CAGE

Exploiting a Pandemic

The Security Industry's Race to Infiltrate Public Health

Briefing Paper May 2020

Contents

Introduction

The Coronavirus/COVID-19 pandemic has brought a political rupture on a scale unprecedented in decades.

Both in terms of the domestic policies of individual states, and in international relations, the onset of the pandemic - and the responses to it - have heralded a significant, and likely irreversible, shift.

It is now clear that the world and the society that emerges after the pandemic will not be the same as the one that we knew before it.

What awaits us on the other side will, ultimately, be determined by the ongoing contestation between very different visions of the post-pandemic world.

It is evident, however, that vested interests - in particular, elements of the state apparatus and security industries - are pushing forward their vision in the direction of further securitisation, surveillance and a deepened ‘national security’ framework.

Left to them, the exceptional circumstances we are now experiencing will likely become the new norm.

Indeed a report by rightwing thinktank Policy Exchange states this clearly:
“The public will need to commit to a new social contract with its government, one that accepts that some infringements on privacy are a necessary
prerequisite for restoring and maintaining wider freedoms”[1].

This briefing paper aims to trace the emerging shape of security and surveillance in Britain under the pandemic.

It will also outline the interventions made by entrenched interests in the world of security and surveillance, in order to inform the concerned public, so it is better equipped to challenge these threats.

Legislative developments

The outbreak of COVID-19 was declared a pandemic by the World Health Organisation on 11th March 2020[2], while UK Prime Minister Boris Johnson announced a lockdown on the evening of 23rd March 2020[3].

Two days later, on 25th March, the Coronavirus Act received royal assent as law, granting the government and its agencies sweeping powers[4].

The Act includes the power to detain, isolate, assess and force disclosures about infections from individuals[5];
to ban events and gathering of more than two people[6];
and loosened safeguards over the use of investigatory powers - i.e. powers granted by the 2016 ‘snooper’s charter’ - allowing for intrusive surveillance warrants to be extended from three days up to twelve days[7].

As the then-Bill was being debated in Parliament, CAGE warned of the ‘possibility of these powers being open to abuse, liable to be used for political ends, and that they are in effect, a move towards strengthening the coercive capacity of the state in many ways’[8].

The Health Protection (Coronavirus, Restrictions) (England) Regulations 2020[9] statutory instrument came into force on 26th March, further outlining the scope and conditions of use for certain powers in the Coronavirus Act.

The Regulations allow for the use of force by officers in removing people if caught outside their homes without ‘reasonable excuse’[10], and £60 fines for offenders[11]. They were reaffirmed with slight amendment on 22nd April[12].

Since the introduction of powers in the Act, police forces across the country have, as expected, demonstrated cases of overreach, abuse and trigger-happy implementation[13] [14] [15] [16] [17], as well as false convictions of the public[18] [19].

Over the first month since the statutory instrument came into effect, 9,176 fines were issued by police for breaches of lockdown[20].

Organisations such as Policy Exchange are clear in their promotion of a ‘law and order’ approach to the pandemic.

Their recent report Policing a pandemic: The challenges of maintaining law and order during the Coronavirus response, co-written by former counter-terror chief Richard Walton, called for a reinvigoration of local policing teams to head off the perceived threat of disorder and crime[21].

CAGE have strong concerns that both the legal architecture as well as the techniques of surveillance and policing piloted during the pandemic will persist afterwards in the same way that counter-terrorism legislation was enacted in a fear-based environment and has continued to be amended and extended in violation of rule of law principles.

The Coronavirus Act includes clauses that allow its powers to be extended, modified and effectively made permanent[22].

Moreover, 'exceptional' powers are being regularly normalised; the risk remains high that, through this pandemic, we are seeing a reshaping of the terrain of surveillance and policing for the long term.

It is incumbent on the public and rights defenders to ensure that this is not the case.

Technology & Surveillance

Alongside questions around 'regular' law and order policing, the onset of the pandemic has sparked debate about the use and future of technology in surveillance.

Initial reports indicated the possibility of mobile phone location being used to track and map movement of individuals in order to monitor social distancing[23], or for similar tracking and monitoring capabilities being built into 'Contact Tracing' Apps[24][25] (see below).

Regulations governing the use of unmanned aerial vehicles (drones) by authorities have been relaxed, allowing for broader[26] and more invasive[27] use than before - allowing for drones to fly as close as 10 metres from the public.

Drones have already been used in policing lockdown by forces[28], signifying a militarisation of policing that is extremely concerning.

Contact Tracing Apps

The most significant aspect of the surveillance debate has been over the development of 'Contact Tracing' Apps for the purposes of managing the pandemic.

These are Apps which log - through Bluetooth and/or mobile data - the user's movements and contact with other users, and can be used to alert them if they have been in contact with another user logged as infected with coronavirus.

NHSX - the digital innovation and transformation wing of the health service, drawing together teams from Department of Health and Social Care, NHS England and NHS Improvement[29] - is developing the official Contact Tracing App for the UK[30].

As of the time of writing, this App is due to be piloted in the Isle of Wight.

Firstly, concerns have been raised about the risk of these Apps being made compulsory, or as a precondition to people being released outside[31] - and effectively gifting a potentially vast population-tracking apparatus to the government.

Secondly, there are growing concerns about the centralised mapping and matching model - that will facilitate the processing of contact and location data through a central server - being adopted by NHSX. This is in contrast to a decentralised, device-by-device approach to contact tracing as proposed by Apple and Google[32] and used in other European countries[33].

The centralised model offers a widespread surveillance mechanism that not only compromises user privacy, but can be vulnerable to access and exploitation of App data - both by outside actors and by intelligence services.

A group of over 170 cybersecurity experts published an open letter to NHSX voicing their concerns about 'mission creep' with the use of such a centralised system. They called on NHSX to ensure they they do not end up "[creating] a tool that enables data collection on the population, or on targeted sections of society, for surveillance"[34][35].

Tellingly, despite warning against making Contact Tracing Apps compulsory, a Policy Exchange report - again co-authored by Richard Walton - encouraged the development of a centralised command structure for Tracing and Testing during the pandemic. This command structure would be drawing together healthcare, police, military and intelligence experts, in order to analyse Contact

Tracing data[36], and was inspired by examples from the field of counter-terror policing.

When questioned by press, NHSX Chief Executive Matthew Gould avoided confirming whether or not GCHQ's National Cyber Security Service had influenced the decision to use a centralised model[37][38].

Gould himself has a background in the security and tech fields, and has had a career in diplomacy spanning some of the highest levels of the state.

Prior to joining NHSX, he served as the Director of Cyber Security in the Cabinet Office[39], and as a representative of the Joint Intelligence Committee[40] comprising the various security agencies. Gould has also served as the British Ambassador to Israel from 2010-15, during which time he set up the UK-Israel Tech Hub[41].

The usage and oversight of contact tracing apps must remain a focus for those interested in privacy, to ensure it does not become a mass surveillance mechanism, as is demanding a move to a decentralised model.

Technology and Private-Public Endeavours

The role of public-private partnerships during the pandemic, has raised further alarm bells, since they involve private firms accessing and handling personal data.

The involvement of third party firms like Palantir in processing confidential patient data presents a further danger of this pandemic being exploited for data mining profit[42][43][44].

Meanwhile, call centres to help run the contact tracing system are also reported to be outsourced to private companies such as Serco and G4S[45] - companies whose work include counter-terrorism[46], security and running immigration detention centres[47] - further cementing the merging of public health and private interests in the NHS[48].

Parallel to this, MI5's newly appointed Director General, Ken McCallum, has a history of involvement in cyber security, and has expanded private sector-security service collaboration during his time in MI5[49].
His stated priorities include making use of technical innovations to benefit the agency's work[50][51].

Similarly, Metropolitan Police Commissioner Cressida Dick spoke at the RUSI Annual Security Lecture in February on the police's determination to "seize the opportunities of data and digital tech to become a world leader in policing"[52].

The confluence of private sector involvement in technological development,
the public sector's embrace of these private interests,
heightened levels of surveillance during the pandemic,
and the relaxing of privacy safeguards for data - such as the aforementioned clause in the Coronavirus Act, and potential GDPR exemptions highlighted in the Policy Exchange report[53] - is a chilling mix.

It could fatally undermine rights and privacy protection for the public at large, and could further enmesh private interests in the public sector.

Old Enemies, New Foes

Prevent & Counter-Extremism

One would expect that, in the midst of a global pandemic, pro-PREVENT advocates might have reassessed their priorities to deal with more pressing matters.

This has not been the case.

Rather, certain figures in the counter-extremism industry have sought to tweak their case for PREVENT and counter-extremism by tying it into the proliferation of conspiracy theories accompanying the Coronavirus outbreak, and the apparent danger posed by people staying at home, spending time online, and being off the PREVENT radar.

PREVENT National Coordinator Nik Adams made it quite clear that the reduction in PREVENT referrals seen during lockdown was something to be concerned about, and he appealed to family members to monitor and report individuals who exhibit signs of 'radicalisation'[54][55] in their own homes.

The National Police Chiefs' Council announced that the ACT (Action Counters Terrorism) Awareness e-Learning training on spotting potential terrorist behaviour would be made more easily available online - and encouraged the public to undertake the training to become 'CT citizens'[56].

Meanwhile Commission for Countering Extremism (CCE) head Sara Khan penned an op-ed for The Independent drawing links between online usage at home, conspiracy theories and radicalisation[57] and announced the CCE's adoption of a "specific work stream examining COVID-19 extremism related issues"[58].

Nikita Malik, Director of the Centre on Radicalisation and Terrorism at the Henry Jackson Society echoed these concerns in an article for Foreign Policy, stating the isolation "risks increasing the consumption of fake news, conspiracy theories, and extremist material online", while encouraging "a deliberate, coordinated, and proactive response from social media companies" to deal with disinformation'[59].

There are multiple ways to gauge these interventions.

Nik Adam's appeal does come across rather like a desperate attempt by PREVENT advocates to try and force themselves into relevance.

However, his zeroing in on the home environment as a site of risk - alongside the wider rollout of the ACT e-learning - may indicate an attempt to more forcefully embed PREVENT and counter-extremism measures into the most private of spheres: the family home.

With the proliferation of web seminars being utilised in lieu of physical events, these appeals may also be a hint as to the direction of further counter-extremist surveillance in the online space and platforms, to facilitate clampdowns on these digital spaces of organising.

The other interventions connecting conspiracy theories to extremism, however, relate less directly to PREVENT than to other attempts to police social media discourse through the lens of countering extremism.

The campaign against 'conspiracy theories' has led by key figures in the counter-extremism industry, should be considered in light of ongoing moves to monitor the social media space.

Social media has been identified as a key site for the expansion of counter-extremism and adjacent programmes - the CCE's 2019 report Challenging Hateful Extremism states:
"...social media companies, [need] to demonstrate a deeper understanding of all the ways extremism manifests online...We have seen how their platforms are creating a hostile atmosphere that hateful extremists are exploiting"[60].

Meanwhile the government's Online Harms White Paper 2019 included within its scope of 'harms' to be regulated and targeted online, 'extremist content and behaviour' and 'disinformation' (i.e. 'fake news')[61].

Also stepping in to the field of fake news and extremism are Zinc Network[62] - formerly Breakthrough Media - the favoured partner of the government's Research, Information and Communications Unit (RICU) propaganda unit - have put together a report describing how far-right groups are manipulating the pandemic to build support[63].

As has been previously covered by ourselves[64][65] and media outlets[66], Breakthrough/Zinc have developed communications and for supposedly 'grassroots' organisations[67] with the support of the Home Office, for the purpose of countering extremism and providing counter-messaging at targeted demographics.

The global counter-extremism enterprise Institute for Strategic Dialogue has also conducted an investigation with BBC Click into the exploitation of the pandemic by far-right groups online[68].

The fact that key private actors have been focusing on this question indicates the importance of this campaign against conspiracies/ fake news/disinformation to the overall work of the counter-extremism industry.

Developments with the Online Harms agenda, and apparent pushback from social media companies, are also worth factoring into this trend.

The outcome of the Online Harms White Paper was intended to map out a regulation regime and impose a duty of care for social media and online providers imminently - similar to the way in which the Prevent duty commits public sector bodies to action - with broadcast regulator Ofcom named as a forerunner for the role in February this year[69].

However recent news indicates that plans for the rollout of the Online Harms regime are in doubt - with suggestions that legislation for the duty of care may be pushed back to 2023 amidst lobbying by social media companies[70], as well as the recruitment of a senior official from Ofcom by Facebook - in order to allow the latter to respond to the agenda[71].

Amidst this tug-of-war between government and social media giants, and exploiting justifiable concerns about child abuse online, voices in the counter-extremism industry may attempt to embed counter-extremism and anti-conspiracy deep within the Online Harms agenda.

New organisations, such as the Center for Countering Digital Hate appear to be serving as the campaigning arm of this wider agenda.

‘Conspiracy Theories’ & The Center for Countering Digital Hate

The campaign against ‘conspiracy theories’ during the pandemic appears to be being spearheaded in part by the Center for Countering Digital Hate (CCDH).

The Center [sic] initiated the #DontSpreadtheVirus advice campaign, the press release for which warns of ‘extremists seeking to undermine faith in government and experts’[72], while describing themselves as ‘working with practitioners in diverse fields, such as political science, behavioural science, the law, countering violent extremism and counterterrorism, child protection and identity-based hate to develop strategies that strengthen tolerance, liberalism and democracy, and counterstrategies to the new forms of political hate’[73].

CCDH is a relatively new organisation, which first came to public notice in mid-September 2019 with the release of their report on online ‘trolling’[74] - just over two weeks after rebranding themselves from ‘Brixton Endeavours Limited’[75].

Their latest campaign has also enjoyed widespread coverage in the mainstream press[76][77][78][79] - including a namecheck by the CCE’s Sara Khan in her Independent op-ed[80], and has been endorsed by the British government[81].

They also lobbied successfully to get noted conspiracy theorist David Icke deplatformed from social media for sharing misinformation about the virus[82][83].

Their website features prominent endorsements[84] from the likes of CCE head Sara Khan, Nick Lowles, CEO of Hope not Hate, Fiyaz Mughal, former Director of Faith Matters/Tell MAMA and Sasha Havlicek, CEO of counter-extremism think tank Institute for Strategic Dialogue.

All these organisations are actively involved in counter-extremism, and all of the individuals are part of Commission for Countering Extremism in various capacities[85].

Their founding director Morgan McSweeney has an extensive history of employment in the Blair-era Labour party, including working for a number of years as Campaign Organiser and Conference Administrator under Tony Blair’s leadership[86] as well as directing the leadership campaign of MP Liz Kendall in 2015[87]. More recently, he was announced as Chief of Staff for new Labour leader Keir Starmer[88].

Another of their Directors, University of Bristol lecturer Siobhan McAndrew, previously co-wrote a report for the CCE on Violent Extremist Tactics and the Ideology of the Sectarian Far Left[89] alongside noted pro-Israel activist David Hirsh.
The report sought to draw a connection between left wing, particularly anti-war activists, with extremism[90].

It is necessary to consider the wider ramifications of this campaign against ‘conspiracy theories’ (and/or ‘disinformation’ and ‘fake news’) beyond the context of coronavirus - particular in terms of what is captured by the term, and who gets to define it.

It can often, especially when used by the likes of government and the media, be used as a catch-all to smear any type of view they find unpalatable.

There is a world of difference between 5G conspiracies in the context of coronavirus and 9/11 ‘truther’ theories on one hand, and critiques and challenges about government policy decisions on the other - yet in the eyes of the powerful the two are often conflated.

One need not offer any solidarity to the likes of David Icke, for example, to recognise the dangers posed by having figures in the counter-extremism field act as arbiters of ultimate truth.

Criticisms of government foreign policy motivations are used to being dismissed as ‘conspiracy theorists’, for instance.

As just one example, in 2006 then-Foreign Secretary Jack Straw told the Select Committee on Foreign Affairs that
“Unless we all start to believe in conspiracy theories and that the officials are lying, that I am lying, that behind this there is some kind of secret state which is in league with some dark forces in the United States...there simply is no truth in the claims that the United Kingdom has been involved in rendition full stop”[91]

Yet as the Parliamentary Intelligence and Security Committee made clear in their 2018 report on Detainee Mistreatment and Rendition - and which the very existence of CAGE has been testament to - British intelligence officers knowingly provided and received information about prisoners being renditioned and tortured on hundreds of occasions between 2001-10[92] [93].

The issue of conspiracy theories must be dealt with, but holistically.

Conspiracies are able to gain ground the way that they do in part from widespread alienation and mistrust of power by the public. The hollowing out public education and the subsequent decline of critical thinking capacities also bears responsibility - as do the constant half truths and misinformation propagated by the government and mainstream media, which of course are never criticised as ‘conspiracies’.

This is a social issue that cannot be dealt with by either the punitive responses, counter-extremism, or by outsourcing the responsibility of public education to private enterprises in the counter-extremism industry.

Fundamentally, in this discussion, there is the sleight of hand whereby
a) the boundaries of ‘conspiracy theories’ are expanded,
b) then recast as an issue of ‘extremism’ and ‘radicalisation’,
c) then programmatically built into social media policies and practices, and
d) therefore made liable to removal, blocking and possible sanction against individuals.

This is only a recipe for censorship more broadly, and for ultimately re-asserting the state’s monopoly on truth.

The campaign against ‘conspiracy theories’ preceded the pandemic, and will outlive it - it certainly is not something that will remain exclusive to the present pandemic, and far-right figures like David Icke will not remain the only targets.

The Coming Cold War Against China

One cannot overlook the increasingly aggressive posture towards China and the Chinese government currently being taken by various Western governments.

Efforts to pin the blame for the pandemic on the Chinese government and to try and seek ‘compensation’ from China enjoy a bipartisan consensus among the major political parties in the US[94] [95] - and escalating attacks against China are likely to form part of the general election campaigns there later this year[96] [97].

In the UK too, a harder line than before appears to be taking shape. MP Dominic Raab, deputising for the Prime Minister at the time, stated that there would be no more “business as usual [with China] after this”[98] - albeit appearing to later soften his stance[99].

Fellow Cabinet Member Michael Gove also appeared to blame China for the UK’s poor preparedness for testing[100].

Meanwhile, a number of backbench Conservative MPs have been forming an anti-China bloc, and wrote to Boris Johnson urging a “rethink [of] our wider relationship with China”[101].

The Henry Jackson Society has spent recent recent months zealously attacking and seeking to apportion blame on the Chinese government for the pandemic[102], and its economic and social impact - even going as far as to suggest that its actions were ‘a deliberate act of mendacity’[103].

It published a report, Coronavirus Compensation? Assessing China’s Potential Culpability and Avenues of Legal Response[104], outlining a number of potential avenues for lawfare against China, with the clear intention to discipline, punish and/or embarrass

China on the world stage.

In the context of the pandemic, this discourse around complicity and compensation - ranging from attacks on China to the World Health Organisation[105,106] - are undoubtedly a means, in part, to deflect blame away from the UK and US government's poor handling of the crisis - which have resulted in some the very highest death tolls in the world[107].

However this turn against China is also more a fundamental, more long-term shift, and relates ultimately to its rising economic status, and influence on the international stage - leading to what we can likely expect as a Cold War against China.

Indeed the Henry Jackson Society themselves have a vested interest in opposing China - in 2017 it was reported that they had a £10,000-a-month contract with the Japanese embassy in London to "wage a propaganda campaign against China" and reverse economic co-operation between Britain and China.[108]

This is a break from the collaboration seen between the West and China over the course of the War on Terror - during which China collaborated with the US over the detention of Chinese-national Muslims in Guantanamo Bay.

The political split will, however, be unlikely to dent ongoing areas of consensus between China and the West in terms of security policy.

Chinese authorities have articulated long-standing antagonism between Muslim Uighurs in the Xinjiang/East Turkistan region and the Chinese government through the War on Terror language of 'radicalisation' and 'terrorism' to legitimise the internment of Uighurs in detention camps[109,110,111], and the technological sophistication of Chinese state surveillance continues to outstrip those practiced in the UK or US.

New MI5 Director General Ken McCallum is allegedly gearing up to sharpen the agency's focus on China and the perceived threat it poses to UK interests[112], while both MI5 and MI6 have been considering responses to China[113].

Furthermore, recent moves in the counter-terror field indicate a shift beyond the non-state 'Muslim terrorist' paradigm of the last few decades towards state-based antagonists.

The 2019 Counter-terrorism and Security Act introduced a new category of powers to be used against 'Hostile Actors'.

This category, vaguely defined, refers to activities carried out on behalf of a foreign state that:
(a) threatens national security,
(b) threatens the economic well-being of the United Kingdom, or
(c) is an act of serious crime[114]

While introduced ostensibly in response to the 2018 Novichok poisoning of Sergei and Yulia Skripal - allegedly made on behalf of the Russian state - this category is malleable enough to be used against anyone accused of working on behalf of 'hostile states', which itself is liable to change.

In March of this year, former government Minister for Countering Extremism Baroness Williams of Trafford revealed the existence of a hitherto secret governmental organisation, JSTAT - the Joint State Threats Assessment Team[115].

The work of JSTAT is to assess and combat the threat of 'hostile states'.
At the time of its formation in 2017 this would have applied more to Russia, but it will likely increasingly turn towards China.

This can be expected to herald a major shift in British domestic policy as much as foreign, and we should expect future counter-terror legislation being articulated, shaped around and justified on the grounds of the threat from foreign states such as China.

We can also likely expect some inter-agency contestation, between the fractions of the state that wants to move more stridently against China as a primary threat, and those that are wedded to the more familiar Islamists and the far-right dualism.

In either case, the outcome will most probably be new repressive policies and restrictive legislation, accompanied by racist profiling of those of East Asian origin - which we should be prepared to oppose.

The Muslim threat

This is not, of course, to say that anti-Muslim fervour has been supplanted - and recent weeks have seen traditional scapegoating and attacks on Muslims for various aspects of the pandemic in Britain.

As previously mentioned, the fear of 'Islamists' exploiting the pandemic for their own ends has been voiced by a number of figures in the counter-terror field, including Henry Jackson Society staff Rakib Ehsan[116] and Nikita Malik[117].
Conservative MP Andrew Rosindell questioned Home Secretary

Priti Patel and Foreign Secretary Dominic Raab about increased activities of 'extremist' groups in Britain - such as the Muslim Brotherhood[118].

Meanwhile former UKIP head Lord Pearson of Rannoch found time to enquire, for the purposes of Britain's anti-terror policy, whether the government would be undertaking an inquiry about Islamism and Islamic reform[119].

He also asked whether the government would seek to determine - in order to operationalise - the 'facts' promoted by The Religion of Peace website: an outfit whose stated goal is to 'counter whitewashing and explain the threat that Islam truly poses to human dignity and freedom, as well as the violence and dysfunction that ensues as a direct consequence of this religion's supremacist ideology'[120].

The question of political priorities

What the pandemic has laid out most starkly is the consequences of the government's political priorities, and the systematic privileging of Britain's military and security apparatuses over public health infrastructure.

Over the past two decades and through the course of the War on Terror, over £648 billion has been invested in military spending[121], the 2018 CONTEST strategy committed a further £1.4 billion investment in counter-terror for security and intelligence agencies and £2 billion for the UK Special Forces' counter-terror work[122], while the counter-terror policing budget alone was raised this year to near £1 billion[123].

Meanwhile, the NHS has been left systematically underfunded and under resourced - and manifestly unequipped to deal with a pandemic such as the current one.

This was despite prior forewarning.

The UK's National Risk Register has long identified a flu pandemic as the "gravest threat" to national security[124], advised that it was highly probable and that in the event, society was 'likely to face wider social and economic disruption, significant threats to the continuity of essential services, lower production levels, shortages and distribution difficulties'[125].

Meanwhile, the results of the 2016 flu pandemic simulation exercise Operation Cygnus - which concluded that the "UK's preparedness and response...is currently not sufficient to cope with the extreme demands of a severe pandemic"[126] - were barred from public release[127] and seemingly not properly followed up on[128].

The Crossover Between Security and Public Health

Drawing on this disconnect between public health and national security priorities, a number of counter-terror advocates have been making calls for a security-inspired approach to public health.

Voices within the national security field have called for 'Global Health Security' to be made central to the work of national security[129].

More pointedly, the Henry Jackson Society have drawn explicit, approving comparisons between the CONTEST counter-terror strategy with the response to coronavirus - both in an op-ed in Forbes[130] and in their submission to Home Office Committee's Inquiry in the Home Office preparedness for Covid-19 (Coronavirus)[131].

Policy Exchange made their case for a centralised command structure to tackle the pandemic inspired by the example of the National Police Counter Terrorism Network and Joint Terrorism Analysis Centre (JTAC)[132].

This appears to have been taken on board by the government. An exclusive in the Financial Times revealed that Director-General of the Office for Security and Counter-Terrorism, Tom Hurd, had been being picked to head a new 'Joint Biosecurity Centre' - described as running "along the same lines as Britain's Joint Terrorism Analysis Centre". [133]

Similarly, Associate Fellow at RUSI, Elisabeth Braw, made the case for NATO to take up the task of a co-ordinated response to future pandemics - rather than the World Health Organisation - in part to restore faith in the military alliance[134].

The intention of these interventions appears to be, in part, to seize an opportunity to give new lease of life to the vast, sprawling architecture of counter-terror and security built up over the last decades.

They also appear to be implicitly making the case that the expertise gleaned through counter-terror operations - and therefore, that their ‘expertise’ as counter-terror advocates - are worth transferring over into the field of public health.

But these interventions seem fundamentally to miss the point - that the long-term privileging of security is the problem, not part of the solution.

They also repeat the failures of the past by subordinating the need for a public health infrastructure to the demands and imperatives of the security industry.

The existing entanglement of security and public services - for example, the statutory Prevent duty under the Counter-terrorism and Security Act 2015 - has subverted and undermined the practice and spirit of public services.

The case for renewed investment and prioritisation of public health must be made outside and against the logic of security and surveillance; to try and reconcile these distinct approaches will blur the line between them, and produce a militarised response to public health.

Furthermore, the security-inspired vision of public health being promoted by these counter-terror advocates very much holds the door open for the predatory interests of private sector actors such as Palantir, mentioned above.

The logic is such: if the architecture of security can be adopted for public health ends, then surely the myriad private sector organisations jostling for influence in the security field can be welcomed into the healthcare sector too.

What we need to be collectively demanding is for the restoration of a people-centred approach to public health, and a thorough reassessment of ‘security’[135] - not to subvert public health and services to satisfy the demands of the national security industry.

Conclusion

This briefing paper has outlined the shape of debates and interventions in the field of security made over the course of this pandemic.

The world that awaits us post-pandemic will be determined by the ongoing contestation between very different visions of the post-pandemic world.

Though the forces of the security and counter-terror industries are loud and influential, the outcome is by no means a given.

It is vital, therefore, that the public and civil society develop a wide-ranging, coherent platform of demands for post-pandemic Britain, to provide a real alternative to the failed status quo.

As outlined in this paper, any such demands must be forthright in reining in the excesses likely to be unleashed by the government in this period of instability.

This includes:

- Opposing the mass expansion of intrusive surveillance technology,
- rolling back the vast increase of coercive state powers vested by coronavirus-related legislation,
- reversing the infiltration of the health services by shady private interests,
- stemming the encroachment of counter-extremism models in social media, and their use against ‘conspiracy theories’,
- and challenging the attempted fusion of security apparatus with public healthcare.

However these demands must be proactive as much as they are reactive, and embedded in a vision of healthy, safe societies.

CAGE will work with interested parties in developing a wide-ranging post-pandemic programme for society, and will keep our community involved and informed in this process.

Endnotes

[1] Walton, R & Marionneau, J. Exiting Lockdown - Using Digital Contact Tracing to Defeat COVID-19. Policy Exchange. 2020 [pg 15]

[2] WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. World Health Organisation

[3] Coronavirus: Strict new curbs on life in UK announced by PM, BBC. 24 March 2020

[4] Coronavirus Act 2020, Available at http://www.legislation.gov.uk/ukpga/2020/7/contents/enacted

[5] Coronavirus Act 2020, Schedule 21

[6] Coronavirus Act 2020, Schedule 22

[7] Coronavirus Act 2020, s1 (23)

[8] CAGE. Coronavirus Bill: CAGE Briefing Paper. CAGE. 2020

[9] The Health Protection (Coronavirus, Restrictions) (England) Regulations 2020. Available at http://www.legislation.gov.uk/uksi/2020/350/contents

[10] The Health Protection (Coronavirus, Restrictions) (England) Regulations 2020 s.6

[11] The Health Protection (Coronavirus, Restrictions) (England) Regulations 2020 s.10(6)

[12] The Health Protection (Coronavirus, Restrictions) (England) (Amendment) Regulations 2020. Available at http://www.legislation.gov.uk/uksi/2020/447/contents/

[13] These are being documented in the Policing the Corona State blog by Netpol and the Undercover Research Group: https://policing-the-corona-state.blog

[14] Family told not to feed the ducks in New Milton during lockdown. Daily Echo. 27 April 2020.

[15] Lancashire officer's 'make something up' threat condemned. BBC. 19 April 2020.

[16] Tool to report lockdown rule-breakers 'risks fuelling social division'. The Guardian. 9 April 2020.

[17] https://twitter.com/OdiliTime/status/1249602054252707840

[18] Coronavirus: Woman 'wrongly charged under new law'. BBC. 3 April 2020.

[19] Covid-19: Man wrongly convicted under Coronavirus Act. Express & Star. 14 April 2020

[20] Coronavirus: More than 9,000 fines for lockdown breaches. BBC. 30 April 2020

[21] Walton, R & Falkner, S. Policing a pandemic - The challenges of maintaining law and order during the Coronavirus response. Policy Exchange. 2020 [pg 6]

[22] Coronavirus Act 2020, s.1(88-91)

[23] Phone location data could be used to help UK coronavirus effort. The Guardian. 19 March 2020

[24] The NHS coronavirus app could track how long you spend outside. Wired. 7 April 2020.

[25] UK's coronavirus contacts tracing app could ask users to share location data. Tech Crunch. 28 April 2020.

[26] Drones get 'air corridors' to deliver medical supplies to hospitals in major expansion of unmanned flight. The Telegraph. 4 May 2020.

[27] Drones rules relaxed for police enforcing Covid-19 lockdown. Express & Star. April 15 2020.

[28] Coronavirus: Police use drone to shout messages at people telling them to go home amid Easter crackdown. The Independent. 11 April 2020.

[29] Who we are. NHSX.

[30] Gould, M & Lewis, G. Digital contact tracing: protecting the NHS and saving lives. NHSX. 24 April 2020.

[31] Don't coerce public over contact-tracing app, say campaigners. Guardian. 26 April 2020.

[32] NHS rejects Apple-Google coronavirus app plan. BBC. 27 April 2020.

[33] Britons may be unable to travel abroad because of UK failure to join international tracing app system. The Telegraph. 4 May 2020.

[34] 170 cybersecurity experts warn that British government's contact tracing app could be used to surveil people even after coronavirus has gone. Business Insider. 29 April 2020

[35] Joint Statement. 29 April 2020. Available here: https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view

[36] Walton, R & Marionneau, J. Exiting Lockdown - Using Digital Contact Tracing to Defeat COVID-19. Policy Exchange. 2020 [pg 10]

[37] UK's coronavirus contacts tracing app could ask users to share location data. Tech Crunch. 28 April 2020.

[38] NHS rejects Apple-Google coronavirus app plan. BBC. 27 April 2020.

[39] Matthew Gould biography. HM Government.

[40] UK CLIENT EVENT Risk: A view from the boardroom [event]. Marsh. 2015

[41] Matthew Gould biography. HM Government.

[42] Revealed: Palantir commits 45 engineers to NHS coronavirus data project, earns £1. New Statesman Tech. 27 April 2020.

[43] UK government using confidential patient data in coronavirus response. The Guardian. 12 April 2020.

[44] 10 questions to Palantir from privacy organisations [Press Release]. Privacy International et al. 29 April 2020

[45] Coronavirus: Plan to use private firm at centre of outsourcing scandal to run contact tracing attacked. The Independent. 4 May 2020.

[46] What we do - Events Security. G4S.

[47] Brook House: Serco take over immigration centre from G4S. BBC. 20 February 2020

[48] UK government 'using pandemic to transfer NHS duties to private sector'. The Guardian. 4 May 2020.

[49] New Director General of MI5 appointed. MI5. 30 March 2020.

[50] Ken McCallum named as new head of MI5. Civil Service World. 31 March 2020.

[51] New MI5 head promises to focus on China and harness AI. The Guardian. 30 March 2020.

[52] Dick, C. RUSI Annual Security Lecture. RUSI. 24 February 2020.

[53] Walton, R & Marionneau, J. Exiting Lockdown - Using Digital Contact Tracing to Defeat COVID-19. Policy Exchange. 2020 [pg 14]

[54] Coronavirus: Terror threat to hospitals as extremists call for hospital attacks during lockdown. The Independent. 21 April 2020.

[55] CTP warn about greater risk of radicalisation during COVID-19 lockdown. Counter Terrorism Policing. 22 April 2020.

[56] Access to online counter terrorism training made easier for home users. National Police Chiefs' Council. 7 April 2020.

[57] The 5G conspiracy theory shows just how fast extreme ideas spread across our society. The Independent. 23 April 2020.

[58] Second Newsletter: April 2020. Commission for Countering Extremism.15 April 2020

[59] Self Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. 26 March 2020.

[60] Commission for Countering Extremism. Challenging Hateful Extremism. Home Office. 2019 [pg 134]

[61] HM Government. Online Harms White Paper. 2019 [pg 31]

[62] Our work. Zinc Network.

[63] Far right hijack coronavirus crisis to push agenda and boost support. The Guardian. 25 April 2020.

[64] CAGE. "We are Completely Independent" The Home Office, Breakthrough Media and the PREVENT Counter Narrative Industry. 2016.

[65] Going global: the UK government's 'CVE' agenda, counter-radicalisation and covert propaganda. Open Democracy. 4 May 2016.

[66] Inside Ricu, the shadowy propaganda unit inspired by the cold war. The Guardian. 2 May 2016.

[67] 'This Is Woke': The media outfit that's actually a UK counter-terror programme. Middle East Eye. 15 August 2019.

[68] Coronavirus: Far-right spreads Covid-19 'infodemic' on Facebook. BBC News. 4 May 2020.

[69] Government minded to appoint Ofcom as online harms regulator [Press Release]. Department for Digital, Culture,

Media & Sport. 12 February 2020.

[70] New duty of care laws to protect children from online harms could be pushed back to 2023, says NSPCC. The Telegraph. 26 April 2020.

[71] Facebook poaches social media regulator Tony Close from Ofcom. The Times. 29 April 2020.

[72] Press Note: #DontSpreadTheVirus [Press Release]. Center for Countering Digital Hate. 27 March 2020.

[73] Center for Countering Digital Hate. #DeplatformIcke How Big Tech powers and profits from David Icke's lies and hate, and why it must stop. CCDH. 2020 [pg 2]

[74] Stop engaging with online trolls altogether, public figures say. The Guardian. 16 September 2019.

[75] Center for Countering Digital Hate/Brixton Endeavours Limited. Notification to Companies House of Change of name by resolution, 8 August 2019. Available at https://beta.companieshouse.gov.uk/company/11633127/filing-history/MzI0MzA0MzczM2FkaXF6a2N4/document

[76] Coronavirus: Call for apps to get fake Covid-19 news button. BBC News. 9 April 2020.

[77] Influencers among 'key distributors' of coronavirus misinformation. The Guardian. 8 April 2020.

[78] Digital Secretary promotes five-step plan to fight against Covid-19 'fake news'. ITV News. 27 March 2020.

[79] Coronavirus: Viral WhatsApp messages 'drop 70%'. BBC News. 27 April 2020.

[80] The 5G conspiracy theory shows just how fast extreme ideas spread across our society. The Independent. 23 April 2020.

[81] Press Note: #DontSpreadTheVirus [Press Release]. Center for Countering Digital Hate. 27 March 2020.

[82] Center for Countering Digital Hate. #DeplatformIcke How Big Tech powers and profits from David Icke's lies and hate, and why it must stop. CCDH. 2020

[83] YouTube deletes David Icke's channel over pandemic misinformation. Sky News. 3 May 2020.

[84] Endorsements. Center for Countering Digital Hate.

[85] More information on each figure and their respective organisations can be found in our 2019 report, CCE Exposed: https://www.cage.ngo/cce-exposed

[86] Morgan McSweeney. LinkedIn.

[87] Labour's past is killing its future. The Telegraph. 3 April 2020.

[88] https://twitter.com/SamCoatesSky/status/1246390026491105281

[89] Allington D, McAndrew S & Hirsh D. Violent extremist tactics and the ideology of the sectarian far left. Commission for Countering Extremism. 2019

[90] Demonising The Left. Tribune. 3 August 2019.

[91] Select Committee on Foreign Affairs. Examination of Witnesses (Questions 20-39). UK Parliament. 2005.

[92] True scale of UK role in torture and rendition after 9/11 revealed. The Guardian. 28 June 2018.

[93] Torture and Rendition report confirms claims made by survivors for decades, but now there must be accountability: CAGE [Press Release]. CAGE. 28 June 2018.

[94] U.S. officials crafting retaliatory actions against China over coronavirus as President Trump fumes. Washington Post. 30 April 2020.

[95] Biden Campaign Slams Trump On China And Coronavirus In New Battleground Ad. The Huffington Post. 18 April 2020.

[96] The Utter Futility of Biden's China Rhetoric. The Atlantic. 20 April 2020.

[97] Trump says coronavirus worse 'attack' than Pearl Harbor. BBC. 7 May 2020

[98] Raab fires warning shot at China over Coronavirus. The Financial Times. 16 April 2020.

[99] State Councilor and Foreign Minister Wang Yi Speaks on the Phone with UK Secretary of State for Foreign and Commonwealth Affairs Dominic Raab. Embassy of the People's Republic of China in the United Kingdom of Great Britain and Northern Ireland. 30 March 2020.

[100] Michael Gove appears to blame China over lack of UK coronavirus testing. The Guardian. 29 March 2020.

[101] UK spy agencies urge China rethink once Covid-19 crisis is over. The Guardian. 12 April 2020.

[102] Public Attitudes on the Response to Coronavirus. Henry Jackson Society. 20 April 2020.

[103] Henderson, M, Mendoza, A, Foxall, A, Rogers, J & Armstrong, S. CORONAVIRUS COMPENSATION? ASSESSING CHINA'S POTENTIAL CULPABILITY AND AVENUES OF LEGAL RESPONSE. Henry Jackson Society. 2020 [pg 3]

[104] Henderson, M, Mendoza, A, Foxall, A, Rogers, J & Armstrong, S. CORONAVIRUS COMPENSATION? ASSESSING CHINA'S POTENTIAL CULPABILITY AND AVENUES OF LEGAL RESPONSE. Henry Jackson Society. 2020

[105] Trump halts World Health Organization funding over coronavirus 'failure'. The Guardian. 15 April 2020.

[106] Who controls WHO?. Declassified UK. 9 April 2020.

[107] Britain now has Europe's second-highest COVID-19 death toll. Al Jazeera. 30 April 2020.

[108] Rifkind a stooge in secret PR war on China. The Times. 29 January 2017.

[109] The Uighur issue: excuses offered by the War on Terror. CAGE. 27 July 2015.

[110] Brophy, D. China's Uyghur Repression. Jacobin. 31 May 2018.

[111] Brophy, D. Good and Bad Muslims in Xinjiang. Made in China Journal. 9 July 2019.

[112] New MI5 head promises to focus on China and harness AI. The Guardian. 30 March 2020.

[113] UK spy agencies urge China rethink once Covid-19 crisis is over. The Guardian. 12 April 2020.

[114] Counter-Terrorism and Border Security Act 2019, Schedule 3 Part 1(6).
Available at: http://www.legislation.gov.uk/ukpga/2019/3/contents/enacted

[115] Baroness Williams of Trafford. Counter State Based Threats:Written statement - HLWS159. 17 March 2020.

[116] How Islamists are exploiting Covid-19. Spiked. 24 March 2020.

[117] Self-Isolation Might Stop Coronavirus, But It Will Speed The Spread Of Extremism. Foreign Policy. 26 March 2020.

[118] British government asked to account for rise in Muslim Brotherhood activity. The National. 29 April 2020.

[119] Lord Pearson of Rannoch. Anti-terrorism Policy (HL). 17 March 2020. Available at: https://hansard.parliament.uk/Lords/2020-03-17/debates/B7927A43-8EDE-4640-A8AF-1D3DC78EDADE/Anti-TerrorismPolicy

[120] About Us. The Religion of Peace.

[121] Public sector expenditure on defense in the United Kingdom (UK) from 2000/01 to 2018/19. Statista. 24 October 2019.

[122] Secretary of State for the Home Department. CONTEST - The United Kingdom's Strategy for Countering Terrorism. HM Government. 2018 [pg 60]

[123] Tougher sentencing and monitoring in government overhaul of terrorism response. Home Office & Ministry of Justice. 21 January 2020.

[124] British security services have ignored global health pandemics — the UK's biggest threat. Declassified UK. 24 March 2020.

[125] National Risk Register [pg 13]. Cabinet Office. 2008.

[126] Public Health England. Exercise Cygnus Report Tier One Command Post Exercise Pandemic Influenza 18 to 20 October 2016 [pg 6]. 2017

[127] If ministers fail to reveal 2016 flu study they 'will face court'. The Guardian. 26 April 2020.

[128] Revealed: the secret report that gave ministers warning of care home coronavirus crisis. The Guardian.7 May 2020.

[129] Coronavirus: How will it change national security and spying?. BBC. 2 April 2020.

[130] How Can Lessons Learned From Countering Terrorism Assist In The Fight Against COVID-19?. Forbes. 20 March 2020.

[131] Malik, N. Written evidence submitted by Henry Jackson Society (COR0018). Inquiry into Home Office preparedness for Covid-19 (Coronavirus). 15 April 2020. Available at https://committees.parliament.uk/work/184/home-office-prepared-

ness-for-covid19-coronavirus/publications/

[132] Walton, R & Marionneau, J. Exiting Lockdown - Using Digital Contact Tracing to Defeat COVID-19. Policy Exchange. 2020 [pg 9]

[133] UK turns to counterterror chief to run Covid-19 security hub. Financial Times, 11 May 2020.

[134] The Coronavirus Pandemic Should Be NATO's Moment. Defence One. 31 March 2020.

[135] See our report Beyond PREVENT: A Real Alternative To Securitised Policies: https://www.cage.ngo/cage-beyond-prevent-report

IIICAGE

CAGE is an independent advocacy organisation working to empower communities impacted by the War on Terror policies worldwide. The organisation highlights and campaigns against such policies in hope to achieve a world free from oppression and injustice.

📍 CAGE Advocacy UK Ltd, Premier Business Centre,
47-49 Park Royal Road, London, NW10 7LQ
☎ +44 (0) 207 377 6700
✉ contact@cage.ngo
🌐 www.cage.ngo