



[Cyber attacks](#) by Christiaan Colen on flickr/[CC by 2.0](#)

Alemania se prepara para la guerra del futuro

Berlín ha creado una nueva rama militar para tomar la delantera en la guerra híbrida de alta tecnología.

- Josue Michels
- [17/8/2017](#)

Cientos de miles de objetivos alrededor del mundo fueron impactados por peligrosas armas en mayo. Estas armas no eran cinéticas, biológicas, químicas ni nucleares; éstas eran electrónicas. Los objetivos eran computadores en 150 países, incluyendo un estimado de 70.000 dispositivos dentro del Servicio de Salud de Gran Bretaña, como computadores, escáneres y equipos de almacenamiento. El ataque también afectó a FedEx, Deutsche Bahn, Telefónica, Taiwan Power Co., empresas de inversión, compañías de seguros y otras numerosas compañías, organizaciones e individuos.

Las armas son variaciones de un ciberataque llamado WannaCry. El software malicioso accesa archivos de computador, los encripta, y pide rescate por ellos, demandando pagos de 300 a 600 dólares por computador a cambio de regresar los archivos a su estado sin cifrar. Europol dijo que fue un ataque sin precedentes.

WannaCry es el más reciente recordatorio de que el mundo ha entrado en una nueva era, que anteriormente sólo era de la ciencia ficción. La ciberguerra ya no es una fantasía del cine sino más bien un hecho del mundo real que amenaza a naciones enteras. Una nueva carrera armamentista ha comenzado, no con buques de guerra, aviones, tanques o incluso armas nucleares, sino con ciberarmas.

Y Alemania simplemente se ha lanzado hacia adelante, en gran manera.

El 1 de abril el ejército alemán lanzó su mayor iniciativa para combatir las ciberamenazas, estableciendo una nueva sexta rama: Comando del Ciberespacio y la Información. El Comando operará en el mismo nivel del Ejército, la Fuerza Aérea y la Naval.

La ministra de Defensa Úrsula von der Leyen designó al teniente general Ludwig Leinhos para ser el primer cibergeneral de Alemania. Leinhos eventualmente liderará un equipo de 13.500 especialistas de computador, muchos de los cuales ya son empleados de la Bundeswehr en varios lugares. Ésta es una gran fuerza. El personal es cercano en número a la naval alemana.

Alemania quiere llevar este inmenso ciberejército y entrenarlo, no sólo para defenderse contra ataques como WannaCry, sino también para lanzar su propio ciberataque.

‘Más que un hito’

El 5 de abril fue el primer día en el cargo para el nuevo equipo y un gran día en la historia militar alemana. Von der Leyen lo llamó “más que un hito” para la Bundeswehr. “Esto nos pone en el nivel superior internacionalmente”, dijo ella (traducción de *Trompeta* en todo).

El periódico semanal del ejército alemán, *Bundeswehr Aktuell*, alabó el nuevo comando y dijo que con el ejército alemán “adquiere un papel pionero dentro de la OTAN”.

La ministra de Defensa de Alemania dice que la ciberseguridad es crucial. Se estima que más del 80 por ciento de los nuevos desarrollos militares relevantes están ahora tomando lugar en la ciberarena, y dice que la mayoría de los conflictos hoy se combaten —en parte o completamente— en el ciberespacio.

En tan sólo las primeras nueve semanas del año, 284.000 ataques fueron dirigidos a los computadores de la Bundeswehr.

Alemania también está creando un centro de ciberinvestigación en la Universidad de la Bundeswehr en Múnich. Este centro de innovación cibernética pretende combinar los recursos de la Bundeswehr con el ingenio de emprendedores empresariales del sector privado. En 2016, la Bundeswehr contrató un 60 por ciento más de científicos informáticos que lo que contrató en 2015, gracias en gran parte a las exitosas campañas de relaciones públicas y subsidios generosos. Si esta tendencia continua, la obtención de personal calificado será un problema del pasado.

La mejor defensa: una buena ofensiva

Como cualquier otro tipo de guerra, la ofensiva es la mejor defensa. La única forma de eliminar completamente la amenaza de ciberataque es eliminar la fuente.

“Si las redes militares alemanas llegan a ser atacadas, entonces podremos defendernos” dijo von der Leyen en el lanzamiento de la nueva instalación. “Tan pronto como un ataque ponga en peligro la disponibilidad funcional y operacional de las fuerzas de combate, nosotros podremos responder con medidas ofensivas”.

La secretaria adjunta de Defensa Katrin Suder describió parte de la misión extranjera del Comando del Ciberespacio y la Información, como monitorear, perturbar y aislar las comunicaciones de los oponentes.

El nuevo equipo tendrá los medios tecnológicos y entrenamiento para conducir estos golpes ofensivos, pero el fundamento legal aún necesita aclaración. En una entrevista con *Die Welt* publicada el 16 de abril, von der Leyen indicó que, según la Ley Fundamental Alemana (Constitución), a la Bundeswehr le era permitido contraatacar cuando el ejército mismo estuviera bajo ataque directo. Ella dijo que lo mismo es cierto en el ciberespacio. Pero la situación es diferente cuando el Estado alemán es atacado. Si hay un ataque en el Bundestag, por ejemplo, von der Leyen quiere que el ejército sea capaz de contraatacar. Dado que las cibercompetencias fueron desarrolladas mucho después de que el fundamento legal fuera formulado, las cortes alemanas tendrán que clarificar hasta que punto el equipo puede usar sus capacidades ofensivas.

Una era de post disuasión

Independientemente de la legalidad, Alemania está construyendo las competencias para lanzar ciberataques en una era donde nosotros hasta ahora estamos empezando a ver el poder potencial de tales ataques. Los líderes están comparando la fuerza potencial de las ciberarmas con las armas nucleares. En 2013, el senador estadounidense John Kerry llamó a las cibertecnologías, “el equivalente de las armas nucleares del siglo 21”.

Una nación ya no necesita temer a las armas nucleares de su oponente si ésta puede usar la ciber-guerra para paralizar la habilidad de lanzar estas armas. La nación con cibertecnología suficientemente superior podría congelar la infraestructura de su oponente e inmovilizar su habilidad para ir a la guerra.

Tan sólo hace unas décadas, Alemania era la más grande amenaza de la paz mundial. Hoy está comenzando a desarrollar poderosa tecnología que podría plantear una mayor amenaza, sin embargo, el mundo no se preocupa.

La economía y ejército estadounidenses confían poderosamente en la exactitud de los tipos de sistemas de información que pueden ser explotados por ciberataques. Alguien pensaría que EE UU haría todo lo posible por mantenerse a la vanguardia en la carrera para que así nadie pudiera explotar su debilidad. Pero en la realidad, EE UU de hecho está instando al ejército alemán para ponerse al día. Washington ha alentado a Alemania duplicar su presupuesto militar y ha mejorado las armas nucleares que tiene estacionadas en Alemania.

El mundo se sorprendería de ver a Alemania repentinamente entrar en la carrera armamentista nuclear; sin embargo, ha avanzado dramáticamente en otra carrera amenazante, cuyo ganador podría tomar control sobre su oponente sin lanzar un solo misil ni dejar caer una sola bomba.

Nadie va a la batalla

¿Cómo sería una guerra cuando una nación como la estadounidense se encuentra bajo ataque y llama a su ejército para ir a la guerra —pero ni una embarcación, avión o tanque hace ningún movimiento?

La Biblia describe exactamente este escenario. El editor en jefe de *Trompeta*, Gerald Flurry se refirió a esa descripción en 2005: “Creo que una clave que la profecía bíblica del tiempo del fin podría ser cumplida a través de (...) ciberterrorismo...: ‘Tocarán trompeta, y prepararán todas las cosas, y no habrá quien vaya a la batalla; porque mi ira está sobre toda la multitud’ (Ezequiel 7:14). La trompeta de guerra tiene que sonar en Israel —principalmente EE UU y Gran Bretaña. (...) Pareciera que todos esperan que nuestro pueblo vaya a la batalla, ¡pero la más grande tragedia imaginable ocurre! Nadie va a la batalla, ¡aunque la trompeta es tocada! ¿Será esto por causa del terrorismo cibernético?” (*Trumpet*, mayo de 2005).

La tecnología finalmente se ha emparejado con una profecía que fue registrada hace más de 2.000 años.

Las amenazas son reales, y cualquiera puede reconocerlas. Pero, aparentemente se han olvidado lo que sucedió en dos guerras mundiales; el mundo parece despreocupado acerca de los avances alemanes en guerra cibernética. Esto ciertamente prueba ser un error de cálculo crítico. Mientras la tecnología nos lleva hacia un futuro incierto de nuevas dimensiones de hacer la guerra, Alemania se posiciona para estar en la vanguardia. ■

Trompeta Boletín



La próxima guerra civil de Estados Unidos

Pero los estadounidenses no saben por qué viene.

POR GERALD FLURBY

Después que los estadounidenses eligieron un nuevo presidente el 8 de noviembre, sus apasionados reaccionaron con ferocidad. ¿Sus agresivos discursos son más peligrosos de lo que ni aun ellos se dan cuenta?

[Leer el resto del artículo](#)

Trompeta Boletín

Manténgase informado e inscribese para recibir nuestro boletín.