Internet y nuevas tecnologías

Roberto Plá
Coronel de Aviación
http://robertopla.net/

CIBERGUERRA

ALEMANIA CONSOLIDA SU ESTRUCTURA DE CIBERGUERRA

Recientemente la Ministra de Defensa alemana, la señora Ursula von der Leyen, ha anunciado la creación de una estructura militar dedicada a la ciberguerra en el seno de la fuerzas armadas alemanas.

Esta unidad militar contará con la nada despreciable plantilla de trece mil quinientos efectivos. Es un paso más en el proceso de reconocimiento de la ciberguerra como una de las formas más importantes de la guerra moderna, en función de las amenazas en el campo de las tecnologías de la información, comunicaciones y computación, y de las graves consecuencias que podría tener permanecer vulnerables a las mismas.

En Alemania, como en otras naciones, este fenómeno no ha surgido de la noche a la mañana, sino que se ha desarrollado como una respuesta a las crecientes amenazas o ataques producidos en las redes de ordenadores estatales o en la industria estratégica del pais. Antes de 2006 en alemania se había iniciado la preparación de un sistema de defensa contra ataques de hakers. Es a partir de este año cuando ponen las bases para la formación de un "ejército de hackers" con capacidades ofensivas.

El verano de 2010 supuso un punto de inflexión importante en la forma en que muchos gobiernos y analistas internacionales consideraban las operaciones de ciberguerra. El hecho que marcó esta inflexión fue el descubrimiento del virus Stuxnet. Desde un principio estaba claro que se trataba de un arma, con un objetivo específico y desarrollada con una complejidad y medios que señalaban a organismos gubernamentales, mostrando desde el principio a Estados Unidos e Israel como posibles orígenes de este arma revolucionaria.

No hay que olvidar que el objetivo de Stuxnet eran las centrifugadora de uranio de Iran, pero tampoco que la vía de entrada fueron unas tarjetas controladoras que usaban estas máquinas que habían sido fabricadas por Siemens, una empresa multinacional de origen alemán con más de 362.000 empleados. El virus causó la infección de algunas de estas tarjetas fuera de Iran y este hecho probablemente sugirió a las autoridades la idea de que la infraestructura del país no estaba preparada para enfrentarse a esa amenaza.

El año siguiente, Siemens abandonó el negocio nuclear, según dijo a través de su director general, debido al posicionamiento de Alemania en contra de la energía nuclear y al desastre de Fukushima.

La división del Bundeswehr, con sede en la ciudad de Gelsdorf, quedó lista para participar en operaciones de ciberguerra ofensivas a partir de finales de 2011.

A mediados de 2012, el ministro de defensa alemán presentó un informe a la comisión parlamentaria de defensa en el que confirmaba la existencia de esta unidad específica de las fuerzas armadas alemanas dedicada a la ciberguerra, denominada "unidad de operaciones en redes informáticas", Desarrollo de la creada en 2006.

En Alemania se han producido importantes ataques contra las redes y ordenadores del gobierno. A principios de 2015, la administración del Bundestag descubrió que sus ordenadores estaban infectados con virus que no hubo forma de erradicar. Para solucionar el problema, los técnicos tuvieron que desmantelar la red e instalarla nuevamente. También se han producido incidentes en su infraestructura más sensible, como la infección con el gusano Conficker detectada en la central nuclear de Gun-

dremmingen en abril este mismo año.

Esta situación llevó a la ministra von der Leyen a anunciar en septiembre de 2015 durante una conferencia sobre ciberseguridad, la potenciación de las estructuras de ciberdefensa. Por entonces ya trabajaban en Alemania unas quince mil personas en esa cuestión, pero solo 320 realizaban funciones puramente militares.

En abril de este año la ministra ha anunciado la creación de un mando militar dedicado específicamente a la ciberguerra que se sumará a los cinco ya existentes: Ejército, Armada, Fuerzas Aéreas, Servicio Sanitario y Servicio de Apoyo Conjunto, y que estará al mando de un Teniente General a partir de 2017. Se ha habilitado un presupuesto de 3,6 millones de euros para realizar una campaña de reclutamiento de 1500 técnicos en la materia cada año. En el campo de la enseñanza, se crea un grado en la Universidad de las Fuerzas Armadas en Múnich para formar los cuadros de mando de esta organización. En el mismo centro de enseñanza se creará un centro de investigación y conocimiento en colaboración con la industria civil.

La importancia de la organización creada, indica que Alemania toma muy en serio las amenazas en el campo de la ciberguerra.

http://delicious.com/rpla/raa854a

INTELIGENCIA ARTIFICIAL

LA LOCURA DE TAY

En aquellos años de pantallas de fósforo verde y procesadores de ocho bits, ya existía un curioso programa de conversación llamado “Eliza”. Se trataba de una aproximación muy lejana a la Inteligencia Artificial. Tan lejana que de ninguna forma podría englobarse en este concepto. La versión de Eliza que recuerdo estaba escrita en BASIC. En su propio código mediante sentencias “DATA” almacenaba una colección de palabras y expresiones. Cuando el operador humano introducía alguna de estos términos en la frase de entrada, Eliza respondía con una u otra frase según su programación. Así, si el usuario

mencionaba la palabra 'padre', Eliza respondía: “hábleme más de su padre”. Sin embargo para un profano, las respuestas de Eliza podían parecer -durante un breve espacio de tiempo- coherentes, para luego transformarse en una cantinela de pseudo-psicoanalista y finalmente caer en alguna trampa, ya que Eliza tendía a responder a las frases incoherentes con respuestas estereotipadas o sin sentido. Al fin y al cabo era un programa conversacional muy básico, muy lejos de aquella máquina imaginada por Turing que tendría que hacerse indistinguible de un humano.

Desde entonces la inteligencia artificial ha avanzado mucho. Paradójicamente, muchos de los avances en inteligencia artificial se han producido gracias a un mejor conocimiento sobre el funcionamiento de la inteligencia biológica. En cualquier caso, la inteligencia artificial se distingue por la solución con un porcentaje de exactitud aceptable de problemas complejos a partir de datos incompletos, así como la capacidad de adquirir 'experiencia' y mejorar los resultados con la práctica.

Las grandes empresas de la red realizan modelos e investigaciones en este campo porque la profusión de datos procedentes de la red son una auténtica mina de oro para quien pueda procesarlos en busca de conclusiones. Muchos gigantes de la red ofrecen servicios sorprendentemente útiles de forma gratuita para el usuario porque su negocio no está en cobrar por sus servicios, sino en obtener datos sobre los gustos, hábitos y deseos de sus usuarios. Datos que hábilmente estudiados, ofrecerán una fuente de información valiosísima sobre los hábitos y tendencias del mercado. La inteligencia artificial debería ayudar a que estos resultados sean más exactos y por tanto, a multiplicar los beneficios.

En esta linea de investigación, Microsoft desarrolló un robot conversacional, basado en inteligencia artificial y con forma de cuenta de twitter. Su nombre, Tay es también un juego de palabras recursivo, ya que quiere decir 'Tay and you”. Dirigido a los adolescentes que pueblan la red Tay debía asimilar su lenguaje y sus costumbres hasta mimetizarse como uno de ellos convertido en un agente de captura de datos.

Sin embargo, en menos de 24 horas, Tay se había convertido en un conversador violento, racista, sexista y mal hablado.

Microsoft alegó que usuarios malintencionados le habían enseñado estas barbaridades, saturándolo de información sesgada y negativa, hasta que rezumó improperios. Estas excusas infantiles no hicieron más que aumentar el ridículo de los creadores del engendro y el consiguiente cachondeo en las redes sociales.

Sin embargo este incidente puede resultar extremadamente útil para meditar sobre los límites de la automatización, el equilibrio entre la tecnofobia y el robotismo utópico y en definitiva sobre si sería prudente confiar decisiones morales o la propia vida humana a algoritmos matemáticos por muy perfeccionados que puedan parecer.

Por otra parte, el razonamiento artificial, ¿podría llegar a la conclusión de que el factor erróneo de la ecuación es precisamente el ser humano?. Quizás deberíamos preocuparnos de que las matemáticas y la física no adelanten a la moral, la ética y la filosofía.

http://delicious.com/rpla/raa854b

Enlaces

Los enlaces relacionados con este artículo pueden encontrarse en las direcciones que figuran al final de cada texto