CÁPSULAS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA COORDINACIÓN DE SISTEMAS DE CÓMPUTO

POR CUAUHTÉMOC VÉLEZ MARTÍNEZ

Cápsula TI NO. 28

CIBERGUERRA

Como todos sabemos, el desarrollo tecnológico ha transformado la forma en que se han enfrentado los conflictos humanos. Desde ataques con flechas, lanzas o catapultas hasta el uso de modernos aviones de combate, tanques y portaviones; la tecnología ha jugado un papel fundamental en el triunfo o la derrota de una contienda. Sin embargo, el siglo XXI ha creado otro tipo de guerra muy distinta a todo lo anterior pero con efectos que a la larga, serán igualmente devastadores: la ciberguerra o *cyber warfare.*

En una guerra convencional, los adversarios generalmente conocen sus capacidades, armamentos y tácticas específicas donde existe un frente de batalla común claramente delimitado por factores geográficos; en la ciberguerra, el ambiente, las estrategias y las armas son totalmente distintas pero con un potencial destructivo similar a las armas físicas. Las fronteras son inexistentes y los atacantes virtualmente invisibles; su objetivo, desmantelar o deshabilitar la infraestructura informática del enemigo con todo lo que ello implica: bloquear accesos, ocasionar retrasos en la red, provocar denegación de servicio, lanzar *malware* masivamente (*spyware*, virus, gusanos, troyanos), crear *botnets,* robar información, entre muchos otros. Debido a que gran parte de la infraestructura militar, financiera, económica e industrial de los países desarrollados se basa en la efectividad de sus sistemas de comunicación, almacenamiento y procesamiento de datos, cuando se elige a la víctima de un ataque masivo por distintos medios y hacia objetivos específicos, es factible vulnerar, quebrantar o paralizar indefinidamente los flujos de operación normal de ese país. En efecto, en un ciberataque (o *cyber-operation* como lo llama la OTAN) es posible inmovilizar redes de comunicación, cortar suministros de energía o incluso causar malfuncionamiento en las plantas industriales capaces de inducir fugas, explosiones o destrucción masiva. Tal es el caso del virus *Stuxnet* (ver edición 19 de Cápsulas de TI) considerado como la primer arma digital, que en 2010, fue capaz de alterar las válvulas de centrifugado de la planta nuclear de Natanz en Irán retrasando al menos 20 años en su programa atómico; o bien el caso de Estonia que durante 2007 recibió ciberataques continuos del gobierno ruso provocando denegación de servicio, alteración y bloqueos de operaciones financieras en los bancos y parálisis del servicio de internet en la administración pública. Todo ello, como represalia por haber movido una estatua de la era soviética y ubicarla en un cementerio ruso en las afueras de la ciudad.

La ciberguerra está originando tensiones cada vez mayores y frecuentes entre muchos países. Por ejemplo, antes de los acuerdos firmados en 2015, Estados Unidos aseguraba registrar ataques masivos a su infraestructura crítica provenientes de China que, según el gobierno norteamericano, no se caracterizaban por ser de *hackers* que operaran aisladamente; por su parte, el gobierno chino había detectado miles de ciberataques cuyo origen se centraba en Estados Unidos, más los sistemas de espionaje que buscaban robar información militar del país asiático. Al parecer dichos acuerdos quedaron en el tintero ya que meses después, se detectaron más de estos a empresas farmacéuticas y tecnológicas de E.U. procedentes de China.

Estos son sólo algunos ejemplos de los muchos que existen y que han obligado a diversos países a tomar distintas medidas para proteger su información, creando leyes más duras contra los *hackers* que intenten vulnerar los servicios básicos imponiendo penas económicas y corporales. Un extremo de lo anterior, es el manual "Tallin" publicado en 2013 por la OTAN, donde es permitido liquidar a cualquier *hacker* en legítima defensa que intente transgredir los sistemas de un país.

Apenas estamos conociendo los primeros efectos de la ciberguerra y no son prometedores. Desafortunadamente, entre más dependamos de la tecnología, mayor será el impacto derivado de un ciberataque; así pues, la solución no es inmediata ni sencilla, son los gobiernos quienes deberán legislar leyes justas en esta materia y empresas de tecnología que se adapten rápidamente a los nuevos métodos de ataque y protección de la información.

Referencias

Department of Defense (2015). Law of war manual-.
Tomado de http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf
European Parliament (2014). Cyber defence in the EU Preparing for cyber warfare?.

Tomado de http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf
NATO (2016). NATO review magazine.
Tomado de http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Otras fuentes

-https://actualidad.rt.com/themes/view/45214-ciberguerra
-http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/
-http://www.theguardian.com/technology/cyberwar
-http://www.cyberwar.news/
-http://global.britannica.com/topic/cyberwar
-http://csis.org/files/attachments/ts150930_Lewis.pdf
-http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf
-http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_06_shakarian_s.pdf
-http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf
-http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario
-http://www.isaca.org/chapters7/Monterrey/Events/Documents/20130704%20Respondiendo%20Ciberataques.pdf
-http://www.independent.co.uk/news/fine-for-boy-who-hacked-into-pentagon-1274204.html
-http://www.eldiario.es/turing/escenarios-ciberguerra-nuevo-orden-mundial_0_129837338.html

Fe de erratas Gaceta del Intituto de Igeniería UNAM, No. 117. página 5, últimos párrafos. Debe decir:

Al término de la ceremonia el doctor William Henry Lee felicitó al Instituto por estos 30 años "se dice rápido pero vale la pena reflexionar lo que esto representa. En esta ocasión –agregó- vamos a entregar al Laboratorio de Ingeniería Ambiental el certificado ISO 9001:2008 que le otorga el Instituto Mexicano de Normalización y Certificación, A.C.".

"Esta certificación a nivel nacional abarca los procesos de uso de la infraestructura y de apoyo analítico, los cuales cuentan con los procedimientos que requiere el laboratorio y asegura que los investigadores cuenten con la estructura para llevar a cabo sus proyectos. Esta certificación representa un arduo trabajo por parte del grupo que encabeza la doctora Susana Saval coordinadora de Ingeniería Ambiental y jefa del laboratorio".