Extrait du El Correo

http://www.elcorreo.eu.org/La-OTAN-incrementa-su-politica-de-ciberdefensa-reforzada

La OTAN incrementa su « política de ciberdefensa » reforzada

- Empire et Résistance - OTAN -

Date de mise en ligne : dimanche 28 septembre 2014

Según un comandante de EE.UU., la anexión de Crimea por parte de Rusia y el posterior conflicto que estalló en Ucrania demostraron que Rusia supo integrar en su operativo militar una estrategia ciberofensiva que resultó muy eficaz.

La confrontación en curso entre Rusia y Occidente reactivó una disciplina cuyo imaginario ha sido alimentado por la informática, el cine, la literatura, los rumores y un puñado de hechos constatados : la ciberguerra. El desplazamiento de un conflicto desde un territorio al ciberespacio lleva años generando especulaciones y, en algunos casos, enfrentamientos reales como el ciberataque masivo de que fue objeto Estonia en 2007, el ataque contra los sistemas de misiles aire-tierra de Siria en el mismo año, los operativos en Georgia, el permanente hostigamiento digital que protagonizan China y Estados Unidos de América, o la operación (2010) contra el programa nuclear iraní urdida por Estados Unidos e Israel mediante el virus **Stuxnet**. Este dispositivo es el descendiente de la **Operación Olympic Games** desarrollado por la **Agencia Nacional de Seguridad** (NSA) usamericana y la « **Unidad 8200** » de Israel. La crisis que se desató con Rusia aceleró el recurso a la ciberguerra. Durante la última cumbre -4 y 5 de septiembre- celebrada en plena crisis con Moscú, la OTAN actualizó sus estándares de defensa de Europa por medio de un programa llamado política de ciber*defensa* reforzada. Según el comandante us de las fuerzas aliadas en Europa, la anexión de Crimea por parte de Rusia y el posterior conflicto que estalló en Ucrania demostraron que Rusia supo integrar en su operativo militar una estrategia ciber*ofensiva* que resultó muy eficaz. Moscú habría conseguido interrumpir todas las comunicaciones electrónicas entre las tropas ucranianas estacionadas en la península y los centros de comando repartidos en el resto de Ucrania. Este es el argumento de Occidente para desarrollar en el ciberespacio un frente de conflicto.

El documento elaborado por la OTAN sobre la ciber*guerra* es de hecho una postura amenazante. La *Alianza Atlántica* (OTAN) extendió al ciberespacio todas las garantías del Tratado. Ello quiere decir que cualquier ataque contra las redes informáticas de un país miembro será considerado como un ataque contra todos, o sea, equivalente a una agresión clásica. Occidente crea con este texto un ciberespacio « indivisible ». La consecuencia es evidente : si un Estado exterior a la Alianza Atlántica aparece como responsable de un ciber*ataque* será objeto de represalias que pueden incluir incluso los medios clásicos. Con su recurrente cinismo hambriento de confrontaciones, la *Alianza Atlántica* hace el papel de futura víctima como si la OTAN o sus miembros más poderosos, Estados Unidos por ejemplo, nunca hubiesen lanzado ciber*ataques* contra alguno de sus adversarios, o espiado la intimidad de cada ser humano del planeta mediante el dispositivo « **Prism** » montado por la NSA, con la servil colaboración de empresas privadas -Google, Yahoo, Facebook, Microsoft, etc.-. Sorin Ducaru, adjunto al secretario general de la OTAN y encargado de los « desafíos emergentes » aclaró que el organismo se limitará a defenderse. Según Ducaru, está « excluido lanzar operaciones ciberofensivas. Estás son del dominio de cada país miembro ».

La ciber*guerra* se convierte así, y ahora a nivel colectivo, en el nuevo *El Dorado* de los ejércitos. La *Alianza Atlántica* ya cuenta con una infraestructura, el **Ccdcoe** (Ver : **Cooperative Cyber Defence Centre of Excellence**), situado en Estonia y en plena fase de desarrollo y ejercicios de « pirateo » de servidores civiles, vigilancia de las redes y ataques reales. Todo parece estar listo para una gran confrontación deslocalizada hacia el ciberespacio. La retórica occidental está ampliamente dominada por la idea de que es la única solución para defenderse del gran enemigo ruso. El general Keith Alexander -ex director de la NSA- acusó a Moscú de haber pirateado hace unos meses el banco JP Morgan para robar datos sensibles como una forma de represalia, luego las sanciones financieras adoptadas por Washington contra Rusia a raíz del conflicto en Ucrania. El primer expoliador mundial de datos privados planetarios se presenta ahora con el perfil de un *gatito inocente*, víctima de un ciberataque organizado por una potencia repentinamente enemiga.

El otro gran acusado es China.

Beijing aparece regularmente citado como responsable de contaminar el ciberespacio con ataques destinados a hurtar los secretos de Europa y los Estados Unidos. Sin embargo, tal y como lo demuestran los documentos revelados por el ex analista de la *NSA* y de la *CIA* Edward Snowden, Estados Unidos tiene ojos y oídos enchufados en cada casa, incluidas las de sus aliados como Francia y Alemania. Washington espió a decenas de responsables alemanes y llegó a pinchar el teléfono celular de Angela Merkel. En represalias, a mediados de julio, el jefe de los servicios secretos US en Alemania fue invitado por la canciller alemana a dejar el territorio. En una entrevista publicada por la revista Wired, Edward Snowden contó que la NSA tenía entre su arsenal un arma orientada hacia los ciberconflictos. Se trata de « **MasterMind** ». Según Snowden, este dispositivo está totalmente dedicado a la ciberguerra. *MasterMind* fue construido para analizar el tráfico en la red, detectar y detener los ciberataques contra Estados Unidos. Sin embargo, el ex analista de la CIA y la NSA, hoy exiliado en Rusia, reveló que *MasterMind* también está dotado de « un aspecto ofensivo automático, sin intervención humana ».

Los analistas militares no siempre están de acuerdo con lo que encierra el concepto de ciber*guerra*. Por ejemplo, Maxime Pinard, director de Ciber*estrategia* en el **Instituto de Relaciones Internacionales y Estratégicas** (IRIS), anota con pertinencia que el término de ciber*guerra* no está sustentado por ninguna realidad concreta. Pinard resalta que « ciertamente hay ciber*ataque*s, pero no ciberguerra en el sentido de un conflicto entre, al menos, dos protagonistas identificados que causan daños humanos y económicos el uno contra el otro ». El investigador francés también pone de relieve otra incoherencia en el uso excesivo del término ciber*guerra* : « *Los ciberataques parecen nuevos cuando en realidad sólo corresponden a técnicas clásicas de sabotaje y perturbación de las comunicaciones del enemigo* ». En suma, un mero espionaje digital o la costosa pero simple contaminación de servidores con un virus. Esto no le quita pertinencia a otra idea muy extendida en estos tiempos de nuevas guerras : la carrera armamentista digital. Hasta ahora, sus principales actores eran Estados Unidos de América y China. Sin embargo, la inclusión de la OTAN y su « **política de ciber***defensa* reforzada » agregan un protagonista suplementario y aumenta el riesgo de que, efectivamente, se plasme una ciberguerra generalizada, mucho más aguda que las ciberestrategias nacionales de defensa y contraataque actualmente en curso. El contraalmirante Arnaud Coustillière, responsable de la ciber*defensa* en el Ministerio francés de Defensa, asegura con realismo : « *Si podemos neutralizar los radares con el arma informática antes que con un misil, es mucho mejor* ». El contraalmirante francés no cree que pueda darse algún día una suerte de Hiroshima informático : « Estamos tan globalizados que no lo creo. Sin embargo, un ataque catastrófico contra las infraestructuras vitales sí puede producirse ». Para Maxime Pinard, el resultado de estas nuevas políticas carece de secretos : « *Nos dirigimos hacia una militarización reforzada del ciberespacio con un riesgo certero de engranaje donde los cibernautas* (simple usuarios) *serán las principales víctimas* ».

Eduardo Febbro para Página 12

Título original : « **Rusia y Occidente aceleran su ciberguerra** »

Página 12. Desde París, 28 de septiembre de 2014.

El Correo. París, 28 de septiembre de 2014.