observed spreading their opinions over Covid 19 and who might emerge in future incidents. These appear to be a shifting prolific mix of motivations, prolifically generating dissenting messaging. Ostensibly, they include openly determined sceptics and Covid deniers, cultists, eccentrics, contrarians, self-proclaimed libertarians, pranksters, QAnon devotees, anti-Bill Gates and 5G conspiracy theorists, as well as "accelerationists" and other extremists. For some of them wider disorder and confusion may be only a more or less unanticipated and regrettable by-product of transmitting burning convictions. Complicating the entire problem are genuine, intellectually honest dissenters,[34] including those with scientific credentials, who may - or may not - turn out to be eventually empirically vindicated, and insist on loud direct challenges to the technocratic logic of public policy. [35] If those crafting state backed disinformation campaigns are skilled, infodemic flows of disinformation and misinformation may superficially look very similar. Some apparently informed dissenters or well-meaning but misinformed eccentrics will consequently turn out, if their output is analysed and traced, to be professional disinformation conduits.

The Psychological Advantage of Malicious or Irresponsible Infodemic Behaviour

Pessimistic predictions of the potential power of Virtual Societal Warfare are supported by disturbing findings from social psychology, emphasising the unique potency of social media

[33]Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke J. Matthews "The Emerging Risk of Virtual Societal Warfare Social Manipulation in a Changing Information Environment,", Rand Corporation, 2019 https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2714/RAND_RR2714.pdf

[34] see, for example: https://lockdownsceptics.org/

[35] "White House Embraces Covid-19 'Great Barrington Herd Immunity' Declaration" New York Times 13 October 2020 https://www.nytimes.com/live/2020/10/13/world/coronavirus-covid

in creating information disorder: the distasteful experience of cognitive dissonance[36] tends to move people into filter bubbles, or even opaque “filter shrouds”, [37]where their opinions are reassuringly confirmed, and they may even lose awareness that the opposing views and evidence exist. Falsehoods on Twitter seem to be more persuasive and persistent than the truth[38]. Refutation of errors is very hard to achieve.[39] Moreover the tools of online propaganda, including fake identities[40], are spreading to a wider variety of actors[41] . And reaching out persuasively to the wide middle ground of the public may have little impact on the scale and volume of an infodemic. In the UK, at present, it has been established that even relatively small numbers of determined activists empowered with social media contribute disproportionately to information disorder. [42]

There are no obviously easy solutions to these troubling imbalances. Even discussing and raising public awareness of the problem may, according to at least one 2019 study, risk perverse results:

[36] Elliot Aronson and Carol Tavris, "The Role of Cognitive Dissonance in the Pandemic: The minute we make any decision we begin to justify the wisdom of our choice and find reasons to dismiss the alternative." The Atlantic, 12 July 2020
https://www.theatlantic.com/author/elliot-aronson/

[37] Joshua Geltzer "It's Not a Filter Bubble. It's a Filter Shroud" Just Security
March 26, 2018
https://www.justsecurity.org/54262/its-filter-bubble-its-filter-shroud/

[38] Soroush Vosoughi, Deb Roy, Sinan Aral, " Lies spread faster than the truth: The spread of true and false news online ", Science, 09 Mar 2018: Vol. 359, Issue 6380, pp. 1146-1151 DOI: 10.1126/science.aap9559
https://science.sciencemag.org/content/359/6380/1146

[39] Robinson Meyer “The Grim Conclusions of the Largest-Ever Study of Fake News: massive new study analyses every major contested news story in English across
the span of Twitter's existence—some 126,000 stories, tweeted by 3 million users, over more than 10 years—and finds that falsehoods almost always beat out the truth on Twitter, penetrating further, faster, and deeper into the social network than accurate information.” The Atlantic, 8 March 2018
https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/

[40]Mary Anne Franks "A dangerous form of unanswerable Speech - Deepfakes are not ideas that can simply be countered with different and better ideas." Boston Globe, 12 October 2020,
https://www.bostonglobe.com/2020/10/12/opinion/dangerous-form-unanswerable-speech/

[41]Hannah Murphy "The new AI tools spreading fake news in politics and business: Growth of artificial intelligence software is driving ‘democratisation of propaganda’" Financial Times, 10 May 2020
https://www.ft.com/content/55a39e92-8357-11ea-b872-8db45d5f6714

[42]“The desire to fight a “culture war” is the preserve of a small group on the political extremes that does not represent most British voters, according to a major new project on political polarisation in the UK.
A disproportionate amount of political comment on social media is generated by small, politically driven groups…. It found that there was actually widespread agreement in the UK over topics such as gender equality and climate change – often seen as culture war issues.” Michael Savage, ‘Culture wars’ are fought by tiny minority – UK study Report by the More in Common thinktank found that 12% of voters accounted for 50% of all social media users", Guardian 24 October 2020
https://www.theguardian.com/society/2020/oct/24/culture-wars-are-fought-by-tiny-minority-uk-study

"exposure to elite discourse about fake news leads to lower levels of trust in media and less accurate identification of real news. Therefore, frequent discussion of fake news may affect whether individuals trust news media and the standards with which they evaluate it. This discourse may also prompt the dissemination of false information, particularly when fake news is discussed by elites without context and caution."[43]

Indefinite - So Far Controllable - Dispute over Government Responses

Announcements of serious contagious disease can evidently create an initial sense of social unity, (*"We are all in this together").* But Covid 19 experience suggests a high likelihood that, at least without rapid and successfully draconian intervention, as claimed by China, underlying societal strains will, over time diminish social cohesion and mutual help [44], and create, accentuate and inflame potential national fault lines, and reveal new ones, Biosecurity crises as protracted and severe as Covid 19 evidently reveal many pretexts for societal dispute within liberal democracies.

The coverage, costs and burdens of public health responses and compensation schemes will seem genuinely unfair, unproven and disproportionate to affected groups in ways which can be maliciously emphasised and misrepresented. Disputes, including rioting, about appropriate state responses, may be spontaneous and unavoidable, but could also be deliberately fed - to a stage when they can all too obviously take up much of the oxygen of national political debate and the energy of senior decision-makers. Politicians are all aware that governmental reputation or even survival can now depend on their publicly perceived record in responding to Covid 19.

Argument about large-scale biosecurity responses can be expected to be *interminable*-endemic in Parliament, Twittersphere, and other spaces of public debate, even after the epidemic peters out. Arguments are not only about *facts*, though these are intractable enough. Medically, they include the complex, multidimensional, slowly established, ambiguous and often deliberately misrepresented epidemiological and therapeutic evidence about new strains of pathogens (e.g. contagiousness: basic reproduction number (R zero), effective reproduction number (Re), degree of dispersion (Rk) of the suspected pathogen, vectors of transmission, timing and detectability of symptoms, age profiles of the most vulnerable, overall lethality, in terms of case fatality rates, and long-term sequelae - and the estimated impact in excess deaths from reduced resources for the treatment of other illnesses .) It is painfully apparent that these dimensions are not easily discovered and have even now not been universally publicly accepted after 10 months in the case of Covid 19. (And in the

[43] Priming and Fake News: The Effects of Elite Discourse on Evaluations of News Media
Emily Van Duyn &Jessica Collier Mass Communication and Society Volume 22, 2019 - Issue 1
https://www.tandfonline.com/doi/abs/10.1080/15205436.2018.1511807

[44] Magda Borkowska & James Laurence (2020) Coming together or coming apart? Changes in social cohesion during the Covid-19 pandemic in England, European Societies, DOI: 10.1080/14616696.2020.1833067
https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1833067

chemical field the full logical and psychological consequences of novichok agents also do not yet seem to be fully determined.)

Disease modellers joke that "*when you've seen one pandemic, you've seen… one pandemic":* a laconic reminder of the inevitable risks of confusing a new bio security event with remembered past crises. That is a cognitive distortion likely to affect not just health authorities' decisions on responses, but manipulable public judgements of those unfolding choices.

More generally, additional impacts on mental health and social well-being of epidemic mitigation measures are hard to research and measure, though they are certainly adverse. The macroeconomic and regional consequences of various forms and durations of lockdown are hard to establish and their acceptability needs to be judged against the overall fiscal capacity of the state to bear additional costs arising from chosen pandemic response measures. This cannot be a straightforward and undisputed series of econometric calculations. Moreover, economic damage will partly - perhaps principally - arise from changes in individual behaviours prompted by personal, potentially manipulable, levels of fear rather than government prohibitions.[45] Given the huge human and commercial losses and the enormous scale of government support during Covid 19, even small fluctuations in fear determined behaviours would be economically significant.

Even more fundamental problems emerge from profound disagreements over *values* : the fairness and relative importance of goods and harms resulting from government responses, such as preservation of human life (in simple additional, or, alternatively, quality adjusted, life years), among different age groups , occupations and population subsectors, excess deaths from non-pandemic causes, fairness of mitigation effects between devolved legislative areas, regions and cities, and of the consequential economic compensation schemes - all incommensurably set against opposing values of freedom of choice, movement and association, national economic growth, local prosperity, maintenance of individual living standards, and varying, deeply held, concepts of civil liberties and human dignity. Part of the Covid 19 Infodemic, within at least some democracies, is a loud and chaotic moral debate seizing on dubious empirical evidence from all sources to justify personal intuitions. There will always be audiences for information and arguments, however disputable, or even disreputable, which challenge government policies in any health crisis. At least some of those demanding proof of "the scientific basis" behind policy decisions, and the absolute certainty of trials data, may be simply weaponizing and propagating their own agendas, well aware that the field of evidence is still under discussion, in a scientific context of complex probabilities that are frequently neither certain nor easily comprehensible by the general public.

[45] "Gertjan Vlieghe, of the Bank of England's monetary policy committee, [told] MPs last month that most of the damage to the economy arises from restrictions that people impose on themselves: "Government restrictions ... have had a much smaller additional direct impact on aggregate economic performance ... once we account for the prevalence of the virus." Dominic Lawson, lockdown didn't need this dodgy dossier, the government's advisers are slipshod, but their critics are deluded" Sunday Times, 8 November 2020 https://www.thetimes.co.uk/article/lockdown-didnt-need-this-dodgy-dossier-0v3ktm0mv

In these circumstances it is unlikely to be possible *ever* to justify, even in minutely analysed retrospect, to vociferous and highly personally motivated sceptics within divided audiences, any optimally effective and justified mix of public measures. And if it is impossible to demonstrate conclusively what success looks like, then hostile commentators will always be able to help create an impression of national or state failure.

Costs and Harms from Virtual Societal Warfare and Information Disorder

Information disorder risks lowering chances and levels of consensual social agreement. As the WHO pointed out, in the public health field, infodemics will tend to raise already debilitating and medically serious levels of anxiety, exacerbating the other mental health consequences of epidemics, and impose political distortions in policy. Infodemics may also decrease acceptance of onerous, reportedly medically necessary, restrictions and obligations. These are difficult or impossible to monitor and enforce. For Covid 19, so far, they include: hand washing, disinfection of purchases, observance of lockdowns, travel bans, social distancing measures, mask wearing, limits on social and family mixing, conscientious self-quarantining and scrupulous provision of accurate contact tracing information. Coercive enforcement and deterrent sanctions can have only limited effect on many of these activities. Research newly conducted during the pandemic finds the major predictor of individual compliance with health precautions is subjective belief in their medical effectiveness for avoiding Covid 19.[46]Perceptions of such effectiveness may be significantly affected by levels of misinformation and disinformation circulating in family groups and social networks. Analogously, loss of public trust in public statements about the effectiveness and safety of medical measures would also induce low take-up of testing or, eventually vaccines [47] (“*The MMR Effect"),* very probably alongside discontent about slow provision or limited availability.

This well identified obstacle to the U.K.’s management of the Covid 19 Pandemic has attracted both official and commercial responses. Only around 50% of British citizens currently express themselves as willing to be vaccinated. As a result a Whitehall unit dedicated to the promoting Covid vaccination has been set up with civil servants from the Department of Health and Cabinet Office” [48] In step with recently revealed, but

[46] " Predictors of COVID-19 voluntary compliance behaviors: An international investigation " Cory Clark, Andres Davila, Maxime Regis, Sascha Kraus, Global Transitions October 2020 https://reader.elsevier.com/reader/sd/pii/S2589791820300098?token=A638B0B31E273511CE2F56AA57A71716DF845CF37A7D9A43BC527FBAAF347AE995AFE6BCEAE7EEC371CD4572A8BE56FD

[47] Alex Tyson, Courtney Johnson and Cary Funk, " U.S. Public Now Divided Over Whether To Get COVID-19 Vaccine: Concerns about the safety and effectiveness of possible vaccine, pace of approval process", Pew Research Centre, 17 September 2020 https://www.pewresearch.org/science/2020/09/17/u-s-public-now-divided-over-whether-to-get-covid-19-vaccine/

[48] Chris Smyth and Lucy Fisher "Vaccine campaign will admit that jab may not be hundred percent safe" Times, London 7 November 2020 https://www.thetimes.co.uk/article/coronavirus-vaccine-campaign-will-admit-that-jab-may-not-be-100-safe-wszgv3k86

confidentially implemented, efforts by GCHQ and 77 Brigade , Facebook, Google and Twitter will mitigate matters by their recent public pledge not to profit from or promote "anti-vax" propaganda-partly because major companies had threatened to end their advertising on websites promoting false claims about autism and covert implantation of tracking chips . This limited, and well-intended public and private censorship will make some difference to the information ecology surrounding Covid 19. But it will also prompt rage and intensified misinformation efforts from conspiracy theorists.[49]

The passions revealed so far over Covid 19 suggest that some commentators and social media activists find the escalation of dispute over the crisis morally justified whatever the disruption and public uncertainties involved. There are indeed genuine dilemmas over how to conduct debates within civil society about pressing health issues and how to distinguish strongly held individual views from deliberate disinformation. They need to be considered in relation to the explosively controversial issue of Internet governance and regulation.

Recurrent Structural Probabilities of Future Infodemics

At the most fundamental biopolitical[50], level, then, there is abundant reason to expect recurrent disagreements over recognising suspected new infections or chemical hazards as real (rather than hysteria, hoaxes or false flag operations). It may never be easy to agree rapidly on their seriousness and whether they should be understood principally as threats to public health or to economic well-being-or, in future situations involving intensified international confrontation, perhaps operational readiness. Related difficulties can be expected in reaching consensus on underlying individual or institutional culpabilities, or legal powers and administrative responsibilities for consequence management. Decisions flowing from these fundamental framings often be unavoidable, far-reaching and yet misconceived and continually questioned and criticised.

Motives for State Disinformation over Biosecurity

Virtual Societal Warfare, exploiting scientific uncertainties and value disputes is a permanent uneliminable possibility to mobilise and amplify these frictions of interest and disputes over values of values and scientific judgement.

In future, deliberately planned, or maliciously improvised, infodemics might be stimulated to achieve, as their main intention rather than a by-product, the acrimoniously partisan hyper politicisation of public health, the distraction of national politics and public policy, the

[49] Caroline Wheeler "Tech giants vow to support jab with anti-vax boycott ", The Times, 8 November 2020. No URL

[50] ...." biopolitics can be understood as a political rationality which takes the administration of life and populations as its subject: 'to ensure, sustain, and multiply life, to put this life in order'.... Biopower thus names the way in which biopolitics is put to work in society .... ", Rachel Adams, " Michel Foucault: Biopolitics and Biopower"10 May 2017
https://criticallegalthinking.com/2017/05/10/michel-foucault-biopolitics-biopower/
The concept of biopolitics is potentially relevant to epidemics and Infodemics but the Foucauldian tradition has been so critically sceptical of state actions that it seems so far to have provided very few insights relevant to the management of public health.

delegitimation of political leadership, the collapse or contraction of wider public trust in governmental competence and good faith, and reduction in national self-confidence.

Intense, expanding infodemics could generate agonisingly difficult choices within democratic political cultures. It might, for example, become hard to determine the crossover point between loyal but critical citizen concern, expressing widely shared complaints and misgivings about sincerely perceived government errors and incompetence, against, on the other hand, destructive, covertly choreographed, criticism and obstruction of harsh but unavoidable government decisions at a time when national unity is critical. Those reaching opposing judgements might subsequently find it hard to forgive each other - an attractive outcome for a disinformation and malinformation effort.

These may appear huge and unrealistically ambitious goals, but Russian[51][52] and Chinese Influence and Information[53] operations often seem to involve attempting small increments of advantage which would seem individually to make little measurable sense to Western observers. The relative success of different systems in dealing with Covid 19 is becoming a key theme of Chinese triumphalism over the superior performance, and therefore the legitimacy, of the Chinese Communist Party. A form of ideological competition provides an additional motive for malicious disinformation or expertly obtained malinformation. Russian motives in this may be similar, though not identical, given lower national self-confidence in its own health arrangements. According to the US Center for Strategic and International Studies,

"Russian influence centres on weakening the internal cohesion of societies and strengthening the perception of the dysfunction of the Western democratic and economic system". [54]

[51] William J. Broad "Putin's Long War Against American Science: A decade of health disinformation promoted by President Vladimir Putin of Russia has sown wide confusion, hurt major institutions and encouraged the spread of deadly illnesses." NYT, April 13, 2020
https://www.nytimes.com/2020/04/13/science/putin-russia-disinformation-health-coronavirus.html

[52] Julian E. Barnes and David E. Sanger, "Russian Intelligence Agencies Push Disinformation on Pandemic: Declassified U.S. intelligence accuses Moscow of pushing propaganda through alternative websites as Russia refines techniques used in 2016" NYT, July 28, 2020
https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html

[53] Jennifer Rankin, "EU says China behind 'huge wave' of Covid-19 disinformation:
Brussels shifts position by accusing Beijing for first time of running false campaigns" Guardian, 10 June 2020
https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign

[54] "The Rise of Strategic Corruption: How States Weaponize Graft"
By Philip Zelikow, Eric Edelman, Kristofer Harrison, and Celeste Ward Gventer
Foreign Affairs, July/August 2020
https://www.foreignaffairs.com/articles/united-states/2020-06-09/rise-strategic-corruption

as well as the contributions to the relative prestige of their national biomedical sectors, there may also soon be straightforward commercial self-interest in promoting sales of competing Russian and Chinese vaccines – "*vaccine nationalism* ".

"No More Guard Rails "

It needs now to be more widely appreciated that some regimes have chosen to give up previously expected restraints over information offensives relating to Covid 19. In the US the Federal Government under President Trump has been calculated to be the most prolific spreader of mis-and disinformation[55], the Russian government has been prepared to see the propagation of open attacks on the safety of competing vaccines, and China has repeatedly suggested that, not only is it not responsible itself for the appearance of Covid but implied that there are good grounds to suspect the US military. As ex-President Obama recently put it, criticising his successor's record:

"… *misinformation. Social media, media infrastructure, the conservative media infrastructure…. That is a problem that is going to outlast Trump. Trump is a symptom of it and an accelerant to it. But he did not create it…. it has gotten turbocharged because of social media...When you look at insane conspiracy theories like QAnon seeping into the mainstream of the Republican Party, what that tells you is that there are no more guardrails within that media ecosystem,* " [56].

This amounted to the strong claim that President Trump had been openly conducting a prolonged information offensive (strictly speaking, in this context, deliberate *disinformation)* relating, amongst other issues, to a major public health emergency, for personal electoral advantage in the domestic processes of American democracy. Trump's approach to truth may not recur within later US Administrations, but the four years of the Trump Presidency could still become a symbolic milestone in the worldwide evolution and normalisation of exacerbated information disorder as a tool of disinhibited statecraft.

As Obama pointed out, there do indeed now seem no evident limits to how hard and how unashamedly political, including informational, warfare may be waged internally and externally, by Great Powers, whether over Covid 19 - or presumably other diseases, or chemical biological or radiological (CBR) incidents. Despite pleas from the WHO for responsibly cooperative behaviour, aggressive, openly attributable disinformation seems to carry no international sanction or punishment, though some democratic systems, like the UK, continue to resist it for internal cultural reasons.

[55] Sheryl Gay Stolberg and Noah Weiland, "Study Finds 'Single Largest Driver' of Coronavirus Misinformation: Trump, Cornell University researchers analyzing 38 million English-language articles about the pandemic found that President Trump was the largest driver of the "infodemic.",, New York Times, 30 September 2020 https://www.nytimes.com/2020/09/30/us/politics/trump-coronavirus-misinformation.html

[56] " Obama says Trump is a "symptom of" and "accelerant to" misinformation" Caitlin O'Kane, CBS News 15 October 2020
https://www.cbsnews.com/news/obama-criticizes-trump-misinformation/

British Parliamentarians, Governments and official agencies should consequently ensure that this condition, and the threat it represents to the British national interest, is widely publicly appreciated and taken fairly into account in judging government preparation and performance. But necessary warnings could carry some political costs. They may be rejected by many as special pleading intended to justify government repression and censorship, irresponsible securitisation [57], Russophobia[58] or Sinophobia.

Messaging strategies about looming dangers and disagreeable policy choices to manage and mitigate information disorder will therefore need to be particularly well thought out if they are not to be internationally damaging and excessively controversial domestically. Measures to restrict *disinformation* will be technically and legally difficult, continued *misinformation* is certain and rebuttals will not be completely effective in changing public understandings. Preventing circulation of *malinformation* will probably be politically impossible as well as legally problematic because, whatever its provenance and its probably ingenious blending with disinformation, its very purpose is to spotlight and force debate on otherwise confidential issues of intense public interest. And opponents of state action in the information sphere can justifiably point to real risks of prejudicing freedom of speech. There is already evidence that numerous countries around the world are tightening politically repressive measures using Covid 19 as an excuse[59], and that increased state control of the Internet has been a depressing feature of a widespread "pandemic effect".[60]

Disturbing Future Possibilities: Exacerbated Infodemics from Sharpening Great Power Conflict, WMD, Cyber, and AI

Advanced State Supported Cyber Threats

In conducting Virtual Societal Warfare, there are major potentially malicious synergies which might be achieved by a concomitant cyber campaign to undermine public responses to a natural or artificially introduced biosecurity threat. This could relatively easily include penetration of hospital, GP and other public health data systems, in order to covertly corrupt,

[57] Paul Rogers, "COVID-19: The Dangers of Securitisation", Oxford Research Group 29 September 2020 https://www.oxfordresearchgroup.org.uk/covid-19-the-dangers-of-securitisation

[58] Mary Dejevsky, "The Russia delusion: Cold War-style paranoia continues to grip the UK's political and media class" Spiked Online, October 2020 https://www.spiked-online.com/2020/10/16/the-russia-delusion/

[59] "No vaccine for cruelty: The pandemic has eroded democracy and respect for human rights -Strongmen have taken advantage of covid-19 in numerous ways", Economist October 2020 https://www.economist.com/international/2020/10/17/the-pandemic-has-eroded-democracy-and-respect-for-human-rights

[60] Charlotte Jee, "Governments are using the pandemic as an excuse to restrict internet freedom", MIT Technology Review, October 14, 2020 https://www.technologyreview.com/2020/10/14/1010361/governments-are-using-the-pandemic-as-an-excuse-to-restrict-internet-freedom/

ex-filtrate and then misleadingly leak [61]health data, research results, or additionally manipulated evidence of damaging internal disagreements over controversial public health decisions. It is worth remembering that the Russian and Chinese doctrine about Information Warfare and Information Sovereignty recognise little distinction between technical attacks on cyber systems and propagation, suppression or modification of content.

The 2019 RAND Report on Virtual Societal Warfare[62] warned that, amongst other societal damage, cyber campaigns could aim at:

"-generating massive amounts of highly plausible fabricated video and audio material to reduce confidence in shared reality

-discrediting key mediating institutions that are capable of distinguishing between true and false information

-corrupting or manipulating the databases on which major components of the economy increasingly rely

-manipulating or degrading systems of algorithmic decision-making, both to impair day-to-day government and corporate operations and to intensify loss of faith in institutions, as well as increase social grievances and polarization

-using the vulnerabilities inherent in the connections among the exploding Internet of Things [IoT] to create disruption and damage

-hijacking virtual and augmented reality systems to create disruption or mental anguish or to strengthen certain narratives" .

These ugly possibilities are worth fleshing out in relation to sports disputes over the handling of Covid 19. Highly damaging narratives could be fabricated over biosafety and biosecurity crises in the UK. They might create synthetic evidence for apparent underinvestment, inadequate training , stock levels or maintenance, errors in political direction and in police and hospital decision making , confecting sinister, inexplicable cover-ups of imaginary incidents, failures to respond to emails which were never actually sent, and apparent lapses in regulation, together with simulated or exaggerated timelines of bureaucratic obstruction, corruption and incompetence – perhaps most damagingly , the engineered impression of deliberate inflation or concealment of a pathogen's or chemical's health effects. Trust destroying initiatives of this kind might be combined with pre-existing medical anxieties like the inability of antibiotics to treat alleged or suspected pathogens, or fast spreading rumours that diagnostic tests were unreliable

[61] James Shires "Hack and Leak Operations and US Cyber Policy," War on the Rocks" 14 August 2020 https://warontherocks.com/2020/08/the-simulation-of-scandal/

[62] Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, Luke J. Matthews, "The Emerging Risk of Virtual Societal Warfare - Social Manipulation in a Changing Information Environment,", Rand Corporation, 2019, Page XIII
https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2714/RAND_RR2714.pdf

Given past problems with NHS cyber security, no one can guarantee that IT systems in the health sector will be reliably protected against advanced, persistent state-sponsored cyber threats[63] (Perhaps no available cyber defences can do that, even without the dangerous possibilities of quantum computing). But health sector IT security may not even be able to protect against talented nonstate hackers.[64] It is therefore probably impossible to be certain that data has not been expertly exfiltrated from UK health institutions and doctored for maximum impact if ever leaked or dumped

Ambiguous Hybrid Biological and Informational Attack?

Chemical and Radiological WMD attacks have already occurred in the UK. But they were not intended to create widespread public fear or even, probably, to be detected. The perpetrators were able to depart in good time for total sanctuary without risk of extradition, and, even when identified, were later covered by Russian government denials and counter accusations.

"The unwillingness to enforce international norms against chemical weapons use has in part stemmed from the blizzard of disinformation that has descended following attacks." [65]

A major failure of biosafety and biosecurity, or a deliberate, high-profile, attack with highly lethal and persistent chemicals, radiological materials, or lethal and contagious pathogens, would be so daunting that even severely dis-informed public opinion might not delay the rapid and forceful government responses which would be required[66]. But even here the extent of public suspicion, lack of cooperation, passive resistance or even active opposition would still matter. The US "Dark Winter" Exercises of 2001 eventually revealed the extraordinarily difficult choices (for example over mass ring vaccinations, and blocking public movement out of infected zones)[67], which would face governments who seriously believed that their populations were potentially threatened by highly contagious and lethal pathogens.

[63] Guy Martin and colleagues "Cybersecurity and healthcare: how safe are we? Rising cybersecurity threats to healthcare require policy makers to tackle fragmented governance, to develop and implement security standards, and to help organisations to improve their resilience," British Medical Journal , July 2017 https://spiral.imperial.ac.uk/bitstream/10044/1/51379/2/bmj.j3179.full.pdf

[64] for alarming examples in the US hospital sector, see Laura Dyrda, " The 12 largest healthcare data breaches in 2020 so far", Becker's Hospital IT, 19 June 2020 https://www.beckershospitalreview.com/cybersecurity/12-largest-healthcare-data-breaches-in-2020-so-far.html

[65] Dr Jack Watling, Conference Report Royal United Services Institute for Defence and Security Studies" Countering CBRN at Home and Abroad", October 2020, https://rusi.org/conference/countering-cbrn-home-and-abroad

[66] Shining Light on "Dark Winter" Tara O'Toole, Mair Michael, Thomas V. Inglesby
Clinical Infectious Diseases, Volume 34, Issue 7, 1 April 2002, Pages 972–983, Published: 01 April 2002, https://doi.org/10.1086/339909

[67] Lawrence K Altman , "Traces of Terror: The Bio Terror Threat; Panel Rejects Immunising All against a Smallpox Outbreak" New York Times, 21 June 2002

This is not the place to consider the probability of real threats from new generations of synthetically engineered biological weapons, although the technical capacity is quite certainly widening and deepening and there is an uneasy awareness of this among policymakers, academics and journalists[68]. Risks and vulnerabilities created by relentless developments in cyber and biotechnology are perhaps best understood as interconnected, and apparently, ineluctable, consequences of the "Fourth Industrial Revolution". Key technologies emerging from this huge global process have in common that they are "*disruptive, digital, diffused, decentralised, de-skilled,* and *"do it yourself""*. They are therefore intrinsically hard to regulate or control and most could impact on biosecurity, including, but certainly not only, its informational dimensions.[69] Worst case apprehensions about possible BW attacks by madmen, terrorist groups or states are regular features of printed and filmed fiction. The public imagination is already primed by these familiar dystopian narratives. New fears would probably propagate rapidly, at least in the uncertain first phases of future biosecurity incidents. "Dark Winter" was fictitious, but not fantastical. It will not quickly or entirely be forgotten.

Rather than concentrating upon catastrophic contagion with high mortalities[70], scenario planning related to the National Security Strategy should also consider the opposite scale of biological risk: small, semi-covert, attack, or moving sequences of attacks, with less lethal, or non-lethal, infectious pathogens, creating slowly apparent, possibly novel, symptoms, whose preplanned purpose was to be exaggerated into an infodemic. That might prove a temptingly cost effective, disinformation-facilitated national distraction during a politico military confrontation, and/or, conceivably, a financial crisis.

Antagonists with information warfare capabilities would find it entirely technically possible to disseminate claims that British (and course allied) Deep State circles were concealing a public health crisis, and misusing available health resources, in order to rush towards military confrontation -and, simultaneously, via different botnets, that the uncertain but highly publicised bio security event was a false flag operation intended to stir up hatred of Russia or

https://www.nytimes.com/2002/06/21/us/traces-terror-bioterror-threat-panel-rejects-immunizing-all-against-smallpox.html

[68] Katherine Charlet "The New Killer Pathogens: Countering the Coming Bioweapon Threat ", Carnegie Endowment. April 17, 2018 https://carnegieendowment.org/2018/04/17/new-killer-pathogens-countering-coming-bioweapons-threat-pub-76009

[69] Gregory D. Koblentz (2020) Emerging Technologies and the Future of CBRN Terrorism, The Washington Quarterly, 43:2, 177-196, DOI: 10.1080/0163660X.2020.1770969 https://www.tandfonline.com/doi/abs/10.1080/0163660X.2020.1770969?journalCode=rwaq20

[70] Elizabeth Cameron, Ph.D., Rebecca Katz, Ph.D., M.P.H., Jeremy Konyndyk, M.S.F.S., and Michelle Nalbandian, M.F.S. "A Spreading Plague: Lessons and Recommendations for Responding to a Deliberate Biological Event " Nuclear Threat Initiative, 2019 https://media.nti.org/pdfs/A_Spreading_Plague.Lessons_and_Recommendations_for_Responding_to_a_Deliberate.pdf

other antagonists. Actual human fatalities could be few or even zero, minimising international energy to follow up biological war crimes allegations when there would be many other aspects of a serious, and therefore potentially nuclear, crisis and its aftermaths. An engineered infodemic could be kept going indefinitely by largely self-sustaining information disorder, including demands for positive proof that post-remediation samples of naturally occurring pathogens were "back to normal", or that all possibly affected buildings and vehicles had been guaranteed as completely decontaminated from any conceivable residual chemical threats, - and then systematically discrediting what might be unavoidably patchy government data.

Informational and Cyberwarfare as A New Era in Biowarfare?

There are now more disturbing predictions about much wider and more lasting societal and security impacts of infodemics and information disorder. Their consequences could encompass and exceed all the malign possibilities discussed above. Bernard et al ventured a momentous conclusion in detailed research published in the last few weeks on "*Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare*[71] .

They assert that the world is *already* entering

"... a fifth era of biowarfare, one that incorporates the use of cyber capabilities and does not depend on the existence of a manufactured biological weapon per se. Biowarfare in the fifth era aims to undermine sociopolitical systems through social, political, and economic means by ''weaponizing'' or ''virtually escalating'' natural outbreaks, rather than directly inducing mortality and morbidity in populations through the deployment of harmful biological agents"

Their article provides convincing corroborative data on the extent of past hostile state disinformation over biowarfare allegations. The authors focus particularly on

"the rise of measles cases following disinformation campaigns connected to the US 2016 presidential elections, the rise of disinformation in the current novel coronavirus disease 2019 pandemic, and the impact of misinformation on public health interventions during the 2014-2016 West Africa and 2019-2020 Democratic Republic of the Congo Ebola outbreaks,

This leads to far-reaching warnings that

"...we anticipate the advent of a combined cyber and biological warfare. The latter is not dependent on the existence of a manufactured biological weapon; it manages to undermine sociopolitical systems and public health through the weaponization of naturally occurring outbreaks.'....

[71] Rose Bernard, Gemma Bowsher, Richard Sullivan, and Fawzia Gibson-Fall Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare.
Health Security Volume 19, Number 1, 2020 ª Mary Ann Liebert, Inc. DOI:
https://www.liebertpub.com/doi/10.1089/hs.2020.0038

"*The effects of disinformation campaigns on public health can produce consequences potentially comparable to biological warfare and terrorism: to weaken and undermine an opponent or to cause disruption and panic within a population"*

They caution that this kind of "biological "weaponry will no longer necessarily be limited, like BW agents as currently understood, by normative or cultural restraints, difficulties in storage of deployment or anxiety over retaliation escalation and international reaction.

These are large, unproven, though not ridiculous, claims. They will no doubt spark a productive debate in a vital field which it is becoming less and less possible to ignore. Yet, as scholars have pointed out, treating "cyber - bio" or virtual attacks as equivalent to actual biological weapons risks not only exaggeration, but reducing the unique stigma which nonvirtual biological agents rightfully carry given their threat to the basics of human physiology and social organisation. The UK, in particular, as a depository for the Biological and Toxin Weapons Convention should be interested in maintaining that distinction and the special pariah status of weaponised pathogens.

The Further, But Not Necessarily Far, Future: Hyper Malicious, Open-Ended, Possibilities of AI-intensified Infodemics.

But even if hybrid cyber/informational/BW threats are not yet overwhelming biosecurity threats at present, it is important to remember that they could well become so, unless means of limitation can be found. Written before recent infodemics, a 2017 research paper by Matt Chessen for the Atlantic Council[72] postulated a dauntingly inevitable wild card: the application of ever more powerfully evolving Artificial Intelligence to engineer uncontainable infodemics of information disorder

*"Over the next few years, MADCOMs—**the integration of AI systems into machine-driven communications tools for use in computational propaganda**[73]—will gain enhanced ability to influence people, tailoring persuasive, distracting, or intimidating messaging toward*

[72] Matt Chessen: " The MADCOM Future: How Artificial Intelligence Will Enhance Computational Propaganda, Reprogram Human Culture, And Threaten Democracy... And What Can Be Done About It." Atlantic Council, 2017
https://www.atlanticcouncil.org/wp-content/uploads/2017/09/The_MADCOM_Future_RW_0926.pdf

[73] "*Computational propaganda* involves the "use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks" (Woolley & Howard, 2018). While propaganda has existed throughout human history, the rise of digital technologies and social media platforms have brought new dimensions to this practice.
These technologies allow bad actors to deliver their messages to more people than ever before, regardless of geographical location. The anonymity enabled by many platforms has led to the proliferation of fake and automated accounts, which can be used to amplify misleading information or silence opposition. Finally, the monitoring and profiling of social media users by tech firms enables bad actors to target messages to audiences who might be particularly susceptible to disinformation campaigns. This online landscape presents a real challenge to organizations working on pressing social, political, and environmental issues. "
Oxford Internet Institute Project on Computational Propaganda
https://navigator.oii.ox.ac.uk/what-is-comprop/

individuals based on their unique personalities and backgrounds, a form of highly personalized propaganda….[74]. "

With the Covid 19 Global Infodemic in mind, an Australian military analyst pointed out that,

"*in the context of the …. [pandemic] … localised 'tactical' divides in Europe would have been identified and exploited by MADCOMs long before the disease reached [each] country, heightening emotions, fuelling panic and increasing the difficulty of containment efforts.*" [75]

This concept, as the uneasily ironic acronym suggests, is a Strangelovian extrapolation. MADCOMs will never appear as discrete, all-powerful, identifiable entities, partly because AI will also be used to defend against them, but there is no reasonable doubt that AI will be used to support all future forms of warfare including bio- cyber strategies. Since the barriers to entry into Information Warfare are so low, and no significant costs or risks have so far been incurred by its most aggressive practitioners, the baseline expectation must be increasing use of more and more advanced AI in the computational propaganda resources of hostile states. Biosecurity will always remain an attractive, emotionally salient, propaganda target. As the Fourth Industrial Revolution progresses - and probably accelerates - MADCOMs therefore represent a theoretically inescapable worst-case possibility to be kept in mind - unless they can be averted by changes in state behaviour or agreements on restraining the international spread and cognitive development of malicious technologies, as Chessen hopes, and makes (not entirely convincing) suggestions to achieve.

CONCLUSION

The picture set out above in this submission addresses only one aspect of the challenges facing HMG over biosafety and biosecurity. The informational field is important, complex, ambiguous, rapidly evolving, and increasingly disturbing. Its problems are unavoidable and, today, apparent. It is a potentially serious British vulnerability which is already being exploited, and which a comprehensive National Security Strategy needs to take into account. Yet it remains pervaded by methodological uncertainties about the real and potential impacts of information disorder and the potential of Virtual Societal Warfare, as well as practical, and democratically acceptable, solutions to defending key national values and interests against them. Some of the recent research triggered by increasing political disputatiousness in key democracies, together with the Covid 19 infodemic, may turn out to have exaggerated near-term impacts and inflated future risks. Rapid, competent, well-coordinated and consistently communicated state responses to biosecurity threats may decisively mitigate associated

[74] Perils and remedies of "personalisation " , for ever more precise targeting are further discussed in" The Role Of Technology In Online Misinformation", Sarah Kreps, Brookings , June 2020 https://www.brookings.edu/wp-content/uploads/2020/06/The-role-of-technology-in-online-misinformation.pdf

[75] Maj Lee Howard " Disinformation and misinformation campaigns - the Australian context", 26 August 2020, Australian Army Research Centre https://researchcentre.army.gov.au/library/land-power-forum/disinformation-and-misinformation-campaigns-australian-context

infodemics and even the cleverest disinformation. But it is too early for complacency about the negative consequences of information disorders that are genuinely new and far from well understood.

Much crucial information, on originators, motivations, target audiences and dissemination routes, of the three components of the information disorder swirling round Covid 19 will be sensitive and, at least initially, classified. But it would be highly desirable for the public to better understand what may, in the best available national judgement, come to affect their own perceptions of public health emergencies. And if Parliament is to conduct proper scrutiny of the development of policy, capability and law for this sensitive and expanding new field, it will need to gain an improved understanding of Government and wider public sector interpretations of the problem, and at least of their outline plans to address it. Against that background, non-governmental experts from a surprising number of relevant disciplines could bring their specialist knowledge to bear to build a composite understanding to inform the public.

RECOMMENDATIONS

If the Joint Committee accepts the picture presented in this submission, in combination with the other evidence received for the inquiry, it might reasonably consider, in its forthcoming Report,

1) pressing HMG to:

a) explain its underlying assumptions and accumulated evidence about:

i) the seriousness, motivations, composition (misinformation, disinformation and malinformation) and observed consequences of information threats in the biosecurity field, and

i i) their predicted development, especially in the light of rapid progress in computational propaganda, and the offsetting possibilities of “infodemiology”, together with

i i i) its overall strategy to respond to the problem, the constituent contributions of different departments, agencies (including intelligence agencies) and military units, and the consequent distribution of lead ministerial responsibilities.

b) Additionally, the Committee might wish to ask some of the following specific questions in order to understand and evaluate Government planning and resourcing to overcome informational vulnerabilities over biosecurity:

i) Will UK produce and provide a National Action Plan, presumably by the Department of Health, to combat infodemics, as requested by the WHO? If so, in what timescale is this contemplated and will there be a separate classified version for appropriate Parliamentary Committees to consider? Which department would lead in preparing that?

ii) How far is a National Action Plan likely to go beyond the recommendations in the EU High-level Group on Fake News and Online Disinformation, advanced in the less pressured circumstances of 2018? Following completion of Brexit, how will the UK coordinate its anti-disinformation activities with EU states? Or, especially for the offensive cyber operations to counter disinformation which have just been announced, will it rely exclusively on bilateral arrangements or collaborative efforts among NATO Allies or Five Eyes partners?

iii) Does the Government intend to develop and announce a comprehensive, whole of government, UK Counter Disinformation Strategy, encompassing the forthcoming Online Harms Bill? If so, what specific features and capacities might be required to address the special problems and sensitivities of infodemics and information disorder in the health sector?

iv) Does the Government consider it practical to build up general critical public awareness of malicious information, through wider online literacy and informed scepticism (a kind of cognitive herd immunity), as proposed in the EU HLG report? What evidence is there of success in this? What measures, by which organisations, might achieve it? How much could it be relied on as a factor in national resilience against malicious campaigns within general information disorder?

v) Are there Government or NHS systems capable of continuously shared internal horizon scanning for mis, dis, and mal information in the biosafety and biosecurity areas, in order to determine what, or who, motivates it, and to permit rapid rebuttal or improved explanation to reduce public apprehensions and misapprehensions? If so, where does this continuous diagnostic, attribution and response capacity reside? Is it wholly concentrated in the Cabinet Office? Or is it being developed elsewhere?

vi) Could such accepted national expertise be connected to support the judgements of a publicly sponsored UK Disinformation Observatory? If so, could and should this be established at arm’s length from government? Might an Observatory usefully mitigate information disorder by producing open, periodic, and, if necessary, frequent updates on the content and presumed authorship of disinformation backed by states or sophisticated nonstate actors? Should it also, perhaps more controversially, report on misinformation and the processes, culprits and motivations behind malinformation?

vii) How, and where, should responsibility for public sector efforts to counter misinformation and disinformation be best integrated with decision-making over the medical and logistic handling of biosecurity events? Do informational problems to date suggest a need for additional informational skills within Government, GCHQ, the Army, or the NHS?

viii) Should HMG deliberately build up, in advance of the next biosecurity crisis, the public visibility and credibility of expert individuals or groups of experts on biosafety and biosecurity? For this should it designate a British Dr Fauci equivalent, or Fauci Group, to sift, endorse and reinforce critical health-related messages, in order to reassure the public against disinformation and malinformation, including from self-appointed groups of alternative experts? How far does Covid 19 experience to date suggest that special training might be needed for designated, high-profile bio medical experts, in public presentation, including over coordinated visual materials and statistics?

ix) What actions, possibly including provision of evidence to the UN, would HMG propose to take to respond to identified state disinformation efforts aimed at the UK public over Covid 19, or other bio security events?

x) Should it become an acknowledged Government objective to ensure that, in the inevitable reviews of decisions over the handling of Covid 19, maximum efforts are made, even at the cost of delay, to reach a strongly supported consensus set of judgements on lessons learned, to help mitigate exploitable national divisions in handling future controversial biosecurity events?

2. The Committee will presumably also wish to take additional evidence from non-governmental experts. The diversity of references in this submission indicates the wide and expanding range of disciplines and professions who might productively contribute to this.

Paul Schulte

Birmingham ICCS and KCL

9 November 2020