Guerra digital ¿sensacionalismo o realidad?

Imagen de woodleywonderworks (CC by 2.0)

Definición

Una guerra digital, guerra cibernética o ciberguerra es un acontecimiento que tiene lugar exclusivamente en el ciberespacio y que ha sido definida como las acciones de un Estado o nación para penetrar en los equipos o redes de otro país a los efectos de causar daños o perjuicios (Richard A. Clarke, *Cyber War*, mayo de 2010).

Algunos referentes

Abril 2007. Estonia. El ministro de Exteriores acusó al Kremlin de dejarles sin varios servicios: la Bolsa, periódicos y web estatales.

Agosto 2009. Georgia. Se sabotearon oleoductos desde los mismos orígenes que el ataque a Estonia.

Enero 2010. Google denuncia el espionaje por China a través de cuentas de correo.

Septiembre 2010. Irán. El virus Stuxnet ataca la instalación nuclear de enriquecimiento de Natanz.

Enero 2011. Canadá. Máquinas instaladas en China accedieron a los sistemas del ministerio de Finanzas.

Objetivos

La tecnología del ciberespacio se convierte cada vez más en un instrumento de poder al alcance de individuos u organizaciones que pueden utilizarla para degradar o interrumpir las comunicaciones y alterar la información. Dado el carácter anónimo de las actividades en el ciberespacio y las posibilidades de acceso a él, la lista de adversarios potenciales es muy extensa. Los objetivos de la guerra digital son tan amplios como se desee: servicios públicos y privados, sistemas industriales, militares, banca y finanzas, transporte, educación, salud o gobiernos. Entre sus fines se incluyen el espionaje para obtener información sensible o confidencial de los gobiernos, de los individuos, de los competidores o de los enemigos; para obtener una ventaja militar, política o económica a través de métodos ilegales de explotación de los recursos de Internet, redes, *software* u ordenadores. Cualquier sistema, red o máquina podría, de no estar suficientemente protegida, ser objeto de sabotajes interceptando sus órdenes y remplazándolas por otras.

Ataque y defensa

Las ciberarmas preferidas para la guerra digital son los programas «día cero» (*0 days* en inglés), las vulnerabilidades del *software*, los virus, los gusanos, los troyanos, la técnicas de denegación de servicio, las máquinas zombis, las *botnet*, la ingeniería social, etc. Y por el lado contrario, las defensas contra los ataques se fundamentan en medidas preventivas que refuercen la seguridad de los sistemas, en resistir en el ataque y en su recuperación posterior. Un sistema seguro con las últimas actualizaciones del *software*, con despliegue de *antimalware*, con cortafuegos y detección de intrusos, constituye una buena defensa frente al ataque.

Análisis

Como un ataque o un incidente se puede incluir cualquier cosa, desde elementales intentos para obtener una contraseña o la infección de un virus fácilmente detectable, hasta un ataque altamente sofisticado para impedir el acceso a un sitio. Quizás habría que matizar más las diferencias entre las expresiones de ciberguerra, ciberdelincuencia o ciberespionaje. Un informe por encargo de la OCDE redactado por dos profesores universitarios, Peter Sommer e Ian Brown, indica que los ataques contra la ciberseguridad usando *malware*, ataques por denegación de servicio, espionaje, *crackers* y ciberdelincuentes, *hackers* y *hacktivistas*, en la mayoría de los casos estarán relativamente localizados, su impacto sería de corto plazo y su carácter en absoluto global. El reciente ataque a Irán contra sus instalaciones nucleares da una pauta para el futuro, pero también muestra las dificultades inherentes.

Aunque los efectos de los ataques cibernéticos son difíciles de predecir, es poco probable que alguna vez se dé una verdadera guerra digital. Las razones son que muchos sistemas informáticos críticos están fuertemente protegidos contra ataques y *malware*, por lo que los diseñadores de ciberarmas tendrán que identificar nuevas debilidades y vulnerabilidades del *software*, algo cada vez más difícil. Además, las circunstancias en las que el mundo o las naciones podrían enfrentarse a riesgos de seguridad cibernética con importantes efectos a largo plazo probablemente serían eclipsadas por otras amenazas mundiales en las que las infraestructuras de información jugarían un papel subordinado. El análisis de las cuestiones de la guerra digital está sin duda influenciado por el uso de un lenguaje exagerado.

Jesús Sanz