SEMANARIO HEBREO

“ESTO TODAVÍA NO ES TERROR EN LA

CON YAEL SHAHAR, DIRECTORA DE UNO DE LOS MÁS SINGULARES INTERDISCIPLINARIO DE HERZLIA , SOBRE LOS MUTUOS

por Ana

Por ahora, no hay muertos ni heridos. Nadie llega al hospital ni abre fuego. Pero la guerra… es a muerte.
Se trata de un nuevo campo de batalla, en el que los disparos virtuales se han intensificado claramente en las últimas semanas y no se vislumbra para nada la tregua: un abierto enfrentamiento por computadora, en cuyo marco hackers árabes han logrado irrumpir a importantes sitios israelíes en la red neutralizándolos temporariamente, sin que los israelíes se queden atrás en absoluto.

Las víctimas, por el momento: el sitio de la Bolsa de Valores de Tel Aviv y de la compañía de aviación israelí El-Al , entre otros, y las Bolsas de acciones de Arabia Saudita (Tadawul) y los Emiratos Arabes Unidos (Abu Dhabi Securities Exchange). Este fue sólo el último capítulo en la ciberguerra, en la que no faltan por cierto las amenazas directas.
“Esto es en respuesta al hackeo patético “ de los sitios israelíes este lunes, advirtieron los israelíes que lograron entrar a los mencionados sitios del Golfo, agregando que si los ataques continúan, “pasaremos a una segunda etapa y paralizaremos los sitios por no menos de dos semanas ..o por un mes”.
El primer tiro salió supuestamente de Arabia Saudita, cuando hace pocas semanas hackers de dicho país revelaron haber entrado a sitios de empresas de crédito israelíes, sacando de allí los datos exactos de un millón de ciudadanos del Estado hebreo. Varios miles fueron publicados y las compañías israelíes repararon el daño de inmediato. Rápidamente llegó el “contra-ataque” con datos similares de ciudadanos saudíes… y nadie sabe cuáles pueden ser los próximos pasos.

Para conocer un poco más de cerca sobre este nuevo tipo de guerra, recurrimos a Yael Shahar, especializada en la materia. Shahar es experta en el estudio de tendencias tecnológicas aplicadas al terrorismo y a las fuentes abiertas de Inteligencia, en terrorismo no convencional y evaluación de amenazas. Da clases en el Instituto Interdisciplinario de Herzlia, en el marco del Instituto de Política Anti Terrorista.

P: Yael… usted está al frente de un proyecto que estudia, de hecho, el campo más nuevo en la investigación del terrorismo.. ¿verdad?

R: Así es, es el terrorismo de la era moderna..pero en cuanto a lo que ha estado pasando aquí en las últimas semanas, creo que hay que aclarar que aún no llegó a ser “terrorismo” sino actividades de hackers..aunque claro está que este tipo de cosas ya son parte de la guerra. Cuando cada uno ya ataca los sistemas computarizados del otro, es una forma de guerra.Pero lo que se ha estado dando por ahora entre hackers sauditas, según se publicó, e israelíes, no llega todavía a ese nivel. Es que aún no se ha atacado redes gubernamentales.

P: O sea que hay diferentes niveles de amenazas…pero a terrorismo cibernético no diría que se ha llegado..

R: Todavía no, pero estoy segura que el otro lado tendría gran interés en poder concretarlo, en terrorismo en la red, que logre cobrar víctimas.

P: ¿O sea que lo que determina que se le pueda llamar ciber terrorismo no es el tipo de sitios que logren atacar o al que se logren infiltrar sino que con ello cobren víctimas mortales?

R: O que logren alterar seriamente la vida de la sociedad…Por ahora no se lo ha hecho. Yo diría que por ahora lo que lograron fue algo así como crear mal olor en una tienda , de modo que nadie se acerque a ella o que su actividad se vea alterada. Pero aún no es como alterar totalmente su desempeño. No se puede comparar con el terrorismo en los autobuses, por el cual la gente se abstenía por ejemplo de mandar a sus hijos a la escuela en transporte público..

P: Pero al hablar de terrorismo, siempre se dijo que este no constituye una amenaza existencial para Israel pero que su daño consiste en que logra , tal cual el nombre lo indica, aterrorizar, desestabilizar, atemorizar a la gente.. Pues claro que no se puede hablar de que los israelíes están aterrorizados porque hackers árabes lograron entrar a los sitios de la Bolsa de Valores en Tel Aviv o de la compañía aérea El Al, pero seguro que eso no da mucha tranquilidad…

Yael Shahar, especializada en terrorismo no convencional. La tecnología es una de las armas más sofisticadas.

R: Eso es cierto..Aclaro ante todo que en la Bolsa de Valores no hicieron realmente ningún daño serio sino que lograron que sea muy difícil entrar al sitio. Imaginemos que mucha gente se aglomera a la entrada de un negocio.. eso puede causarle daño porque no se puede entrar. Es evidente que aquí no se ha llegado todavía a algo similar a lo que ocurrió en el 2006 en Estonia, que prácticamente paralizó al país..Eso fue como un ataque terrorista a través de la red. El gobierno no sabía qué hacer.Los estonios no sabían que tenían esos enemigos..

P: Israel sí lo tiene claro..O sea que la conciencia al respecto puede ayudar a protegerse de ataques en la red..

R: Así es. Israel siempre lo supo y desarrolló una gran conciencia sobre el particular. Hay que dar los pasos necesarios para proteger los sistemas claves, sin duda, aunque todos comprenden que no se puede garantizar plena y absoluta seguridad en cada sitio en la red.

P: ¿Le parece que para que llegue a nivel de cyber terrorismo es imprescindible que haya una orden de arriba, de un establishment oficial, del Estado? ¿O alcanza con que fanáticos de la computación, hackers particulares con gran motivación, se dedican a atacar?

R: No creo que cualquiera pueda hacerlo. Pero hoy la gran pregunta es si acaso un grupo de buenos hackers puede hacerlo o necesariamente precisarán el rol de un Estado. Algo como lo que pasó con el ataque a Irán, eso sí que es guerra cibernética.. algo que requiere el rol de Estados, porque son necesarios muchos recursos humanos y materiales. Pero además, eso requiere a menudo información e adentro.A veces esos ataques son tan precisos y puntuales, que no se pueden lanzar sin una información concreta desde adentro, lo cual se consigue sólo con espionaje…

P: Con lo de Irán usted se refiere al logro de introducir un virus al sistema de computadoras del plan nuclear de modo que paralizaron por un tiempo las centrifuga…

R: Así es. También hubo otras cosas como lograr que compren materiales que no están perfectos, máquinas con problemas… lo cual en el transcurso de los años se tradujo en demoras y problemas con los que el plan nuclear tuvo que lidiar..

P: Hace pocos años se habló en Israel del riesgo de terror en la red, desde otro punto de vista: los problemas de las redes sociales y cómo pueden llevar mediante el engaño e identidades ocultas, a que israelíes caigan en manos de terroristas, por ejemplo en secuestros en el exterior… Y ahora, resurgió el tema en los titulares, por esta “guerra” entre hackers de Arabia Saudita y los israelíes que respondieron. ¿Le parece que la respuesta de los israelíes fue adecuada? Lanzaron serias advertencias y parece que lograron infiltrarse a la Bolsa de Valores de Arabia Saudita y de los Emiratos Árabes Unidos…

R: Parecería que de ambos lados hay una misma idea, pero mi impresión es que del lado árabe sus computadoras están mucho menos protegidas.

P: ¿O sea? ¿Qué significa eso en forma práctica?

R: Que están mucho menos prontos que Israel para estos ataques por lo cual el potencial de los israelíes de causar daño a los sauditas, es mayor. Pero eso no significa que los israelíes realmente vayan a publicar todo lo que consiguieron al infiltrarse. Hasta ahora han dicho, por ejemplo, que publicarán números de tarjetas de crédito, pero no las cifras de seguridad, por ejemplo. O sea que no querían causar un daño a fondo en serio. Pero sí advirtieron que si los hackers sauditas, o quienes sean, continúan con sus ataques, ellos endurecerán su respuesta.

P: Usted dice “o quienes sean”, y justamente le iba a comentar que aquí, en el mundo de la red, hay formas de

RED, PERO PUEDE LLEGAR A SERLO”.

PROYECTOS EN EL INSTITUTO DE POLÍTICA ANTI TERRORISTA EN EL

ATAQUES ENTRE HACKERS “SAUDITAS” E ISRAELÍES.

Jerozolimski

(Las fotos de esta página son de Ariel Jerozolimski)

encubrirse…. O sea que quizás ni siquiera son saudíes… ¿puede ser?

R: Puede ser… por supuesto. Puede ser alguien interesado en provocar tensiones entre Israel y Arabia Saudita, por ejemplo, teniendo de fondo la crisis con Irán..No necesariamente quien se dice que es, es realmente el responsable.

P: Se usa aquí, por supuesto, servidores no identificados.. ¿Es posible, siempre, llegar al fin a la identidad de una persona que hace todo este proceso totalmente encubierta?

R: Se puede, pero es cuestión de tiempo. Cuanto más protegido está su sistema, más tiempo llevará. Puede ser como con un ladrón en serie de bancos, que actúa con gran inteligencia… hay que esperar que cometa un error..

P: Hace varios años vi una película con Bruce Willis en la que los malos de la historia eran unos terroristas que lograban neutralizar un aeropuerto, apagar las luces de la pista… ya ni recuerdo si había muertos, pero tensión sí ..y mucha.. En ese momento no diré que parecía ciencia ficción, pero no tan real como ahora… ¿Imagina un escenario así en la guerra de hoy en la red?

R: Los aeropuertos, por suerte, no pueden ser neutralizados de esa forma ya que sus sistemas no están conectados a internet.. De lo contrario, sería como abrir la puerta principal e invitar a todo el que lo desee, que entre a hacer lo que quiera..imposible.Pero eso no significa que no pueda alguien entrar al sistema de computadoras del aeropuerto e introducir algún virus o materiales problemáticos con su usb…

P: ¿Diría que Israel está bien protegido de posibles ataques e intentos de infiltración por la red?

R: Depende en qué. Desde 1994 hay leyes que determinan que toda compañía que tiene materiales delicados, debe tomar las medidas necesarias para protegerlos. Pero no todos lo hacen debidamente ya que los negocios, lo que quieren, es ganar, y no siempre protegen todo al nivel que deberían. En El Al, por ejemplo, no consiguen provocar un daño verdadero sino que mandaban tantos pedidos que no se podía entrar al sitio.. fue algo de ese estilo.

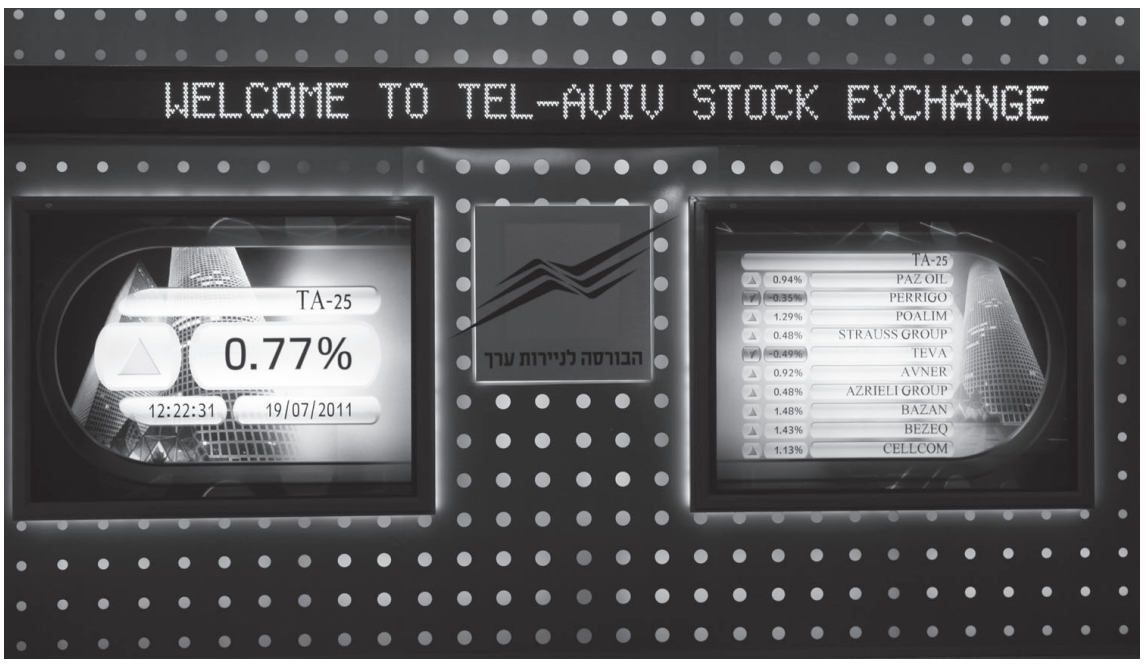
P: ¿Desde cuándo se puede decir que Israel es plenamente consciente de la posibilidad de amenazas de cyber terrorismo? Eso equivaldrá, supongo, a preguntar desde cuándo se toman medidas serias al respecto.. Sabemos que en el ejército hay unidades enteras que se ocupan del tema..

R: Yo diría desde el 2003. Se formó entonces un equipo gubernamental de protección del sistema de computadoras. Desde entonces la conciencia al respecto fue en aumento. Y creo que lo que ha pasado ahora será para bien, ya que más gente comprendió que no se hizo lo suficiente y que hay que proteger los sistemas en forma efectiva. No todos podrán hacerlo, pero una compañía como El Al, por ejemplo, que lleva el nombre de Israel, seguro sí que debe hacerlo en forma más estricta.

P: ¿Qué se puede decir sobre lo que hace Tzahal, las Fuerzas de Defensa de Israel, en este campo?

R: Creo que no hay mucho que decir al respecto pero estimo que el ejército israelí se ocupa en este campo de tener tantas posibilidades de defenderse como de atacar . La concepción de las cosas van cambiando. Y los hechos que suceden, ajustan a veces la conciencia al respecto. Lo claro es que aquí hay grandes recursos humanos al respecto, empresas de alta tecnología muy desarrolladas..y si se llegara a una situación de verdadera guerra en este campo, hay elementos a los que recurrir.

El sitio de EL AL fue hackeado.



También el de la Bolsa de Valores de Tel Aviv.

P: Según lo que se publicó en la prensa local, el grupo de hackers israelíes que actúa al parecer por su cuenta, se dio a si mismo un nombre que comienza con IDF, la sigla en hebreo de Fuerzas de Defensa de Israel.. ¿Cree que es sólo para amedrentar, para dar la sensación de que son una unidad secreta y poderosa del ejército israelí?

R: Exactamente, eso es lo que me parece. No es realmente el IDF..

P: Pueden simplemente ser locos de la computación, bastante talentosos además..

R: Justamente..

P: ¿Cree que puede llegar un momento en el que la guerra en la red sustituya la guerra en el frente?

R: No creo que haya una revolución absoluta pero sí puede haber mucha influencia. Lentamente, lo que está claro es que van entrando cada vez nuevos tipos de armas..El potencial de la computadora es cada vez más usado por todos lados..Pero otro elemento que creo que hay que destacar es que la retaguardia civil es cada vez más parte activa del cuadro…

P: No sólo le caen misiles a los poblados civiles sino que la guerra cibernética le puede afectar directamente la vida…

R: No sólo eso. Como civil, puede verse dañado, pero también puede atacar…

P: Acá parece estar claro que , por ahora al menos, los que están en esta “lucha” que como usted dijo todavía no es guerra abierta..son hackers que actúan por su cuenta. ¿Le parece que necesariamente los sistemas oficiales que deberían tener la responsabilidad de hacer algo al respecto, ven esta situación con buenos ojos? Es que los hackers dijeron que contraatacan para defender a Israel..La pregunta es si le están haciendo bien a Israel…

R: No estoy segura en absoluto. Pensemos por un momento quién puede ganar algo de toda esta historia. Todo tipo de tensión entre Israel y Arabia Saudita favorece a Irán…No descartaría que esto, por lo tanto, está relacionado a Irán. Quizás sea resultado de alguna acción de los iraníes, sin que lo sepamos..Es que aquí hay muchas probabilidades de causar daño a canales secretos de contacto entre Israel y Arabia Saudita… y quienes sin duda tienen interés en hacerlo es Irán.

P: O sea que quizás los primeros hackers que atacaron no sean sauditas….

R: Quizás….