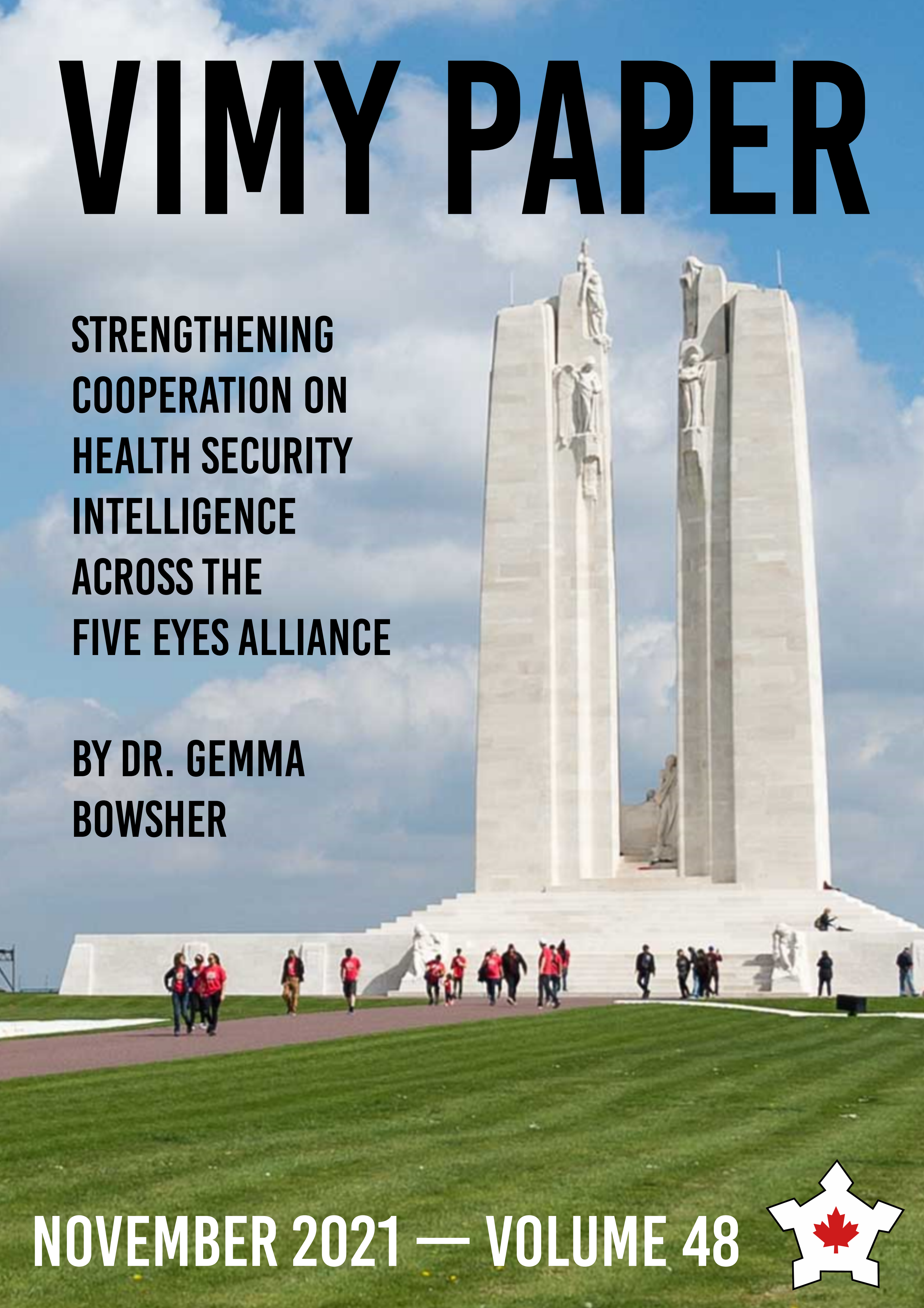
VIMY PAPER



STRENGTHENING COOPERATION ON HEALTH SECURITY INTELLIGENCE ACROSS THE FIVE EYES ALLIANCE

BY DR. GEMMA BOWSHER

NOVEMBER 2021 — VOLUME 48

Conference of Defence Associations Institute

The Conference of Defence Associations Institute is a charitable and non-partisan organisation whose mandate is to provide research support to the CDA and promote informed public debate on security and defence issues and the vital role played by the Canadian Armed Forces.

Conference of Defence Associations Institute 75 Albert Street, suite 900
Ottawa, Ontario K1P 5E7 613 236 9903 www.cdainstitute.ca

Views expressed here are those of the authors and do not necessarily reflect those of the CDA Institute.

All logos and trademarks used are the property of their respective holders. Use in this publication is under non-commercial and normative fair use provisions of applicable Canadian law.

Institut de la Conférence des associations de la défense

L'Institut de la Conférence des associations de la défense est un organisme caritatif et non partisan dont le mandat est de fournir l'appui de recherches à la CAD, et de promouvoir le débat public sur les questions de sécurité et de défense, et le rôle essentiel des forces armées canadiennes.

Institut de la Conférence des associations de la défense 75 rue Albert,
bureau 900 Ottawa (Ontario) K1P 5E7 613 236 9903
www.cdainstitute.ca

Les opinions exprimées sont celles des auteurs, et ne reflètent pas nécessairement les opinions de L'Institut de la CAD.

Tous les logos et les marques de commerce utilisés sont la propriété de leurs détenteurs respectifs.

L'utilisation qui en est faite dans cette publication l'est en vertu des dispositions de la loi canadienne applicable sur l'utilisation équitable non commerciale et nominative.

STRENGTHENING COOPERATION ON HEALTH SECURITY INTELLIGENCE ACROSS THE FIVE EYES ALLIANCE BY DR. GEMMA BOWSHER

INTRODUCTION

COVID-19 has marked a period of substantial rupture in international norms across security, global health and peace-building domains. Pre-pandemic anxieties regarding the growing convergence of health and security logics have been replaced by novel forms of engagement between civil, military, security and humanitarian groups (Elbe 2010). Worldwide, governments responding to the pandemic threat have used a range of tools at their disposal, which have almost universally included the use of security sector assets (Gad et al. 2021). Key global alliances such as NATO have shown the power of diversified mandates in response to biological cross-border threats (Tardy 2020), and the utility of such security-orientated organizations has been demonstrated at various stages of the complex delivery of pandemic response measures.

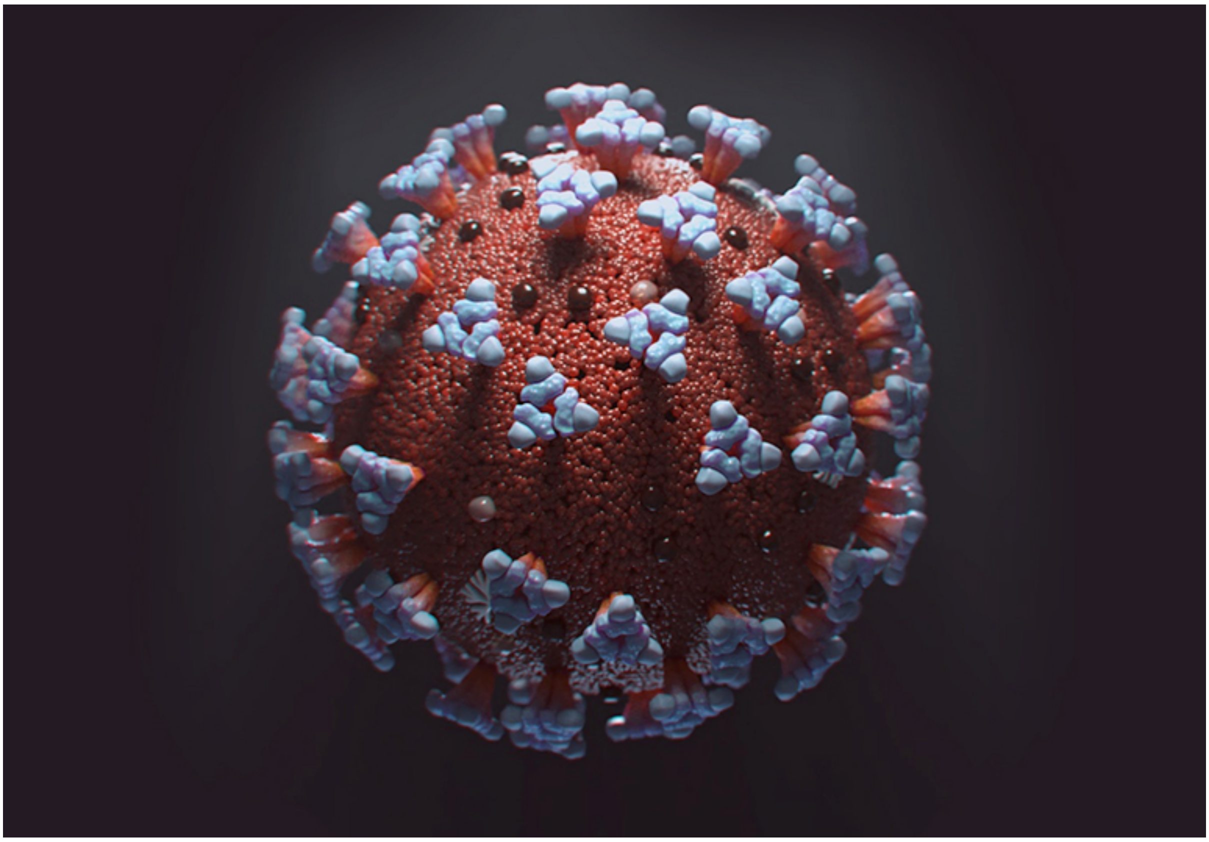
Information sharing has emerged as a particular weakness of pandemic response (Bowsher & Sullivan 2021). International collaboration in this regard has been notable for its lack of strategic notice of the emerging threat of SARS-CoV-2. Additionally, intelligence alliances, such as Five Eyes have been challenged to counter a range of unique threats both within and well beyond their traditional remits. The disparate nature of health information networks, including early-warning tools, has illuminated poorly connected global indicator and warning systems in the face of well-recognized high impact threats (Lentzos et al. 2020). Furthermore, diverse political approaches to disease response have polarized the advancement of common goals and revealed health security machinery that poorly integrates intelligence approaches across the Five Eyes alliance (Bowsher et al. 2020). In the context of these trends, an important question emerges; how can the tools, systems and processes of the security and intelligence sectors be used to deliver improved domestic and international responses to health security emergencies? Importantly, how can Five Eyes better integrate health security capabilities into its operations whilst continuing to address the full diversity of global threats from cyber-warfare, to conflict and terrorism?

The Australian scholar and former intelligence analyst Patrick Walsh has considered in depth, the leadership and governance challenges facing Five Eyes in the context of bio-threats and risks, particularly in regard to evolving genomic technologies (Walsh 2018, 2020). This paper seeks to expand on this important work by drawing lessons from the COVID-19 pandemic to consider emerging strategic and technical requirements in this space. Pragmatic approaches are required as the alliance faces a drastically altered post-pandemic security environment. It is plain that the health crisis has influenced almost every aspect of an already challenging period in international security. Strategic re-orientations towards the Indo-Pacific, the escalation of information and cyber-warfare operations, the ascendance of hostile state actors such as Russia and China, and the chaotic drawdown in Afghanistan have repeatedly underpinned the need for operational agility amidst a cluttered security landscape.

Addressing health security within these intelligence matrices can no longer be seen as a peripheral concern, rather a cross-cutting security issue of significance across Five Eyes. The UK death toll alone (at time of writing) exceeds 130,000 deaths – nearly twice the mortality of British non-combatants during the Second World War (Johns Hopkins Virtual Dashboard 2021). US Deaths sit at more than 700,000, Canada 28,000. Australia and New Zealand, who have pursued fundamentally different control strategies between them have approximately 1000, and 28 deaths respectively (ibid). Alongside deaths, the pandemic has triggered, according to the OECD *'the deepest economic recession in nearly a century'* (OECD 2021). Emerging from this period of profound turbulence, international governance and security regimes are pressed to consider anew what it really means to be secure, and what their responsibilities are in the protection of their populations against biological threat entities at this scale.

In this context, the complexity of the bio-sphere presents novel intelligence requirements cutting across existing geo-political tectonics. Biological risks extend well beyond the traditional remit of Five Eyes, with biological weapons featuring only as a small element of a wider landscape of emerging threats. Issues such as climate change, ecological destruction and wildlife extinction intersect with information warfare, territorial disputes and cyber hostilities to produce a threat paradigm requiring expanding interdisciplinary attention. Zoonotic diseases (pathogens transmitted between animal and human populations) such as SARS-CoV-2, Ebola and the MERS have demonstrated the volatility of this space as well as the lack of durable international infrastructure for combatting pandemic threats. The newly instituted WHO Pandemic Intelligence Hub signals a shift in direction towards more focused approaches for delivering early situational awareness, however a reliance on genomic techniques risks neglecting the interplay of geo-political and strategic concerns, with direct epidemiological and public health consequences.

FIVE EYES AND THE COVID-19 PANDEMIC



The COVID-19 pandemic has brought into stark relief the disjointed nature of health and security processes governing domestic and international responses to diverse biological threats. Increasingly the role of the health and security sectors overlap for high income countries and in particular members of the Five Eyes Alliance. Walsh has argued that ‘‘initiatives such as the [GHSA] established by the Obama Administration could provide opportunities for ‘Five Eyes’ to increase awareness of potential biothreats and risks in addition of course to their public health capacity-building effects’’ (Walsh 2020). During the pandemic, the security sectors[1] of all members of the alliance; Canada, Australia, USA, New Zealand and. the UK have been deployed to fulfil public health roles in support of domestic responses (Gad et al. 2021). Additionally, intelligenceAgencies, such as the UK's GCHQ have been tasked with handling specific threats such as vaccine disinformation, whilst the CIA has been examining questions of viral origins (Fisher & Smyth 2020).

Nevertheless, the nations of Five Eyes have individually struggled to match their highly-sophisticated intelligence, security and associated scientific apparatuses with the impact of COVID-19 in the context of (perhaps most importantly) highly variable political domestic responses (Bowsher et al. 2021). Despite 4 of the 5 nations of Five Eyes being ranked in the top 5 countries in the Global Health Security Index (GHSI), performance in public health metrics has notably lagged behind projections. The Macdonald-Laurier Institute's *COVID Misery Index,* a comparative tool for appraising comprehensive government responses to COVID-19, has singled out Canada, the UK and USA as below average for performance across a range of metrics. According to this ranking, Canada in particular suffered the ‘worst pandemic economic performance among comparable nations’ (Macdonald-Laurier Inst. 2021). The United Kingdom's House of Common's inquiry has questioned why international expertise was not part of the UK's advisory process, reflecting an intelligence failure that resulted in what the report described as “one of UK's worst ever public health failures’ (House of Commons 2021).

What has become clear is that the translation of intelligence capabilities into effective bio-/ health security responses is not a *fait accompli*. Although the deployment of security and

[1] The term security sector is used according to the definition provided by the Geneva Centre for the Democratic Control of Armed Forces. This definition understands the term to encompass "all the structures, institutions and personnel responsible for security provision, management and oversight at national and local levels. The security sector includes both actors that use force and those responsible for controlling how force is used through management and oversight".

intelligence tools in response to health emergencies has increased over the course of recent crises, the application of such tools to anticipate and detect threats across the spectrum of biological hazards has not kept pace with requirements. In the 2016 'Exercise Cygnus', a 3 day pandemic influenza simulation in the UK predicted health system failure (DHSC 2020). The threat posed by this result was raised in the UK's 2018 Biosecurity Strategy (HMG 2018), however a planned inquiry into preparations for emerging outbreaks was postponed to give way to other parliamentary activity. Repeated failures - both real and simulated - to effectively synthesize current capabilities in public health and health security, with intelligence processes have revealed the fragile support upon which biosecurity is maintained across Five Eyes.

This reality is notable given that pandemic threats have long been on the radar of participating nations. Professor Sir David Omand, the former director of GCHQ has written; "During my time as UK Intelligence and Security Coordinator after 9/11, a mutated flu pandemic occupied the top right-hand corner of the strategic notice risk matrix — of all the threats and risks, it poses the most lethal potential combination of impact and probability" (Omand 2020). Canada first referenced pandemics in its 2004 National Security Strategy within its 'all hazards' approach in response to the threat of SARS, and in anticipation of pandemic influenza (Wark 2020). The US Directorate of National Intelligence has included pandemics since 2009 in its annual threat assessment (DNI 2009). The UK produced a national biosecurity strategy in 2018 expressly aligning outbreak preparedness with the need for intelligence framework development (HMG 2018). Australia also, has long been recognized as a global leader in health security, taking a particular interest in leading on health security across the Asia-Pacific Region.

Lessons from previous epi-/pandemics have been better learned by other nations following health emergencies ranging from SARS to MERS and Ebola. Taiwan for example, in 2004, established a National Command Centre for response to pandemic threats, whilst South Korea activated the Central Disaster and Safety Countermeasures Headquarters within days of the country's first SARS-CoV-2 case (Wang 2020, Kim et al. 2021). The protocols for information sharing and joint response by the ASEAN network have shown the strength of multilateral health security intelligence coordination in this domain; the ASEAN Emergency Operations Centre Network for public health emergencies coordinated regional health intelligence sharing with member states (ASEAN 2021). The ASEAN BioDiaspora Regional Virtual Centre (ABVC) for big data analytics and visualization delivered regional situational reports using flight data to anticipate viral transmission patterns. These measures were developed as part of the 'Mitigation of Biological Threats Programme Phase 2' implemented in cooperation with Canada's Weapons Threat Reduction Programme, again revealing the high capability hubs centred within Five Eyes nations.

INDICATORS AND WARNINGS

How signal of an emerging hight threat pathogen is detected is essentially an intelligence problem (Levy & Wark 2021, Wilson & McNamara 2020). Novel pathogens and biological hazards emerging sporadically across geographies, both in remote territories and closer to home, pose enormous challenges for international detection and surveillance systems (Ostergard 2020, Bernard & Sullivan 2020). Developing indicators and warnings capable of providing early strategic notice to be fed into a broader health intelligence framework is thus a vital imperative for Five Eyes as high-consequence biological threats continue to emerge naturally. The chaos around the failures detecting this epidemic at an early stage, as well as the ongoing difficulties with the WHO-China COVID-19 origins investigation highlight the need to synthesize collection methods, some of which are accessible through standard bio-surveillance approaches, as well as information that is more specific to the covert collection techniques of intelligence agencies.

Canada took early steps in this direction following its identification of pandemics as a one of the eight key threat vectors in its 2004 security policy. The Federal government established a range of civil and military entities from the Global Public Health Intelligence Network (GPHIN), a biosurveillance platform based at the Public Health Agency of Canada, to the Integrated Threat Assessment Centre based at Canadian Security Intelligence Service (CSIS), which was intended to generate wide-ranging products including pandemic risk assessments (Wark 2020). It is generally accepted that this mechanism has failed to materialize substantive health security intelligence dividends in this space. The Canadian GPHIN has however been recognized as a world-leader for early warning situational awareness of chemical, biological, radiological and nuclear threats (CBRN), and has played a vital role in the detection of previous international epidemics such as H1N1 Influenza, MERS and Ebola. For reasons outlined in an independent review commissioned by the Minister of Health (Independent Review Panel 2021), GPHIN was sidelined in the COVID-19 response. Having detected a new atypical pneumonia-like disease in China, it was stopped from issuing global alerts and sharing early data streams.

This specific detection failure delayed early threat recognition by Canadian agencies which have traditionally collaborated with international partners. Subsequent failures of intelligence fusion have been replicated across Five Eyes governments. Previous work has interrogated the weak intelligence fusion of the UK's COVID-19 response framework and outlined the absence of health security intelligence frameworks across government as a key weakness in pandemic response (Bowsher et al. 2020). Canada, in particular has the opportunity to leverage its deep experience in public health intelligence and biosurveillance by leading the development of stronger transnational engagement on this issue. The UK has recently established a new 'Health Security Agency' but there remains no consolidated Five Eyes strategy for coordinated responses to health security threats.

Delivering improved health security intelligence is an attainable goal of Five Eyes allies; strengths in pathogen surveillance, genomic sequencing and public health intelligence mark a high capability alliance in need of a strategy (Bernard et al. 2018). The recent G7 meeting of world leaders reported on the need to develop approaches to improve and strengthen capabilities for One Health horizon scanning and intelligence, signalling a shift in international motivation (G7 2021). Establishing a clear policy for information sharing on early warning approaches coupled with intelligence coordination mechanisms for threat detection and response could ensure timely recognition of potential cross-border biological threats. There is scope for the creation of a cadre of 'health security liaison officers' to disseminate expertise across the intelligence agencies of the alliance in the same manner as is done for signals intelligence. Strengthening the professional and procedural health security intelligence infrastructure emerges as a key area of focus.

BEYOND HEALTH: NEW FRONTIERS IN INTERNATIONAL SECURITY

COVID-19 has demonstrated the grave risks of global *health insecurity*. A singular pathogenic threat entity opens up threat opportunities well beyond the immediate catastrophic population health effects. Health is ascending as a new frontier of international security, mobilizing strategic anxieties, condensing diplomatic efforts, and acting as a vehicle for traditional hostilities. Health disinformation in particular has appeared as a tool of cyber-warfare by hostile states, and so too has the targeting of health sector infrastructure, both digital and physical. Throughout the pandemic the increasing involvement of health within a wider security paradigm has reinforced the relevance of health security intelligence as a field of co-operative development for Five Eyes and wider international security regimes.

MIS-/DISINFORMATION

Health disinformation has been characterized as the future of biowarfare (Bernard et al. 2020); able to perpetuate and propagate pathogen transmission through secondary effects, as well as engendering hostility and violence towards health actors (Broniatowski et al. 2018). Disinformation operates to amplify the strategic influence of hostile actors through 'soft power' effects, eroding confidence and subverting population behaviour.

The COVID-19 pandemic is just the latest episode in the developing story of false narratives and factual distortion in critical health events. From Ebola to Measles the advent of 'fake news' has implicated hostile actors from the Kremlin to North Korea in the weaponization of health information (Barnes et al. 2020). Misinformation is an "accidental falsehood," shared without malice, while disinformation is a "deliberate falsehood," shared in full knowledge of its deception and often with malicious intent. Both phenomena have been amplified during the course of the pandemic to the extent that the World Health Organization (WHO) took the novel step of declaring an 'infodemic' – or a crisis of information detracting from disease control efforts (Ghebreyesus 2020). Even prior to COVID-19, concern about the health effects of disinformation was increasing; during recent Ebola epidemics in the Democratic Republic of Congo, disease misinformation was identified as a driver of persistent disease transmission, hampering public health efforts and costing lives in the process (Fidler 2020, Vinck et al. 2019). Measles too has been transmitted along pathways of misinformation spread by antivaxxers whose misinformation campaigns have also impaired immunization efforts for the cervical cancer-causing human papilloma virus (Boseley 2018).

Disinformation campaigns can be traced to groups such as the Russian State-linked Internet Research Agency, and the Chinese Government, which amongst other activities, are seeking to erode confidence in US and UK linked vaccination programmes (Bernard et al. 2021). A report by CSIS has accused Russia of "actively spreading disinformation blaming the West for the virus," and China of being "focused on a propaganda campaign that protects its own reputation and domestic legitimacy while touting its pandemic aid abroad" (Bell 2020).

A growing burden of evidence suggests that COVID-19 marks a significant inflection point; both in terms of the sudden growth in online participation and the diversity of health-related narratives (Zarocostas 2020). In particular, the enmeshment of COVID-19 narratives with themes of ethnic nationalism, insurrection, civil disorder, intra-state aggression and conflict raises the potential of these communicative forms to disrupt domestic and global stability (House of Commons 2020). Reports from late 2020 indicated that the British Government recognized this threat and tasked GCHQ with disrupting hostile-state linked content (Fisher & Smyth 2020). Collaboration on this issue is a clear opportunity for Five Eyes to bring their existing capabilities to bear on the evolving but familiar threat modality of information warfare. Leveraging the power of the alliance to engage with key stakeholders such as social media and technology companies would also ensure a joint approach to counter the expansion of subversive online influence resulting in real-world health security outcomes.

HEALTH SECTOR TARGETING

The health sector has become fertile territory for assault in both physical and cyber terrains. Previous work from Bernard et al. (2020) has identified an increase in attacks on health services encompassing 'infrastructure, medical devices, surveillance and outbreak response, research data and personnel and patient data. In 2020 a joint advisory notice was issue by the US government stating that "the Cybersecurity and Infrastructure Safety Agency, Federal Bureau of Investigation (FBI), and Department of Health and Human Services have credible information of an imminent cybercrime threat to US hospital and healthcare providers" (CISA 2021), a threat to critical national infrastructure that the Director of the FBI has compared with the 9/11 attacks (Viswanatha & Volz 2021). Cyber-attacks on COVID19 vaccine developers have raised serious concerns that cyber-actors are seeking to manipulate the pandemic to further strategic objectives (NCSC 2020).

A recent study by Joyce et al. focusing on radiation oncology services has identified major cyber-attacks on services in the US, Ireland and New Zealand, all of which compromised the delivery of clinical care (Joyce et al 2021). The 2021 Waikato DHB cyber-attacks on a New Zealand health board had wide-ranging effects across regional health services from delivery of radiotherapy, to delays to the COVD-19 vaccination programme. One of the most publicized attacks on the health sector was the 2017 Wannacry ransomware attack, which particularly affected the UK's national health service, caused failures of critical clinical services, and cost the UK government approximately £92 million (DHSC 2018, House of Commons 2018). The weaponization of health cyber-space is concerning given that the health sectors across the Five Eyes have not generally been afforded the same protections as other critical national infrastructures (e.g. energy). Reliance on legacy systems and network fragmentation has resulted in vulnerable cyber-terrains towards which novel state and non-state actors are increasingly turning their attentions (Bernard et al. 2020).

Physical attacks and security incidents have also increased in number during the course of the COVID-19 pandemic. Attacks on health workers, destruction of health facilities and the theft of equipment have all been identified in wide-ranging escalation of aggression towards health services (Larkin 2021). Already a high-risk field, in 2018 health and social care worker risk of attack was 5 times that of all other workers, comprising 73% of nonfatal workplace injuries and violence requiring time off work (US Bureau of Labour 2018, ICRC 2018). During the pandemic however attacks have increased and a recent study by the International Committee of the Red Cross has recorded a third of assaults as pandemic related. A recent study by Garrett et al. (2021) reports an increase of 57% in terrorist attacks against health services since 2001 – in part due to the nature of healthcare as a "soft target" with weak physical security (Garrett et al. 2021). Protection by national security services has not reached the levels afforded to other CNIs, and sharing of best practices across Five Eyes and wider security alliances remains a clear pathway for strengthening in the same manner as is afforded to terrorism or other forms of civil disorder.

As a sector, healthcare has been neglected as a prime concern of security and intelligence organizations, leaving unique proximate and distal consequences for overall population health and wider security. Recognizing the health sector both as a vital source of intelligence, and a critical sector in need of specific protections, is a universal imperative for Five Eyes nations who have all implemented restrictive population measures, such as lockdowns, stay at home orders and border closures, to prevent health systems from being overwhelmed (Garcia & Henry 2021). Healthcare is unique in its need to remain both accessible and secure; protections for the sector may necessitate greater focus on criminal &/or diplomatic sanctions for actors targeting physical and digital health infrastructure. The need for a joined up anticipatory approach is needed to embed health sector protections fully within cross-governmental and transnational efforts on health security.

CONCLUSION

The growing calls for 'intelligence-led approaches' to disease control reflect an overdue focus from the intelligence sector on 'health security', a domain encompassing a variety of traditional and evolving threats ranging from pandemics to engineered bioweapons (Walsh 2020, Bowsher et al. 2016, Bowsher et al. 2020, Lentzos et al. 2020). Repeated inattention to this critical threat paradigm demands high-level recognition from decision-makers and practitioners across health and security networks to remedy the systematic failures experienced across Five Eyes nations.

Coordination across Five Eyes on issues such as terrorism, provides a promising operating model for inter-allied liaison, especially in the context of global realignments in international strategy. Matching capabilities with policy to deliver strengthened health security is an attainable goal for the alliance and its partners. Sustaining attention on the technical and strategic requirements of inter-allied cooperation will require expertise from the intelligence and public health sectors – greater harmonization of approaches will be necessary to meet the ongoing challenge of COVID-19 and the certain appearance of health security threats of similar or even greater consequence in the coming years.

Dr. Gemma Bowsher is a medical doctor and social scientist working on global health security with a focus on health intelligence systems and public health in conflict settings.
In January 2015, Gemma joined the Conflict and Health Research Group at King's whilst completing her medical degree. Her work at CHRG has focused on health security intelligence linking clinical domains with intelligence processes within national governance systems. She received her master's degree in medical anthropology from Harvard University in 2016 where she was supervised by Arthur Kleinman, producing a dissertation examining the framing of the global surgery agenda within global health governance systems. Gemma commenced her PhD in September 2019, funded by the London Interdisciplinary Social Science Doctoral Training Partnership, for which she is working on antimicrobial resistance in conflict settings with a focus on Syria. In August 2020 Gemma took up the post of research associate on the 'research for health in conflict – MENA' project based at CHRG.

She is the 2021 winner of the CDA Institute's Graduate Student Conference was awarded the Metro Supply Chain Group Graduate Student Fellowship.

REFERENCES

ASEAN (2021) ASEAN Health Sector Efforts in the Prevention, Detection and Response to Coronavirus Disease 2019 (COVID-19). https://asean.org/asean-health-sector-efforts-in-the-prevention-detection-and-response-to-coronavirus-disease-2019-covid-19-1/

Barnes, J. (2020). Russia is trying to steal virus vaccine data, western nations say. *The New York Times*. https://www. nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia. html

Bell S (2020) CSIS accuses Russia, China and Iran of spreading COVID-19 disinformation. Global News December 3 2020. https://globalnews.ca/news/7494689/csis-accuses-russia-china-iran-coronavirus-covid-19-disinformation/

Bernard R, Bowsher G, Milner C, Boyle P, Patel P, Sullivan R. Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. Z Gesundh Wiss. 2018;26(5):509-514

Bernard R, Bowsher G, Sullivan R, Gibson-Fall F. Disinformation and Epidemics: Anticipating the Next Phase of Biowarfare. Health Secur. 2021 Jan-Feb;19(1):3-12

Bernard R, Bowsher G, Sullivan R. Cyber Security and the unexplored threat to global health: a call for global norms. Global Security: Health, Science and Policy 2021 5(1): 134-141

Bernard R, Sullivan R. The use of HUMINT in epidemics: a practical assessment. Intelligence Natl Secur. 2020;35(4):493- 501

Boseley, S. (2018). Measles cases at highest for 20 years in Europe, As anti-vaccine movement grows. *The Guardian*. https://www.theguardian.com/world/2018/dec/21/measles- cases-at-highest-for-20-years-in-europe-as-anti-vaccine- movement-grows.

Bowsher G, Milner C, Sullivan R. Medical intelligence, security and global health: the foundations of a new health agenda. J R Soc Med. 2016;109:269-273.

Bowsher G, Bernard R, Sullivan R. A Health Intelligence Framework for Pandemic Response: Lessons from the UK Experience of COVID-19. Health Secur. 2020 Dec;18(6):435-443

Bowsher G, Sullivan R. Why we need an intelligence-led approach to pandemics: supporting science and public health during COVID-19 and beyond. J R Soc Med. 2021 Jan;114(1):12-14

Broniatowski D, Jamison A, Qi S, et al. Weaponised health communication: Twitter bots and Russian trolls amplify the vaccine debate. Am J Public Health. 2018;108(10):1378- 1384.

Cybersecurity and Infrastructure Security Agency. "Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector." Accessed Online on February 1, 2021: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Department of Health and Social Care (2020) Annexe A: About Exercise Cygnus. 5th November. https://www.gov.uk/government/publications/uk-pandemic-preparedness/annex-a-about-exercise-cygnus

Di Matteo L. Canada's COVID performance on key measures among worst in developed world. Fraser Institute. May 26 2021. https://www.fraserinstitute.org/article/canadas-covid-performance-on-key-measures-among-worst-in-developed-world

Director of National Intelligence. Annual Threat Assessment of the Intelligence Community for the Select Committee on Intelligence. 12 February 2009. https://irp.fas.org/congress/2009_hr/021209blair.pdf

Dobrowolski D, Gioe DV, Herr T. What Would Winston do? Cooperative Approaches toward securing the Five Eyes Information Environment. The Atlantic Council. May 10 2021. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/what-would-winston-do-cooperative-approaches-toward-securing-the-five-eyes-information-environment/

Elbe S. Security and Global Health. Cambridge, UK: Polity Press; 2010.

Fidler DP. Disinformation and Disease: Social Media and the Ebola Epidemic in the Democratic Republic of the Congo. Council on Foreign Relations website. Published August 20, 2019. Accessed October 7, 2020. https://www.cfr.org/blog/disinformation-and-disease-social-media-and- ebola-epidemic-democratic-republic-congo

Fisher L, Smyth C, GCHQ in Cyber-War on Vaccine Propaganda. The Times. November 9th 2020. https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2

G7 (2021) Health Minister's Communique, 4th June 2021. https://www.g7uk.org/g7-health-ministers-meeting-communique-oxford-4-june-2021/

Gad M, Kazibwe J, Quirk E, Gheorghe A, Homan Z, Bricknell M (2021) Civil-military cooperation in the early response to the COVID-19 pandemic in six European countries. BMJ Mil Health. 167(4):234-243

Garcia S, Henry TD (2021) The Hidden Costs of Regional Lockdowns, The Lancet Regional Health – Europe. doi.org/10.1016/j.lanepe.2021.100035

Garrett A. Cavaliere, Reem Alfalasi, Gregory N. Jasani, Gregory R. Ciottone, and Benjamin J. Lawner.Health Security.ahead of print http://doi.org/10.1089/hs.2021.0004

Ghebreyesus TA. Speech presented at: Munich Security Conference; February 15, 2020. Accessed October 8, 2020. http://www.who.int/dg/speeches/detail/Munich-security-conference

Global Public Health Intelligence Network (GPHIN) Independent Review Panel Final Report. May 28, 2021. https://www.canada.ca/en/public-health/corporate/mandate/about-agency/external-advisory-bodies/list/independent-review-global-public-health-intelligence-network/final-report.html

HM Government. UK Biological Security Strategy. London: The Home Office; 2018. Accessed September 15, 2020. https://assets.publishing.service.gov.uk/government/uploads/ system/uploads/attachment_data/file/730213/2018_UK_ Biological_Security_Strategy.pdf

House of Commons Health and social Care and Science and Technology Committees (2021) Coronavirus: Lessons Learned to Date. 21 September 2021. https://committees.parliament.uk/publications/7497/documents/78688/default/

House of Commons Select Committee. (2018). *Faster Action Needed On Lessons Of Wannacry Attack*. https://www.parliament.uk/ business/committees/committees-a-z/commons-select/pub lic-accounts-committee/news-parliament-2017/nhs-cyber- attack-report-published-17-19/.

International Committee of the Red Cross (2021) Health services deal with a pandemic and violence in Colombia https://www.icrc.org/en/document/health-services-deal-pandemic-and-violence-colombia

International Committee of The Red Cross. (2018). *ICRC: Health-care workers suffer attacks every single week*. ICRC. https://www.icrc.org/en/document/icrc-health-care- workers-suffer-attacks-every-single-week.

Johns Hopkins Virtual COVID-19 Dashboard. https://www.arcgis.com/apps/dashboards/bda7594740fd40299423467b48e9ecf6

Joyce C, Roman L, Miller B, Jeffries J, Miller RC (2021) Emerging Cybersecurity Threats in Radiation Oncology, *Advances in Radiation Oncology*

Kim J-H, An JA, Oh SJJ, Oh J, Lee JK. Emerging COVID-19 Success Story: South Korea Learned the Lessons of MERS. Our World in Data. March 5 2021. https://ourworldindata.org/covid-exemplar-south-korea

Larkin H (2021) Navigating Attacks Against Health Care Workers in the COVID-19 Era. *JAMA* 325(18):1822–1824.

Lentzos F, Goodman MS & Wilson JM (2020) Health Security Intelligence: engaging across disciplines and sectors, Intelligence and National Security, 35:4, 465-476,

Levy A & Wark W. The Pandemic Caught Canada Unawares: It was an Intelligence Failure. Centre for International Governance Innovation. July 23 2021. https://www.cigionline.org/articles/the-pandemic-caught-canada-unawares-it-was-an-intelligence-failure/

Macdonald Laurier Institute (2021). Canada has worst pandemic economic performance among comparable nations : MLIs COVID Misery Index. June 17. https://www.macdonaldlaurier.ca/canada-worst-pandemic-economic-performance-among-comparable-nations-mlis-covid-misery-index/

National Cyber Security Centre. (2020). *Advisory: APT29 targets COVID-19 vaccine development.* National Cyber Security Centre. https://www.ncsc.gov.uk/news/advisory- apt29-targets-covid-19-vaccine-development

OECD – COVID-19 Focus on the Global Economy. 2021. https://www.oecd.org/coronavirus/en/themes/global-economy

Omand D (2020) Will the Intelligence Agencies spot the next Outbreak. The Article. May 18. https://www.thearticle.com/will-the-intelligence-agencies-spot-the-next-outbreak

Ostergard RL Jr. The West Africa Ebola outbreak (2014- 2016): a health intelligence failure? Intelligence Natl Secur. 2020;35(4):477-492.

Pfluke C (2019) A history of the Five Eyes Alliance: Possibility for reform and additions,Comparative Strategy, 38:4, 302-315

Tardy T (2020) COVID-19: NATO in the Age of Pandemics. NATO Defence College Research Paper 9. 25 May 2020. https://www.ndc.nato.int/news/news.php?icode=1440

UK Department of Health and Social Care (2018) Securing Cyber Resilience in Health and Care: October 2018 Update. https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update - last accessed 22nd March 2021

UK Department of Health and Social Care (2018) Securing Cyber Resilience in Health and Care: October 2018 Update. https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update - last accessed 22nd March 2021

US Bureau of Labour Statistics, Violence in Healthcare 2018. https://www.bls.gov/iif/oshwc/cfoi/workplace-violence-healthcare-2018.htm

Vinck P, Pham P, Bindu K, Bedford J, Nilles E. Institutional trust and misinformation in the response to the 2018–19 Ebola outbreak in North Kivu, DR Congo: a population- based survey. Lancet Infect Dis. 2019;19(5):529-536.

Viswanatha, A. and Volz, D. ” FBI Director Compares Ransomware Challenge to 9/11.” The Wall Street Journal. Accessed Online on June 4, 2021 at: https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003?mod=e2twp

Walsh P (2020) Improving ‘Five Eyes’ Health Security Intelligence capabilities: leadership and governance challenges, Intelligence and National Security, 35:4, 586-602

Walsh PF. Intelligence, Biosecurity and Bioterrorism. London: Palgrave Macmillan UK; 2018

Wang CJ, Ng CY, Brook RH. Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing. *JAMA*. 2020;323(14):1341–1342

Wark W (2020) Health Intelligence, National Security and the COVID-19 Pandemic. Canadian Global Affairs Institute. March 2020. https://www.cgai.ca/health_intelligence_national_security_and_the_covid_19_pandemic

Wilson JW & McNamara T (2020) The 1999 West Nile virus warning signal revisited, Intelligence and National Security, 35:4, 519-526

Zarocostas J. How to fight an infodemic. Lancet. 2020; 395(10225):676.