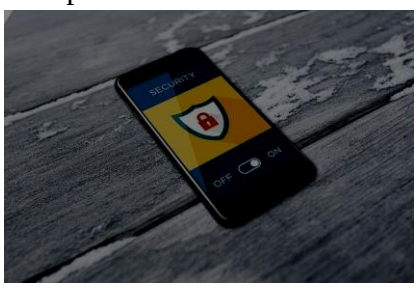
Coronavirus, seguridad y el ciberorden

Por Dr. George N. Tzogopoulos

Comparte esta noticia.Jeannet.



La crisis del coronavirus representa una oportunidad para analizar el concepto de seguridad más allá del poderío militar. La pandemia, que se asemeja a una forma de guerra biológica, está siendo acompañada por ataques cibernéticos incesantes, y la mayoría de los países se muestran incapaces de enfrentar las amenazas asimétricas de manera efectiva. La cooperación internacional en la gobernanza de internet no será fácil. En diciembre de 2019 la Asamblea General de la ONU adoptó una resolución respaldada por Rusia sobre la lucha contra el cibercrimen. El debate sobre la gobernanza cibernética resaltará las diferencias entre países occidentales y no occidentales y complicará el orden posterior al coronavirus.

El coronavirus está inyectando incertidumbre en casi todas las dimensiones de la vida, y hay mucho debate internacional sobre las posibles consecuencias de la pandemia en los asuntos mundiales. En un comentario de The Wall Street Journal, Henry Kissinger afirma que "el mundo nunca será el mismo después del coronavirus". El secretario general de la OTAN, Jens Stoltenberg, considera que el objetivo principal de la alianza "es garantizar que la crisis de salud no se convierta en una crisis de seguridad". Los medios informan un rápido aumento en la incidencia de la enfermedad a bordo de buques militares, y el caso del portaaviones USS Theodore Roosevelt recibe atención particular. Los ejercicios militares, por ejemplo, entre Israel y EE. UU. se están cancelando, lo que está causando rupturas.

La preparación operativa de las fuerzas armadas podría ser probada a corto y mediano plazo. Las FDI se enfrentan a mantener saludables a sus soldados y personal, contribuir con las necesidades médicas del Estado y cumplir su misión de seguridad nacional. El impacto de la pandemia en la seguridad israelí podría ser un arma de doble filo. Por un lado, hay un aumento en las oportunidades para una colaboración más estrecha entre Israel y los palestinos. La ONU ha elogiado la coordinación entre ellos para reaccionar al coronavirus. Pero, por otro lado, los enemigos de Israel ciertamente tratarán de explotar la inestabilidad y atacar.

Esta amenaza no solo se aplica a Israel. Los terroristas podrían inspirarse para lanzar ataques biológicos, y las guerras civiles en Siria y Libia podrían ver nuevas rondas de violencia y áreas de fragilidad.

Si bien las fuentes de amenaza siguen siendo generalmente las mismas, los medios de acción se multiplican. El teniente general de las FDI, teniente general Aviv Kochavi, advirtió que durante este período puede ocurrir un ataque, otra ronda de confrontación violenta e incluso una operación a gran escala.

Si bien el poder militar es la condición *sine qua non* para la noción de seguridad, la pandemia de coronavirus expone la dificultad que tienen los gobiernos occidentales y no occidentales para prevenir y responder a las amenazas asimétricas. El presidente de Francia, Emmanuel Macron, está pidiendo un alto al fuego global, pero para que la comunidad internacional pueda trazar una ruta segura se requieren compromisos difíciles y un enfoque holístico.

Un elemento crítico es la ciberseguridad, que es un elemento básico de la seguridad internacional en la era moderna y relevante tanto para la guerra biológica como para la llamada revolución genética. La ciberseguridad sigue siendo un problema constante a medida que avanza la pandemia. Según Microsoft, todos los países del mundo han visto al menos un ataque relacionado con el coronavirus. Interpol ha detectado un aumento de los ataques cibernéticos contra hospitales. El jefe de la Dirección Nacional de Cibernética de Israel, Yigal Unna, dijo recientemente que aspectos importantes de los esfuerzos del país para desarrollar una vacuna contra el coronavirus se han conectado en red y podrían ser vulnerables al ataque cibernético.

En 2017 el presidente de Microsoft, Brad Smith, habló sobre la necesidad de una “Convención Digital de Ginebra”, y los académicos están debatiendo la posibilidad de una convención de guerra cibernética. Para sorpresa de nadie, las tensiones internacionales sobre cómo lidiar con la ciberseguridad han sido altas durante años y reflejan diferencias entre países occidentales y no occidentales, así como entre economías desarrolladas y emergentes.

En diciembre de 2019, días antes del brote del coronavirus, la Asamblea General de la ONU adoptó una resolución patrocinada por Rusia sobre la lucha contra el cibercrimen. El documento exige el establecimiento de un comité de expertos mundiales que redacte una convención internacional para combatir el uso criminal de las tecnologías de la información y las comunicaciones. Estados Unidos se muestra escéptico debido a la falta de consenso sobre la redacción de un nuevo tratado y anticipa una menor apertura y libertad en la gobernanza de internet. Le preocupa la resolución porque ve que tanto Rusia como China han explotado con éxito las reglas y normas internacionales para promover sus propios objetivos.

El posible reemplazo de la Convención de Budapest, establecida en 2004 por el Consejo de Europa, es un escenario distante pero posible. La primera reunión de este comité intergubernamental de expertos tendrá lugar este agosto.

Con la mayoría de las personas atrapadas en sus hogares durante la pandemia, el uso de internet ha aumentado en todo el mundo. Como el orden posterior al coronavirus tendrá una forma significativa en el ciberespacio, se espera que aumenten los antagonismos geopolíticos. Ciertamente, Estados Unidos seguirá alejando a sus socios de Huawei y posiblemente se pondrá al día con la tecnología 5G. Pero con su mercado cada vez mayor de más de 850 millones de usuarios de internet (el más grande del mundo), China dependerá del multilateralismo y, en ocasiones, de las alianzas con Rusia.

Washington necesita alterar el equilibrio de la Asamblea General de la ONU o construir alianzas *ad hoc*, más allá del marco ruso adoptado en diciembre pasado. Una nueva fragmentación digital solo se sumará a los desafíos de seguridad existentes.