Vladislav B. SOTIROVIĆ

La guerra futura "puede ver ataques a través de virus informáticos, gusanos, bombas lógicas y caballos de Troya en lugar de balas, bombas y misiles"

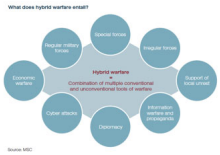
[Steven Metz, los conflictos armados en el 21st Century: La revolución de la información y de la guerra post-moderna, Carlisle, PA: Instituto de Estudios Estratégicos, 2000, xiii].

Las instalaciones de Internet en la política.

Internet o la WWW (World Wide Web) se extendió masivamente en todo el mundo desde fines de la década de 1980 o más precisamente desde 1989, en el mismo año en que se derrumbó el Muro de Berlín y, por lo tanto, permitió que la Guerra Fría 1.0 entrara en la etapa final. Es por eso que estos dos eventos históricos marcan el comienzo de la Era de Turbo-Globalización en todas las esferas, desde la economía hasta la cultura, incluida la política. [1] Con la creciente importancia de Internet, es bastante comprensible que se esté convirtiendo en un escenario de rivalidad política e ideológica con crecientes implicaciones sobre los problemas de seguridad nacional. [2]

La difusión de los medios de comunicación a través de Internet seguida de las comunicaciones en el marco del ciberespacio [3] permite que cada vez más personas, incluso en rincones remotos del mundo, estén informadas (o mal informadas) sobre los asuntos mundiales, las opiniones sobre ciertos eventos y participar en la política de maneras que hace unos 30 a 35 años habrían sido inimaginables. Hoy, incluso los campesinos pobres en muchas partes del mundo tienen acceso a Internet que proporciona información y brinda a los grupos gubernamentales y antigubernamentales una nueva forma de luchar por sus ideas, ideologías y

programas para adoctrinar a los públicos.



Internet ya se convirtió en el instrumento central de todos para facilitar el intercambio de diferentes puntos de vista, la difusión de información, noticias falsas o propaganda, el movimiento de dinero electrónico y, finalmente, la coordinación de actividades por la razón obvia, ya que es económico y de fácil acceso. Los blogueros con sus weblogs están influyendo en masas de personas en todo el mundo al transmitir información, desinformación y opinión en Internet. [4] Después del final de la Guerra Fría 1.0, comenzó una nueva Guerra Fría 2.0 en la que las Grandes Potencias comenzaron a adoptar armas inteligentes para combatir guerras convencionales, armas que utilizan nuevas tecnologías de información y comunicación como Internet o el ciberespacio. Surgió un nuevo tipo de guerra: la ciberguerra. [5]

Lo que concierne a la política, el impacto focal de Internet en él se puede resumir en cuatro puntos básicos:

1. La posibilidad técnica real de Internet de aumentar y mejorar la transparencia del Gobierno mediante el libre acceso a contenido en línea, documentos oficiales y todo tipo de informes y puntos de vista gubernamentales sobre diferentes temas y problemas.
2. La capacidad de Internet para aumentar el conjunto de información políticamente relevante tanto de naturaleza objetiva como falsa.
3. Su poder para organizar y acelerar la coordinación de diferentes grupos de interés, grupos extremistas y la llamada sociedad civil más allá de algo que antes se conocía como áreas y barreras políticas tradicionales.
4. La creación de nuevas formas de actividades delictivas conocidas como cibercrimen, ciberterrorismo o problemas de ciberseguridad.

Con respecto al primer punto de la posibilidad de aumentar la transparencia, los gobiernos, las

ONG y las diferentes instituciones de gobernanza global (como la OUN) han creado varios millones de páginas web con el fin de ofrecer información política como informes oficiales, puntos de vista, comentarios, foros de contacto o racionalizaciones de estrategias. Muchos gobiernos establecieron objetivos crecientes para la máxima proporción de su comunicación con los ciudadanos a través de Internet.

Sin embargo, si hablamos de flujos de información, Internet ofrece una plataforma segura y barata para muchos tipos de movimientos, partidos u organizaciones populistas que buscan adoctrinar y atraer a un posible público votante en las elecciones. [6] Uno de esos ejemplos muy exitosos, a título ilustrativo, fue el de los demócratas estadounidenses en la elección presidencial de Barack Obama en 2008.

La facilidad de Internet permite una mayor comunicación de las políticas de identidad como, por ejemplo, los testigos durante el referéndum británico para abandonar la UE: el Brexit. [7] Sin embargo, otra cosa que Internet ofrece en la práctica es la difusión de propaganda [8] por parte de personas u organizaciones extremistas para los propósitos más diferentes. El ISIS [9] y otros grupos islámicos fundamentalistas o radicales [10] es uno de estos ejemplos recientes más evidentes de mal uso de las instalaciones de Internet con fines políticos o ideológicos para las estrategias de reclutamiento.

Internet en general y las redes sociales en particular, además de proporcionar plataformas poderosas para una mayor difusión de las llamadas noticias falsas. Dichas noticias son una forma de medios no corroborados que se popularizan por muchas de las vistas en línea generadas, en lugar de las formas tradicionales de canales de verificación independientes. Con respecto a lo anterior, muchos expertos argumentarían que tanto la promoción de noticias falsas como el perfil de los espectadores específicos en Internet (particularmente en Twitter) participaron tremendamente en la elección de Donald Trump para presidente de los Estados Unidos en noviembre de 2016.

Una de las características de poder cruciales del ciberespacio es que plantea desafíos reales a los gobiernos, ya que Internet facilita la movilización y coordinación por parte de profesionales, luchadores por la libertad, insurgentes, delincuentes y terroristas de todo tipo. Un buen ejemplo del uso de Internet contra regímenes puede ser el caso de WikiLeaks en abril de 2010 cuando apareció en la red un video que mostraba un helicóptero estadounidense en Bagdad matando a una docena de iraquíes, incluidos dos periodistas.

Cibercrimen

El delito cibernético, en esencia, se refiere a los tipos tradicionales de delitos que acaban de migrar al ciberespacio (Internet), como el lavado de dinero o la explotación sexual. Sin embargo, el delito cibernético incluye actividades criminales específicas de Internet, como el acceso ilegal a información electrónica, comercio, secretos nacionales o políticos, y finalmente la creación y propagación de virus informáticos peligrosos que pueden provocar daños políticos o de seguridad nacional.

Los delitos cibernéticos cometidos por individuos o los ataques cibernéticos patrocinados por un estado, sin duda, representan serias amenazas para la comunidad internacional en general o una parte en particular por la misma razón por la que, en principio, están diseñados para degradar, negar o incluso destruir la información que reside en las computadoras o comprometer las computadoras mismas. Dichas actividades de ciberataques o ciber-terrorismo están comprometidas con la tarea final de causar disrupción, destrucción o pérdidas humanas.

El cibercrimen puede ser una amenaza principal para las personas, la industria y / o las organizaciones políticas. Pero en términos políticos, el delito cibernético puede cuestionar la función adecuada del estado y su sistema político si este último persistentemente no controla dicha actividad criminal o si sufre fallas en la seguridad cibernética.

Uno de los tipos muy específicos de cibercrimen es el ciberterrorismo. Básicamente se refiere al uso (incorrecto) de las instalaciones de Internet por parte de diferentes organizaciones para promover propaganda y actividades terroristas. Los grupos terroristas pueden usar Internet como un dominio para cometer ciberataques, por ejemplo, atacando redes o computadoras que pertenecen a las infraestructuras gubernamentales, públicas o militares. El programa cibernético más conocido hasta ahora utilizado en los delitos cibernéticos es el llamado caballo de Troya, un programa en el que un código está contenido dentro de un programa o datos para que pueda controlar una computadora y dañarla. Sin embargo, las puertas trampa de la computadora o las puertas traseras pueden presentar un peligro adicional.- agujeros deliberados en los programas informáticos que se utilizan para obtener acceso no autorizado a una computadora o una red informática por motivos de espionaje y / o destrucción del sistema informático. [11]

Sin embargo, Internet también puede (mal) usarse para perpetrar actos de terror que producen daños físicos o mentales, pero en casos extremos, los ciber-terroristas pueden incurrir en

responsabilidad penal individual en virtud del derecho penal internacional donde se entiende que su conducta apoya el crimen de guerra, agresión, crímenes de lesa humanidad o genocidio. En terminología de guerra, la guerra cibernética es el uso del sistema de información con el fin de explotar, interrumpir o destruir las redes informáticas militares o civiles de un enemigo con el objetivo final de interrumpir esos sistemas y las tareas que realizan. [12] La guerra cibernética es la guerra en el ciberespacio que ya es un nuevo quinto dominio militar después de la tierra, el mar, el aire y el espacio.

Las medidas legales contra el cibercrimen

Durante la última década más o menos, el cibercrimen de todo tipo se entiende cada vez más como ataques contra los estados y su infraestructura y, por lo tanto, están regulados principalmente por el marco legal internacional relacionado con el uso de la fuerza o, en el caso cometido en el momento de la guerra (conflicto armado), por el derecho internacional humanitario.

Todos los países, o grupos de países, que se consideran pertenecientes al bloque de las Grandes Potencias implementaron ciertas medidas legales y prácticas para contrarrestar el delito cibernético en su territorio. Uno de los mejores ejemplos exitosos hasta el momento es el Consejo de Europa, que adoptó la Convención sobre la delincuencia cibernética en 2001 y 2004, mediante la cual estableció una política penal común entre los Estados miembros al adoptar un marco legislativo apropiado y alentar la cooperación transnacional a nivel mundial y en la práctica, vencer al delito cibernético en todas las esferas, incluida la política. Si podemos hablar en términos legales más precisos, de acuerdo con el marco legal del Consejo Europeo sobre la lucha contra el delito cibernético, los Estados miembros deberían penalizar el acceso ilegal y, al mismo tiempo, la interferencia ilegal,[13]

La OUN tiene la clara decisión de que tales actividades cibernéticas están socavando el proceso de paz y la seguridad mundial o regional y, por lo tanto, la organización llamó a todos sus Estados miembros a prohibir la incitación a cometer terrorismo, tomar las medidas más activas posibles por el bien de evitar la incitación y negar refugio a personas o grupos de personas que son culpables de incitación. Sin embargo, está claro que cualquier tipo de medida de seguridad cibernética adoptada debe cumplir con la protección de las normas internacionales de derechos humanos como la libertad de expresión y asociación o el derecho a la privacidad.

De hecho, dentro del marco legal de los acuerdos internacionales destinados a la represión del terrorismo en general, y más particularmente en Internet, los estados están sujetos a muchas obligaciones legales internacionales que requieren su lucha contra el ciber-terrorismo dentro del espacio de Internet que es controlado por ellos. Es, por ejemplo, el caso del CSNU, que adoptó varias resoluciones por las cuales todos los Estados miembros de la ONU deben actuar contra actividades terroristas dentro de sus fronteras, incluido el ciber-terrorismo.

Notas:

[1] Michael Meyer, *El año que cambió el mundo: la historia no contada detrás de la caída del muro de Berlín* , Nueva York: Scribner, 2009; Brian McCullough, *Cómo sucedió Internet: de Netscape al iPhone* , Nueva York – Londres: Liveright Publishing Corporation, 2018.

[2] Ver más en [John Erikkson, Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?", *International Political Science Review* , 27/3, 2006, 221–224].

[3] El ciberespacio es "medio electrónico de redes de computadoras en el que se lleva a cabo la comunicación en línea" [Richard W. Mansbach, Kirsten L. Taylor, *Introducción a la Política Global* , Segunda Edición, Londres-Nueva York: Routledge Taylor & Francis Group, 2012, 575].

[4] Daniel W. Drezner, Henry Farrell, "Web of Influence", *Foreign Policy*, 145, 2004, 32-40.

[5] Sobre la guerra cibernética, ver más en [Richard A. Clarke, Robert Knake, *Guerra Cibernética* , Nueva York: HarperCollins, 2010]. Este libro ofrece una imagen de la guerra cibernética y sus capacidades que permiten enemigos potenciales.

[6] Véase, por ejemplo, [Pipa Norris, Ronald Inglehart, *Cultural Backlash: Trump, Brexit, and Authoritarian Populism* , Cambridge,

Reino Unido: Cambridge University Press, 2019].

[7] El brexit es un término abreviado por los británicos, que significa taquigrafía literaria para la salida británica de la Unión Europea. El Brexit se refiere a los debates en las conexiones directas con June 23 de rd , 2016 referéndum para el Reino Unido para salir de la UE. El referéndum Brexit se convirtió en un debate entre dos campos en el Reino Unido: los de los británicos que abandonan la UE frente a los de los británicos en la UE. Sobre el tema del Brexit, vea más en [Harold D. Clarke, Matthew Goodwin, Paul Whiteley,
Brexit: Por qué Gran Bretaña votó para abandonar la Unión Europea
, Cambridge, Reino Unido: Cambridge University Press, 2017].

[8] El término *propaganda* se originó históricamente en una oficina de la Iglesia Católica Romana en el Vaticano encargada de la propagación de la fe (católica romana)
de propaganda fide
. El término
propaganda
entró en uso común en la década de 1930 para describir en ese momento los regímenes autoritarios para lograr la subordinación total del conocimiento a la política del estado. Basado en la política de diferentes tipos de regímenes políticos autoritarios y totalitarios en Europa para desarrollar la legitimidad y el control social por parte de las instituciones gubernamentales centralizadas, la propaganda pronto se dirigió a las poblaciones de otros estados (generalmente los vecinos), provocando reacciones de los otros estados. Por lo tanto, por ejemplo, el Reino Unido estableció el Ministerio de Información. Dichos ministerios emplearon medios impresos, radio, cine, artes gráficas y la palabra oral para justificar la política oficial de sus gobiernos (la propaganda blanca) pero al mismo tiempo para vencer a la propaganda del enemigo (la propaganda negra). La propaganda fue bastante importante en las relaciones internacionales durante la Guerra Fría 1.0, especialmente a través de estaciones de radio como Radio Free Europe o Voice of America, que han estado propagando los valores oficiales de la democracia política liberal occidental y la economía de mercado. Hoy, la propaganda política occidental, ya sea a través de Internet u otros medios técnicos, se dirige principalmente contra Rusia y China en forma de (extrema) rusofobia y sinofobia. Ver más sobre propaganda en [Jason Stanley,
Cómo funciona la propaganda
, Princeton, Estados Unidos-Oxford, Reino Unido: Princeton University Press, 2015].

[9] El ISIS (Estado Islámico de Irak y Siria) es una organización terrorista internacional con sede en Irak y Siria. La organización es conocida como el Estado Islámico de Irak y el Levante (el EIIL) y como el Daesh (el Da'esh). Ver más en [Gus Martin, *Comprender el terrorismo: desafíos, perspectivas y problemas*
, Thousand Oaks, California: SAGE, 2017; William McCants,

The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State , New York: St. Martin's Press, 2015].

[10] El término fundamentalismo islámico o como sinónimo de islamismo se usa en Occidente (especialmente en los EE. UU. y el Reino Unido) para marcar cualquier movimiento u organización que favorezca el respeto estricto de la enseñanza tanto del Corán como de la Sharia, la ley islámica.

[11] Ver con más detalle en [Jonathan Kirshner (ed.), *Globalización y Seguridad Nacional* , Nueva York: Routledge, 2006].

[12] Richard W. Mansbach, Kirsten L. Taylor, *Introducción a la política global* , segunda edición, Londres-Nueva York: Routledge Taylor & Francis Group, 2012, 575.

[13] Ver más en [Robert W. Taylor, et al, *Cyber □□ Crime and Cyber □□ Terrorism*, Pearson, 2018].