Guerras del Siglo XXI: De drones a ciberguerras

PRABIR PURKAYASTHA :: 18/10/2011

"Wired" informa de que un virus ha afectado a la flota de drones que opera desde la Base Aérea Creech en Nevada, EE.UU.

No ha impedido que los drones Predator y Reaper operen en Afganistán, Asia Occidental y ahora en el Norte de África, las áreas que EE.UU. considera “zonas de guerra”, una zona tenebrosa en la cual la ratio de objetivos de alto valor a “muertes” reales es ahora (cifras 2009-2010) de 1:147.

El tema sobre el que escribo no tiene que ver con drones per se, sino con la forma más reciente de guerra que nos espera, la ciberguerra. Y el virus contra la flota de drones no es el primer acto en este nuevo juego de guerra, el primero fue sin duda Stuxnet, el virus que atacó la instalación Natanz de enriquecimiento de uranio de Irán.

El actual virus que aflige a la flota de drones parece que está registrando los teclazos del “piloto”, antes de recodificar sus acciones. Por cierto, los pilotos de los drones se encuentran, no en la zona de guerra, sino a miles de kilómetros de distancia en lo que llaman “estación de control desde tierra” o cabinas virtuales del piloto en Nevada. Desde ahí, utilizando una hilera de ordenadores, el piloto realiza sus misiones mortales. El virus parece que ha infectado tanto las redes clasificadas a las cuales están conectadas las cabinas virtuales como las redes públicas conectadas al mundo exterior. Sin embargo, se supone que dos conjuntos de máquinas –las que están en la red clasificada y las de la red pública- no tienen conexión y la infección en una no debería afectar a la otra; el uso de memorias USB puede llegar a superar esa “brecha aérea”. Por el momento cuesta decir si este virus es simplemente un virus que ha viajado por la red pública e infectado en un descuido la red clasificada o si es un ataque selectivo montado por un adversario como Irán, similar al que EE.UU. lanzó contra la planta de enriquecimiento de uranio iraní en Natanz.

¿Qué es esta nueva forma de guerra, la ciberguerra? Si por ejemplo un virus que ataca una instalación puede utilizarse para dañar parcial o enteramente un equipo, ¿cómo se diferencia del ataque con una bomba? ¿Es posible utilizar un virus para tomar un “control malicioso” del equipamiento en una planta de energía nuclear y llevarla a hacer cosas que puedan llevar a la fusión del núcleo? Esto puede llevar a un accidente de proporciones catastróficas: el desastre de Fukushima ya ha totalizado una cuenta de 52.000 millones de dólares en daños. ¿Entonces cómo debemos considerar ese software malicioso que puede provocar un daño semejante, especialmente si la creación de ese software y el ataque a una instalación específica se realizan intencionalmente? No se trata solo de individuos inadaptados sentados en algún sitio creando virus para generar un caos indiscriminado en las redes informáticas. ¿Cómo se diferencia de un acto de guerra?

EE.UU. proclamó en su Doctrina Estratégica, la “Visión Conjunta 2020” del Pentágono, que apareció primero en el año 2000, la dominación de espectro completo. Habla de una dominación de espectro completo como si involucrara no solo cuatro dimensiones –espacio,

mar, tierra, aire– como he indicado anteriormente, sino también la quinta dimensión: "información" o ciberespacio. La dominación de espectro completo significa capacidades defensivas así como ofensivas. En mayo de 2010 el Pentágono estableció su nuevo Ciber Comando de EE.UU. (USCYBERCOM), que complementa sus otros Comandos.

Hasta ahora EE.UU. ha resistido todos los intentos de establecer un tratado internacional sobre la ciberguerra. Esto está en línea con su actitud básica respecto a todos los aspectos del derecho internacional, que se aplica a todos los países excepto a EE.UU., prueba del excepcionalismo estadounidense. Desde los ataques de drones –guerra no declarada y asesinatos extrajudiciales a la ciberguerra– todo se permite únicamente a EE.UU. No obstante, EE.UU ha declarado públicamente que cualquier ataque cibernético a su infraestructura se considerará un acto de guerra y provocará una represalia física. "Si desconectáis nuestra red eléctrica, tal vez lancemos un misil por una de vuestras chimeneas" como citó el Wall Street Journal. Lo que vale para uno no vale para el otro.

Es importante definir lo que constituye un acto de guerra en comparación con el intento de acceder a datos no autorizados o el crimen. Se ha informado ampliamente en la prensa de una serie de intentos por grupos, aparentemente originados de China, de acceder a datos de ordenadores; el que tiene que ver con Google condujo a un altercado público entre EE.UU. y China. Todo esto podría clasificarse como espionaje, sea relacionado con la seguridad o con el robo de datos comerciales valiosos. Se clasificaría como equivalente a espionaje convencional, lo que no es bonito, pero que al parecer lo hacen todos los gobiernos. Esto cambia si, por ejemplo, el software puede acceder a los controles de equipos vitales –centrales eléctricas, redes nacionales, redes de telecomunicaciones, etc. y hacer que fallen o se detengan-. La detención de una red puede tener consecuencias catastróficas. Ocasionar fallas de equipos utilizados para infraestructura vital como centrales eléctricas puede causar fallas de las centrales. A juicio de la mayoría de la gente esto constituiría un acto de guerra. La zona gris sería un ataque que conduciría a datos vitales, para algunos esto equivale a un acto de guerra, para otros no.

Según esta definición, Stuxnet es un virus que parece creado explícitamente para atacar las centrífugas de la planta Natanz de Irán. Existen informes detallados sobre el virus Stuxnet. Fue analizado por Symantec cuando apareció por primera vez en 2010, y estableció que afectó a más de 100.000 ordenadores, cerca de un 60% en Irán, un 20% en Indonesia, e India está en tercer lugar con infecciones en cerca de un 10%. El objetivo fue una combinación específica de máquinas, atacó a los PC con Sistema Operativo Windows y conectado a PLC de Siemens. Desde el principio, quedó claro que no se trataba de un virus común y corriente, sino que estaba hecho para un fin específico. También fue sorprendente el modelo de infección, no reflejaba el modelo de uso de los ordenadores sino que obviamente tenía un objetivo geográfico.

PLC, o Controladores Lógicos Programables son tipos de ordenadores que controlan procesos físicos, se utilizan para controles industriales. Pueden controlar diversos procesos y frecuentemente se encuentran en todas las plantas y equipos. Después de analizar el código, se estableció que el objetivo era aún más específico, parecía haber tenido como objetivo dos sistemas de transformadores de frecuencia, uno fabricado en Finlandia y el otro en Irán. De ahí un pequeño salto a la conclusión de que el objetivo era la planta de

enriquecimiento de uranio de Natanz.

La confirmación tuvo lugar por el tipo de números y configuración que produjo el análisis del código, identificó una gama de equipamiento del que se sabía que era similar a la gama de centrífugas de uno de los bloques de Natanz. El código se diseñó para acelerar y ralentizar a intervalos periódicos las centrífugas mediante los transformadores de frecuencia. Una vez que esto se relacionó con lo que se sabía gracias a los inspectores de la planta de Natanz del OIEA –que una gran cantidad de centrífugas resultó dañada y se pudo fuera de servicio– toda la secuencia de operaciones quedó clara. Se trataba de un ciberataque que había puesto fuera de servicio equipamiento vital de Natanz.

Algunos de los temas que surgen de esto es si Natanz era una instalación "ilegal" y por lo tanto un objetivo legítimo. Es obvio según el TNP que Irán tiene derecho a enriquecer uranio. EE.UU. y otros países occidentales argumentan que Irán ha "perdido" ese derecho por sus violaciones de ciertas estipulaciones del OIEA. Si consideramos el derecho internacional, es obvio que la decisión del OIEA de denunciar a Irán por semejantes violaciones fue de carácter político y tuvo muy poco que ver con las obligaciones reales del TNP o con trasgresiones respecto al OIEA. Por eso el hecho de que India haya roto filas con otros países no alineados en el Consejo del OIE que se habían opuesto a la acción de EE.UU. es particularmente exasperante y ha afectado desde entonces las relaciones entre India e Irán.

Sin consideración al OIEA y a las subsiguientes sanciones de la ONU, cualquier ataque físico contra la planta Natanz de Irán constituiría un acto de guerra. Cabe poca duda de que EE.UU. interpreta que cualquier ataque contra Natanz –un ataque aéreo estadounidense o israelí como el ataque israelí contra el reactor Osirik– escalaría rápidamente hacia una guerra, en la cual ese ataque sería el primer acto. Por ello, se eligió un ataque con un virus en lugar de físico que todavía podría retardar o desbaratar la planta de enriquecimiento de uranio de Natanz.

Cabe poca duda de que EE.UU. formó parte de este ataque, aunque algunos afirman que fue una operación conjunta estadounidense-israelí. La sofisticación del virus y el conocimiento que tenía que tener de Natanz excluye que fuera una iniciativa privada. En todo caso, EE.UU. e Israel han tenido una actitud de "ya lo sabíamos" respecto al ataque de Stuxnet, dejando pocas dudas sobre el origen del virus.

Lo que hay que preguntar es si se cambia el modo de ataque, ¿es algo diferente de un ataque convencional que cumpla el mismo objetivo? La segunda pregunta es, ¿qué pasaría si Irán tomara represalias con un ataque similar de virus contra instalaciones estadounidenses?, ¿cuál sería la reacción de EE.UU.? Y la tercera, y tal vez la más importante, ¿cómo impedimos que semejantes virus ataquen otras instalaciones vitales en cualquier país que tal vez no sea un objetivo, pero que a pesar de ello podría resultar infectado?

La posición de EE.UU. es obvia, aunque se permite que EE.UU. ataque a otros países utilizando semejantes ciberataques, todo ataque contra instalaciones estadounidenses provocaría una represalia convencional. En la posición estadounidense no existe diferencia alguna entre un ataque convencional y un ciberataque mientras se logre un impacto similar.

Pero a pesar de ello retiene el derecho a atacar a otros si considera que el ataque vale la pena. Como ha sido explicado en privado y sus proponentes lo declaran en público, Stuxnet estaba justificado ya que “evitó” que se bonbardease Irán.

Lo que nos debería preocupar a todos es que ahora hemos agregado una nueva dimensión a la guerra tal como se conoce. La guerra en el ciberespacio también es guerra, pero el problema de quién la origina y si el ataque es deliberado es mucho más difícil de definir. Al iniciar esta nueva forma de ataque, EE.UU. ha puesto en juego a propósito todo un nuevo tipo de guerra y de armas. Y como muestra la infección del centro de ataque de drones, y otros que seguramente tendrán lugar por el camino encabezado por EE.UU., sea con drones o en cualesquiera otra forma de guerra.

Bienvenidos a las nuevas guerras del Siglo XXI: guerras de drones y de ordenadores.

Information Clearing House. Traducido del inglés para Rebelión por Germán Leyens

---

https://www.lahaine.org/mundo.php/guerras-del-siglo-xxi-de-drones-a-ciberg