# Ciberguerra: ¿la amenaza menos contemplada?

**Carolina Zaccato**[11]

El Siglo XXI nos obliga a repensar conceptos, objetos y amenazas en materia de Defensa y Seguridad, así como también las herramientas y métodos con los que respondemos a estas nuevas amenazas.

Ante todo, es pertinente aclarar que este breve escrito no abrevará en lo que se conoce como la corriente de *securitización*, de la escuela Barry Buzan, Ole Waever, Japp de Wilde y Lene Hansen (1998; 2009), en la que nuevos temas y sujetos entran a la agenda de seguridad (obteniendo así novedosos conceptos como *seguridad alimentaria* o *seguridad medioambiental*). Por el contrario, este artículo se enfoca en la agenda de seguridad tradicional, esto es, aquella que tiene el foco puesto en la guerra y las amenazas militares "convencionales" (Walt, 1991), pero lo hace adoptando temáticas, objetivos y desafíos propios del nuevo milenio.

Dentro de esta agenda de seguridad convencional *aggiornada* (si se me permite la expresión), la ciberdefensa y la ciberseguridad deben tener un lugar central, puesto que la ciberguerra es uno de los medios de ataque más poderosos en nuestra época, así como también uno de los más subestimados. Puesto de otro modo, si bien el objetivo principal sigue siendo poner en jaque a un Estado enemigo, atacando el corazón mismo de su infraestructura crítica y sus reservorios de poder nacional, los métodos usados y los blancos de ataque cambian de manera radical al considerar el caso de la ciberguerra.

Un claro ejemplo para entender esta nueva dinámica es el caso del hackeo a las bases de la Convención Nacional del Partido Demócrata (DNC, por sus siglas en inglés) durante las elecciones presidenciales estadounidenses de 2016. Mediante el acceso a cuentas de e-mail personales y profesionales de prominentes miembros del Partido Demócrata, incluyendo a la entonces candidata presidencial Hillary Clinton, y la difusión de su contenido a través de Wikileaks - lo que además tuvo una amplísima repercusión en medios nacionales y extranjeros -, los *hackers* lograron poner de cabeza la DNC, exponiendo irregularidades de la Fundación Clinton, así como correos comprometedores de la propia Hillary y de varios de sus asistentes y funcionarios clave de la campaña; forzando inclusive a renunciar a la presidente de la Convención, Mrs. Wasserman Schultz, horas antes de que ésta se llevase a cabo. Como resultado, el Partido Demócrata se vio

11 Licenciada en Relaciones Internacionales

seriamente perjudicado por la exposición de los escándalos e irregularidades de su principal candidata, beneficiando así al candidato republicano, el actual presidente Donald Trump. En este sentido, el ciberataque - que, según se presume, fue además ejecutado desde Rusia - tuvo una profunda incidencia en nada menos que la elección presidencial de la principal potencia mundial.

Como bien señala un artículo de *The New York Times* (2016) "el ciber poder demostró ser el arma perfecta: barata, difícil de anticipar y difícil de rastrear". Con ello, permite al país, o cualquier actor – sea individual o colectivo -, que domine esta tecnología aumentar su ratio de poder y convertirse en una amenaza real e inminente frente a países que no puede vencer mediante los medios convencionales de la guerra.

En el caso argentino, las mayores amenazas de ciber que puede enfrentar nuestro país son un ataque a infraestructuras críticas, es decir, aquellas instalaciones, redes, servicios, y equipos físicos y de tecnología de información, cuya interrupción o destrucción ocasione un impacto de gran magnitud en la seguridad, salud y/o bienestar económico de los ciudadanos, y/o en el eficaz funcionamiento de las instalaciones del Estado y de las administraciones públicas[12].

Estos ciberataques tendrán diferentes efectos según cuál sea el blanco de dicho ataque. Entre ellos, puede mencionarse un hackeo a una central hidroeléctrica que deje sin energía a los principales centros urbanos. El mismo escenario podría aplicarse para el caso de centrales nucleares: mientras que en nuestro país su incidencia en la generación de energía es muy pequeña, en casos como el de Francia, fuertemente dependiente de la energía nuclear, su efecto sería catastrófico. Además de las pérdidas económicas que este ataque conlleve (por empresas que no podrán desarrollar sus actividades con normalidad, entre otros efectos), un desabastecimiento de energía masivo y no previsto podría generar además un importante número de víctimas mortales, al dejar sin energía eléctrica a hospitales y centros de salud, desactivando un número aparatos y maquinarias que necesitan una constante fuente de alimentación energética para cumplir sus funciones.

Otro escenario posible sería un hackeo a un sistema de armas que ocasionase su disparo hacia centros urbanos o hacia bases militares. O, por el contrario, un hackeo que las vuelva obsoletas; por ejemplo, interviniendo un sistema de navegación o de radares de buques, submarinos y aviones militares, modificando su marcha e imposibilitando su locación. Del mismo modo, podrían hackearse sistemas de radares de la aviación comercial, y así desviar vuelos de sus cursos

[12] Definición basada en las Directivas de la Comisión Europea: 2008/114/CE, del 8 de diciembre de 2008.

programados, o inclusive ocasionar choques entre dos aviones, o algún otro tipo de incidentes intencionales, generando cientos de víctimas fatales.

Otro potencial ataque puede ocurrir en laboratorios y centros de investigación médicos, biológicos, nucleares y químicos; alterando los sistemas de seguridad y control de estos establecimientos y generando la dispersión de algún agente biológico, químico o nuclear con propiedades tóxicas en grandes centros urbanos, también con desastrosos efectos y potenciales víctimas fatales.

Además, del mismo modo en que ocurrió en los EE. UU., puede ocurrir un hackeo a las cuentas de correo electrónico del presidente, ministros o de prominentes políticos, de manera de afectar su imagen pública, exponer escándalos personales, malversaciones de fondos y redes de corrupción - si las hubiere -, y potencialmente tornar la opinión pública en su contra, modificando así el escenario político del país y poniendo en riesgo su gobernabilidad. Asimismo, si se adoptara definitivamente el sistema electrónico de votación - que ya ha sido testeado en la Ciudad de Buenos Aires y en Salta -, podría darse un hackeo a las bases de recolección de datos, modificando de manera directa el resultado de una elección.

Finalmente, se podría vulnerar la red de conectividad del país, por ejemplo, hackeando los sistemas de algunas de las principales empresas de telecomunicaciones; dejando así a millones de usuarios incomunicados (sin acceso a Internet ni telefonía), y ocasionando grandes pérdidas económicas por la cantidad de empresas que no podrán continuar su labor mientras dure el ataque.

En cuanto a los actores que tendrían un mayor incentivo para vulnerar la infraestructura digital del país, es más difícil hacer predicciones, y es precisamente en este punto en el que hay que estar más alerta.

En el caso de Argentina, un potencial ciber-ataque podría venir de algún país vecino, que obtuviese como resultado algún beneficio tangible con ello (por ejemplo, un potencial escenario podría ser un hackeo desde Chile hacia bases de datos militares argentinas para anticipar ejercicios secretos a realizarse en la frontera). Del mismo modo, el ataque podría provenir de algún país con el que se tenga una disputa latente (como podría ser el hipotético caso del Reino Unido hackeando sistemas de radares militares argentinos en la zona de Atlántico Sur). Esto es lo que se cataloga como *hipótesis de conflicto,* pero ahora a través de medios no tradicionales, como lo es un ataque cibernético.

Asimismo, un ciberataque puede ser perpetrado por alguna red de crimen organizado transnacional que necesite burlar la vigilancia en las fronteras para realizar contrabando, narcotráfico o trata de personas, como es el caso de la denominada "Triple Frontera" en el noreste argentino.

Un potencial ciberataque también podría provenir de alguna red terrorista internacional, como, por ejemplo, alguna célula del Estado Islámico en la región que hackee un centro de investigación médica y consiga dispersar un agente tóxico. Si bien en el caso argentino esta hipótesis no pareciera plausible en el futuro cercano - aunque no debe ser del todo descartada -, es un peligro muy real en países pertenecientes a Europa Occidental, el Medio Oriente, e inclusive en los Estados Unidos.

Volviendo a Argentina, un partido político nacional también podría tener buenos motivos para realizar un hackeo a gran escala, por ejemplo, para modificar el resultado de las elecciones en su favor (riesgo que, como ya se mencionó, se vería incrementado de manera exponencial de implementarse un sistema de votación electrónica). O, como pareciera haber ocurrido en el caso estadounidense, puede suceder que un actor extranjero con especial interés en alterar el curso de las elecciones consiga, mediante el hackeo, que un determinado candidato/partido (afín a los intereses y cosmovisión del país en cuestión) acceda al poder para así implementar políticas que favorezcan los intereses del país extranjero que ha realizado el ciberataque.

Por último, este tipo de ataques incluso podría provenir desde alguna empresa que se beneficie adquiriendo datos personales de los habitantes del país para su posterior uso comercial. En este escenario, puede ocurrir, por ejemplo, que una multinacional acceda a los sistemas de datos de agencias pertenecientes al Ministerio del Interior, Obras Públicas y Vivienda, o de la AFIP, para hacerse con una base de datos de potenciales clientes, o para luego revender esa base de datos a otras empresas. Si bien este ataque podría parecer "inofensivo" en su comienzo, una vez que se pierda el rastro de tamaña base de datos -especialmente aquellos datos confidenciales como números tarjetas de crédito, identificaciones o direcciones de domicilio -, podría convertirse en un riesgo muy importante para los damnificados, dependiendo de quiénes logren hacerse con esos datos y cuáles sean sus fines ulteriores.

En suma, debido a que existe un vasto número de blancos plausibles de ser atacados mediante un hackeo, y dado que contamos con variadas fuentes de ataque, con diferentes motivos e intenciones, nuestro país no debe desestimar la peligrosidad de sufrir un ciberataque y debe, por tanto, dedicar parte de sus servicios de inteligencia, y de sus Fuerzas de Seguridad a contrarrestar esta amenaza que está cambiando radicalmente el modo en que se entienden los combates y las amenazas en el siglo XXI.

En este sentido, la reciente creación de un Comisión de Ciberseguridad. perteneciente a la esfera del Ministerio de Modernización, en el marco del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), lanzado en 2011, es sin dudas un paso en la dirección correcta hacia una mayor comprensión, monitoreo, evaluación y defensa frente a estas nuevas amenazas.

No obstante, resta mucho camino por recorrer, particularmente en Argentina, para poder contar con personal entrenado específicamente para el área de la ciberdefensa y la ciberseguridad, y con organismos estatales, tanto civiles como militares, que se dediquen a contrarrestar este tipo de amenazas y elaborar estrategias de defensa de manera conjunta, entre sí y con el resto del aparato estatal. En consecuencia, es necesario reentrenar y reequipar nuestras fuerzas para el modo en que se combate en el siglo XXI y los nuevos tipos de amenazas que han surgido en las últimas décadas.

El trabajo por hacer es mucho, y es urgente. Pero es preciso una voluntad política que apuntale estos temas en la agenda pública y lleve adelante las reformas necesarias para garantizar la seguridad de nuestro territorio, nuestras infraestructuras críticas, y nuestra población, para las amenazas propias de la era digital.

Como bien señalan Peter Singer y Allan Friedman en su libro *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2014), no hay un tema *tan importante* del que se sepa *tan poco* como la ciberguerra. Es momento de revertir esta tendencia, si es que se quiere diseñar políticas de defensa y seguridad capaces de anticipar, responder y contrarrestar de manera eficiente a las amenazas de nuestra época.

**Bibliografía y fuentes**


- Buzan, Barry, Ole Waever, Jaap de Wilde, (1998), *Security A New Framework for Analysis*, Boulder, Colorado: Lynne Reinner Publishers.
- Buzan, Barry and Lene Hansen, (2009), *The Evolution of International Security Studies*, New York: Cambridge University Press.
- Comisión Europea (2008), “Directivas de la Comisión Europea”, 2008/114/CE, 8 de diciembre de 2008.

- Lipton, Eric; David Sanger y Scott Shane, (2016), "The Perfect Weapon: How Russian Cyberpower invaded the U.S.", en *The New York Times*, 13 de diciembre de 2016. Disponible en: https://mobile.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?referer= , consultado el 03 de noviembre de 2017.
- Singer, Peter y Allan Friedman, (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, New York: Oxford University Press.
- Walt, Stephen, (1991), "The Renaissance of Security Studies", en *International Studies Quarterly*, vol. 35, n. 2, 1991 (June), pp. 211-239.