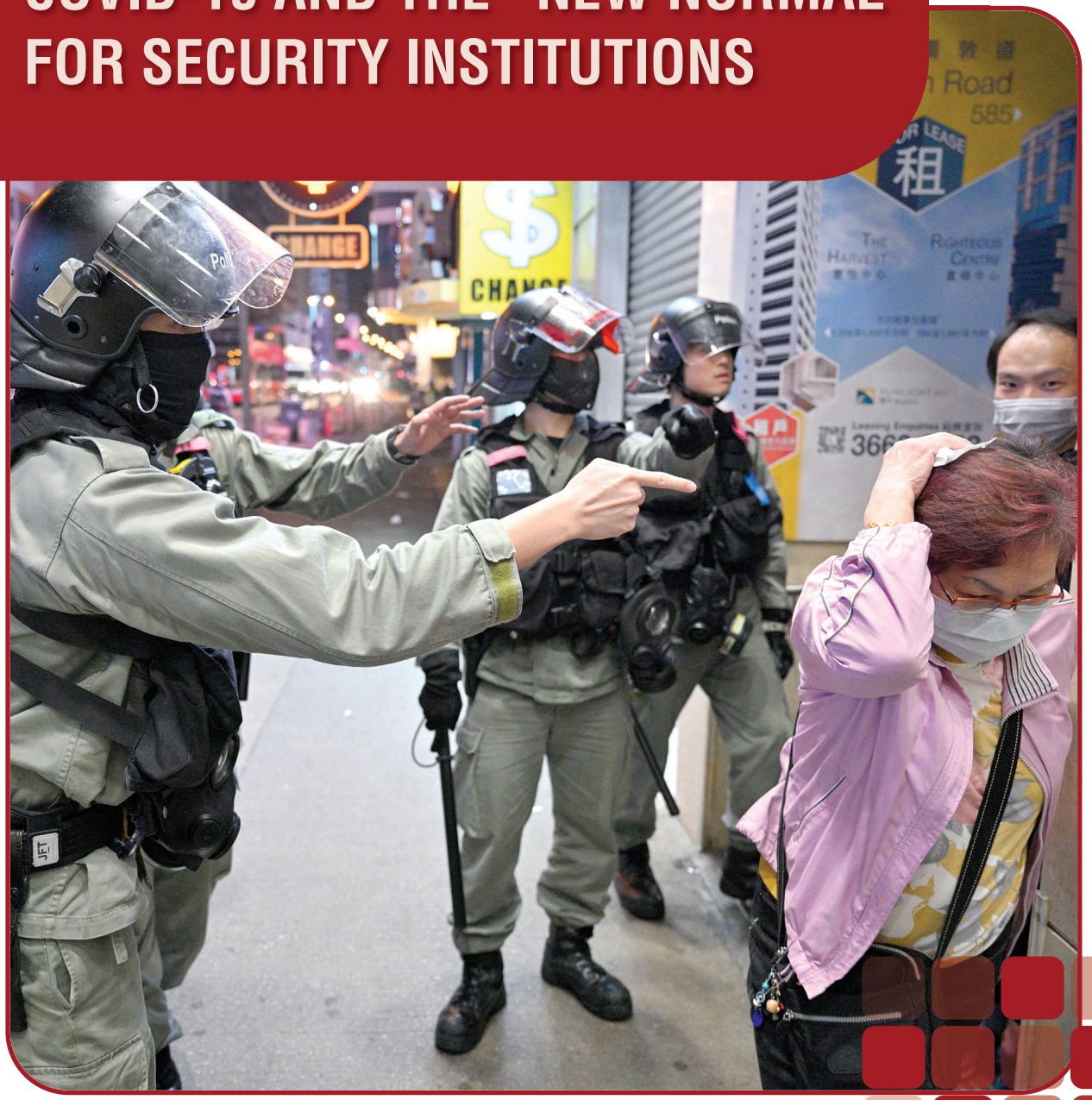
Ortadoğu Araştırmaları Merkezi
مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies
ORSAM

Analysis

No: 247 / May 2020

DIGITAL FIGHT AGAINST COVID-19 AND THE "NEW NORMAL" FOR SECURITY INSTITUTIONS



GÖKTUĞ SÖNMEZ & EMİNE ÇELİK

Copyright

ISBN: 978-605-06852-8-2

Center for Middle Eastern Studies

Adress : Mustafa Kemal Mah. 2128 Sk. No: 3 Çankaya, ANKARA
Phone : +90 850 888 15 20 Fax: +90 312 430 39 48
Email : info@orsam.org.tr
Photo : Shutterstock

Ortadoğu Araştırmaları Merkezi
ORSAM مركز دراسات الشرق الأوسط
Center for Middle Eastern Studies

ANALYSIS

DIGITAL FIGHT AGAINST COVID-19 AND THE "NEW NORMAL" FOR SECURITY INSTITUTIONS

About the Authors

Asst. Prof. Dr. Goktug Sonmez

Received his bachelor's degree in International Relations from Bilkent University, his master's degree in International Relations at London School of Economic (LSE), and his PhD from the School of Oriental and African Studies (SOAS), University of London. His research areas are International Relations Theory, Turkish Foreign Policy, and Radicalization and Violent Extremism. He conducted research on these areas at several think-tanks including the Center for Strategic Research of the Ministry of Foreign Affairs of the Republic of Turkey, Global Strategy Institute and the ORSAM. He currently works as the Director of Security Studies at ORSAM.

Emine Çelik

Emine Çelik, after getting her bachelor's degree from Anadolu University, completed his master's at Necmettin Erbakan University, Department of Political Science and Public Administration and continues her PhD at the same university. Her academic research areas include terrorism, cyber terrorism, and the link between radicalization and poverty.

May 2020

Table Of Contents

Introduction

Beyond its medical aspects, the Covid-19 pandemic provides a suitable atmosphere for significant changes in terms of the international security agenda, the future of the international system, relations between the hegemon and potential challengers, and cyber security. In addition to that, it has brought about some results such as some national and/or regional security mechanisms utilizing new instruments or tailoring the old ones to the current situation, and/or employing their current operational capacity to pandemic-related actions. The situation, which has emerged due to the growing area of interest of security for the first time in the last century, encompasses human health in a serious and global manner and will have ramifications. Considering the direct and indirect effects of the pandemic on the traditional subjects of Security Studies, it is likely that health-related and biological risks will take place in the agenda of, not only health-related national, regional and global actors, but also all national and international organizations, as a much more important and prioritized issue in the post-Covid-19 period. Therefore, as of its current progress, the Covid-19 pandemic constitutes the agenda of, not only the health institutions of states, but also the security institutions.

Lockdown measures have been adopted to different degrees all around the world as the Covid-19 outbreak was declared a pandemic and the number of infections and the death toll rapidly increased. This article mainly discusses the way that states transform their capabilities and diversify their instruments against current challenges.

Even though some prominent countries had predesigned measures and a general action plan against disease outbreaks, the struggle against the Covid-19 pandemic has been more difficult than expected. The reasons for this are the difficulty in the execution of such plans, problems about timing, and the unprecedentedly rapid spread of the Covid-19 disease, which has been more than the plans had foreseen. The concerns,

which are arising from the possibility that the outbreak would overcome the medical capabilities of countries, have aggravated the scale of the threats and take place on the agenda of many sectors as well as the health sector. Similar concerns about a possible increase in the health-related security risks that are likely to emerge unless the outbreak is stopped, have brought the Covid-19 pandemic as an item to the top of the agenda in the security domain and security institutions.

> In China, each individual was assigned a medical code, thanks to the Health Code system that is active in the platforms of Alipay and WeChat.

Different Methods and Instruments in the Digital Struggle: Examples from the World

As a response to the Covid-19 pandemic, countries seeking to control the outbreak have adopted various methods such as partial quarantines, lockdowns and social distancing. These measures aim to slow the spread of the disease. The foremost concerns about the pandemic are related to determining not only the infected people, but also their contacts both before and after the infection and their means of transportation, limiting their mobility after diagnosis, applying diagnosis and treatment to those with whom the infected have interacted, and the process after hospitalization. In this context, countries have started fighting against the pandemic in cyberspace through websites and/or various mobile applications. Mobile applications, however, have also brought about various security problems as well as raised fundamental questions related to freedoms. These concerns include the possible integration of the surveillance system that brings together various data from different databases used for following the infected in addition to the face recognition systems that seek to minimize the risks in this process. Applications vary because not all countries are equally capable of or willing to managing data and/or democratic dynamics of countries pose important challenges. China and Israel are among the countries which have devised effective initiatives. Similar measures have been implemented in South Korea, Canada and Britain or they are currently in the data collection phase -. The latest news from Singapore, Japan and Germany indicate that these countries also undertake similar processes with different dynamics and in different phases.

In China, each individual was assigned a medical code, thanks to the Health Code system that is active in the platforms of Alipay and WeChat.[1] This application was designed by the Chinese government and users need to provide information during their sign up about their ID numbers, places of residence, contacts with infected people and whether they carry the symptoms.[2] After the information is retrieved, users are assigned a color code that is either Green (Covid-19 negative), Yellow (Covid-19 potential carrier) and Red (Covid-19 positive). People with Green codes have freedom of mobility, while the Yellow and Red codes bring an obligatory quarantine of 7 and 14 days respectively.[3] The Alipay Health Code system in China, which is online in two hundred cities, shares information with local police forces about users' locations and movement. Also, the identity and route information of passengers in mass transportation is transferred to the same repository. As the face recognition and remote body temperature measuring systems are implemented in the existing

> The Israeli Ministry of Health has launched a mobile application called HaMagen (Shield) for the purpose of preventing the Covid-19 outbreak. HaMagen is available for download at Google Play and App Store, and was developed by Shin Bet, the domestic intelligence service of Israel.

systems, China will be able to upgrade its face recognition and person monitoring systems with an integral and the most solid feature up to now. In another respect, there is discussion about whether the digital monitoring of Chinese people constitutes a breach of human rights.[4] The fact that the China-based Alipay and WeChat digital platforms, that have 900 million-1.5 billion users, have become integral parts of the effort, underlines the importance of cooperation between the private sector and the state institutions.[5] China has acted on this opportunity in order to enact "uninterrupted intelligence and monitoring", overcoming concerns about personal liberties due to its regime and has achieved near perfection.

Many countries that are struggling against the pandemic have started to apply different versions of China's practices. The Israeli Ministry of Health has launched a mobile application called HaMagen (Shield) for the purpose of preventing the Covid-19 outbreak. HaMagen is available for download at Google Play and App Store, and was developed by Shin Bet, the domestic intelligence service of Israel. In this context, Prime Minister Netanyahu has expanded the area of operations and powers of Shin Bet.[6] The application seeks to develop the capability to be aware instantly if any user has been in contact with a Covid-positive case in the past fourteen days. Israeli officials claim that the ap-

plication aims to control the outbreak and personal data remains in users' phones. It is stated that the data is updated constantly by the Health Ministry and is unilaterally sent to users by the system, which is reliable due to its open-source codes.[7] This system has been expanding its platform, which was already being used for Hamas and Hezbollah attacks, and has utilized its database for keeping the data for some time. Netanyahu denied criticisms about data protection and personal liberties by stating that any delay under such circumstances might claim the lives of Israelis. Consequently, one and a half million Israeli citizens are registered to HaMagen and users are notified when diseased people are passing by. The Israeli Constitutional Court, however, recently ruled against such an expansion of HaMagen which can also be regarded as an extension of domestic power struggle.

A Europe-based project has been launched for a mobile application that would help people avoid the Covid-19 pandemic. The developers claim that the application named Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) will not be obligatory and users are free to download the application, which ensures the protection of personal data thanks to end-to-end encrypted algorithms. Chris Boos, the CEO of the Berlin-based artificial intelligence company, the digital policies advisor to Angela Merkel, and one of the founders of the project states that the project will not breach personal privacy and Europe has a long tradition of privacy.[8]

The project mentions the necessity to monitor the infected people in order to control the outbreak and to ensure that other people remain isolated by processing the coordinates of the infected people. As a non-profit entity, the PEPP-PT was developed to inform people about the risks of being exposed to the virus. The Bluetooth signals, as the main operating principle of the application, were designed to measure the distance between people and transmit the coordinates of infected people to others. In this context, the movement of infected people will be monitored and the speed of the outbreak will be slowed down.[9]

The National Center for Medical Intelligence in the USA, which is a defensive instrument against diseases and focusing primarily on the US troops abroad, has been giving one of the most critical tests since its establishment. NCMI has rapidly increased its capacity, from satellite imagery to human intelligence and the intercepting communication, in addition to the participation of additional leading names in the medical field.[10] Disease outbreaks near military bases of global powers, which have global military projection capability in different geographies and dissemination of such information or disinformation, pose possible challenges on these powers' global reach and power. In the context of the USA, this development is particularly important at a time when the country has been debating about its withdrawal from countries such as Afghanistan, Iraq, and Syria.

The mobile application launched in Toronto, Canada, collects interaction and location information from telephone companies, aims to identify the places where people are gathered and possible areas of spread of the disease. At first, inconsistent statements came from the Toronto administration about the application, which was finally confirmed by the Toronto governor, and health officials announced that a similar practice could begin in Ottawa. Although it is claimed that the data is anonymous and aims to put pressure on people not to come together, it is doubtful as to how realistic this function is, how much it serves the purpose and whether it is restricted by this purpose.

According to a statement, the project developed jointly by Oxford University and the NHS in the UK seeks to develop a counterpart to the Chinese application, which is deemed "more suitable for democracy", collects and deletes data with consent, and is expected to be implemented in a short time.[11] In its current state, the application will be very similar to tools such as coronavirus100m and coronamap.site, which are similar monitoring applications in South Korea, where the people who get the disease publish their data with their own consent. South Korea pursues a holistic method that combines mobile data, credit card information and facial recognition technology, similar to China, but in a more transparent way based on voluntary sharing of data.[12] Similarly, the Stopp Corona application that is based on voluntary use in Austria, is being used by more than 130 thousand users.[13] The telecommunications institute of HHI in Germany and the Robert Koch Institute, the public health agency, stated that they are working on an application based on consent.[14] Control-oriented systems have been implemented to ensure that people suffering from the disease comply with quarantine in Poland and Singapore. In addition to mobile data and phone tracking, Russia has started using face recognition systems in a similar way to China, in an integrated manner.[15] The application developed by Agree company in 2018 for rain and earthquake events in Japan is offered for free access in the context of COVID-19 and collects data from the users about personal and health status on a voluntary basis.[16]

The Health Ministry of Turkey launched the website koronaonlem.com in the context of the digital fight against Covid-19. This processes the data that the users share voluntarily, evaluates their risks to be infected with the disease, and advises those who are likely to have been infected to visit the nearest health institution as soon as possible. In addition, the people are also asked to provide information on the countries they visited in the last fourteen days, whether they have been in a medical facility, whether they have been in contact with people with respiratory diseases and whether they have any chronic illnesses. Furthermore, a mobile application called 'Hayat Eve Sığar' was developed and is available

for download on the Android and App Store platforms. The system works on a voluntary basis and enables users via Bluetooth signals to become aware of any positive cases nearby and to receive location data about people who passed there and were tested positive later. Users can also see the infection density near their location. At the same time, the application asks users their health status every day and sends a warning if their family members are infected or get in contact with positive cases. In mid-April, the Scientific and Technological Research Council of Turkey (TÜBITAK) launched a joint call within the scope of the EUREKA program to fund research in topics such as diagnosis and treatment, critical production in the COVID-19 process, development of education technologies and protection of risk groups, and safe use of public transports in addition to another call mainly focusing on the social sciences-related dimension of the pandemic and its aftermath.

Personal Data and Privacy Debates

The use of these instruments for monitoring and surveillance of the spread and prevention of the disease by different state institutions alongside intelligence agencies and private companies raises important questions due to the impact on privacy and the pressure it can exert on personal freedom of expression. These questions refer to issues such as the duration of time that these tools will be used, that the data will be kept, and the way that data is stored. In this context, the Human Rights Watch has presented eight conditions to states for the fight against the outbreak, in order to raise awareness of digital monitoring in cyberspace.

1. Surveillance measures adopted to address the pandemic must be lawful, necessary and proportionate. They must be provided for by law and must be justified by legitimate public health objectives, as determined by the appropriate public health authorities, and be proportionate to those needs. We cannot allow the COVID-19 pandemic to serve as an excuse for indiscriminate mass surveillance.

2. If governments expand monitoring and surveillance powers then such powers must be time-bound, and only continue for as long as necessary to address the current pandemic. We cannot allow the COVID-19 pandemic to serve as an excuse for indefinite surveillance.

3. States must ensure that increased collection, retention, and aggregation of personal data, including health data, is only used for the purposes of responding to the COVID-19 pandemic. Data collected, fed, and aggregated to respond to the pandemic must be limited in scope, time-bound in relation to the pandemic and must not be used for commercial or any other purposes. We cannot allow the COVID-19 pandemic to serve as an excuse to gut individuals' right to privacy.

4. Governments must make every effort to protect people's data, including ensuring sufficient security of any personal data collected and of any devices, applications, networks, or services involved in collection, transmission, processing, and storage. Any claims that data is anonymous must be based on evidence and supported with sufficient information regarding how it has been anonymized. We cannot allow attempts to respond to this pandemic to be used as justification for compromising people's digital safety.

5. Any use of digital surveillance technologies in responding to COVID-19, including big data and artificial intelligence systems, must address the risk that these tools will facilitate discrimination and other rights abuses against racial minorities, people living in poverty,

and other marginalized populations, whose needs and lived realities may be obscured or misrepresented in large datasets. We cannot allow the COVID-19 pandemic to further increase the gap in the enjoyment of human rights between different groups in society.

6. If governments enter into data sharing agreements with other public or private sector entities, they must be based on law, and the existence of these agreements and information necessary to assess their impact on privacy and human rights must be publicly disclosed – in writing, with sunset clauses, public oversight and other safeguards by default. Businesses involved in efforts by governments to tackle COVID-19 must undertake due diligence to ensure they respect human rights, and ensure any intervention is firewalled from other business and commercial interests. We cannot allow the COVID-19 pandemic to serve as an excuse for keeping people in the dark about what information their governments are gathering and sharing with third parties.
7. Increased surveillance efforts related to COVID-19 should not fall under the domain of security or intelligence agencies and must be subject to effective oversight by appropriate independent bodies.
8. COVID-19 related responses that include data collection efforts should include means for free, active, and meaningful participation of relevant stakeholders, in particular experts in the public health sector and the most marginalized population groups.[17]

The eight points of digital monitoring conditions mentioned above have been signed by 106 institutions including national and international trade unions of several sectors, think-tanks, social groups, student associations and private companies.

There is no doubt that this situation, which is discussed more in the field of security in the context of the pandemic, will deepen the security-freedom dilemma, which is a fundamental

problem both during and after the outbreak. However, a period is approaching that, among many actors that have developed smart chip and facial recognition systems, the countries that have achieved a certain level of progress about these can both gain more acceptance and increase their access by testing their capacities.

> Over time, controlling equipment and technology transfer has become one of the key battlegrounds for intelligence services as well as criminal organizations.

Competition for Medical Equipment and Technology in the Context of COVID-19

In addition to the digital dimension mentioned above, medical equipment is rapidly gaining importance as commodities with strategic importance, which security institutions seek to access before other actors. One of the first points of tension about the disease related to espionage is that the US, based on its intelligence sources, claimed that China has hidden the severity and outbreak speed of the virus from the world for a long time. The same assertion was made by the British secret service MI6 during the briefing it gave to British ministers that information about coronavirus cases and deaths in China was numerically and deliberately incomplete in January and February.[18] Over time, controlling equipment and technology transfer has become one of the key battlegrounds for intelligence services as well as criminal organizations. On the one hand, countries impose restrictions on the export of medical devices and equipment, on the other hand, some actors make significant investments for the post-pandemic world and foreign policy via aid to various countries, and on the other hand, some actors are engaged in a race to transfer equipment. This situation creates a new arena where both intelligence agencies and operational security forces, which have different

features and coordination mechanisms in each country, need to increase their capacities. The actors of this new sphere and such steps that they take against the pandemic bear certain similarities with some previous "races" such as the arms race or technology theft. Considering not only the prestige and financial gain of the actor, who develops a solution for the disease, but also the potential to increase its political influence in the post-Covid-19 world, security agencies of countries would need to be able to procure the necessary equipment to have the situation under control, then monitor the progress of others, and copy and/or steal them. It is already possible to see news about the technology theft dimension of the issue and it seems that the number of such news items will increase in the near future, let alone the efforts that will go untold. Considering that many of the technology thefts known in history were revealed after years and generally after the transfer and/or neutralization of the technology had been completed and many of them were not more than an exchange of mutual accusations, this is a likely that such efforts will be brought up in the decades after the pandemic unless an important intelligence leak makes a substantial change in that respect.

Several media outlets put forward claims that the Israeli Defense Forces and MOSSAD acquired COVID-19 tests from the countries that Israel does not have diplomatic relations with and hundreds of medical masks from several different sources.

In the context of "equipment operations", two important cases appear to have been implemented by the USA and Israel. Several media outlets put forward claims that the Israeli Defense Forces and MOSSAD acquired COVID-19 tests[19] from the countries that Israel does not have diplomatic relations with and hundreds of medical masks from several different sources. This happened while Israel had only two thousand respirators at the beginning of the pandemic. These claims have been confirmed by the Israeli participants of the TV show 'Fact' of Channel 12, whose names were not disclosed. Despite low numbers, it is claimed that 1.5 million surgical masks and tens of thousands of N95 masks were brought to the country and, additionally, technology "transfers" were carried out, particularly on testing, mask manufacturing and respirator production for the diagnosis and treatment of the disease, which confirms the above-mentioned possibility.[20] 680 thousand masks sent to Italy from China were stolen and sent to Czechia where they were followed. Despite the fact that Czechia has sent the masks to Italy, it seems possible that the mistrust between countries will escalate with similar events. Organizations that steal the masks from their production sites and/or people who sell stolen masks at excessive prices are caught in operations that are performed very frequently in the European countries and the USA.[21]

In an incident described as "modern piracy" by the German Ministry of the Interior, it was claimed that 200 thousand masks were seized by the US while being brought to Germany. The American manufacturing company, 3M, denied the existence of such an order, while it was claimed that the shipment was seized at the Bangkok Airport, after having been sent to Germany from China via Thailand.[22] Moreover, Germany claimed that 6 million masks with FFP2 features that it should have been received

in mid-February had been lost in Kenya, and no definitive explanation has been made for their fate.[23] Germany, on the other hand, restricted the sale of masks to neighbors Switzerland and Austria, preventing these countries from obtaining their ordered masks, and consequently, tensions rose between Switzerland, Austria and Germany. The two countries accused Germany of behaving in contrast with unity in Europe.

Shortly before that, France made a similar accusation, claimed that the masks that it was supposed to receive went to the USA, and the USA denied the allegations through diplomatic channels. However, restrictions on the export of medical equipment by 3M, which has two-thirds of its N95 mask production capacity outside the USA, may lead to the assessment that such processes for orders received before the restriction are highly likely.[24] Other accusatory statements from France and Spain indicate that the US companies indirectly prevented the supply of masks.[25] The US companies overtook other countries with both their demand size and price offers of up to three times the amount of other offers. In this context, 250 thousand masks granted by the UN[26] to New York are likely to be one of the important items of the debate that will begin after the pandemic. It is likely that trans-border organized crime, both between states and across borders, will increase its illegal activities for obtaining masks, respirators and medical technology from states and from each other, due to statements by the WHO that the illness can maintain its lethality until 2021 or even 2022. This situation has made security with respect to anti-Covid-19 tools very critical, especially in equipment and technology production and transfer-wise. It is possible that similar operational moves will be observed in the next two years, especially on N95 masks, respirators, and scientific advances in the treatment of the disease, rather than materials that are relatively easier and can be produced by more countries, such as surgical masks.

> "It is claimed that the CIA and the NCMI (The National Medical Intelligence Service of the US) prepared a report by analyzing satellite images and computer frequencies related to an epidemic that occurred in China in November."

The Moves by Intelligence Services with respect to COVID-19

Intelligence agencies further played important roles to prevent the spread of the outbreak before and during the COVID-19 outbreak. After the emergence of the disease, the activities, modus operandi and capacities of the intelligence services have been revisited. The capability of intelligence services in countries where the disease has spread to collect data and warn governments against threats plays an important role in countries' struggle with the pandemic.

It is claimed that the CIA and the NCMI (The National Medical Intelligence Service of the US) prepared a report by analyzing satellite images and computer frequencies related to an epidemic that occurred in China in November. The claims also point out that the White House was informed until the beginning of January through briefings and various analyses.[27] Until January and February, despite elaborate intelligence reports about the COVID-19 outbreak, the Trump administration did not take them seriously and praised China's fight against the dis-

ease towards the end of January.[28] Trump's underestimation of the disease and intelligence reports came to be mentioned as the worst and most dangerous policy failure in the history of the United States as the disease reached the US and claimed the lives of thousands.

In the United Kingdom, the capacities of intelligence agencies for conveying information and collecting data was regarded as insufficient as they failed in informing the government beforehand and this led to discussions about the budget allocated to MI5 and MI6 that is over 3 billion Pounds. The absence of specialists in the ranks of MI5 and MI6 that can work under the conditions of pandemics, and the lack of intelligence information that would hasten the decision making of the government are evaluated as the liability of the British intelligence infrastructure.[29]

Iran has adopted strict measures and MoP Hassan Norouzi, stated that those who publish fake news will be sentenced to one to three years in prison leading to doubts and discussions pertaining to the undisclosed case numbers and death toll in Iran.

Following the rapid COVID-19 outbreak in Iran, the government handled the pandemic issue with a total political and security perspective, and the intelligence services IRGC and MOIS started to hide information about the cases. Intelligence units retain the authority to define what information healthcare professionals are allowed to disclose and have forbidden the disclosure of this information to the public, the media and the international community. Iran has adopted strict measures and MoP Hassan Norouzi, stated that those who publish fake news will be sentenced to one to three years in prison leading to doubts and discussions pertaining to the undisclosed case numbers and death toll in Iran.[30]

In the course of the epidemic, intelligence service activities are generally regarded as hiding information about the cases and mortality rates and the propaganda war that is carried out in the international system, especially on digital platforms. The oppression by China enabled it to hide the start date of the outbreak and keep away the statistics about the case and death toll, Spain attempted to relate the deaths in nursing homes with reasons other than the pandemic, Italy did not associate those who lost their lives outside the hospitals with the outbreak[31], and the USA did not register the deaths of homeless people who are vulnerable to the outbreak and did not receive aids where only New York and Florida had general aid campaigns.[32] The reason for hiding case and death numbers is that governments seek to minimize economic and commercial concerns and citizens' reactions as well as domestic and foreign policies of countries.

While the intelligence agencies and governments of many countries affected by the pandemic conceal information about the cases, propaganda activities are continuing about issues such as China having given incorrect information about the start date of the outbreak, having covered up cases, and the disease having spread to the entire world because China had not acted prudently. Trump's words labeling the virus as the 'Chinese Virus' since the beginning of the pandemic and Macron's accusation against China, that it has given incomplete information about the virus, can be evaluated in this respect.

Conclusion

The Covid-19 pandemic triggered the emergence of new debates in the world about the field of security as well as health systems. On the one hand, it is possible to evaluate new digital applications and websites that many countries launched and sought to expand as an important step to reduce the speed of the outbreak and ensure the isolation of the infected people. On the other hand, the digital aspect of the struggle raises questions about the human rights violations and data security problems that may emerge due to the monitoring of identity and mobility information of millions of people as well as artificial intelligence applications and facial recognition systems. The new phase of “digitalization” during the Covid-19 pandemic brings the risk of data theft by non-state armed actors, transborder criminal groups and other states, while at the same time constituting one of the most important questions with regard to the security-liberty dilemma due to the risk of increased rights violations.

Intelligence agencies and different security institutions of states carry out operations for maintaining security both with and outside their countries, and for supporting the fight against the outbreak especially for equipment and technology transfers. These operations are increasing in number and becoming more visible day by day. After the Covid-19 pandemic, it is highly likely that intelligence agencies will experience changes in their instruments and planning as well as the scope and method of their operational efforts. They will have a more active role on the ground in terms of collection and classification of data about the pandemic, equipment procurement and technology transfer. In addition to that, a new period is emerging in which state institutions, that work in the field of health and human security as well as information and communication companies, will come forward, new investment will be observed in these fields, and cooperation between actors will be promoted. Rather than for stopping the epidemic, processing and reporting of the data compiled by the intel-

ligence agencies and the transformation of these reports into state policies are related to a context that involves achieving superiority in certain areas. These areas are the technological capabilities of other states, the pharmaceutical industry capacity, and the level of development of health systems. Intelligence agencies will also closely monitor the process that will produce the vaccination or drug for the disease, and will likely have important roles in their countries' efforts related to vaccine development. Moreover, it is possible to foresee that both national, regional and global cooperation mechanisms will prioritize the topic of health, question unsuccessful cases among existing structures, form new international organizations focused on health or add new tools to existing ones.

At the national level, institutions and ministries working on human security or more specifically on health will gain importance and new professional and specialized units for epidemics are likely to be formed under these. These institutions will continue to be main actors at the national level in both the struggle against the current disease and in similar cases of disease in the future. Private firms and universities are indispensable elements of this struggle particularly in the digital dimension. It is possible that software companies and related university departments will develop new ways to work together with state institutions for the purposes of designing the struggle, developing tools, and protecting the aggregate data from misuse by others. Therefore, these actors need to be equipped with the required capacity and resources. Potential failure in these areas is likely to bring about economically and socially isolated states that question their relations with each other, a process of questioning about alliance systems, bilateral relations and international organizations, an expanding room of maneuver for illegal groups and non-state actors as well as more human resources for radical movements. The struggle against this unexpected international security threat that caught the world by surprise must be carried out at both national, regional and global levels.

Endnotes

1 Helen Davidson, "China's Coronavirus health code apps raise concers over privacy", The Guardian,1/4/2020.

2 Maya Wang , "China: Fighting COVID-19 with automated tyranny", HRW, 1/4/2020.

3 China launches Coronavirus 'close contact detector'", BBC, 11/2/2020.

4 Wang, a.g.e.

5 Paul Mozur, Raymond Zhong ve Aaron Krolik, "In Coronavirus fight, China gives citizens a color code, with red flags", The New York Times, 1/3/2020.

6 Tova Cohen, "1.5 million Israelis using voluntary coronavirus monitoring app", Reuters, 1/4/2020; Judah Ari Gross, "Netanyahu sparks privacy scare with move to track corona patients' phones", The Times of Israel, 15/3/2020.

7 Stuart Winer, "Health Minister Launches Phone App to Help Prevent Spread of Coronavirus", The Times of Israel, 23/3/2020.

8 Janosch Delcker and Stephen Brown, "Europe shares code for new Coronavirus warning app",Politico, 1/4/2020.

9 Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, 2020.

10 Ken Dilanian, "spying on coronavirus: a little-known U.S. intel outfit has its most important mission yet", NBC News, 13/3/2020.

11 Jennifer Valentino-DeVries, "Translating a surveillance tool into a virus tracker for democracies", The New York Times, 19/3/2020.

12 Mark Zastrow, "South Korea is reporting intimate details of COVID-19 cases: has it helped?", Nature, 18/3/2020; Amanda Shendruk, "South Koreans are using smartphone apps to avoid the novel coronavirus, Quartz, 29/2/2020.

13 "Covid-19: Thousands download coronavirus tracking app in Austria", The Star, 2/4/2020.

14 "World risks permanent surveillance with coronavirus controls", DW, 2/4/2020.

15 Steven Feldstein, "Beware the ımplications of coronavirus surveillance", Carnegie Endowment, 31/3/2020.

16 "Free Japanese-language medical app offers advice about coronavirus", The Japanese Times, 23/2/2020. Bhaswati Guha Majumder, "Free medical app with 120 doctors in Japan comes to rescue of users on Coronavirus scare ", IBT, 24/2/2020.

[17] Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights", Human Rights Watch, 2/4/2020.

[18] San Dabbagh, "UK spy agencies urge china rethink once covid-19 crisis is over", The Guardina, 14/4/2020.

[19] Toi Staff, "Mossad said to bring in 100.000 virus tests, but usefulness of kits doubted", The Times of Israel, 16/3/2020.

[20] "Coronavirus: Israel's spy agency Mossad admits to stealing face masks overseas amid global PPE shortage, The New Arab, 14/4/2020; Ben Caspit, "Mossad, Netanyahu's secret weapon against the coronavirus", 1/4/2020.

[21] Connor Perrett, "People are stealing masks and other sterile supplies from hospitals and research facilities amid a global shortage", Business Insider, 7/3/2020; Cindi Cook, "Coronavirus: 2K face masks stolen from French hospital", Anadolu Agency, 4/3/2020.

[22] "US firm denies German 'piracy' claims over vanished face masks", DW, 4/4/2020; "Berlin accuses US of 'piracy' over face masks", Politico, 4/3/2020.

[23] "Intelligence services, armies wage 'war' over masks amid COVID-19 outbreak", Daily Sabah, 27/3/2020.

[24] "US hijacking mask shipments in rush for coronavirus protection", The Guardian, 3/4/2020.

[25] "Coronavirus: US accused of 'piracy' over mask 'confiscation'", BBC, 4/4/2020.

[26] Israel Salas-Rodriguez, "UN donates 250K face masks to NYC health care workers", New York Post, 28/3/2020.

[27] Josh Margolin and James Gordon Meek, "Intelligence Report warned of coronavirus crisis as early as november: sources", ABC News, 9/4/2020.

[28] Caroline Kelly, "Washington Post: US Intelligence warned trump in january and february as he dismissed coronavirus threat", CNN, 21/3/2020.

[29] Matt Kennard, "British security services have ıgnored global health pandemics The UK's biggest threat" Daily Maverick, 24/3/2020.

[30] Majid Rafizadeh, "How Iran is cracking down on the truth on coronavirus", Arab News, 19/3/2020.

[31] Lucy Williamson, "Coronavirus: The Grim crisis in Europe's care homes", BBC, 31/3/ 2020.

[32] Laura Romero, "For American's Homeless Staying Home During Coronavirus Outbreak Is Not An Option", ABC News. 25/3/2020.

Bibliography

"Coronavirus: Israel's spy agency Mossad admits to stealing face masks overseas amid global PPE shortage, The New Arab, 14/4/2020.

"Coronavirus: US accused of 'piracy' over mask 'confiscation'", BBC, 4/4/2020.

"Covid-19: Thousands download coronavirus tracking app in Austria", The Star, 2/4/2020.

"Free Japanese-language medical app offers advice about coronavirus", The Japanese Times, 23/2/2020.

"US firm denies German 'piracy' claims over vanished face masks", DW, 4/4/2020; "Berlin accuses US of 'piracy' over face masks", Politico, 4/3/2020.

"US hijacking mask shipments in rush for coronavirus protection", The Guardian, 3/4/2020.

"World risks permanent surveillance with coronavirus controls", DW, 2/4/2020.

"China launches Coronavirus 'close contact detector'", BBC, 11/2/2020.

"Intelligence services, armies wage 'war' over masks amid COVID-19 outbreak", Daily Sabah, 27/3/2020.

"Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights", Human Rights Watch, 2/4/2020.

Amanda Shendruk, "South Koreans are using smartphone apps to avoid the novel coronavirus, Quartz, 29/2/2020.

Ben Caspit, "Mossad, Netanyahu's secret weapon against the coronavirus", 1/4/2020.

Bhaswati Guha Majumder, "Free medical app with 120 doctors in Japan comes to rescue of users on Coronavirus scare ", IBT, 24/2/2020.

Caroline Kelly, "Washington Post: US Intelligence warned trump in january and february as he dismissed coronavirus threat", CNN, 21/3/2020.

Cindi Cook, "Coronavirus: 2K face masks stolen from French hospital", Anadolu Agency, 4/3/2020.

Connor Perrett, "People are stealing masks and other sterile supplies from hospitals and research facilities amid a global shortage", Business Insider, 7/3/2020.

Helen Davidson, "China's Coronavirus health code apps raise concers over privacy", The Guardian,1/4/2020.

Israel Salas-Rodriguez, "UN donates 250K face masks to NYC health care workers", New York Post, 28/3/2020.

Janosch Delcker and Stephen Brown, "Europe shares code for new Coronavirus warning app",Politico, 1/4/2020.

Jennifer Valentino-DeVries, "Translating a surveillance tool into a virus tracker for democracies", The New York Times, 19/3/2020.

Josh Margolin and James Gordon Meek, "Intelligence Report warned of coronavirus crisis as early as november: sources", ABC News, 9/4/2020.

Judah Ari Gross, "Netanyahu sparks privacy scare with move to track corona patients' phones", The Times of Israel, 15/3/2020.n

Ken Dilanian, "spying on coronavirus: a little-known U.S. intel outfit has its most important mission yet", NBC News, 13/3/2020.

Laura Romero, "For American's Homeless Staying Home During Coronavirus Outbreak Is Not An Option", ABC News, 25 /03/2020.

Lucy Williamson, "Coronavirus: The Grim crisis in Europe's care homes", BBC, 31/3/ 2020.

Majid Rafizadeh, "How Iran is cracking down on the truth on coronavirus",Arab News, 19/3/2020.

Mark Zastrow, "South Korea is reporting intimate details of COVID-19 cases: has it helped?", Nature, 18/3/2020.

Matt Kennard, "British security services have ıgnored global health pandemics The UK's biggest threat" Daily Maverick, 24/3/2020.

Maya Wang ""China: Fighting COVID-19 with automated tyranny, HRW, 1/4/2020.

Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, 2020.

Paul Mozur, Raymond Zhong ve Aaron Krolik, "In Coronavirus fight, China gives citizens a color code, with red flags", The New York Times, 1/3/2020.

San Dabbagh, "UK spy agencies urge china rethink once covid-19 crisis is over", The Guardina, 14/4/2020.

Steven Feldstein, "Beware the ımplications of coronavirus surveillance", Carnegie Endowment, 31/3/2020.

Stuart Winer, "Health Minister Launches Phone App to Help Prevent Spread of Coronavirus", The Times of Israel, 23/3/2020.

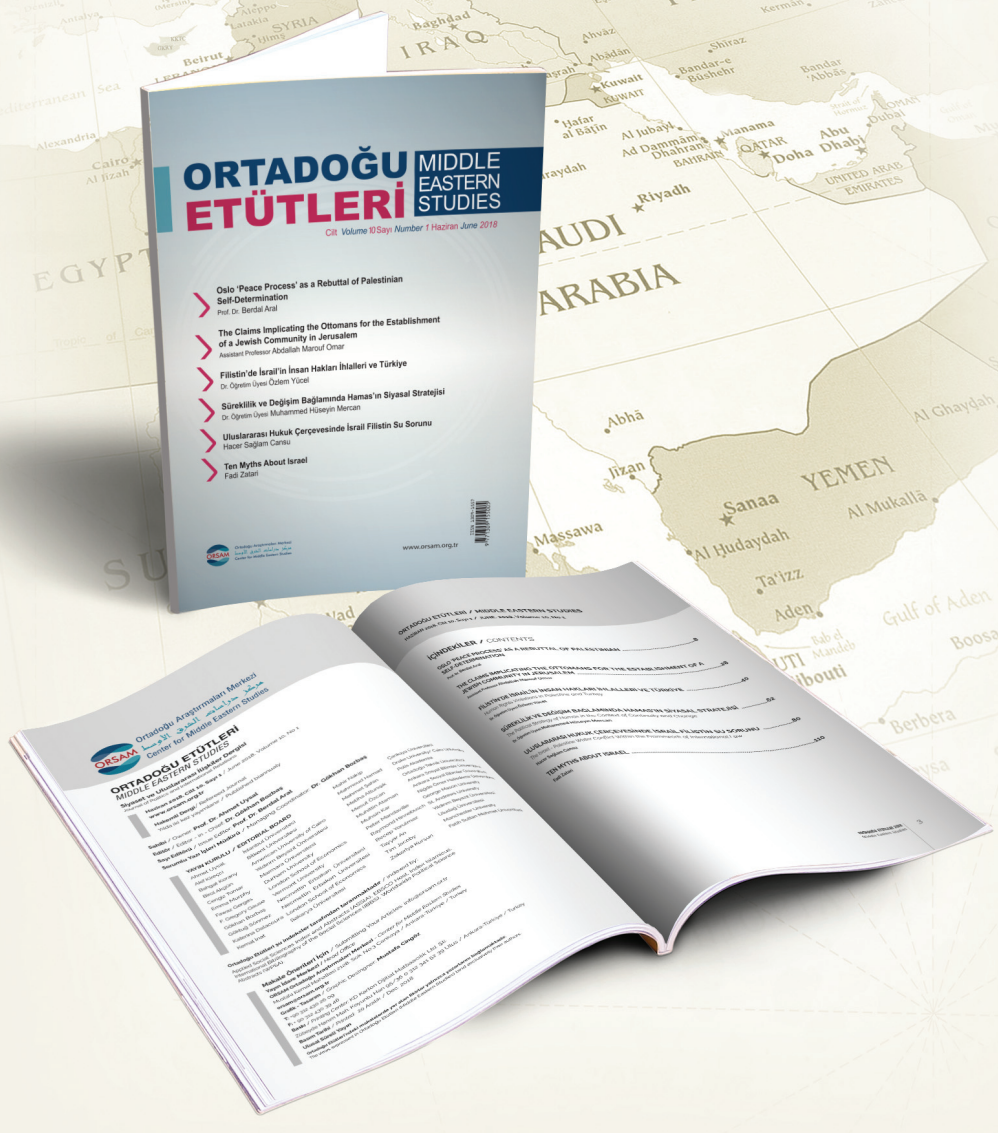
Toi Staff , "Mossad said to bring in 100.000 virus tests, but usefulness of kits doubted", The Times of Israel, 16/3/2020.

Tova Cohen, "1.5 million Israelis using voluntary coronavirus monitoring app", Reuters, 1/4/2020

Notlar

ORTADOĞU ETÜTLERİ

MIDDLE EASTERN STUDIES



Hakemli Siyaset ve Uluslararası İlişkiler Dergisi

ORSAM Yayınları

ORSAM, süreli yayınları kapsamında Ortadoğu Analiz ve Ortadoğu Etütleri dergilerini yayınlamaktadır. İki aylık periyotlarla Türkçe olarak yayınlanan Ortadoğu Analiz, Ortadoğu'daki güncel gelişmelere dair uzman görüşlerine yer vermektedir. Ortadoğu Etütleri, ORSAM'ın altı ayda bir yayınlanan uluslararası ilişkiler dergisidir. İngilizce ve Türkçe yayınlanan, hakemli ve akademik bir dergi olan Ortadoğu Etütleri, konularının uzmanı akademisyenlerin katkılarıyla oluşturulmaktadır. Alanında saygın, yerli ve yabancı akademisyenlerin makalelerinin yayımlandığı Ortadoğu Etütleri dergisi dünyanın başlıca sosyal bilimler indekslerinden Applied Sciences Index and Abstracts (ASSIA), EBSCO Host, Index Islamicus, International Bibliography of Social Sciences (IBBS), Worldwide Political Science Abstracts (WPSA) tarafından taranmaktadır.

Ortadoğu Araştırmaları Merkezi
ORSAM
مركز دراسات الشرق الأوسط

Mustafa Kemal Mah. 2128. Sok.
No:3 Çankaya/Ankara

+90 (850) 888 15 20
+90 (312) 430 39 48

info@orsam.org.tr
www.orsam.org.tr

orsamorgtr