Armas inteligentes, sistemas de telecomunicaciones, ciberguerra a través de la Red y supersoldados mejorados para ser más fuertes y letales serán parte del arsenal bélico que luchará en la primera línea de combate en los años venideros.

Las ciberguerras del siglo XXI

Fernando Cohnen, *Jefe de Prensa del COITT*

Son más diestros que los humanos a la hora de establecer el blanco adecuado. Soportan cualquier tipo de clima. No se cansan y no requieren alimentos. Son capaces de emboscarse y, los más desarrollados, pueden volar, improvisar sus movimientos y bombardear con precisión los puntos neurálgicos del enemigo. Son los robots que acompañarán a los soldados en las guerras del siglo XXI. A mediados de siglo, los mandos seguirán siendo militares de carrera, pero el trabajo sucio lo realizarán los robots.

Aunque esos escenarios bélicos nos parecen sacados de relatos de ciencia ficción, como los que muestran «Terminator» o «La guerra de las galaxias», algunos ya son reales. La primera generación de estos complejos ingenios militares combate ahora mismo en primera línea de batalla en Afganistán. Estados Unidos cuenta con miles de vehículos terrestres robotizados así como con cientos de aviones aéreos sin piloto.

Entre ellos, el pequeño Raven, que puede ser lanzado con la mano, o el gigantesco Global Hawk, un aeroplano espía de 13 metros de longitud y 35 metros de envergadura que puede volar a gran altitud durante más de 15 horas. Los

más mortíferos son los aviones teledirigidos Predator y Reaper, que van armados con misiles Hellfire de alta precisión. El Ejército estadounidense los ha utilizado para efectuar misiones de fuego real contra posiciones talibanes en el noroeste de Pakistán.

El primer capítulo de la ciberguerra del siglo XXI hay que buscarlo en enero de 1991, cuando comenzó el primer conflicto armado contra Irak. Hace casi veinte años, en las ardientes arenas del desierto, hicieron aparición unos nuevos ingenios tecnológicos que anunciaron cómo serán los conflictos bélicos del futuro. En aquel entonces, Saddam Hussein desplegó sus ejércitos de forma clásica y masiva, escalón tras escalón de soldados y blindados.

El líder iraquí quería causar un gran número de bajas al enemigo y lograr que las televisiones de todo el mundo mostraran miles de féretros llegando a los aeropuertos estadounidenses, provocando la desmoralización de la opinión pública americana y europea. De esa forma, Saddam podría quedarse de forma indefinida en Kuwait y explotar a placer sus ricos pozos petrolíferos. Pero el resultado fue el contrario. Su estrategia se dio de bruces con la empleada por el Pentágono.

«El guerrero robot no siente miedo, ni tampoco frío ni calor. Puede trabajar en cualquier clima. Poco le importa el calor asfixiante del desierto o el frío intenso de las noches en Afganistán»

El 17 de enero de 1991, días antes de que los reactores F-117 bombardeasen Bagdad, tres helicópteros Pave Low de la Brigada de Operaciones Especiales de las Fuerzas Aéreas estadounidenses fueron la punta de lanza del primer ataque en suelo iraquí. Volando a nueve metros del suelo para no ser detectados por el enemigo, los helicópteros concentraron el fuego en las torres repetidoras de microondas, centrales telefónicas, nódulos de fibra óptica y cruces de cables coaxiales del enemigo.

Aquella incursión dejó a ciegas a los iraquíes y abrió una vía segura para los centenares de aviones que horas después destruirían el arsenal bélico de Saddam. En un abrir y cerrar de ojos, los mandos iraquíes dejaron de recibir información sobre la ofensiva estadounidense. Tras efectuar bombardeos tradicionales sobre los fortines iraquíes, las fuerzas estadounidenses lanzaron misiles Tomahawks y bombas guiadas por láser para alcanzar objetivos precisos en Bagdad.

En aquella guerra se emplearon los aviones de información AWACS, repletos de radares, equipos de comunicación y detectores que localizaron aviones o misiles enemigos, y los aviones J-STARS (sistema conjunto de radar de vigilancia y ataque), que exploraron el suelo para analizar cada movimiento del enemigo. Gracias a esa tecnología, los americanos lograron destruir el enorme, aunque anticuado, arsenal iraquí.

Hacia el final de la «Tormenta del Desierto», nombre que se le dio a la campaña militar contra Saddam, había en la zona de combate más de tres mil ordenadores conectados con otros ubicados en Estados Unidos. Casi todas las funciones de los americanos estuvieron automatizadas. En los niveles superiores de mando, los ordenadores analizaron las formaciones y los movimientos de enemigo. Se hicieron miles de simulaciones de posibles ataques, eligiéndose los más adecuados en cada momento. El ejército iraquí, que estaba muy lejos de poder manejar unas herramientas bélicas tan complejas, se derrumbó en pocas semanas.

En la «Tormenta del desierto» hubo mucha innovación. El coronel Alan Campen aseguró que antes de cruzar la frontera de Arabia Saudí, el 24 de febrero de 1991, el ejército de choque estadounidense disfrutaba de una extensa red de ordenadores que les facilitaba la información necesaria para salir airosos en los primeros ataques. «Seis meses antes no existía aquella red de ordenadores, fue improvisada en pocos meses», recuerda Campen. Los ingenieros y técnicos del ejército tuvieron luz verde del Alto Mando para tomar decisiones y tener iniciativa. Y los resultados fueron excelentes.

Los anticuados carros de combate iraquíes poco pudieron hacer contra los modernos M-1 estadounidenses, que podían disparar sin detenerse. Sus visores nocturnos, los ordenadores que corregían automáticamente los efectos del calor y otras variables, como la velocidad del viento, hicieron posible que las tripulaciones de los carros de combate lograsen acertar en el blanco nueve de cada diez veces. Algunos tanquistas americanos aseguraron que era como disparar con rayos láser de alta precisión a unas viejas dianas en una barraca de feria.

Las llamadas «armas inteligentes» de los estadounidenses fueron vitales en la guerra del Golfo. Sin embargo, algunas de esas armas fallaron de forma estrepitosa, causando miles de víctimas civiles. Sin embargo, a pesar de algunos errores, aquel arsenal mortífero fue el primer capítulo de la guerra digital del futuro. Un escenario bélico en el que tendrán gran protagonismo los robots, los aviones sin tripulantes, las telecomunicaciones y la informática. Los ejércitos de mañana utilizarán armas inteligentes capaces de detectar sonidos, calor, emisiones de radar y cualquier tipo de señales electrónicas. Serán instrumentos bélicos autónomos que localizarán y exterminarán los objetivos enemigos.

Pero no sólo mejorará el armamento. Los soldados del siglo XXI tendrán que utilizar mucho más su cerebro. Vestidos con uniformes antibalas, los nuevos guerreros portarán pequeños ordenadores, instrumentos de telecomunicaciones móviles y armas complejas de tiro casi infalible. Tendrán que ser soldados que sepan tolerar la ambigüedad, asumir la iniciativa, improvisar en todo momento e imponer su propio juicio. Su adiestramiento será muy completo y distará mucho de los valores militares que ahora se inculcan en algunos cuarteles: machismo, fuerza bruta y violencia ciega. Al menos, eso es lo que prevén los expertos.

En su libro «Las guerras del futuro», Alvin Toffler recuerda un seminario sobre estrategias de defensa que se celebró hace años en Estados Unidos y al que asistieron empresarios relacionados con la industria armamentista. Estos preguntaron al coronel Michael Simpson, del

Mando de Operaciones Especiales del Ejército de Estados Unidos, cuáles iban a ser las futuras necesidades en el campo bélico. Simpson respondió que sería importante desarrollar vehículos especiales para la nieve y el hielo.

Ante la insistencia de los empresarios, el coronel estadounidense aseguró que el Ejército iba a requerir generadores ultraligeros, cámaras electrónicas, tejidos de camuflaje que cambien de tonalidad según las necesidades del terreno, sistemas de traducción oral automática y equipos de radio ligeros que cuenten con una unidad de localización global y medios de cifrado y descifrado. Otro militar recordó la necesidad de diseñar un avión de despegue y aterrizaje en vertical que tuviera una capacidad de vuelo de unos dos mil kilómetros. Y lo cierto es que más de una década después de aquellas peticiones de tecnología militar, algunas ya son operativas en el Ejército estadounidense.

El caza para los próximos años es el Lockheed – Martín F-22 Raptor, que ya convive en la Fuerza Aérea estadounidense con aviones y bombarderos casi indetectables, los famosos «stealth» (sigilosos), como el F-117 y el ala volante Northrop B-2. A ellos se añaden los aviones sin piloto, controlados a distancia, que ya han participado en operaciones bélicas en Afganistán y el noroeste de Pakistán. Se utilizan preferentemente para misiones de reconocimiento táctico y estratégico y en misiones de ataque de mucha precisión.

«Barack Obama ha llegado a comparar los efectos de un ataque cibernético con los que tendría un ataque nuclear o bacteriológico»

Estos aviones, llamados UCAV (Unmanned combat air vehicle, vehículo de combate no tripulado), como el sistema experimental X-45 A, pueden llevar a cabo misiones de supresión de defensas aéreas enemigas, las más peligrosas de la guerra moderna. Al no ir tripulados, los UCAV evitan bajas humanas y reducen los costes, ya que no es preciso entrenar durante meses a tripulantes específicos para misiones tan complejas y arriesgadas. Su capacidad de maniobra, imposible para un avión con piloto a bordo, les permite sobrevivir en un entorno de defensa con alta densidad de fuego enemigo.

Por lo que se refiere a vehículos terrestres, el Ejército estadounidense ya utiliza un robot llamado «Sword» (espada) que carga ametralladoras M240 y M249, cuatro cámaras con zoom y binoculares con visión nocturna. Los ingenieros de la empresa Foster-Miller se han inspirado en las peticiones de los propios soldados americanos, hartos de jugarse el pellejo cuando tienen que inspeccionar

cuevas y refugios que pueden albergar minas o explosivos.

Este robot no siente miedo, ni tampoco frío ni calor. Pueden trabajar en cualquier clima. Poco le importa el calor asfixiante del desierto o el frío intenso de las noches en Afganistán. Es un soldado inmune al desaliento. Tiene una autonomía de cuatro horas gracias a las baterías de litio que le alimentan. De momento, funciona con control remoto que sólo opera a una distancia máxima de 800 metros. Pero los ingenieros ya trabajan en un sistema que pueda incrementar esa distancia.

Son los primeros autómatas terrestres que disparan al enemigo. A estos robots «Sword» se unirán otros ingenios, como pequeños tanques inteligentes que no necesitarán conductor ni artillero, ambulancias autónomas, bombarderos sin piloto y minas inteligentes que se desplazarán por el campo de batalla y se activarán cuando encuentren objetivos a su alcance. En el futuro, un avión nodriza automático lanzará cientos de robots que, al igual que un ejército de insectos, se desplegarán por el campo de batalla en movimientos coordinados y efectuando asaltos mortíferos a las líneas enemigas.

Pero la herramienta militar del futuro más espectacular será el propio soldado. Al menos, eso es lo que pretenden algunos expertos estadounidenses. Su objetivo sería crear una especie de biorrobot capaz de funcionar a pleno rendimiento las veinticuatro horas del día. La Agencia para investigaciones de Proyectos Avanzados en Defensa (DARPA) es la encargada de desarrollar este inquietante guerrero del siglo XXI. Esta agencia patrocina docenas de proyectos para aumentar la resistencia de los soldados. Combatientes capaces de no dormir durante horas, que puedan nutrirse con alimentos impensables y con un desarrollo celular que aumente su fuerza.

«Estos aviones robóticos UCAV pueden llevar a cabo misiones de supresión de defensas aéreas enemigas, las más peligrosas de la guerra moderna»

El mando de todas las operaciones se encontrará lejos, en el interior de un bunker. Allí, miles de ordenadores, analistas y altos mandos analizarán los datos que recojan los robots y los aviones AWAC. Paradójicamente, esa red de ordenadores que simula y procesa toda la información es el talón de Aquiles de la guerra del siglo XXI. ¿Cómo proteger ese complejo sistema informático de los ataques cibernéticos del enemigo? Algunos analistas occidentales temen que se pueda producir un «Pearl Harbor» digital.

Barack Obama ha llegado a comparar los efectos de un ataque cibernético con los que tendría un ataque nuclear o bacteriológico. De hecho, Washington ya ha creado un nuevo cargo que coordina las estrategias de defensa y ataque cibernéticos. El pasado 22 de diciembre, la Casa Blanca nombró a Howard Schmidt coordinador nacional de ciberseguridad. La creciente oleada de asaltos a las páginas Web gubernamentales ha acelerado el nombramiento de Schmidt.

El problema de los ciberataques no sólo afecta a Estados Unidos. En 2007, las autoridades de Estonia decidieron retirar de la capital una estatua que repre-

sentaba al soldado soviético. Según afirmó Tallin, el monumento fue erigido en 1947, fecha en la que el país báltico fue ocupado por la Unión Soviética. Por su parte, los rusos aseguraron que la estatua recordaba a los héroes que lucharon contra los nazis. Días después de ser retirada, Estonia comenzó a sufrir un ciberataque ruso que bloqueó sus sitios oficiales en Internet. Los ciberpiratas secuestraron sus páginas Web y las redirigieron hacia sitios de propaganda rusa.

El ministro de Defensa estonio y responsable de la seguridad informática del país, Mijaíl Tammet, señaló que se trataba de un ataque político ordenado por Moscú, aunque las autoridades rusas habían declarado que no eran responsables de los problemas que atravesaban las páginas Web estonias. El bloqueo afectó a páginas gubernamentales, la del propio presidente del país y a otros sitios gubernamentales, causando el colapso informático en Estonia, un país que ingresó en la Unión Europea en 2004. La situación fue tan grave que tuvo que intervenir la OTAN.

Los ejércitos de Estados Unidos y Europa se toman muy en serio los ciberataques, capaces de anular las comunicaciones, los transportes y la energía de una nación. En España, la Sección de Seguridad de la Información CIS del Estado Mayor es la que sigue de cerca la evolución de esta nueva arma estratégica. La componen ingenieros militares en telecomunicaciones e informática e ingenieros civiles de la empresa pública ISDEFE especializados en seguridad. Estos expertos en ciberguerra participan en ejercicios militares organizados por el Departamento de Defensa de Estados Unidos.

Lejos de ser un escenario de ciencia ficción, los ataques a través de Internet son muy reales. Expertos estadounidenses aseguran en un informe reciente que China ha incrementado sus ataques de «ciberespionaje» contra las direcciones y archivos en Red de su Defensa. En su opinión, Pekín estaría preparando un comando de *hackers* para paralizar las capacidades financieras, de comunicación y militares de su principal enemigo.

Según estos expertos, China pretendería la paralización de las capacidades financieras, militares y de comunicación de Estados Unidos o de cualquier otra nación enemiga en caso de conflicto bélico. Los militares chinos considerarían que esta nueva estrategia ofensiva sería crítica para tomar la iniciativa en el primer estadio de una guerra. Larry M. Wortzel, autor del informe sobre el Colegio de Guerra del Ejército de Estados Unidos, aseguró hace dos años que los continuos ciberataques chinos a los sistemas de defensa estadounidenses deberían hacer reflexionar al Pentágono.

«Muchos manuales militares chinos identifican a Estados Unidos como el país con el que probablemente irán a la guerra. Se están moviendo muy rápidamente para dominar esta nueva forma de guerra», señaló Wortzel. Sólo cabe esperar que estos juegos de guerra sean exactamente eso: juegos de guerra en el tapete de los altos Mandos y que limiten su radio de acción a un escenario bélico virtual entre las dos grandes potencias.