GLOBAL STRATEGY FORUM

EDITION No. 47 - NOVEMBER 2020

*The 47th in our series of expert comment and analysis, by **Rose Bernard**, **Richard Sullivan** and **Gemma Bowsher** of the Conflict & Health Research Group, King's College London. As always, the views expressed are those of the authors and not of Global Strategy Forum unless otherwise stated. To read more, see A Health Intelligence Framework For Pandemic Response: Lessons From The UK Experience of COVID-19 (Bowsher, G., R. Bernard and R. Sullivan) Health Security, volume 18, number 6, 2020.*

Becoming More Intelligent About Health Security

The Covid-19 global pandemic has become an (inter)national security threat, and as such a sole reliance on a 'science-led' approach is no longer adequate. In a series of articles over the last six months the Conflict and Health Research Group at King's College London have examined the case for rethinking biosecurity within a health intelligence framework. Our contention has been that scientific disciplines, such as public health or epidemiology, are just one technical component of what should be a broad intelligence-led approach to pandemic preparedness and response.

Furthermore, the process of science alone is not fit for purpose when it comes to meeting the exacting requirements of pandemic management[1].

As Paul Rimmer (former Deputy Chief of UK defence Intelligence) and Martin Bricknell (Professor of Conflict, Health & Military Medicine KCL and former Surgeon General of UK Armed Forces) have reflected, there is a need or a wider fusion of disciplines into a properly managed all sources intelligence process[2].

Whilst the creation of the UK Joint Biosecurity Centre is a step in the right direction, its creation in haste during the pandemic emergency should only be seen as a temporary stopgap.

Deriving a new health intelligence framework fit for purpose for the UK will require rebuilding hybrid expertise in health security and intelligence across the board[3]. Expertise should be cross-discipline, all-source and include relevant and as yet undervalued capabilities such as veterinary intelligence on zoonotic threats. Public health crises caused by zoonotic diseases are increasing globally, and expertise must be developed to reflect this, such as in-field veterinary specialists able to perform necropsies for unexplained mass die offs in wildlife.

Furthermore, whilst much of the focus during the pandemic has been on open sources intelligence, social media intelligence and signals intelligence, the importance of human intelligence (HUMINT) should not be overlooked[4].

The experience of Ebola in West African and Eastern DR Congo (DRC) is illustrative; not understanding burial practices and public sentiment for example, reflected a lacuna in pandemic HUMINT that goes well beyond the boundaries of behavioural sciences as well as traditional modelling and e-disease surveillance. In many parts of the world, including conflict ecosystems, digital representation is low so that relying on electronic reporting (OSINT, SOCMINT) for disease signal detection will inevitably fail.

Any health intelligence framework in practice will therefore require a long-term commitment to developing skills as well as processes that are able to fuse the languages of public health, veterinary intelligence, and intelligence capabilities.

Much has been written about the necessary boundaries between civil-military actors and capabilities in public health, domestic security, and humanitarian operations. Further work is certainly necessary to address this interaction specifically in domestic and international health intelligence frameworks.

Examining the rise of what we term Participatory SIGINT, in particular government surveillance through mobile applications, we have found worrying trends[5]. The COVID-19 pandemic has been used by many governments as a Trojan horse for expanding surveillance without adequate legal or regulatory oversight, for the mobilisation of emergency states to justify programmes curtailing personal freedoms and privacy rights that may endure long after the intervention's purpose has been served. Technologies, including those for SIGINT, have a crucial role to play in pandemic preparedness and response but only as part of a transparent, well governed system.

Furthermore, the political weaponization of naturally occurring outbreaks through mis- and dis-information creates an altogether more complex and volatile health security threat[6]. This type of 'cyber-bio' warfare can rapidly undermine socio-political systems, delegitimise science through disinformation campaigns targeting pre-existing communities such as anti-vaxxers, and even propagate conflict as we saw in Ebola outbreaks in Eastern DRC.

Given this rapidly changing and increasingly complex landscape, we believe significant resources are needed to develop an intelligence-led approach to health security threats, able to cope with this breadth at the same time as being accountable to democratic systems.

Rose Bernard, Gemma Bowsher & Richard Sullivan
November 2020

KING'S College LONDON
Conflict & Health Research Group

1 Bowsher, G. and R. Sullivan (2020). "Why we need an intelligence-led approach to pandemics: supporting science and public health during COVID-19 and beyond." J R Soc Med 9: 1-3.
2 Rimmer, P. and M. Bricknell (2020). "Are you ready for the next pandemic." Diplomat (Sept/Oct): 42-43.
3 Bowsher, G., R. Bernard and R. Sullivan (2020). "A Health Intelligence Frameworfor Pandemic Response: Lessons from the UK Experience of COVID-19." Health Security 18: 1-9.
4 Bernard, R. and R. Sullivan (2020). "The use of HUMINT in epidemics: a practical assessment." Intelligence and National Security 6:1-9.
5 Bernard, R., G. Bowsher and R. Sullivan (2020). "COVID-19 and the Rise of Participatory SIGINT: An Examination of the Rise in Government Surveillance Through Mobile Applications." Am J Public Health 5:e1-e6.
6 Bernard, R., G. Bowsher, R. Sullivan and F. Gibson-Fall (2020). "Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare." Health Security 19:1-10