ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

La criptografía como centro de gravedad del campo de batalla del siglo XXI

Rubén García Servert)
Academia de las Artes y las Ciencias Militares
Sección Futuro de las Operaciones Militares
Marta I. García Cid (Colaboradora)

21 de septiembre de 2024

Hay una novedad común a todos los programas actuales de desarrollo de armamento, la insistencia en tecnologías diseñadas para operar en un campo de batalla hiperconectado, en el que el elemento clave es el dato. El dato estará accesible a todas las fuerzas empeñadas en el combate. Al mismo tiempo, se insiste en el diferencial tecnológico como el paradigma de análisis que asegura el triunfo en el campo de batalla.

La cuestión que queremos plantear en esta comunicación es relativamente sencilla de abordar, pero no tan fácil de responder de forma coherente. ¿Basta la superioridad tecnológica para asegurar un resultado favorable a nuestros intereses en el conflicto? ¿Hasta qué punto la tecnología puede suponer una vulnerabilidad si no está desarrollada con criterios de seguridad?

Se abre aquí una doble polémica que relativiza el paradigma de la ventaja tecnológica.

Una primera cuestión es la dimensión humana del conflicto, de los combatientes, en sus aspectos formativos y éticos. Un ejército muy tecnológico con soldados sin voluntad de vencer, difícilmente ganará la guerra.

Ha aparecido en este entorno humano, además, un aspecto adicional, determinante, el del combate en el Dominio cognitivo. Estamos comprobando cómo unas Fuerzas Armadas sin apoyo de su sociedad, tampoco pueden ganar la guerra, abriéndose aquí una vulnerabilidad ante la posibilidad de que el enemigo sea capaz de influir sobre la opinión pública, cuestión relativamente sencilla en un mundo globalizado e hiperconectado.

En esta Academia hay profusa documentación publicada, dedicada a esta batalla en el dominio cognitivo que, sin lugar a dudas, hará ganar o perder guerras en el futuro. Y ello con independencia de los resultados en el campo de batalla, tal y como estamos viendo en los conflictos actuales.

Reconociendo la importancia de los dos temas anteriores, nos proponemos reflexionar en esta comunicación sobre un tercer aspecto que pone en cuestión el peso determinante de la diferencia tecnológica para asegurar el triunfo en la guerra. Se trata del imprescindible equilibrio entre tecnología y seguridad, que pasa a ser elemento capital en el desarrollo de los nuevos sistemas de armas hoy en día. Así lo demuestran las vulnerabilidades en el ámbito ciber, que son mayores cuanto más dependientes sean las fuerzas propias de las tecnologías de la información y las comunicaciones.

Antes de seguir adelante y abordar la cuestión central de esta comunicación, se necesita expresar un último aviso, que nunca debiera ser olvidado. Hoy como ayer y como siempre, el resultado de una guerra no convencional es incierto, lo cual es una llamada más de atención sobre la locura que representa el culto a la tecnología como el eje central del planeamiento de operaciones.

Recuérdese, y forma parte de la propia peripecia personal, que Afganistán se perdió frente a combatientes insurgentes con tácticas de guerrilla, siguiendo un esquema que ya quedó patente en Vietnam. Hoy mismo es incierto el resultado de una guerra urbana en Gaza, en un enfrentamiento en el que la superioridad tecnológica de Israel es apabullante.

Con todo lo anterior en mente, afrontemos ahora una inquietud sin respuesta clara, más allá de desarrollos en marcha, que no siempre plantean las interrogantes en toda su extensión, ni responden a dudas razonables.

En el marco del Programa del Avión de Combate de Nueva Generación (NGWS en sus siglas en inglés), que desarrollan hoy las industrias de Francia, Alemania y

España, la componente de I+D es prioritaria. Se trata de un programa tecnológico que pondrá en el campo de batalla en 2040 un caza de 6º generación, que en realidad es un sistema de sistemas. De hecho, más que un caza, se está desarrollando un sistema de mando y control llamado a revolucionar el combate aéreo en las próximas décadas. El caza estará interconectado en tiempo real con sistemas aéreos no tripulados que le acompañan y con los sistemas terrestres y navales, en un campo de batalla global, en el que el dato se comparte en tiempo real entre todos los medios empeñados en el combate.

Dentro de este programa, se han definido siete pilares, uno de los cuales consiste en el desarrollo y puesta en servicio de una nube de combate, donde residirán en tiempo real los datos procedentes de todos los sensores que operan en un determinado campo de batalla, permitiendo que dichos datos estén accesibles a todos los medios empeñados en el combate.

Se abre así una nueva era, la que posiciona al dato en el centro de gravedad del combate, y, a partir de ahí, imagina un mando y control distribuido.

Nos adentramos, hoy más que nunca, como comentaba al principio de esta comunicación en un paradigma de culto a la tecnología, que se establece como dogma indiscutible a la hora de diseñar nuevas capacidades, pero también en la conformación de tácticas militares, lo cual obliga a una reflexión de fondo. ¿Estamos haciendo lo correcto o corremos hacia adelante sin meditar sobre los riesgos implícitos en estos desarrollos?

Hay un necesario equilibrio entre la necesidad operativa, que tenga presente las posibles acciones del enemigo, y el desarrollo tecnológico. Dicho con otras palabras, una interacción permanente entre el ingeniero que desarrolla el sistema y el operador con experiencia, que puede plantear las dudas razonables a cada paso de dicho desarrollo.

No se trata de cuestionar en esta comunicación las ventajas iniciales de la superioridad tecnológica en el enfrentamiento, sino lo absoluto de dicha superioridad. Propongo reflexionar sobre la vulnerabilidad que representan las nuevas tecnologías ante las actuaciones de un enemigo de primer nivel, particularmente en los campos ciber y de destrucción de elementos críticos de nuestros sistemas de combate.

Sigue subsistiendo la idea peligrosa de que todo posible adversario será siempre muy inferior tecnológicamente, de forma que nuestra tecnología permanecerá siempre fuera del alcance de sus acciones.

Ejemplo de lo anterior es la hiperdependencia operativa de los sistemas espaciales, que ha obligado conceptualmente al establecimiento de un Dominio espacial de las operaciones. La creación *per se* de este Dominio y las medidas de protección de los medios espaciales propios, no ha traído consigo algo mucho más elemental y previo, imaginar la conducción de operaciones sin poder recurrir a los medios espaciales, lo que obliga a tácticas y procedimientos alternativos para los que hemos ido perdiendo entrenamiento.

En el fondo, la reflexión que se propone es profunda y compleja. Hay que imaginar circunstancias en las que es imprescindible la continuidad de las operaciones con una tecnología degradada. Se trata de entrenar, como hasta hace poco se ha hecho, en entornos en los que nuestros sistemas de armas pueden tener que operar sin mucha de su sofisticación técnica.

Hace un mes, en una de las sesiones conceptuales sobre el sistema NGWS surgió la pregunta clave. ¿Qué pasaría si la interconexión de datos en tiempo real se interrumpiese, las comunicaciones estuvieran perturbadas o los links degradados? No hay una respuesta clara, más allá de imaginar métodos para que esto no ocurra.

Consideramos que es de sentido común una aproximación simultánea de doble entrada que implique a la vez blindar nuestros sistemas y entrenar de forma que podamos operar sin disponer de ellos. Algo de esto se está imaginando cuando se habla de la operación de los sistemas en entornos *Anti Acces Area Denial A2AD*, que en el fondo trata de sobrepasar defensas antiaéreas de alta intensidad. A mi juicio, no es suficiente.

Lo que se propone en estas líneas va mucho más allá. Hay que poner en práctica modos de empleo y entrenamiento que nos permitan operar sin nuestra tecnología de última generación y ello por dos razones plausibles: degradación por la acción del enemigo y simple colapso técnico, todo ello con un aviso adicional. Las redundancias son importantes, pero en el fondo trasladan una mentalidad de paz siendo, por ello, insuficientes. Necesitamos prepararnos para operar frente a una acción de un enemigo que, por definición, puede ser tan sorprendente y tecnológica como la nuestra.

Pues bien, de todo lo anterior, hay una vulnerabilidad en la arquitectura de los futuros sistemas de armas que considero debería repensarse desde la óptica de la seguridad.

No se cuestiona que las tecnologías en desarrollo y las tácticas y procedimientos que se valdrán de ellas van a representar un cambio profundo en la forma de combatir, sin duda. Estamos ante un cambio de era en el combate que, como he comentado, vendrá marcado por la tecnología.

Sin embargo, hay factores que, a nuestro juicio, no están siendo debidamente considerados en estos desarrollos. La cuestión, de forma simplificada, sería preguntarse hasta qué punto la vulnerabilidad de la hiperconectividad en general, y del acceso a nuestros datos por parte del enemigo, en general y, en particular, en el caso de una nube de combate, no pueden ser un factor que aconseje limitar estos desarrollos, o al menos obligue a un replanteamiento de fondo de los requisitos ciber y criptográficos.

Hemos visto algunas reflexiones al respecto, con propuestas concretas para intentar blindar los sistemas; pero ningún análisis de seguridad cuestiona estas iniciativas en su conjunto. Caminamos de una forma clara y decidida hacia la operación con nubes de combate en todos los casos, y ello pudiera no ser una buena idea en determinadas circunstancias.

El punto de partida de un análisis en términos de seguridad parece claro. Colocar todos los datos de nuestros sensores en una nube de combate agiliza nuestra actuación y mejora la efectividad y conciencia situacional de nuestros combatientes, pero nos puede dejar a merced del adversario.

Ya hemos comentado la necesidad de no acostumbrar a nuestros soldados a operar siempre con todos los datos a su alcance. Viene ahora una cuestión todavía más inquietante. ¿Cómo asegurar que el adversario no accede al núcleo de nuestros datos y los utiliza en beneficio propio? La respuesta tiene mucho que ver con una criptografía que tendrá que ser revolucionaria y con unos operadores muy estrictos en el manejo de los sistemas interconectados.

Este requisito de una criptografía de nuevo cuño es mucho más complejo en un campo de batalla que será, en un futuro predecible, cuántico y por tanto, vulnerable a los métodos y procedimientos actuales. Da la sensación que estamos ante un requisito tecnológico que debiera tener la máxima prioridad antes siquiera de imaginar que los medios de combate puedan operar en red.

Esta nueva criptografía no puede ser, esta es mi llamada de atención, de un desarrollo tecnológico más de los variados que tenemos en marcha, en particular en el campo de las tecnologías disruptivas. La criptografía es, en nuestra opinión, el núcleo central e imprescindible sobre el que volcar todas nuestras capacidades de investigación y desarrollo, obligados por estos nuevos sistemas de combate.

El punto de partida es preocupante. Nuestros sistemas actuales no van a resistir frente a tecnologías cuánticas. Estamos en los inicios del desarrollo de sistemas alternativos… También el adversario. Pero, ¿dónde estamos en esta materia?

Pues bien, si todo lo anterior es cierto, analicemos a continuación y de una manera resumida, cuál es la situación actual en esta materia.

Criptografía hoy frente al reto cuántico, un punto de situación

La criptografía es un arte que existe prácticamente desde el surgimiento de la escritura, y su finalidad es evitar que la información transmitida sea leída por personas no autorizadas.

Con el paso de los años, los métodos para enviar información de forma segura se han vuelto cada vez más sofisticados gracias a los avances tecnológicos en el campo de las comunicaciones y, especialmente, con la aparición de los sistemas informáticos. La principal diferencia es la aparición o concepción del ciberespacio como un nuevo Dominio en el que actualmente viaja la información.

Sin embargo, al igual que los métodos criptográficos han evolucionado y se han beneficiado de las nuevas tecnologías para proporcionar cada vez mayor seguridad a la información, estos avances han traído consigo nuevas formas de atacar la información transmitida por actores maliciosos. Así, históricamente, las soluciones criptográficas han ido evolucionando a medida que aparecían nuevas formas de vulnerarlas, y viceversa.

Para protegerse de estas amenazas, se utilizan los siguientes dos paradigmas criptográficos: criptografía simétrica, en la que las partes implicadas en el proceso comparten una misma clave secreta que podrán utilizar para, por ejemplo, cifrar la información; y criptografía asimétrica, donde cada una de las partes implicadas dispone de un par de claves, una de las cuales será pública y la otra privada, y permanecerá secreta.

La llegada del ordenador cuántico supone un cambio de paradigma en la computación que ha abierto todo un panorama de retos y oportunidades para las próximas décadas. En concreto, dado el salto de rendimiento que supondrán los ordenadores cuánticos, se espera un gran impulso en áreas como la simulación molecular, la ciencia de los materiales o la biología.

Sin embargo, en áreas tecnológicas como la inteligencia artificial, la ciberseguridad o las criptomonedas, estas nuevas capacidades pueden suponer una nueva amenaza. Peter Shor publicó un algoritmo que, implementado en un ordenador cuántico es capaz de factorizar números enteros grandes en tiempo polinomial, haciendo vulnerable la criptografía asimétrica utilizada en las comunicaciones actuales, como RSA o ECC.

Además, el algoritmo de búsqueda cuántica de Grover es cuadráticamente más rápido que cualquier algoritmo clásico equivalente. En este caso, el algoritmo de Grover no viola directamente un mecanismo criptográfico como lo hace el de Shor, pero es capaz de reducir a la mitad la seguridad de los sistemas de criptografía simétrica.

En vista de la amenaza del ordenador cuántico y la creciente necesidad de proteger los sistemas criptográficos, se están invirtiendo grandes esfuerzos en dos tipos de soluciones para hacer un sistema resistente a ataques con el algoritmo de Shor. Estos dos nuevos paradigmas son la criptografía cuántica y la criptografía post-cuántica (PQC).

Para hacer frente a esta nueva amenaza, el NIST inició en 2016 un concurso de PQC, basado en una serie de rondas competitivas para definir nuevos estándares criptográficos asimétricos basados en problemas matemáticos alternativos a los ya conocidos.

Tras varias rondas de competición se seleccionó para ser estandarizados un algoritmo de encapsulación de claves (KEM) CRYSTALS-Kyber (FIPS 203), y uno principal de firma digital (DSA) CRYSTALS-Dilithium (FIPS 204) y dos alternativos SPHINCS+ (FIPS 205) y FALCON (cuyo estándar está en desarrollo). Además de los algoritmos seleccionados para su estandarización, NIST anunció una ronda adicional del proceso con el fin de estandarizar al menos un esquema KEM más y la creación de un concurso de estandarización adicional dedicado exclusivamente a las firmas digitales.

De manera paralela, nos encontramos con la criptografía cuántica. Las propiedades cuánticas de los sistemas físicos se conocen desde hace poco más de un siglo. Sin embargo, su control y manipulación para el desarrollo de aplicaciones tecnológicas es más reciente y aún no se ha descubierto todo su potencial. En las últimas dos décadas se ha propuesto y promovido el uso de estos sistemas mecánicos cuánticos para aplicaciones informáticas, pero también en el desarrollo de nuevos sensores, comunicaciones y aplicaciones criptográficas.

A lo largo de los años se han propuesto una serie de primitivas criptográficas. Hoy en día, la Distribución de Claves Cuánticas (QKD) es la primitiva criptográfica más analizada, desarrollada e implementada. Pero también se han propuesto primitivas que van más allá de la distribución de claves, como las firmas digitales cuánticas o protocolos de conocimiento cero cuánticos, entre otros. La primitiva QKD permite la distribución de claves simétricas secretas completamente aleatorias entre dos nodos de una red. Estas claves pueden ser utilizadas posteriormente, por ejemplo, para cifrar información mediante un mecanismo de cifrado simétrico como AES.

El proceso por el que se establecen estas claves no depende de ningún algoritmo o hipótesis matemática, y se ha demostrado que son claves seguras para la información (ITS), tal y como defienden los teóricos del campo. Sin embargo, este tipo de sistemas presentan vulnerabilidades a la hora de ser implementados, las cuales se han convertido en el foco de investigación para muchos expertos en la materia.

Las distintas agencias de seguridad nacional y organismos tan relevantes como la OTAN han seguido de cerca la sucesión de rondas del proceso de estandarización de algoritmos postcuánticos del NIST. También han seguido el avance de los proyectos de comunicaciones cuánticas, ayudando a identificar los retos que presentan los sistemas criptográficos cuánticos y que necesitan ser abordados por la comunidad científica e industrial.

Dado el estado actual de los nuevos estándares de PQC, estas organizaciones han hecho pública, parcial o totalmente, su visión y posicionamiento respecto a las soluciones basadas en criptografía cuántica y postcuántica.

La conclusión es que se recomienda la implementación de soluciones basadas en criptografía postcuántica para hacer frente a la amenaza del ordenador cuántico y la hibridación de PQC con algoritmos precuánticos. No obstante, se propone la continuación de las actividades de investigación relacionadas con las tecnologías cuánticas, para un posible uso de estas tecnologías a largo plazo si se resuelven los retos tecnológicos identificados para aumentar su nivel de madurez y poder llegar a lograr la certificación de los dispositivos.

Conclusiones

Parece claro que la industria y los centros de investigación son cada vez más conscientes de los problemas criptográficos que plantean los nuevos desarrollos tecnológicos.

Se esperan, en los próximos años, cuantiosas inversiones en esta materia, dado que todos los avances en conectividad dependen de sus respuestas. Sin embargo, la prioridad asignada a estas cuestiones sigue siendo limitada.

Se echa, sin embargo, de menos un alineamiento de todos los actores en la materia y una inclusión desde su origen en los requisitos de estado mayor de los nuevos sistemas de armas de esquemas que protejan de una forma adecuada nuestros datos en el campo de batalla del siglo XXI.

De igual manera, un impulso decidido nacional en estos temas parece esencial. Porque en materia de protección de datos de combate es mala idea depender de desarrollos extranjeros, aunque sea de países aliados.

Se propone una iniciativa criptográfica cuántica y postcuántica nacional, bien dotada e impulsada que permita una autonomía tecnológica y estratégica en la materia. Nuestros centros de investigación y nuestras empresas están a la altura del reto, sólo falta el impulso claro desde instancias oficiales.

Desde el punto de vista nacional convendría, sin duda, un impulso decidido por parte de la Dirección General de Armamento, que además ordene las iniciativas existentes y las agrupe. De esta manera podrían proponerse iniciativas nacionales interoperables por diseño, que se implementarían en los sistemas de mando y control de los distintos dominios de combate, que deben además federarse entre ellos.

No debería haber en esta materia, y en muchas otras, competencia entre empresas nacionales pues al final la solución adoptada debería ser única e implementada en todas nuestras capacidades.

Nos jugamos en ello la superioridad futura en el combate. ▮