BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Coronavirus, Security, and the Cyber-Order

by Dr. George N. Tzogopoulos

BESA Center Perspectives Paper No. 1,537, April 21, 2020

EXECUTIVE SUMMARY: The coronavirus crisis represents an opportunity to analyze the concept of security beyond military might. The pandemic, which resembles a form of biological warfare, is being accompanied by incessant cyberattacks, and most countries are showing themselves unable to tackle asymmetric threats effectively. International cooperation on internet governance will not be easy. In December 2019, the UN General Assembly adopted a Russian-backed resolution on fighting cybercrime. The debate on cyber governance will highlight differences between Western and non-Western countries and complicate the post-coronavirus order.

The coronavirus is injecting uncertainty into almost every dimension of life, and there is much international debate about the potential consequences of the pandemic on world affairs. In a *Wall Street Journal* commentary, Henry Kissinger asserts that "the world will never be the same after the coronavirus." NATO Secretary General Jens Stoltenberg considers a primary objective of the Alliance "to ensure that the health crisis does not become a security crisis." Media are reporting a rapid increase in incidence of the disease aboard military vessels, with the case of aircraft carrier USS Theodore Roosevelt getting particular attention. Military exercises, for example between Israel and the US, are being canceled, which is causing disruption.

The operational readiness of armed forces could be tested in the short and medium term. The IDF is faced with keeping its soldiers and personnel healthy, contributing to the medical needs of the state, and accomplishing its national security mission. The pandemic's impact on Israeli security could be a double-edged sword. On the one hand, there is a rise in opportunities for closer collaboration between Israel and the Palestinians. The UN has praised the coordination between them in reacting to coronavirus. But on the other hand, Israel's enemies will certainly seek to exploit the instability and strike.

This threat does not only apply to Israel. Terrorists might be inspired to launch biological attacks, and the civil wars in Syria and Libya could see new rounds of violence and areas of fragility.

While the sources of threat remain generally the same, the means of action are multiplying. IDF Chief of Staff Lt. Gen. Aviv Kochavi has warned that an attack, another round of violent confrontation, and even a large-scale operation can occur during this period.

While military might is the *sine qua non* for the notion of security, the coronavirus pandemic exposes the difficulty both Western and non-Western governments have in preventing and responding to asymmetric threats. President of France Emmanuel Macron is calling for a global ceasefire—but for the international community to chart a safe route, difficult compromises and a holistic approach are required.

A critical element is cybersecurity, which is a basic element of international security in the modern era and relevant to both biological warfare and the so-called genetic revolution. Cybersecurity continues to be a constant problem as the pandemic proceeds. According to Microsoft, every country in the world has seen at least one coronavirus-themed attack. Interpol has detected an increase of cyberattacks against hospitals. Israel National Cyber Directorate Chief Yigal Unna said recently that important aspects of the country's efforts to develop a vaccine for the coronavirus have been networked and could be vulnerable to cyberattack.

In 2017 Microsoft president Brad Smith talked about the need for a "Digital Geneva Convention," and the possibility of a cyberwarfare convention is being debated by scholars. To no one's surprise, international tensions on how to deal with cybersecurity have been high for years, and they reflect differences between Western and non-Western countries as well as between developed and emerging economies.

In December 2019, days before the outbreak of the coronavirus, the UN General Assembly adopted a Russian-sponsored resolution on fighting cybercrime. The document calls for establishing a committee of world experts to draft an international convention to fight the criminal use of information and communications technologies. The US remains skeptical due to the lack of consensus on drafting a new treaty and anticipates less openness and freedom in internet governance. It is concerned about the resolution because it sees that both Russia and China have successfully exploited international rules and norms to promote their own objectives.

The possible replacement of the Budapest Convention, set up in 2004 by the Council of Europe, is a distant but possible scenario. The first meeting of this intergovernmental committee of experts will take place this August.

With most people stuck at home during the pandemic, internet usage is up around the globe. As the post-coronavirus order will be significantly shaped in cyberspace, geopolitical antagonisms are expected to rise. The US will certainly continue to push its partners away from Huawei and possibly catch up with 5G technology. But with its ever-growing market of more than 850 million internet users (the biggest in the world), China will rely on multilateralism and occasionally on partnerships with Russia. Washington needs to either alter the balance of the UN General Assembly or build ad hoc alliances beyond the Russian framework adopted last December. A new digital fragmentation will only add to existing security challenges.

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