BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The Internet in the Coronavirus Era

by Dr. George N. Tzogopoulos

BESA Center Perspectives Paper No. 1,511, March 30, 2020

EXECUTIVE SUMMARY: The coronavirus (COVID-19) pandemic is causing an online revolution—one that provides opportunities but also creates risks. Surveillance of infected and quarantined individuals through mobile applications is helping to slow the spread of the contagion, but contains an implicit threat to privacy. Cybersecurity is being tested as hackers look for ways to use the unprecedented situation to strike governments, companies and individuals.

The identification and isolation of individuals infected and quarantined with coronavirus (COVID-19), as well as people with whom they have been in contact, is considered a priority in the international fight against the pandemic. Government policies differ on methods of monitoring these citizens and the legal terms under which their data can be held and shared.

A *New York Times* article discusses online surveillance practices currently being applied in Australia, China, Italy, Mexico, Singapore, South Korea, and the US to trace the movements of coronavirus patients or send warning messages. In Israel, PM Benjamin Netanyahu announced that all means—both technological and digital—will be used to fight the spread of the virus.

Under normal circumstances, the use of online surveillance tools would spark an immediate and intense debate about privacy implications. The mission of the UN Global Pulse initiative is to ensure that big data, artificial intelligence, and emerging technologies are harnessed safely and responsibly for the public good.

But at the present moment, saving lives is deemed a more urgent concern. A March 2020 study conducted at the University of Oxford shows that several methods of direct online contact, including first-degree instantaneous contact tracing and the practice of informing users when they can move about safely

or when they should seek medical help and avoid vulnerable individuals, have the potential to stop the spread of the epidemic if used correctly by enough people.

A team of medical research and bioethics experts from the same institution is supporting several European governments in their effort to devise a coronavirus mobile app for instant contact tracing. In Israel, the Health Ministry has already launched a phone app to help prevent the spread of the virus.

Internet usage in the coronavirus era creates both opportunities and risks, and those risks extend beyond the potential for unaccountable and irresponsible use of data by governments or companies. According to Reuters, hackers attempted to break into the World Health Organization at the beginning of March. The US Department of Health and Human Services was also attacked, and the Canadian Centre for Cyber Security issued an alert on risks to national health organizations that are involved in the response to coronavirus.

Cyber and biological weapons can be combined with malicious intent with potentially disastrous results. In a reflection of this concern, cybersecurity is mentioned in the American National Biodefense Strategy. Erel Margalit, founder and chairman of Jerusalem Venture Partners, goes so far as to argue that though there is no proof that the current virus is the result of a cyberattack, it could be.

While the origins of coronavirus are still being debated and researched, a new study in *Nature* calls the scenario of a laboratory-based creation "improbable." But even if the virus is not a biological weapon, the matter of cybersecurity surrounding its outbreak is far from trivial. Cybercriminals seek ways to capitalize on crises, including pandemic scenarios like coronavirus. National security could be jeopardized as politicians, diplomats, and military officials are forced to substitute teleworking and virtual summits for face-to-face meetings. Well-equipped offices are going unused as users resort to remote access and connectivity via computers and smartphones. Measures have been taken in most countries to guarantee the safety of online communications, but efforts to intercept talks will certainly multiply. Carelessness and weaknesses in communication links are gifts for hackers.

Employees in both the public and private sectors will need to work from home for a long period. Unless their agencies, organizations, or companies have provided them with secure tools and applications, their data will be easy to steal. Israel's expertise at preventing this can be beneficial for other countries.

Dangers can be financial, such as credit card leaks and breaching of private bank accounts. Interpol has warned about financial fraud via phishing scams and fake calls about supposed medical cures, international donations, state aid, or tax breaks. And there is another danger: hackers can access private genetic information, either to blackmail companies or individuals to obtain money in exchange for non-publication of sensitive data or to sell the information to interested parties.

Coronavirus is not only affecting public health and the economy. It is also bringing other challenges to the forefront, such as how to handle the sudden "virtual" revolution. When the pandemic is over, world leaders will need to work together to improve digital literacy and international cyber governance. The question is whether the internet will be turned into a new frontier for cooperation or a competitive battleground.

Dr. George N. Tzogopoulos is a BESA Research Associate, Lecturer at the Democritus University of Thrace, and Visiting Lecturer at the European Institute of Nice.