#COVINTELL – CORONAVIRUS AND THE SECURITY AND INTELLIGENCE SECTOR

MEDICAL INTELLIGENCE AND ITS PERSPECTIVES IN THE POST COVID-19 ERA

Nenad S. KOKOŠKOV*

Abstract:

In its basic thesis, this paper presents medical intelligence (MEDINT) as a specific platform of intelligence work, its historical development, and transfer from the military to the civilian intelligence sector, as well as its transformations from the Cold War period to the present day. It also points out the key features of the application of traditional intelligence methods for the purpose of MEDINT. By setting MEDINT in the context of the current Covid-19 pandemic, we aim to show how the intelligence community contributed to the effective health crisis response by applying certain intelligence tools: epidemiological surveillance, gathering relevant intelligence, targeted counterintelligence and epidemiological contact tracing. The aim of this paper is to anticipate the consequences of the Covid-19 crisis on the future of the global security environment, and to point out new perspectives. It is undeniable that the Covid-19 crisis has imposed the need for medical intelligence to adapt to the new security reality. This process implies not only further development of specific resources (in accordance with MEDINT criteria), but also external connection with professional and academic communities, as well as continuous monitoring of activities that carry a certain risk to public health (dual use research). Eventually, it is especially important for the intelligence sector to build different models of international cooperation that can be crucial in the effective response to global health security threats, such as a pandemic.

Keywords: *MEDINT, Covid-19, public health, security, intelligence, pandemic.*

Introduction

If we take into account the fact that after September 9, 2001, terrorism has become the greatest threat to global security, could the current Covid-2019 pandemic be the turning point in affirmation of biosecurity and, say, bioterrorism at the top of the scale of possible

* Academy of National Security, Belgrade, Serbia, email: nkokoskov@gmail.com

threats to national and global security? Throughout history, the intelligence community has adapted to the security environment, trying to contribute to the more efficient work of political leaders in the protection of national interests. Medical Intelligence (MEDINT), as a specific intelligence category, is aimed at anticipation, prevention, detection, identification and counteraction to health risks and threats. The aim of this paper is not to deal with the securitization of public health phenomena, but to point out the key contributions and importance of medical intelligence primarily to the pandemic as a security threat. In that sense, the Covid-19 experiences are very important in the validation of modern intelligence and security systems as a valuable national resource in the prevention and containment of a pandemic outbreak, as well as in the subsequent damage control.

MEDINT

MEDINT is a specific form of intelligence that essentially deals with the phenomenon of human health in various security, military, political and social contexts. The ultimate goal of MEDINT is to provide quality and timely intelligence products to various segments of the state's management apparatus, which translates into better management decisions. In a holistic sense, MEDINT can be defined as "the application of medical and biological knowledge to national defence" (Jarcho, 1991, p. 501). Also, MEDINT can be defined as "A systematic process of collection and analysis of health hazards; health threats; health risks & medical capabilities in a specific area" (La Gioia, 2015). According to the US Ministry of Defence, MEDINT is defined as "category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors" (US DOD Dictionary, 2021, p. 139). In addition, NATO provides the following general definition of MEDINT: "the product of the processing of medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. This intelligence, being of a specific

technical nature, requires informed medical expertise during its direction and processing within the intelligence cycle". (NATO, 2011, p. 1-21)

A timeline of MEDINT

Following the historical development of MEDINT, it has evolved in accordance with the security environment, the available resources of intelligence organisations, but also the needs of end users of intelligence products. MEDINT originally belonged to military intelligence. At the same time, the standard action of the military intelligence community towards the threat of biological weapons is primarily related to gathering information on foreign military systems, equipment and means, intentions for application of biological weapons, as well as for assessing defensive capacities (epidemiological characteristics, development of public health infrastructure etc.) (Kauffman, 2001, p. 11-13). Today, the military MEDINT supports the engagement of military personnel in peacekeeping missions or conflict hotspots, focusing, in terms of intelligence, on assessing and analysing the existing medical infrastructure "in the field", as well as the potential health risks for military personnel and the health risks for their environment after returning to the home country.

The transfer of MEDINT from military to civilian intelligence structures began after World War II and expanded its areas of operation to monitoring scientific research and development, civil health and numerous issues of importance for public health. (Clemente 2016, p. 282). The end of the Cold War along with multi-polarity in the global distribution of political, diplomatic and military power led to the transformation of the traditional concept of warfare into new forms of conflict with a more dominant asymmetry of the participant's power. In that sense, classical warfare, with the use of conventional weapons, was no longer the dominant form of security threat. Hence, the traditional application of MEDINT, as part of the legacy of the Second World War and the later bipolar division of the world, had to adapt to new subjects, new forms and means of endangerment.

After September 11, 2001, acquired experiences with anthrax letters in the USA, intelligence reports on Al Qaeda's intentions and

capabilities to obtain and to use biological and chemical weapons, and episodes with the Aum Shinrikyo apocalyptic sect in Japan, new security actors as potential users of biological weapons were promoted (Leitenberg, 2005). The largest national intelligence organisations have proportionally developed their own resources in the domain of medical intelligence. Finally, current experiences during Covid-19 impose the need for further transformation and adaptation of intelligence communities around the world, with the medical segment of intelligence systems gaining in importance.

Traditional collection methods and MEDINT

MEDINT exploits all traditional methods and techniques of modern intelligence in the process of gathering intelligence and data. However, the choice of method and its application depend on what is being investigated, who is the target of intelligence processing, what are the requirements of the final consumer of the report, and what resources are available?

Open source intelligence (OSINT), as a method of intelligence, is used in collecting various publicly available data, their analytical processing and subsequent preparing of bio-risk assessments reports with possible prediction of events that could pose a threat to public health and national security. In this regard, the largest security intelligence communities utilize their resources in identifying and analysing security indicators that are important for the production of quality intelligence reports, namely: activities in research centres and institutes dealing with biological agents, application and transfer of dual-use technology, equipment and products, analysis of the development and capacity of health infrastructure in other countries, etc. (Clemente 2016, p. 285-286). A special branch of OSINT is aimed at monitoring and analysing publicly available information regarding epidemiological processes in the world that are important for national security. Therefore, there is an interesting opinion advocated by Walsh who claims that “epidemiology is one critical scientific discipline, where the security community requires information in order to understand how and why disease is distributed across populations of interests, particularly if there are suspicious arising from other intelligence

sources that such distributions may be result of an intentional criminal act" (Walsh, 2018, p. 112).

When we talk about OSINT intelligence sources, a special significance is given to various, publicly available, scientific and professional publications that are relevant for biosecurity. In this sense, Walsh points to another important feature of OSINT sources in medical intelligence, and that is the contribution of the scientific community in understanding the various impacts on public health and national security. "So it is clear that law enforcement agencies and intelligence agencies need to engage with this very broad scientific community for their expertise (e.g. molecular biology, virology, microbiology, public or animal health) on who, what and how of bio-threats and risks." (Walsh, 2018, p. 110).

Apart from open source intelligence, diverse techniques of SIGINT methods have also found their place in collecting medical intelligence. However, when we talk about applying SIGINT techniques, there are some opinions according to which they are the least effective and significant in monitoring the outbreak and spread of infectious diseases. This claim is argued not only by sensitive ethical and legal issues, but also with the disproportionate consumption of intelligence resources (Bernard et al., 2018, p. 511-512). Although, the latest experiences in usage of certain SIGINT tools (monitoring the contacts of infected individuals and digital communications surveillance) applied in the suppression of the Covid-19 pandemic seem to refute Bernard's claims (which will be discussed below). Finally, the application of certain SIGINT techniques (interception of communications or monitoring of activities on social media) can be more than useful in early detection and prevention of bio threats, such as potential risk of intentional use of biological agents by malicious organizations, groups or individuals.

The use of human Intelligence (HUMINT), the oldest form of intelligence, might have a very significant contribution in obtaining quality MEDINT products. The potential targets of HUMINT can be scientific (dual-use) research institutions dealing with high-risk biological agents or military biological research facilities of foreign states. Also, recruiting agents in terrorist, criminal or various extremist

organizations can be crucial in terms of early identification of a security threat based on the use of biological weapons or endangering public health by other means. Espionage is also crucial for accurate assessment of the intentions and objective capabilities of the enemy. The importance of HUMINT is particularly important in cases where other intelligence methods show less penetrability, accessibility or reliability. Hence, HUMINT can provide intelligence verifications of certain indications or speculations that incidentally accompany the Covid-19 pandemic. Comparing the role of OSINT resources, social networks and SIGINT methods of intelligence, Bernard et al. came to the conclusion "that there is a place for OSINT and SIGINT in the detection and reporting of outbreaks. However, such tools are not sufficient on their own and must be corroborated for the intelligence to be relevant and actionable". (Bernard et al. 2018, p. 509)

MEDINT and the Pandemic

In the operational-tactical sense, all the activities of intelligence and security services regarding the pandemic can be systematized into two functional segments: PRE-exposure and POST-exposure. In this setting, intelligence activities are observed exclusively in accordance with one time coordinate, and that is the moment of occurrence of the negative event itself (the beginning of the pandemic). The first (pre-exposure segment) is therefore important in the prevention and prediction of infectious disease, with the development of hypothetical models of its possible course and consequences, while the second is aimed at reducing its consequences and controlling the damage. (Kokoškov & Ristanović, 2021, p. 27) POST-exposure intelligence activities begin when a negative event (epidemic/pandemic outbreak) has occurred. Regardless of what caused the epidemic/pandemic (natural or artificial processes), the response to it will be essentially the same. It will be conducted by the national public health system in cooperation with other entities within the state capacities. The goal of these activities will be aimed restrain the negative process and eliminating its consequences.

The role of intelligence communities (MEDINT) during the Covid-19 crisis

The current pandemic caused by SARS-CoV-2 presents a globally distributed infectious disease that has caused massive human diseases as well as numerous functional disturbances in the public health, economic, cultural and every other segment of societies. It is a very convincing and well-argued example of the extent to which the global public health crisis is becoming a geopolitical and a security problem.

By analysing the contributions of security and intelligence agencies in the fight against Covid-19, Walton points to four key courses of action (Walton, 2020). The first one deals with health intelligence monitoring and evaluation of epidemiological processes that are important for national security. The goal of this activity is to timely, accurately and clearly inform political leaders about potential biological threats, their possible course and impact. It can be applied both in the pre-exposure phase and after the outbreak of a pandemic.

The second direction of intelligence action towards the pandemic presents the classic espionage aimed at gathering secret data and information with the aim of revealing the intentions, but also assessing the capabilities of foreign states. One of the most intriguing questions that accompany the Covid-19 crisis is related to the origin of the virus. Apart from the health perspective, this question also encompasses a security, and even a geopolitical connotation. Nevertheless, as the pandemic progressed, interest in information related to the pandemic expanded to the efficacy of certain drugs, research and development of new vaccines and their efficacy and safety, global distribution of new strains of SARS-CoV-2, and others. In this context, it is realistic that some national intelligence services have been actively working to provide information and intelligence assessments that have helped their national leaders in crisis management.

The third direction is especially important because it is aimed at opposing the placement of untruths and misinformation and basically has a counter-intelligence character. It will be discussed in more detail below.

Finally, the fourth model is based on the application of technical measures to monitor the contacts of persons who pose a potential risk

for the spread of infection in the population. According to the WHO, epidemiological contact tracing is one of the crucial health measures in the suppression of contact-communicable infectious diseases (World Health Organization, 2017). In this way, people who have been exposed to the virus and who pose a health risk in the further spread of the infection need to be identified. Hence, "For contact tracing to be an effective public health measure requires most secondary cases to be discovered and isolated before they become infectious" (Keeling, 2020, p. 865). In a research study conducted by the University of Oxford, it was scientifically proven that the traditional way of manually monitoring contact tracing in the case of SARS-CoV-2 is not efficient and fast enough to monitor the behaviour of the current pandemic, suggesting the use of modern digital tools (Ferretti et al., 2020, p. 4). However, although the application of modern digital techniques in epidemiological surveillance has proven to be effective, it has nevertheless initiated very sensitive ethical and legal discussions, which may affect the modality and scope of their application in the future.

Counterintelligence activities during Covid-19

The activities of national intelligence services during the pandemic also play a significant role in the counter-intelligence sense. In the preventive segment, this action is primarily focused on protecting their own sensitive security information and concealing the activities of national entities in legitimate dual use researches that pose a potential risks to public health and biosafety. However, when a pandemic occurs, post-exposure counterintelligence actions are directed towards the application of denial, deception and disinformation (DDD) techniques. In that sense, constant monitoring of activities on the internet and social media is of key importance. Since these communication spaces have an increasing influence on creating public opinion and attitudes, they could be useful for various abuses and malicious actions. (Kokoškov & Ristanović, 2020, p. 37)

During the Covid-19 crisis, the internet and social media were promoted as one of the most powerful platform for offensive counterintelligence. Conspiracy theories about the origin of the virus, its spreading, the effectiveness of personal protective equipment, the

performances of the virus itself; development, efficiency and (non)harmfulness of vaccines, etc. are topics that have gained a lot of attention on social media. The spread of untruths and misinformation on these topics has greatly influenced the attitudes of the public, the loss of credibility in the states' institutions in general, as well as the efficiency of health crisis management, and finally the course of the pandemic. Back in February 2020, addressing the participants of the Security Conference in Munich, WHO Director A. Gebrejesus warned the audience with the words "We are not only fighting a pandemic, we are also fighting an infodemic" pointing to the huge harmful impact of false information on opposition pandemic. (Ghebreyesus, 2020)

By analysing these complex impacts during a pandemic, Bernard et al. make a very bold claim "We are approaching the fifth phase of bio warfare with a cyber-bio framing."[1] According to Bernard, this latest (fifth) generation of biological weapons, actually represents a synergy of two different detrimental impacts: spreading misinformation combined with public health damage (naturally or intentionally caused human diseases). This creates numerous consequences in terms of undermining social and political stability, compromising state institutions, as well as delegitimizing science and its contribution to controlling the health crisis (Bernard et al., 2021, p. 3-4). Thus, we actually have a combined cyber-bio attack, as a synergy of the harmful effects of information with the action of biological agents. In this context, we can say that the future activities of the intelligence community towards this type of threat are further complicated by the fact that in cyberspace may intertwine the influences and interests not only from opposing (or competing) states, but also other relevant actors (movements, organizations, individuals or corporations). This requires

[1] This thesis is based on a historical overview of the development of the biological weapons (BW) given by Koblentz. According to him, the first generation of BW consists of original microorganisms (easily accessible and unprocessed); the second generation of BW is characterized by the production of small quantities of biological agents and their primitive dissemination, the third is characterized by the use of sophisticated methods of dissemination of previously processed biological agents, and the fourth generation is the result of aplying state-of-the-art biotechnological achievements in production and application. (Koblentz, 2009, p. 203-205)

special attention in the intelligence identification, analysis and qualification of information collected from the internet.

The post Covid-19 era and new security reality

Covid-19 shows us the extent to which states, their public health systems, as well as other segments of critical infrastructure were unprepared for a health crisis such as a pandemic. The same can be said for national security and intelligence communities around the world.

Massive deterioration of health, with numerous psycho-social and other consequences in societies, could have very motivating effects on certain security actors in terms of potential use of biological weapons. This would also point to a very realistic reaffirmation of biological terrorism or bio criminal acts.

When we consider possible use of biological weapons in the future, an interesting thesis was presented by Silke, who claims that "an added concern is that historically it has mainly been religiously-motivated or right-wing terrorist who have been most attracted to using biological weapons, and in the west these are currently the dominant terrorist movements". (Silke, 2020, p. 7) Hence, it is an understandable assumption that in the future, biological weapons can pose a real threat of endangerment by jihadists groups such as the Islamic State or various extreme right-wing organizations. (Silke, 2020, p. 7) In support of the reaffirmation of the use of biological weapons, the observation of Ong and Azman (2020, p. 18-20), who point to the proactive behaviour of right-wing organizations in an attempt to use SARS-CoV-2 during the pandemic, is indicative, while the Islamic State did not encourage its supporters to take these steps.[2]

When we talk about the harmful effects of a pandemic on societies, the economic consequences should not be neglected. Arguably, they will have certain reflections on national security. In that sense, Silke points to another negative aspect of Covid-19 on national security: "Looking ahead in the medium and long term, government

[2] Members of right-wing organizations in a primitive way "weaponized" SARS-CoV-2 by using the sputum of their sick members to contaminate public areas or by coughing and blowing in the face etc.

spending is likely to come under the fiercer stress than in the past decade and pressure on counterterrorism budgets going forward is likely to be more intense. Tied into this, the economic impact of the pandemic is almost certainly going to feed into destabilising parts of the world. Countries with less resources may face even greater crises."(Silke, 2020, p. 8)

The intelligence community in the post Covid-19 era

The future adjustment of the intelligence community in the post Covid-19 era encompasses several directions. First, it is necessary to develop and strengthen MEDINT intelligence resources within intelligence systems. The continuous education of existing staff, but also the introduction of new expert profiles in the intelligence and security structures themselves might be a special challenge. In that context, Kauffman pragmatically suggests: "It is far easier to teach a medical – or life-science expert about intelligence than it is to teach an intelligence officer about medicine or biology" (Kauffman, 2001, p. 23).

Second, the broad spectrum of numerous and diverse factors and entities that affect public health imposes the need to engage the intelligence community with representatives of different professional sectors and disciplines. Accordingly, it is necessary to establish external connections of intelligence structures with entities from different expert sectors and disciplines (epidemiology, ecology, molecular biology, medicine, veterinary medicine etc.), as well as with relevant representatives of the academic community. The importance of such multidisciplinary connection is also pointed out by Bowsher who notes "It is also apparent that the possession of highly capable intelligence services does not currently translate into highly effective health intelligence practice and that this domain requires specific multidisciplinary consideration for further development as a state capability." (Bowsher et al., 2021, p. 437)

Third, security and intelligence monitoring of sensitive research in the field of biotechnology and molecular biology (dual-use) should not be neglected. Their reach, dynamic development, but also increasing availability will increase the risks of bio accident threats, as well as bioterrorism or bio criminal acts.

Fourth, full promotion of international cooperation at the regional and wider international level is necessary. Biological threats usually do not recognize national borders. This is especially evident in the case of a pandemic. International cooperation in the MEDINT domain can be achieved on operational and tactical level (information exchange, education etc.)

Conclusions

The pandemic as a health phenomenon in its genesis, spread, consequences, and in our reactions to it, certainly goes far beyond national frameworks. Non-functional international cooperation manifested through the absence of health solidarity, and non-recognition of common interest in the field of biosecurity are also important lessons of Covid-19. Cooperation between international entities is unavoidable in order to prevent and recognize pandemics and similar health threats in a timely manner. In that sense, one should be aware of the existence of certain cyclical patterns in the behaviour of infectious diseases with epidemic/pandemic potential (SARS, MERS, SARS-2, Ebola etc.). It should be considered as a warning and indication of mostly possible bio-risk of new natural epidemics or pandemic outbreaks.

Whether we talk about pandemics as naturally generated processes or pandemics as a consequence of aimed and malicious actions carried through biological weapons, the intelligence community will have to develop and adapt to the new security reality. In this way, MEDINT has also gained in importance. A special segment of international cooperation concerning endangering the health of the population is the potential risk of bioterrorism and other abuses of biological agents. The post-Covid era will certainly require the establishment of a better and more efficient system to counter bioterrorism through existing and new models of international cooperation. The Council of Europe Committee on Counterterrorism (CDCT) reacted in the midst of the pandemic, pointing out the weaknesses of modern societies towards the pandemic, warning that the global spread of the SARS-CoV-2 virus could increase the risks of possible use of biological weapons by terrorists.

Furthermore, this EU body notes that it is necessary for all 47 member states to commit to training and preparations for a potential terrorist attack with biological weapons (Council of Europe, 2020). Finally, medical intelligence should not be the privilege of the most developed national intelligence services, but a necessity of every modern intelligence system in the world. Covid-19 has undoubtedly become the ultimate security issue for the whole world. In a rather traumatic way, we realized that endangering the public health can be far more than a medical issue. If there was ever any doubt regarding the justification of the existence of MEDINT incorporated within security intelligence systems, it now belongs to the past.

References:

1. Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. Zeitschrift fur Gesundheitswissenschaften (Journal of public health), 26(5), 509–514. https://doi.org/10.1007/s10389-018-0899-3

2. Bernard R, Bowsher G, Sullivan R, and Gibson-Fall F. (2021). Disinformation and Epidemics: Anticipating the Next Phase of Bio warfare. Health Security. February 2021, 3-12. http://doi.org/10.1089/hs.2020.0038

3. Bowsher, G.; Milner, C.; Sullivan, R. (2016). Medical intelligence, security and the global health. Journal of the Royal Society of Medicine, Vol. 109, Issue 7, Sage Publishing, UK, 2016, 269-273. DOI: 10.1177/ 0141076816656483

4. Bowsher, G., Bernard, R., & Sullivan, R. (2020). A Health Intelligence Framework for Pandemic Response: Lessons from the UK Experience of COVID-19. Health Security, 18(6). https://doi.org/10.1089/hs.2020.0108

5. Clemente D. Jonathan. (2016). Medical Intelligence. Guide to the Study of Intelligence. The Intelligencer-Journal of Intelligence Studies.

6. The Council of Europe continues working to enhance international co-operation against terrorism, including bioterrorism. Strasbourg. 25/05/2020 https://www.coe.int/en/web/counter-terrorism/-/covid-19-pandemic-the-secretariat-of-the-committee-on-counter-terrorism-warns-against-the-risk-of-bioterrorism

7. Ferretti, Luca et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, American Association for the Advancement Science, Washington, D.C., Vol. 368, Issue 6491.

8. Ghebreyesus, T. A. (2020). Speech presented at: Munich Security Conference; February 15, 2020. https://www.who.int/director-general/speeches/detail/munich-security-conference

9. Jarcho, Saul. (September/October 1991). Historical Perspectives of Medical Intelligence. Bulletin of the. N.Y. Acad. Med. Vol. 67, No 5, 501-506.

10. Kaufman, D. C. (2001). Medical Intelligence: A Theatre Engagement Tool. Strategy Research Project, Carlisle: United State Army War College, 2001.

11. Koblentz, G. (2009). Living Weapons: Biological Warfare and International Security. Cornell University Press. Retrieved May 9, 2021, from http://www.jstor.org/stable/10.7591/j.ctt7z9s0

12. Кокошков, Ненад, Ристановић, Елизабета (2019). Медицинско обавештајно деловање према истакнутим личностима. Национална безбедност, година 6, број 9/2019, стр. 79-96.

13. Кокошков, Н. Ристановић Е. (2020). Обавештајно-безбедносни рад и пандемија, Национална безбедност, година 7, број 11/2020.

14. Keeling, Matt J., Hollingsworth, Deirdre T., Read, Jonathan M. (2020). The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), J Epidemiol Community Health. 2020, 74, 861-866. https://doi.org/10.1101/2020.02.14.20023036

15. La Gioia, Vicenzo, Col ITAF. (November 5, 2015), Medical Intelligence in Biological Issues. Biosecurity & Biosafety: Future Trends and Solutions. Centro Intelligence Interforze.

16. Leitenberg, Milton. (December 2005). Assessing the Biological Weapons and Bioterrorism Threat. Monograph from the Strategic Studies Institute.

17. NATO. (May 2011). Allied Joint Medical Support Doctrine. (AJP-4.10(A), NSA (MED) 0562(2011)1

18. Office of the Chairman of the Joint Chiefs of Staff. (January 2021). DOD Dictionary of Military and Associated Terms. Washington DC: The Joint Staff.

19. Ong, Kyler, Nur Aziemah, Azman. (2020). Distinguishing between the Extreme Farright and Islamic State's (IS) Calls to Exploit COVID-19. Counter Terrorist Trends and Analyses 12, no. 3. 18-21. doi:10.2307/26915446

20. Silke, Andrew (2020), Pool Re and Cranfield University's professor of Terrorism, Risk & Resilience Commentary. Covid-19 and terrorism: assessing the short and long term impacts. https://www.poolre.co.uk/wp-content/uploads/2020/05/COVID-19-and-Terrorsim-report-V1.pdf

21. Walsh, Patrick F. (2018). Intelligence, Biosecurity and Bioterrorism, Palgrave Macmillan UK.

22. Walton, Calder. (April 2020). Spies Are Fighting a Shadow War against the Coronavirus, Foreign Policy, 3. https://foreignpolicy.com/2020/04/03/coronavirus-pandemic-intelligence-china-russia/

23. World Health Organization (WHO). (May 9, 2017). Contact tracing: What is contact tracing and why is it important? https://www.who.int/features/qa/contact-tracing/en/