Jean Périer*

A comienzos del siglo XXI, muchos políticos, científicos y militares adoptaron la idea de que la humanidad se estaba acercando a una nueva era, un mundo construido sobre la base de la superioridad militar de los EE. UU. Sin embargo, este nuevo orden mundial ignoraría con entusiasmo el principio de soberanía nacional que ha sido la piedra angular de la política internacional desde el siglo XVII. Estados Unidos construiría medios de guerra cada vez más sofisticados para probarlos de manera inmediata en varias regiones del mundo. Además, al introducir nuevas tecnologías y asegurar su dominio en el espacio de información, Washington tuvo la impresión de que su orden mundial se ha vuelto imbatible.

Y no es un secreto que este orden mundial ya no se está apoyado solo por las armas regulares, ya que el rápido desarrollo de Internet condujo a la aparición de un nuevo tipo de guerra: la guerra cibernética. Lo hemos visto todo: hackers misteriosos, unidades cibernéticas especiales, brechas de seguridad, ataques DDoS y el uso de redes sociales para la puesta en escena de "revoluciones de color" en todo el Medio Oriente y aquellos estados que se niegan a obedecer el dictado de Washington. Aún más, para socavar los objetos críticos de infraestructura en los llamados "estados revisionistas", Washington lanzaría ciberataques contra ellos.

Por lo tanto, la World Wide Web se ha convertido en una frontera para la confrontación entre las superpotencias globales. Internet, los sistemas de GPS y la física cuántica han sido reclutados por los gobiernos y se están preparando para la batalla en la próxima gran guerra.

De hecho, una operación lanzada por el Comando Cibernético de los Estados Unidos **interrumpió** el acceso de Rusia al segmento de Internet de los Estados Unidos el día de las elecciones parciales de 2018. El ataque se lanzó con el pretexto de que Rusia intentaría interferir en las

elecciones de los EE. UU., Sin embargo, no se han presentado pruebas para apoyar esta afirmación. A su vez, la investigación de Robert Mueller no rastrearía la participación de Rusia en la interferencia de las elecciones presidenciales de los EE. UU. en 2016. Se informó que este ataque cibernético que no era más que un acto de guerra ordenado personalmente por el presidente en funciones, Donald Trump.

No es de extrañar entonces que los juegos militares anuales de seguridad cibernética más grandes del mundo, llamados Locked Shields, se celebraran en Estonia a principios de abril. El ejercicio fue supervisado por la sede de la OTAN, con docenas de estados miembros de la OTAN que se unieron a los Estados Unidos en el esfuerzo conjunto de capacitación, incluido el Ministerio de Defensa de Estonia. Según varios expertos militares, Locked Shields no tiene nada que ver con disuadir a la hipotética agresión de Rusia, al contrario, es una daga cibernética venenosa dirigida a su corazón. Desde que se lanzó por primera vez en 2012, el número de participantes de Locked Shields ha aumentado constantemente. En 2016, 550 militares de 26 países participaron en los juegos militares, lanzando 1,700 ataques con el uso de 1,500 máquinas virtuales; en 2017, el número de militares participantes llegó a 800 personas de 25 países, el número de ataques alcanzó un máximo de 2.500 y el número de máquinas virtuales involucradas superó los 3.000; en 2018, el ejercicio reunió a un gran total de 1.000 militares de 30 países, lo que elevó el número de máquinas virtuales a 4.000.

Los Estados Unidos, como el país más avanzado en el campo de la seguridad cibernética y la tecnología de la información, cada año se vuelve más capaz de desencadenar un ataque cibernético sobre sus enemigos. Desde 2006, los Estados Unidos llevan a cabo juegos militares de Cyber Storm una vez cada dos años. Este ejercicio está diseñado para permitir que los equipos de piratas informáticos altamente capacitados saboteen las capacidades de energía, finanzas, transporte y TI de la mayoría de los jugadores internacionales en ambos lados del Atlántico. Desde 2016, el Departamento de Defensa ha estado realizando todo tipo de ejercicios cibernéticos, incluidos Hack the Pentagon, Hack the Army, Hack the Air Force, Hack the DTS y Hack the Marine Corps. Es curioso que Hack the Air Force 3.0 se llevó a cabo tan recientemente como en noviembre pasado.

Teniendo en cuenta la naturaleza cada vez más agresiva de las acciones de Washington en el ámbito internacional en los últimos años, su negligencia hacia el derecho internacional en su puesta en escena de los conflictos armados en diversas partes del mundo, su retirada completamente injustificada de varios tratados internacionales para frenar la proliferación de Armas y conflictos armados, la comunidad internacional ha seguido con creciente preocupación los pasos de Washington en el ciberespacio. Incluso hoy en día, para muchos países de todo el mundo, un posible ataque cibernético masivo que sería acompañado por declaraciones provocativas en los medios y protestas masivas provocadas por los especialistas en redes sociales ya no es una amenaza teórica. Por esta razón, muchos países han comenzado a

explorar la posibilidad de cortar su segmento nacional de la red desde la World Wide Web.

Se ha observado que hasta ahora, al menos nueve países han cortado sus conexiones nacionales de Internet para ejercer el control político en momentos críticos, entre ellos Egipto, Libia, Maldivas, Myanmar, Nepal, Sierra Leona y Siria, **según** el becario de La Fundación Nueva América, Justin Sherman. Esos estados cerrarán deliberadamente Internet para contener la protesta popular, mientras que Gabón y la República Democrática del Congo pueden mencionarse como los ejemplos más recientes.

En cuanto a China y Rusia, han estado trabajando duro preparándose para tal escenario por una razón. Quieren estar seguros de que, en caso de que haya una crisis o conflicto con los Estados Unidos, cuando Washington intente apagar su Internet, podrán mantener intacta su infraestructura de TI.

El éxito destacado es China. China hace mucho tiempo que descubrió cómo cortar el ataque localmente. Beijing no solo quiere mantener el control soberano de su web y su gente, sino que también debe poder sobrevivir a un embargo de Internet de los EE. UU., el equivalente a un embargo comercial.

A su vez, Moscú aprobó recientemente un proyecto de ley que le permitiría hacer exactamente lo mismo. Se ha revelado que Rusia está planeando cambiar la configuración de su Internet para que pueda ser completamente autónoma y autosuficiente "para garantizar la función estable a largo plazo de las redes de Internet en Rusia".

Sin embargo, el aspecto más fascinante de esos preparativos fue la reacción de Washington a los pasos antes mencionados que Moscú está tomando. ¡Con la ayuda de sus numerosos portavoces, los Estados Unidos y Gran Bretaña lanzaron un aluvión de acusaciones contra Rusia por sus supuestos intentos de "usurpar la democracia de la información" (sic)! Al mismo tiempo, nadie en el MSM se atrevería a mencionar el hecho de que se están haciendo los mismos **preparativos** en los Estados Unidos. De alguna manera, Washington, que ha comenzado todo este lío, no está usurpando la seguridad de la información a los ojos de los periodistas occidentales.

Y hay una explicación perfectamente lógica para todo esto, ya que Washington ha gastado una

gran cantidad de tiempo, dinero y esfuerzo para prepararse para librar guerras cibernéticas en otros estados, pero tras los pasos tomados por Rusia, China y otros estados, todas estas preparaciones son inútiles.

** investigador y analista independiente y un reconocido experto en Oriente Próximo y Medio Oriente*