Publicado en la página web del CEEEP
Fecha: 15 de octubre de 2021

Mundo futuro: La amenaza de los ciberataques en una sociedad hiperconectada

Mariano López de Miguel, es historiador con un máster en Historia Contemporánea por la Universidad de Cantabria, especialista en conflictos de Europa del Este (Ucrania, Balcanes y Antigua Yugoslavia), Cáucaso (Chechenia, Abjasia y Georgia) y Oriente Medio (principalmente en lo concerniente al conflicto Árabe-Israelí). Asimismo, es investigador doctoral en la Universidad de Murcia y miembro del Consejo Editorial del Blog Online "Conversación sobre la Historia". Actualmente, se encuentra cursando estudios de Doctorado en la Facultad de Filosofía y Letras de la Universidad de Murcia.

Resumen

Desde la introducción de la *World Wide Web* en los hogares a fines del año 1995, internet ha evolucionado de modo geométrico, llevando al mundo a un estado de hiperconectividad, denominado por futurólogos de renombre, como Herman Kahn o Marshall McLuhan como "La Aldea Global". Sin embargo, estas sociedades no están exentas de riesgo: Desde la llegada de las autovías de la información hasta los peligros basados en ciberataques han transformado la cultura social, política y de defensa en aras de cómo actuar ante estos embistes. A partir del año 2016, los ataques cibernéticos se han multiplicado por cientos, demostrando así la fragilidad del planeta ante un enemigo que no tiene –necesariamente- presencia física, y que adquiere ventaja debido a la oportunidad que le brinda el anonimato. Sin duda, el mundo está ante un nuevo campo de batalla dentro de las llamadas guerras irregulares o conflictos asimétricos.

Palabras claves

World Wide Web, Redes Sociales, Hiperconetividad, Ciberataques, Seguridad Nacional.

Introducción

El 4 de octubre de 2021, miles de millones de usuarios -a nivel mundial- estuvieron impedidos de acceder a sus principales redes sociales como Facebook, Instagram y WhatsApp (todas ellas dirigidas por el empresario billonario Mark Zuckerberg), durante -al menos- seis horas. Dichas aplicaciones se colapsaron cuando un fallo, sin identificar a la fecha (5 de octubre de 2021), hizo imposible establecer conexión con las mismas a través de *apps* y navegadores web. Este hecho, lejos de ser aislado –ya que es la cuarta caída masiva de dichas aplicaciones y programas de mensajería directa desde 2016- demuestra una realidad cada día más presente: La absoluta dependencia de las nuevas tecnologías de comunicación por un cada vez más amplio sector de la sociedad, en lo que Marshall MacLuhan denominó -cuatro décadas atrás- "La Aldea Global".

Análisis

Hace más de un cuarto de siglo, las nuevas tecnologías se abrieron paso a través de la "democratización" de la *World Wide Web* o, como comúnmente se le conoce, la internet. En 1990, el informático británico Tim Berners-Lee estableció la primera comunicación entre un cliente y un servidor utilizando el protocolo HTTP (Protocolo de Transferencia de Hipertexto), a lo que se le sumó la posibilidad de subir/cargar gráficos e imágenes, pasando de ser un proyecto casi exclusivo de los departamentos de defensa de países occidentales (principalmente la DARPA estadounidense) a ser una valiosa herramienta de uso mundial, permitiendo la apertura de internet a la sociedad civil y, principalmente, al comercio mundial.

Posteriormente, llegarían los foros de texto, los primeros buscadores como Yahoo! o el extinto AltaVista, además de otras posibilidades, que se vieron frenadas súbitamente tras la terrible explosión de la burbuja de las empresas "*.com*" a mediados de 2000[1]. Esta situación demostró que, si bien las nuevas tecnologías disponían de un amplio abanico de posibilidades, también acumulaban un índice de riesgo de 6/6 (siendo "1" el riesgo mínimo y "6" el máximo). Adicionalmente, la implementación de internet a nivel mundial no estuvo exenta de polémica. Países en vías de desarrollo, principalmente de la región MENA (Norte de África y Oriente Medio), se quejaron amargamente de la escasez de inversión para introducir servicios de acceso a la *World Wide Web* frente a países limítrofes como Israel donde, a octubre de 2000, cerca del 67% de la población contaba con acceso a la red.

No obstante, uno de los factores de auge de internet en esa época fue la creación del primer canal internacional de noticias en árabe (la cadena catarí Al Jazeera). Sus reportes fueron de los primeros en verse, tanto a través de televisión vía satélite como a través de vídeos de descarga directa, en una época previa al gigante audiovisual de YouTube. A lo que se debe añadir otro hecho que causó un terremoto geopolítico, como los terribles atentados del 11 de septiembre de 2000, que incrementó el desarrollo de internet dentro de una sinergia civil-militar.

Si bien la creación de leyes draconianas en aras de la seguridad nacional, como fue la tristemente célebre "Ley Patriótica" estadounidense, despertó el recelo entre los usuarios que buscaban proteger su seguridad, no sería hasta el lustro 2004-2009 cuando se dio el notable despegue de internet a nivel casi universal. La postguerra y ocupación militar estadounidense de la República de Irak daría pie a que la insurgencia en el país recurriera a la web para subir sus contenidos, los mismos que incluían desde ataques a tropas de la coalición hasta las tristemente célebres ejecuciones de rehenes llevadas a cabo por el grupo *Ansar Al Sunna* de Abu Musab Al Zarqawi.

El anonimato al subir dichos contenidos dio pie a que internet pasase a ser una herramienta de propaganda por integristas, desde Irak a Afganistán, u otros focos de la "*Yihad Global*" como eran los casos de Chechenia, Mindanao en Filipinas o Uzbekistán en Asia Central. La aparición de portales de vídeo como YouTube, Google Video o Vimeo, junto a servidores de correo alternativos y el inicio de las primeras redes sociales como Facebook o Twitter, permitirían subir contenidos de todo tipo que, si bien aquellos que mostraban altos índices de violencia eran rápidamente eliminados, su difusión había resultado masiva en unos pocos minutos. Durante esa misma época, el ex zar antiterrorista de Estados Unidos,

Richard A. Clarke, advirtió la necesidad de invertir, al menos, un 1.1% del PIB de cada país en fondos de ciberdefensa.

En abril de 2007, se daría el primer toque de atención en Estonia, a través de un ataque supuestamente realizado desde Rusia. Esta agresión mostró "*cuán fácil es para un país hostil aprovecharse de potenciales tensiones dentro de una sociedad para causar daño*"[2]. Las páginas web de bancos, medios de prensa y organismos gubernamentales colapsaron debido a niveles sin precedente de tráfico en internet. Redes de robots informáticos -conocidos como *botnets*- enviaron cantidades masivas de mensajes basura (*spam*) y pedidos automáticos *online* para saturar los servidores. El resultado fue que los estonios se quedaron sin poder usar cajeros automáticos y servicios financieros telemáticos.

Los atentados de 2007 se hicieron desde direcciones de IP rusas, las instrucciones *online* estaban en ruso y el gobierno federal ruso ignoró los pedidos de ayuda de Estonia. Sin embargo, nunca hubo evidencias concretas de que estos ataques los realizase el gobierno ruso. No sería la última vez que el gobierno de Moscú fuese acusado de ciberataques. Posteriormente, en el año 2009, durante el conflicto entre Rusia y Georgia por la región rebelde de Osetia del Sur, Moscú -supuestamente- volvió a realizar otra agresión, colapsando varias redes sociales en represalia contra un bloguero georgiano, conocido como "*CYXYMU*" (nombre en cirílico de Sujumi, capital de otra región rebelde como es la República de Abjasia)[3]. Los ataques fueron en respuesta a los textos en los que *CYXYMU* acusaba a Rusia de invadir militarmente Georgia para arrebatarle dichas regiones, independientes de facto desde 1991, tras la implosión soviética.

Asimismo, durante el año 2009, se demostró el poderío de las nuevas tecnologías y redes sociales o canales de *microblogging* tras las manifestaciones del "movimiento verde" en Irán, en protesta por la reelección fraudulenta de Mahmoud Ahmadinejad, junto al "nuevo músculo" de los disidentes en Egipto, tras casi 30 años de gobiernos autocráticos de Hosni Mubarak. De hecho, sería en Egipto donde los activistas digitales sufrirían su "primer mártir", en la figura del estudiante de programación informática Jaled Said, quien fue brutalmente torturado en la comisaría del barrio cairota de Sidi Gaber.

Resulta indudable afirmar que los blogs, las redes sociales y las aplicaciones de mensajería directa tuvieron una importancia puntal en los acontecimientos que darían pie a la fallida "Primavera Árabe". Países como Egipto, Túnez, Libia, Siria, Irak e Irán, a través de mandatos que negaban todas las garantías democráticas y de libertad de expresión, bloquearon cientos de sitios web de la oposición cívica y cerraron por completo el acceso a internet ("lockdown"), entre las que resaltan las disposiciones dadas por Hosni Mubarak, en enero y febrero de 2011, así como por Bashar Al Assad, entre abril de 2011 y mayo de 2012.

Tras la "Web 2.0", llegaría la normalización y masificación de uso de *apps* de todo tipo, a raíz de la segunda guerra civil iraquí (2014-2017) y de los ataques mundiales realizados por el mal llamado "Estado Islámico", grupo terrorista de filiación yihadista con una visión apocalíptica de la sociedad, y que controló gran parte del territorio sirio-iraquí junto a diversas provincias de estados-nación como Libia, Nigeria, Afganistán o Túnez. En ese sentido, el líder del grupo, Abu Bakr Al Baghdadi, demostró sus competencias tecnológicas heredades de su "padre ideológico", Abu Musab Al Zarqawi. Ante estos acontecimientos, los gobiernos occidentales se vieron ante una tesitura legal muy preocupante: legislar para

entorpecer ciertos accesos a contenidos web de carácter extremista (con el posible cercenamiento de libertades y derechos de los ciudadanos) o revisar uno a uno los contenidos clasificados como dañinos para la seguridad nacional, lo cual requeriría de una inversión millonaria en dispositivos de rastreo y seguimiento.

Por si no fuera poco, el fantasma de una posible inferencia rusa a través del ciberespacio durante las elecciones presidenciales estadounidenses de 2016, que darían la victoria al magnate populista Donald J. Trump, y los problemas durante el referéndum de abandono de la Unión Europea por parte de Reino Unido -conocido coloquialmente como "*Brexit*"- hicieron que no pocos analistas de seguridad y jefes del estado mayor de las respectivas naciones hablasen de la necesidad básica de dirigir más fondos a la ciberseguridad, amén de crear urgentemente departamentos dedicados única y exclusivamente a la vigilancia en la red.

Conclusiones

Los últimos ciberataques sufridos por Occidente desde 2013 (bien sean actos de represalia como los hackers norcoreanos que asaltaron la sede digital de *Sony Pictures* por ofensas de un filme hacia el Líder Supremo Kim Jong Un, o los realizados por la rama de inteligencia de la Fuerza *Quds* iraní tras el colapso del Complejo Nuclear de Natanz, a través del virus Stuxnet), junto a la caída de las principales redes sociales y servicios de mensajería directa durante varias horas del 4 de octubre de 2021, dejan claro cuan necesario es crear un entorno de cultura de ciberseguridad. Si bien es cierto que los CEO de dichas empresas adujeron la caída a un fallo humano generalizado en sus servidores, el hecho de que una portavoz de la Casa Blanca hablase durante las primeras horas de un posible ataque en la red o colapso DNS -mencionado también por la CNN- no hicieron sino levantar dudas y sospechas, así como costarles a los fundadores de estos oligopolios tecnológicos la friolera suma de 7.000 millones de dólares en pérdidas de la bolsa de tecnología (NASDAQ) de Nueva York.

Otro aspecto a resaltar es la dependencia total de la sociedad a servicios como WhatsApp, siendo curiosamente la herramienta de mensajería directa una alternativa laboral al supuestamente obsoleto correo electrónico. Todo ello, sin conocerse las numerosas brechas de seguridad existentes en esta aplicación. ¿Qué hacer en estos casos? La experiencia histórica enseña que la absoluta dependencia a una tecnología o fuente de energía pueden transformar a naciones desarrolladas en gigantes de pies de barro, como los casos de escasez de respiradores durante la pandemia de la COVID-19 o la doble crisis de 1973 y 1979 por la falta de petróleo.

Por consiguiente, educar a la población mundial en el uso razonable de las nuevas tecnologías, así como que los desarrolladores de dichas tecnologías basen sus principios en modelos sostenibles y que los países inviertan en ciberdefensa deberían ser las respuestas lógicas ante este nuevo desafío tras el colapso financiero de 2008-2013 y la emergencia sanitaria de 2020.

Notas Finales

[1] Matthew Lynn, "Las lecciones de la 'burbuja puntocom' veinte años después ," *El Economista* (22 de enero de 2020), https://www.eleconomista.es/opinion-blogs/noticias/10313700/01/20/Las-lecciones-de-la-burbuja-puntocom-veinte-anos-despues.html

[2] Damien McGuinness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país," *BBC News* (06 de mayo de 2017), https://www.bbc.com/mundo/noticias-39800133

[3] Reuters Staff, "Bloguero georgiano víctima de ciberataque dice no le silenciarán," *Reuters* (12 de agosto de 2009), https://www.reuters.com/article/internet-georgia-bloguero-idLTASIE57B2E520090812

Bibliografía recomendada

- Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (2010)
- Robert H. Latiff, *Future War: Preparing for the New Global Battlefield* (2017)
- Frederick Hodges y John R.Allen, *Future War and the Defence of Europe* (2020)