CARI / CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

GRUPO DE TRABAJO SOBRE LA INSERCIÓN DE LA ARGENTINA EN EL MUNDO

1

DICIEMBRE 2016



# El campo de batalla en la actualidad*

*Por Juan Battaleme*

**"Cuando un robot "muere" no tienes que escribirle una carta a su madre"**
Anónimo, comandante de la fuerza de robots antibombas, Irak, 2007

**"La Guerra del futuro... será una guerra en la que las maquinas combatirán, no los soldados. El nuevo soldado no será un soldado sino un maquinista, no derramará su sangre, sino que transpirará en la fábrica de la muerte instalada en la línea de batalla"**
Thomas Alva Edison, 1915

En su libro "La Flota Fantasma" (Ghost Fleet) Peter Singer y August Cole, desde la ficción, construyen un probable escenario de conflagración mundial entre China y Estados Unidos el cual comienza en el espacio exterior para luego extenderse a todos los dominios geográficos y el cibernético. Como resultado de la contienda, ambos enemigos quedan bastante maltrechos y con serios problemas para recomponer su posición de poder, aunque ciertamente Estados Unidos termina la contienda un tanto mejor. Combinando conocimientos de múltiples disciplinas, la novela pone en perspectiva los cambios que se están produciendo y la velocidad de los mismos remarcando el grado de desafío que implican para los planificadores militares de las grandes potencias que dan cuenta de forma simultánea de acciones ofensivas como defensivas, articulando doctrinas militares efectivas para evitar que un desequilibro en las capacidades provea la victoria a un potencial enemigo.

El argumento que prueban ambos autores es sencillo y poderoso: dadas las condiciones tecnológicas actuales y el posicionamiento competitivo existente entre Estados Unidos y China en el Asia Pacífico, es posible una guerra limitada con consecuencias devastadoras, que no necesariamente escalaría en una guerra nuclear total. Dicho escenario está configurándose en la actualidad como resultado de las llamadas tecnologías disruptivas, las cuales se incorporan en los arsenales de ambos países junto con las doctrinas militares que se desarrollan para emplearlas. La combinación de ambas facilitaría una potencial conducta ofensiva, alterando el balance estratégico que primó durante la Guerra Fría y en la posterior unipolaridad. La beligerancia existente en el

* Este artículo fue presentado el 11 de noviembre de 2016 en la reunión del Grupo de Trabajo sobre la Inserción de la Argentina en el mundo.

CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

Uruguay 1037, piso 1°
C1016ACA
Buenos Aires
República Argentina

Tel. +5411 4811 0071
Fax +5411 4815 4742

cari@cari.org.ar
cari.org.ar

ciberespacio y la incorporación de sistemas de armas que corren sobre las tecnologías de la información está facilitando el empleo de las mismas sin tener en claro las consecuencias que ellas generan. Esta parece ser la consecuencia de la creciente tecnificación de la guerra actual, lo cual implica una creciente separación entre el hombre y lo que ellas generan, al punto tal de transformarlas en un poderoso y "real" videojuego.

La incorporación de tecnología genera diferenciales que se traducen en ventajas concretas en los asuntos internacionales, tanto económicas como militares, para quienes las detentan y las pueden explotar. Estos procesos afectan a la estructura de poder tanto doméstica como internacional, aunque no necesariamente quienes inician un ciclo de desarrollo/innovación tecnológica serán quienes saquen mayor ventaja del mismo. Pero algo resulta seguro: quienes no puedan seguirle el paso a estos cambios terminarán perdiendo posiciones de poder y, en determinadas áreas, quedarán en posiciones subordinadas. La tecnología en el campo económico y militar ayuda a la estratificación de sociedad internacional.

La ciencia ficción es la primera en dar cuenta de los cambios tecnológicos, sus impactos, las oportunidades que ofrecen y los desafíos que se presentan para el ser humano, en especial en una actividad tan socialmente humana como es la guerra. En su libro War Star: Guerra, Ciencia Ficción y Hegemonía Imperial, Bruce Franklin (2010) señala la existencia del llamado complejo industrial militar, al que le suma el político, y la literatura. Desde el Siglo XIX en adelante, los libros de ciencia ficción, junto con el género conocido como tecno-thrillers, producen tramas donde el entorno tecnológico muta, los contextos se modifican, pero la condición humana permanece inalterable.

La literatura permite generar el espacio necesario para imaginar y construir mundos a partir del paso tecnológico, cruzándolos con la inmutable condición humana, construyendo el plafón social necesario para implementar las adaptaciones necesarias que den cuenta del impacto que las alteraciones tecnológicas generan. La política canaliza las demandas existentes mediante el miedo, la necesidad, o las oportunidades que estos cambios generan. Utopía y distopía son el resultado del progreso tecnológico y de la aplicación de los ingenios que desarrollamos los seres humanos para alcanzar nuestros objetivos.

El campo militar y el económico son los primeros en sentir el impacto de las nuevas tecnologías creando presión para adaptarse a estos cambios, aunque siempre existen resistencias, límites en el entendimiento y rechazo a ciertas innovaciones. Determinados avances o innovaciones no supone linealidad ni tampoco son tan rápidos como se supone. Excepto por algunos visos de aprendizaje y tal vez de conciencia acerca de las consecuencias que tiene para la humanidad un conflicto nuclear, la cual sigue siendo el arma de mayor devastación del arsenal militar actual pero no la más moderna, siempre buscamos nuevas formas de lograr mediante la fuerza aquello que no podemos lograr mediante la vía diplomática. Robots, virus informáticos, láser, pulso electromagnético, armas de energía, ingeniería genética, entre otras, nos están ayudando de manera creativa a lograr nuestro objetivo de alcanzar nuevas formas de destruir, anular y/o dominar a otros.

Las imágenes de destrucción que encontramos en las novelas de Philip K. Dick, Ray Bradbury, o Isaac Asimov, entre otros autores de los años 50 o 60, cumplían con un doble objetivo: advertirnos de las consecuencias del progreso en determinadas áreas como la nuclear, pero al mismo tiempo promover la capacidad de defensa, evitando la configuración del peor escenario posible reafirmando los mecanismos de disuasión. A los clásicos de la literatura se les sumaban los pensadores de la Rand Corporation, como Albert Wohlstetter o Thomas Schelling, por mencionar algunos autores que en esa época se encargaban de concretar el doble objetivo antes señalado, permitiendo que la cultura popular y acción política se retroalimentaran. El resultado de ello son guerras ficticias con armas muy reales que primero se ponen en papel, algunas de ellas terminan

en obras cinematográficas de Hollywood y todas nutriendo los arsenales de los grandes poderes (1).

Si el paraguas nuclear promovía la estabilidad estratégica, las nuevas armas que se están incorporando a los arsenales modernos están empezando a resquebrajar dicha estabilidad generando la posibilidad de un primer uso que permita obtener ventajas específicas en un lugar determinado. Si la idea durante la Guerra Fría era que un conflicto no se podía ganar, la idea del presente siglo es que un conflicto puede ganarse, como consecuencia de las disrupciones que genera el ciberespacio y las alteraciones estratégicas que ello supone.

Asimismo, el rango de distopías se ha ampliado de tal manera que en nuestro catálogo de fantasías existen edificios y sociedades que en apariencia funcionan, aunque el hombre no funcione excepto como un proveedor de energía para las máquinas; mundos virtuales sumergidos en el más absoluto caos, y la desconexión del hombre con su entorno debido a la creciente mediación tecnológica existente como se presenta en series de gran repercusión como *Black Mirror* o trilogías para adolescentes como Divergente de Veronica Roth (2011) o los Juegos del Hambre de Suzanne Collins (2008) siguiendo un concepto simple pero central en la era cibernética: cuál es el limite de separación de lo real de lo virtual, y en qué medida esa virtualidad afecta nuestro mundo real, tal como lo planteaba la película *The Matrix* a fines de los años 90. Vivimos en un mundo de realidad "aumentada" y "virtual" y, si no fuera por los gráficos, las tramas que se cuentan en ellas son muy reales al igual que las situaciones que en ella se viven.

Una pequeña muestra de ello fue el ataque cibernético sobre la central nuclear de Natanz en Irán utilizando el virus informático stuxnet, conocido como Amenazas Avanzadas Persistentes (Advance Persistent Threat –APT) el cual cumplió con dos misiones militares: en primer lugar, el reconocimiento del escenario donde iba a operar y la trasmisión de la información para luego infiltrarse en el sistema entregar su carga destructiva sobre las centrifugadoras, usando el llamado ataque del hombre del medio, esto es, simulando una acción pero informando otra, por no mencionar la extensa operación de influencia política realizada por la inteligencia rusa sobre las elecciones norteamericanas, la cual, aunque fracasó, dio cuenta una vez más de los efectos reales que tiene el mundo virtual.

Suena "fácil" y según el cliché estándar actual se señala que esta nueva generación de armas son las de los países pobres o que están a disposición de cualquiera. Sin embargo la preparación para semejante acción involucró ingentes sumas de dinero, fue una operación de varias etapas llevándose a cabo mediante algoritmos que producían un daño real, pero informaba en la pantalla al operador que todo estaba bajo normal funcionamiento, provocando desconcierto en los operadores nucleares iraníes (2).

Esta breve introducción conectando ciencia ficción con realidad nos dice varias cosas acerca del campo de batalla actual la primera - claramente perceptible y rápidamente reconocible - es la hibridación tecnológica del mismo el cual involucra aquellas armas que rápidamente podemos identificar, desde un fusil hasta un sistema semiautónomo como puede ser un vehículo aéreo no tripulado (UAV).

La segunda es menos perceptible y esta directamente asociado a las tecnologías cibernéticas las cuales sirven de plafón para los desarrollos que actualmente son considerados disruptivos robótica, biotecnología, nanotecnología y la expansión del ciberespacio.

El cambio y la innovación demanda ingentes recursos monetarios, por lo tanto el tope de gama de estas armas y sus desarrollos se corresponden con los grandes poderes. La proliferación habilita mejoras, pero la creación de estos ingenios se encuentra concentrada, estructurando al sistema internacional jerárquicamente.

El asalto de Crimea, los ejercicios militares de la OTAN, la guerra de Irak, las operaciones contra ISIS, el combate a la piratería en el Índico, etc. Son entornos en los cuales operan soldados equipados con armas tanto "reales" así como "virtuales", sus comandantes toman decisiones en

tiempo real y se dirimen los distintos intereses nacionales mediante la combinación e integración de tanques, aviones, barcos, morteros y fusiles, con robots ciberespacio y satélites que buscan y eventualmente lograran, al menos con los rivales de menor peso eliminar la llamada "niebla de la guerra" (3).

Hablar del campo de batalla actual, implica una fusión entre presente y pasado en escenarios de combate donde se despliegan sistemas que son el estándar de operaciones necesarios para tener alguna oportunidad de éxito militar y eventualmente político, ya que aun en el siglo XXI la idea de que la guerra es la continuación de la política por otros medios parece no haber encontrado un concepto superador inclusive en estas épocas de ciberguerra.

Esa mixtura de componentes reales y virtuales, de armas modernas con aquellas que no lo son, hace que el mundo actual provoque numerosos problemas de planificación estratégica, de equipamiento militar y dinámicas operacionales que se acentúan de manera más acuciantes cuando además se combina una transición de poder internacional, que tiene como rasgo la rápida y creciente difusión del poder y en especial el acceso a capacidades que dan poder a actores no estatales.

Los indicadores existentes provienen del propio desarrollo tecnológico, de las potenciales fuentes de conflicto, de la imaginación humana, y de las ideas que surgen cuando nos encontramos en etapas donde la incertidumbre por el ingreso de tecnologías que aparecen como oscuras para el conjunto de la población que las opera y de las cuales somos cada vez mas dependientes y por lo tanto existen mayores vulnerables cuando aparecen las desviaciones que con ellas se realicen, ya sean porque detrás de ellas se encuentran grupos criminales, activistas o un estado tratando de explotarlas.

A ello se suma el hecho por el cual quienes desarrollan, estudian e innovan en este campo, presentan una importante brecha etaria con quienes deben regular, anticipar y legislar sobre las mismas.

Esto incide en la capacidad que tienen los desarrolladores y quienes las usan ya que depende cada vez más de técnicos que al mismo tiempo tienen la capacidad de orientar el debate y distorsionarlo al público. En términos relativos, aun cuando con el paso del tiempo esto disminuya y sus efectos se morigeren los migrantes digitales continúan dominando la escena política (4).

El campo de batalla actual ya tiene el germen del futuro, en tanto los nuevos ingenios militares se están desarrollando, en algunos casos, e instrumentado en otros ahora. Miramos las proyecciones esperables, sabiendo que ciertas tecnologías se encuentran en etapas de menor desarrollo como puede ser la nano tecnología y la biotecnología, mientras que otras como por ejemplo todo aquello relacionado con el ciberespacio y los robots están en su etapa de proliferación, cambiando de manera perceptible el rostro de la forma en la que peleamos un conflicto internacional.

En este sentido el presente trabajo se estructura en tres breves partes derivadas de los cambios que están transcurriendo en materia militar internacional.

En el plano de las ideas, la primera parte mira las modificaciones sistémicas que esto provoca. Esto es las grandes potencias y *el asentamiento de una estratificación militar* que deja un margen de maniobra muy restringido para poderes estatales menores e inclusive no estatales, aunque estos últimos hayan amplificado su capacidad de acción.

En este caso la estrategia de los grandes poderes es interconectar a estos actores en sus mosaicos o cuadriculas operativas generando un orden internacional basado en esta interconexión.

Ser aliado o socio significa conectarse con una grilla especifica en un área determinada, y salirse tiene costos crecientes. Y si bien existe la posibilidad de estar conectado a varias al mismo tiempo por el desglose que tiene la agenda de seguridad internacional, si existe un conflicto entre conectores, no quedara otra opción que ver con que conector nos quedamos.

El segundo punto de este apartado se relaciona con *la proliferación de estas tecnologías*, y el esfuerzo por limitarlas como sucedió con la tecnologías nucleares, aunque dichos esfuerzos se vean sistemáticamente vulnerados, porque las

mismas se expanden mas rápido y se encuentran relativamente mas socializadas como consecuencias de que operan en un entorno colaborativo y que pueden ser modificadas producto de la acción autorizada o no de sus creadores.

El tercer punto se relaciona con la posibilidad de que *se este terminando el período de estabilidad estratégica*, alcanzado por la disuasión nuclear. Es muy probable que estemos configurando una mente crecientemente ofensiva, por encima de la defensiva, con la consecuente desestabilización estratégica que ello conlleva.

E n el plano material, la segunda parte del trabajo tiene por objeto hablar someramente de algunas de las armas que están ya desplegadas en el campo de batalla y de aquellas las que comienzan a serlo ya que sobre ellas se están elaborando doctrinas de uso dando entre ambos la forma que tendrá el campo de batalla de los próximos años.

Pensemos que los drones aéreos aparecieron por primera vez a finales de la guerra de Vietnam probándose útiles en el campo de batalla aunque su despliegue fue limitado y resistido por los comandantes operacionales quienes no veían (5) en ese ingenio algo significativo. Después de casi treinta años comenzaron su reinado, al punto tal que Martin Van Creveld fue uno de los primero autores en señalar el eclipse del poder aéreo en especial el tripulado, gracias a su creciente presencia en el terreno (6). Junto a ellas debemos sumar aquellas que hoy se consideran como embrionarias, ya sean los cañones de pulso, los humanos mejorados ya sea con la creciente combinación humano-máquinas o los desarrollos biológicos, como la clonación y la nanotecnología.

Finalmente, la tercera parte del presente ensayo se explora las consecuencias que tiene esta transformación para la República Argentina en términos de su política de equipamiento militar (7) junto con las iniciativas existentes.

## Un escenario militar más jerárquico, proliferante e inestable estratégicamente

Uno de los conceptos estructuradores de la disciplina de las relaciones internacionales es la idea de anarquía como principio ordenador, donde la suma de las capacidades de poder, y en especial las militares, establecen el tipo de estructura en la que nos encontramos ya sea multipolar, unipolar o bipolar. Sin embargo, como consecuencia de las propias capacidades existentes, las relaciones internacionales funcionan mayormente en términos jerárquicos y, por lo tanto, limita los márgenes de maniobra a quienes no poseen recursos y amplía la de aquellos que sí los poseen.

En el plano militar esta estratificación actualmente queda plasmada entre quienes tienen capacidades militares para establecer cibercomandos, desplegar robots, conducir operaciones de vigilancia globales, desarrollar armas de energía dirigida, frente a aquellos que no tienen dicha capacidad, la tienen limitada, o la están desarrollando. El número de países que poseen ingenios nucleares es realmente reducido. De la totalidad de los países en el mundo con ejércitos, solo nueve poseen esta capacidad; eso es jerarquía.

La asimetría existente en sus múltiples formas se ve desde las capacidades militares que se despliegan hasta la forma de combatir. Aquellos que tienen y aquellos que no tienen definen la política internacional y la suerte que dichos actores pueden tener en sus interacciones. Esto significa reconocer que existen países que disponen de los medios necesarios para pelear una guerra de manera autónoma ya sea en sus espacios regionales cercanos o lejanos, regional o globalmente, combinando tanto componentes virtuales como reales, para anular las capacidades del oponente en las etapas iniciales del un conflicto. La proyección de poder tradicional hoy se agrega el ciberespacio.

Son pocos los países que pueden considerarse pares en esta situación, e inclusive entre ellos se encuentran diferencias en sus capacidades provocando limites para penetrar determinados sistemas vinculados principalmente a infraestructura que puede considerarse crítica para provocar desajustes en los sistemas defensivos del oponente. Quienes han desplegado sus fuerzas

militares en los actuales campos de batalla, en estos últimos años, reconocen la necesidad de desarrollar el entorno cibernético para que actúe como multiplicador de fuerzas. Siendo que el 80% de las armas que tienen en sus arsenales son clásicas, el mayor esfuerzo se concentra en conectarlas entre sí, mejorar sus capacidades al integrarlas, pero no son ciertamente distintas en su funcionalidad de sus predecesoras. Una bomba sigue siéndolo excepto porque ahora además procesa datos y corrige su rumbo.

Integrar los sistemas de armas existentes para que sean parte de un musculo militar efectivo, al tiempo que se desarrollan nuevas capacidades necesarias a los efectos de explotar los espacios comunes existentes en la estrategia militar y obtener ventajas en las llamadas zonas en disputa ya sean el espacio terrestre urbano, las zonas costeras y ribereñas, es el objetivo militar de las potencias tanto aquellas que quieren mantener el status quo como también las que ascienden y actúan como poderes revisionistas.

Las ventajas que otorga el espacio común en tanto mar, aire y espacio ultraterrestre son integradas en las estrategias militares de un grupo limitado de países, donde la preponderancia norteamericana todavía resulta evidente para todos aquellos que planifican un enfrentamiento con esta potencia en los próximos años. Al ser parte de la estrategia, la implementación doctrinaria se vuelve importe. Por ejemplo, en el campo de robots militares y desarrollos cibernéticos existe una ventaja de Estados Unidos, Gran Bretaña, Francia y Alemania, seguida por Israel, Sudáfrica, Corea del Sur, China, Singapur, Rusia, entre otros (8). Este puñado de países representa más del 80% de las existencias de robots que se aplican en el campo de batalla. Asimismo, estos países son el centro estructurador de las tecnologías de la información por lo cual instauran un sistema tributario de su propia posición estructural. No existen los países independientes en esta dinámica, sino una cierta gradualidad o niveles de dependencia sintiendo los efectos de la vulnerabilidad y la sensibilidad, lo cual los obliga a ir compensado materialmente y estructurar ventajas como consecuencia de establecer los estándares sobre el cual los otros países se conectan.

La creciente interconexión tecnológica, los desarrollos conjuntos, la cooperación en áreas sensibles, junto con amenazas comunes en áreas específicas está provocando una integración que podríamos identificar como cuadricula, la cual se traduce operativamente a partir del funcionamiento de un entorno de seguridad basado en cada una de las cuadriculas donde la provisión de seguridad estará dada por la capacidad de resolver dicha situación a partir de las propias capacidades, ya sea por la vía unilateral o cooperativa generando una micro administración de los espacios de seguridad.

Esto significa tener la capacidad de desarticular al oponente en lugares específicos sin que pueda volver a recuperarse, quedando mutilado y aturdido lo suficiente como para anular cualquier capacidad de acción de respuesta. Cegar se vuelve tan importante como destruir, ya que anula la capacidad de articular contramedidas operativas que permitan recuperar la iniciativa en el campo de batalla.

Cabe destacar que la creciente cuadriculación del mundo no proviene de un solo lugar, es más bien una suma de distintas potencias que articulan en función de las capacidades que van desarrollando, poniendo en sus grillas a sus nuevos "Estados clientes" haciendo complejo romper con dichas conexiones ya que los reemplazos no son sencillos y, además, hay pocos disponibles para cambiar. Es Estados Unidos (y algunos de sus aliados aun cuando estos tengan desarrollos independientes), China o Rusia. Las conexiones no son excluyentes, pero en tiempos de conflicto serán exclusivas lo cual demanda tener en claro que "swichts" se van a perder como consecuencia de las tomas de posiciones, ya que el espacio para la neutralidad puede ser relativamente reducido.

El aumento de interconexión es parte de aquello que comienza a vislumbrarse como un proceso de cerramiento del espacio humano global en áreas bien definidas a los efectos de monitorear y eventualmente castigar aquellas conductas que no sean consideradas adecuadas al orden

internacional, obligándonos a lidiar con el "aprisionamiento" invisible que produce el espectro electromagnético (9), instaurando eventualmente un panóptico internacional donde la capacidad de control aumenta tanto horizontal como verticalmente, al tiempo que se demanda un mayor acceso a las redes, se temen las consecuencias de dicho acceso y, por lo tanto, se demanda mayor control (10). Existe un doble empoderamiento, el Estado al comando de estas tecnologías, y la sociedad civil con aquellas que se van filtrando hacia el mercado y que en manos de actores dispersos como "anonymus" suelen ser un desafío para los Estados.

En este sentido, cada país es "libre" de sumarse a dicha cuadrícula, que tipo de contribución puede realizar y como emplaza su posicionamiento internacional a partir de cómo pueden verse afectados las intereses propios en función de las acciones que los administradores del sistema generen en cada una de ellas en función de sus propios intereses. Este esquema de creciente interconexión busca cerrar los espacios donde se producen las actividades humanas y espacios conexos, principalmente aquellos donde emerge inestabilidad; aunque eventualmente llegaremos a la situación —que fuera bautizada por Glenn Greenwald (2015) en su libro— donde nos quedaremos "sin un lugar para esconderse", tanto digital como físicamente, dando lugar efectivo a la vieja aspiración del panóptico.

En este contexto existe un consenso general acerca del incremento de los riesgos existentes por el aumento de interconexión. Un sistema de defensa integrado es susceptible a ser neutralizado, hackeado o sobrepasado como consecuencia de un ataque sorpresa. Las operaciones de espionaje mediante ordenadores se pueden transformar en operaciones de influencia en una elección como se intento en la reciente contienda electoral norteamericana (Lipton et al 2016). Las empresas del complejo industrial militar que diseñan las armas más sofisticadas del mundo son vulnerables a ser penetradas ya sea en las etapas de tempranas de desarrollo de un arma o en la de producción como lo muestra la creciente evidencia existente de sistemas de armas chinos inspirados en los norteamericanos (11). El llamado "complejo industrial militar" hoy es complementado y a la vez vulnerado por el "complejo militar -internet", generando la crisis sobre la que se estructuraba el equilibrio estratégico internacional comenzando ha tomar un carácter ofensivo. Los chinos han perfeccionado el espionaje industrial vía internet de manera consistente con sus intereses de cerrar la brecha tecnológica lo más rápidamente posible y al menor costo.

La estratificación aumenta la vulnerabilidad de los Estados mas débiles en función de su capacidad para defender sus intereses en la dinámica interestatal, como consecuencia del aumento de conectividad de su infraestructura y sus capacidades para pelear de manera autónoma un conflicto armado, ya que la integración de sistemas navales, terrestres aéreos, espaciales y ciberespaciales se encuentra restringida a unos pocos, quienes también son vulnerables, aunque los recursos necesarios para afectarlos son ingentemente mayores. Los actores no estatales podrán explotar el factor de ocultamiento relativo y la ventaja de la sorpresa, pero en el largo plazo aquellos que desafíen el orden encontraran algún tipo de límite tanto físico como en el mundo virtual aunque después sean reemplazados por otros con nuevas capacidades (12).

Un mundo más estratificado entre quienes tienen las capacidades y quienes no las tienen, no evita la perspectiva de proliferación, en parte como consecuencia de un número mayor de jugadores y en parte como producto de la ausencia de consensos. Esta situación hace que una vez incorporadas ciertas tecnologías que se bajan en el poder cibernético serán difíciles de contener creando la posibilidad de que varios actores saquen ventajas de un escenario que se presenta incierto como consecuencia del incremento de capacidades disponibles, el flujo de información, actores, ideas, y recursos para llevar a cabo aquellas ideas que valen la pena probarse.

De ahí la tensión existente entre incertidumbre y un esfuerzo grande por predecir, limitar y monitorear conductas que promuevan el desorden internacional. Los países centrales han sido

relativamente cuidadosos en relación a que otros pares le han brindado acceso a tecnología cibernética y sus derivados como la robótica, la biotecnología y la nanotecnología, tratando de ser relativamente estrictos. Sin embargo y a diferencia de las armas nucleares, donde los esfuerzos para evitar su proliferación dieron por resultado la firma de un tratado de no proliferación, el aumento geométrico de robots con funciones comerciales, software y hardware hacen muy difícil su contención y regulación por parte de la comunidad internacional, ya que en este caso el problema no es el robot en si sino la combinación de éste con, por ejemplo, un artefacto que pueda hacer daño.

Con mayor o menor nivel de complejidad y costos, los robots con funciones militares están apareciendo en una gran cantidad de países, en un número incremental y los productores de dichos ingenios se están esparciendo. En términos militares, Estados Unidos tiene cerca de 22.000 robots desplegados por todo el planeta (10.000 UAV, y 12.000 UGV y UUV/SUV) siendo el país que mayor número de esos ingenios tiene aplicados militarmente. A ello podemos sumar que hasta el año 2014 existían 76 países con programas activos de drones (13), ya sea producto de su adquisición o como consecuencia de sus propios desarrollos. A su vez, se suma una creciente capacidad para transformar aquellos con fines recreacionales por parte de grupos terroristas o insurgentes a los efectos de emplearlos como parte de sus esfuerzos de obtención de inteligencia.

Actualmente es mayor el número de países que están desarrollando aviones no tripulados armados que quienes ya los han utilizado en combate. Comercialmente la tecnología se ha expandido a casi todo el mundo y, en muchos casos, se superponen. Los mayores diferenciales se dan en la complejidad de los drones a desarrollar (14). Similar situación sucede con robots en el campo terrestre y marítimo. China es el principal exportador de esta tecnología, principalmente a países del África y de Medio Oriente donde las restricciones occidentales aplican efectivamente. Este tipo de acciones también crean cuadriculas de conexión, ya que no es sólo el avión y el misil sino también todo aquello que lo conecta con sus operadores terrestres. Israel hace lo propio con América Latina.

Otra fuente de proliferación es el modelo de "negocios" norteamericano mediante el cual una agencia de desarrollo tecnológico que depende del Pentágono –como es DARPA (15)– se vincula con diversos desarrollos competitivos de universidades, empresas del complejo industrial-militar e instituciones de investigación independientes a los efectos de promover determinados tipos de concursos destinados a resolver problemas operativos de previas invenciones o empujar un poco mas la ciencia que estos institutos exploran. El premio: los fondos necesarios para desarrollar y profundizar sus conceptos. Inglaterra, Francia, Alemania, Rusia y China entre otros, realizan similares tipos de interacciones (16).

Finalmente, estamos asistiendo al ocaso de la estabilidad estratégica que proveían las armas nucleares, núcleo de las relaciones entre los grandes poderes (17). Gran parte de los acuerdos internacionales logrados durante la Guerra Fría eran resultado de la convicción de la incapacidad de obtener ventajas decisivas en caso de una conflagración mundial por el riesgo de que escale a un enfrentamiento nuclear total. Eso hizo primar la defensa sobre la ofensiva, mas allá de que se desarrollaran todo tipo de planes para lanzar un ataque de uno contra otro gran poder. Los acuerdos de Misiles Antibalísticos (ABM), y los Acuerdos de limitación y más tarde de reducción de Armas Estratégicas (SALT-START), cimentaron esa estabilidad, los cuales convivían con doctrinas ofensivas convencionales como la llamada combate Aero-terrestre (Toffler et al 2014) en el caso de Unión Soviética y actualmente en una potencial conflagración contra China, la llamada batalla aero-naval o ASB (AirSeaBattle en inglés).

De forma perceptible estamos retornando al dominio de una estructura internacional ofensiva, por encima de una defensiva. Cuando estas situaciones suceden, aun cuando su duración en el tiempo sea breve, aparecen toda clase de problemas vinculados con el ya clásico dilema de seguridad. La incorporación de capacidades mili-

tares junto con una determinada doctrina de aplicación de esas capacidades termina por provocar desbalances y preocupaciones de todo tipo, en especial la posibilidad de que un ataque "sorpresa" deje inerte la posibilidad de defensa. Ese es el ejercicio mental al que nos somete el libro de Singer y Cole: bienvenido al fin de la estabilidad estratégica.

La incorporación de todo tipo de capacidades enraizadas en el ciberespacio junto con sus derivados como los robots, el desarrollo de capacidades biotecnológicas y su impacto en los soldados, ya sea mediante nuevo equipamiento o con el desarrollo de habilidades específicas como una mayor resistencia y atención están provocando carreras tecnológico-armamentísticas, donde comienzan a primar los sistemas ofensivos por encima de los defensivos, permitiendo generar especulaciones acerca de las ventajas del primer movimiento, además de expandirse las ventanas de oportunidad y vulnerabilidad, y el uso más frecuente de este tipo de armas. Como consecuencia de dichas oportunidades que aparecen en el horizonte, el alcance de los acuerdos son más limitados y los esfuerzos para ponerle un coto de caza a estos sistemas suelen ser lentos, en el mejor de los casos, cuando no inútiles (18).

En esencia se está discutiendo la posibilidad de pelear una guerra limitada contra dos o mas grandes poderes en un espacio geográfico en competencia, en el cual se hace difícil escalar por las consecuencias que puede llegar a tener para los beligerantes, pero al mismo tiempo poder asestar un golpe rápido que favorezca el logro del objetivo militar a un costo relativamente aceptable, quebrando con la lógica de la disuasión garante último de la estabilidad estratégica.

Durante los últimos años y en función de la dinámica existente entre China, Estados Unidos y Rusia, amparados por lógicas de primacía militar, los Norteamericanos desarrollaron una versión naval de la teoría del combate aeroterrestre, llamada el combate aeronaval, que mira la ventaja de ataque que brinda la combinación del poderío de la aviación naval, las defensas de misiles de teatro, y la capacidad de asalto anfibio. A ese despliegue se le contrapone las dinámicas de antiacceso y denegación de área. Combinando poder militar principalmente balístico, capacidades navales submarinas y una mejor capacidad cibernética para incapacitar el comando y control de la fuerza atacante (19).

Sobre este argumento se sitúa la novela Ghost Fleet (2015) de Peter Singer y August Cole. Aun para una potencia nuclear, con amplias capacidades convencionales, la incapacidad de resolver rápidamente un ataque que lo incapacite por un determinado período de tiempo, permite realizar movimientos convencionales al oponente obteniendo una ventaja inicial importante en la consecuencia de los objetivos.

A partir de dicha ventaja consolidar su posición y resistir el seguro contrataque convencional a los efectos de recuperar lo perdido.

El ataque sorpresa además no esta solo determinado a un lugar específico por el contrario un ataque de estas características demanda cierta simultaneidad en distintos planos ya sea el espacio ultraterrestre, mar, aire y ciberespacio.

El componente real se encuentra en un coordinado ataque a Pearl Harbor, y el virtual está determinado por un ataque cibernético que arruina las capacidades del sistema de armas más modernas que tienen los americanos producto de que fueron capaces de insertarles una versión moderna del Caballo de Troya, como consecuencia de la fabricación de partes y sistemas en China (20). Esta idea recurrente de un Pearl Harbor digital impulsa las medidas de defensa que dicho país necesita tomar; temor y oportunidad se combinan para dar contexto y fuerza a la política (21).

Cabe destacar que en el año 2000 Tom Clancy en su libro El Oso y el Dragón trabajó sobre la misma dinámica geopolítica en relación a un conflicto tripartito entre grandes potencias, pero invirtió las alianzas ya que en este caso China sigue siendo el oponente, pero ahora va contra Rusia, el cual es asistido por Estados Unidos. Parte del éxito de la operación militar norteamericana tiene que ver con la capacidad de obtener información sensible sobre las defensas chinas y poder usarlas a tiempo para repeler la invasión

que ese país trata de llevar sobre las riquezas naturales en Siberia. Ambos relatos aun cuando divergen sobre el enemigo y su estructuración comparten la idea del ciberespacio como un elemento central en la articulación efectiva tanto de la defensa como de la ofensiva. Quienes no tengan la capacidad de actuar en este plano, sencillamente estarán limitados y subordinados en su accionar. La táctica que combina estos espacios en una dinámica de "Blitz" ha permitido a que Rusia la ejecute con cierto éxito contra poderes menores en capacidades materiales y virtuales como han sido Georgia y más tarde Ucrania (22).

Las pruebas de este tipo de operación, pueden verse en los ataques que los "ciberguerreros" rusos llevaron a cabo contra los países bálticos al poco tiempo de que ingresaran a la OTAN. Con el paso del tiempo, todas las estrategias militares que tienen por función establecer los principios de acción reconocen que un ciberataque puede ser el inicio de una operación militar ofensiva. Una operación de este tipo siempre busca sobrepasar las defensas, saturarlas, por ejemplo, con ataques de denegación de servicio que impidan coordinar las defensas para luego saturar con comandos o infantería aerotransportada el espacio físico de combate.

La carrera armamentística que apunta a establecer capacidades en materia de ciberespacio, robots, mejoras en los sistemas de defensa contra misiles, armas de energía dirigida, nanotecnología, y mejoras biotecnológicas que realzan las capacidades del ser humano, se encuentran en algunos casos en etapas de implementación y en otros en etapa de desarrollo (Davenport 2016). La clave de la superioridad dependerá de cuánto tiempo se puedan manejar las brechas tecnológicas existentes a favor del actor que tiene que retenerla. El mundo se convierte lentamente en un mundo de dominio ofensivo.

## Las armas del campo de batalla actual

No hay documento que plantee política militar, en especial de ningún gran poder, que no ponga de manifiesto que el campo de batalla es en la actualidad un sistema integrado e interconectado de amenazas aire-aire, tierra-aire, espaciales y ciberespaciales, que conviven con una fuerza militar que se hace cada vez más obsoleta y reducida donde todavía el 80% de los arsenales existentes fueron diseñados y pensados para un conflicto que no concebía estos cambios. Frente a esta realidad, a esos sistemas obsoletos los interconectamos mejor, les sumamos capacidades a las existentes, las hacemos mas eficientes, innovamos, pero no hacemos grandes variaciones en función, en definitiva les hacemos "upgrades", que extiendan su vida y les permita operar en estos nuevos entornos. Integramos, conectamos y mejoramos, pero un tanque sigue siendo un artefacto del mundo físico que ahora realiza más eficientemente su tarea en combinación con otros componentes del mundo físico mediados por el entorno cibernético. El comandante tiene en simultáneo información sobre la situación táctica y la operacional y hace que su fuerza tenga más eficiencia.

Si el conflicto armado continúa siendo una característica de las relaciones humanas el carácter del mismo se encuentra afectado por los desarrollos que se suceden en el campo tecnológico y como este impacta en las sociedades (23) ya sea para absorber dichos cambios y al mismo tiempo organizarse para obtener los beneficios de los mismos. A partir de la velocidad con la que se producen los mismos existe una presión adicional al momento de intentar comprenderlos como consecuencia de que el proceso de visualización acerca de su impacto futuro sucede al mismo tiempo que se despliegan en el campo de batalla. Gran parte de esos cambios producen una profunda discusión sobre la posición humana en las guerras por venir, ya que como consecuencia de ellos el proceso de deshumanización se ha vuelto más evidente.

Ciertamente el ser humano se encuentra en una etapa donde no se siente muy cómodo con las opciones a las que estos sistemas nos ponen enfrente. La idea del "valle de la desolación" (uncanney valley) se hace muy visible al momento de dejar que una máquina tome la de-

cisión de matar a un ser humano de forma independiente de este en base a un algoritmo creado en la cabeza de algún equipo de programadores (24). Asimismo, no es solo el hecho de que estamos creando armas cada vez mas autónomas sino que, además, nos encontramos testeando armas de mayor precisión y más velocidades como los misiles hipersónicos (Mach 5), los cuales acortan los tiempos de decisión y afectan los cálculos sobre los cuales se realizaban las conjeturas en relación a la estabilidad estratégica.

Cuando analizamos detenidamente estas transformaciones, el ciberespacio es particularmente desafiante, como consecuencia de que no es un arma en sí sino una plataforma desde donde se montan complejos sistemas de armas. El ciberespacio es en la actualidad el mejor ejemplo de tecnología de uso dual.

Este ámbito no geográfico devenido estratégico como producto de la capacidad tecnológica primero de un país y luego de varios, integra y cruza todo el campo de batalla actual. Desde esta plataforma donde las nuevas y las viejas armas corren a los efectos de cumplir con su función militar. Aire, mar, tierra y espacio ultraterrestre se encuentran barridos por el ciberespacio dando conectividad e integrándolos para que estos cumplan con el rol que tiene cada una de las componentes que integran las fuerzas armadas provocando el efecto de multiplicadores militares.

Si la hegemonía militar se sostiene a partir de desarrollar estrategias que se basan en la superioridad y la posibilidad de penetrar y anular defensas del oponente, la remoción de la misma demanda desarrollar capacidades para cortar el acceso y limitar la maniobra en un espacio determinado, conocidas como A2/DA. Si miramos el ciberespacio tenemos capacidades tanto ofensivas, en cuanto se dedican a intrusar, anular y luego destruir un determinado sistema enemigo, así como también se poseen distintos mecanismos que actúan como murallas de dichas penetraciones. Los cibercomandos dividen sus funciones en dos grandes áreas. Introducirse subrepticiamente en determinados sistemas a partir de fallas y errores del oponente, desarrollando capacidades ofensivas, al tiempo que se busca evitar que agentes externos ingresen en los sistemas propios, promoviendo el desarrollo de defensas virtuales. Ambas partes se encuentran entrelazadas.

Al leer las estrategias de los países, tanto occidentales como aquellos que no lo son, todos asumen la posibilidad de un conflicto limitado donde la guerra de desgaste y la supervivencia serán el eje de las discusiones para las fuerzas navales y aéreas de los países y para los sistemas cibernéticos que los controlan. Ya no solo se ponderará cuantos soldados un país puede desplegar en el campo de batalla, sino cuantos chips de computadoras darán "la vida" por su país, como bien lo señala Christopher Coker (2013) en su libro *Warrior Geeks*.

El desarrollo de "Amenazas Avanzadas Persistentes" (AAP) es un componente central en las estrategias ofensivas de los países, seguido por un intento de construir mejores defensas por parte de quienes desarrollan dichas capacidades a modo de evitar las consecuencias directas de un ataque, como se pudo probar en el caso del uso de la AAP Stuxnet y otros virus al igual que técnicas de saturación de servidores conocidos como ataques de denegación de servicio inhabilitando la provisión del servicio incapacitando dicho sitio, dejando fuera de línea páginas y sistemas relacionados con ese proveedor.

En el caso de las operaciones en el ciberespacio, la barrera de entrada no es necesariamente alta, aunque determinados desarrollos –en especial aquellos que son considerados complejos – demandan una importante cantidad de información para poder operar efectivamente sobre los sistemas del oponente además de ingentes sumas de dinero, como consecuencia de que realizar dichas operaciones involucran temas físicos. Esas capacidades se destinan a encontrar vulnerabilidades en el software de forma tal de explotarlas para llevar a cabo acciones que van desde el robo de información, operar determinado software malicioso, tomar control de los sistemas, penetrar y dejar preparada una puerta de acceso para futuras penetraciones (25).

La llamada "Internet de las Cosas", que plantea interconectar todo adminículo existente con red –desde lámparas de luz de la casa hasta un automóvil–, plantea desafíos que provienen de las fisuras de seguridad en el software que los conecta a la red, permitiendo a un actor maliciosamente orientado incrementar las fuentes desde donde encontrar puertas de acceso a la información que quiero tener (Greenwald 2015). El mayor número de instrumentos conectados a la red, no solo aquellos que se conocen como "zombies" electrodomésticos, permite que dichos instrumentos sean capturados por hackers para amplificar la fuente de envío de datos hacia algún lugar específico saturando los servidores y generando los ataques de denegación de servicio. Toda la primera generación de aparatos que se encuentran conectados a Internet tienen escasas medidas de seguridad para defenderse de un hackeo, haciéndolos vulnerables a una acción dirigida determinada por alguien que quiera emplear estos dispositivos en contra de un sistema mayor. Así como los hackers han logrado tomar el control de automóviles en las autopistas, se conoce que las fuerzas armadas de Irán –con la supuesta ayuda de chinos– han hackeado vehículos aéreos no tripulados (UAVs) norteamericanos sobre su espacio aéreo haciéndolos aterrizar en sus bases para luego, mediante ingeniera reversa, obtener información sobre qué estaban haciendo esos ingenios en su territorio y extraer aquel conocimiento necesario para desarrollar sus propios drones, haciéndolos, al mismo tiempo, más seguros.

El ciberespacio también se ha vuelto relevante en tanto es utilizable para destruir infraestructura económica, lo cual es considerado un objetivo válido en los conflictos internacionales. Los cibercomandos monitorean las acciones ejecutadas por los cibersoldados desplegados en algún lugar del mundo o, a los efectos de evitar dejar huellas muy visibles, subcontratan actores no estatales con recursos y capacidades sofisticadas para hacerlo, como reveló el New York Times en su investigación al ataque al partido demócrata donde el FSB y el GRU actuaron mediante hackers contratados o la propia iniciativa privada buscando algún fin divergente con el del Estado al que pertenecen. También resulta relevante señalar que se puede generar parálisis y confusión, aunque como desde el ciberespacio se producen efectos reales, cierto software puede usarse eventualmente para provocar un daño masivo a alguna infraestructura considerada estratégica. En este sentido, un virus informático podría ser el equivalente a una bomba guiada, si el efecto que se busca es el de la destrucción física del blanco.

Sobre los sistemas informáticos corren o se suman los robóticos, los cuales han ingresado ya en una etapa de expansión al plano civil y hogareña, habiendo comenzado humildemente en el campo económico para transformarse actualmente en una realidad desde el punto de vista de la planificación militar. Peter Singer (2009), en su libro *Wired for War* traza un recorrido sobre las razones por las cuales la humanidad los está incorporando en el campo de batalla. Los robots realizan tareas por nosotros en los cuales nuestro desempeño es menor, son tediosas o son en extremo peligrosas como consecuencia del ambiente en el que se deben realizar. En este sentido, los robots suponen un cambio en la doctrina militar de empleo, ya que la misma determina cuál es la guía sobre la cual se van a pelear las guerras, por lo tanto da forma a todo aquello que el realiza.

La aparición de robots en todos los posibles escenarios de batalla obliga a pensar en la forma de emplearlos, los cuales se han ido expandiendo desde de la observación, la inteligencia y vigilancia, a las funciones de ataque, guardias de bases o defensores de perímetros, desactivadores de bombas, mini torpedos auto-guiados, exploración acuática, sonares avanzados, etc. Todos ellos formando un punto en nuestra grilla del espectro electromagnético, al servicio de descubrir, identificar, y eventualmente neutralizar al enemigo.

Los sistemas robóticos están sacando ventajas de las mejoras en las comunicaciones, los sistemas de cifrado, la mejora en la recolección y procesamiento de datos, y la evolución en los sistemas de inteligencia artificial y la capacidad de poder hacer de ellos algo esencial en el campo de batalla moderno que es la capacidad de cumplir con los requerimientos solicitados a medida. La

discusión existente en relación a estos ingenios una vez desplegados no solamente pasa por el hecho de que "puedan" matarnos como consecuencia de la decisión de un algoritmo, sino por el hecho de que son más efectivos que nosotros en varias áreas, por lo tanto, más usables cuando dicha capacidad se posea.

Dada la superioridad tecnológica de algunos países, los sistemas robóticos están predominando en el espacio aéreo como el marítimo. En el espacio terrestre los robots no solo se desarrollan para desactivar bombas y trampas varias. Cumplen, además, un rol clave en la supervivencia de la infantería, ya que se los utiliza como exploradores adelantados en edificios, calles y barrios congestionados tanto desde el aire como en tierra empleando, en sus sensores ópticos, la habilidad del reconocimiento facial (26). El campo de batalla urbano es la nueva frontera en materia de guerra robótica.

Ya sea como consecuencia de la obtención de capacidades similares por parte de potencias de igual peso o para enfrentar exitosamente tácticas irregulares o de guerrillas, el mandato que emana desde el comando de las fuerzas es adaptarse a las nuevas condiciones existentes en el campo de batalla, dominado por la asimetría, la resistencia, la voluntad de proteger a los soldados minimizando el número potencial de bajas propias y la posibilidad, junto con el interés, de usar cada vez más estos ingenios.

En este sentido, la Armada norteamericana se encuentra desarrollando una doctrina que involucra usar robots de combate aéreo junto con las defensas navales automatizadas formen una malla de contención frente a una potencial oleada de drones enemigos o lanchas rápidas tripuladas o no con sistemas de misiles antibuques, a los efectos de neutralizarlo. Las características de esta forma de actuar es conocida como la técnica de la "nave nodriza" cuyo accionar hemos visto en cientos de películas de ciencia ficción donde una nave más grande es el transportador de cientos de naves mas pequeñas que se encargan de atacar múltiples y diversos objetivos (27).

Hasta el momento se han realizado pruebas embarcando aviones no tripulados en los portaaviones en cantidades que duplican o triplican el número de aviones embarcados, utilizándolos contra objetivos de práctica en tierra mejorando la supervivencia y la capacidad de ataque existente en un portaaviones al tiempo que se ponen a prueba las defensas en contra de los sistemas anti-acceso, en especial misilísticos existentes para eliminarlos. Aun cuando esto avanza, las resistencias de los mandos han evitado que esta técnica se acelere, como consecuencia de las dificultades para concebir una aviación de ataque sin pilotos en los aviones. La Fuerza Aérea norteamericana enfrenta un dilema similar, pero al mismo tiempo se acepta que cada vez más los pilotos que se entrenan son de aviones no tripulados, aunque eso no ha dejado de tener efectos en los rangos ya que los pilotos de estos ingenios no gozan precisamente de popularidad al interior de la fuerza, como consecuencia de la propia dinámica al interior de la fuerza aérea.

Mayor aceptación ha tenido la versión robótica naval de los desactivadores de bombas terrestres. En este sentido se encuentran avanzadas las incorporaciones de robots navales para funciones de desminado, sobretodo considerando que las fuerzas de asalto de la infantería de marina operan en espacios cercanos a las costas donde el riesgo operacional aumenta exponencialmente como consecuencia de la proximidad terrestre. Asimismo, se espera que los robots formen parte de la dinámica de bloqueos navales frente a potenciales rivales. Ya existen sistemas autónomos que operan en la superficie, y vía submarina, poblando cada vez más un espacio que a simple vista se lo observa inmenso e imposible de llenar.

La segunda doctrina en desarrollo, y que ciertamente está capturando la imaginación y atención en el campo militar, es la llamada doctrina "Swarming" o enjambre, la cual está concebida siguiendo procedimientos descentralizados de ataque pero, al mismo tiempo, cooperativos que sirvan para concentrar poder de fuego sobre una serie de blancos preestablecidos donde no

exista un líder específico que comande la operación, donde los atacantes puedan cumplir con la misión a partir de cooperar entre ellos, reconocer las bajas que se dan entre ellos y reemplazar unidades con otras sobrepasando las defensas del enemigo. Esta doctrina busca que un amplio número de pequeños robots puedan cumplir con una serie de tareas específicas en doblegar a un enemigo fuertemente atrincherado sin estorbarse entre ellos mismos. Esas reglas implican separación de otros robots, alineación y coordinación de velocidad y dirección y cohesión donde puedan percibir cual es el centro de masa de los robots.

En el programa conocido como "lobos de la guerra" trabajan DARPA y Lockheed Martin para que los robots desarrollen, a través de sensores simples, la capacidad de reconocimiento entre ellos y sus blancos basados en una serie de algoritmos donde puedan pasarse información entre sí para atacar el blanco designado. Puesto en las palabras de John Arquilla, "en un futuro cercano existirán una gran cantidad de robots pequeños capaces de atacar una fuerza militar enemiga desde todas las direcciones simultáneamente con el efecto de sobrecargar su capacidad de defensa. El atacante podrá lanzar su ataque, dispersarse, volver a fijar el blanco, reagruparse y lanzar el ataque hasta que las defensas se vean sobrepasadas (28). Las máquinas coordinan mejor, tienen mayor efectividad al momento de establecer sus blanco, y no dudan cuando tienen que actuar.

La discusión que se está llevando a cabo sobre los robots se centra sobre el momento del proceso de decisión de disparo y los temores que genera el dejar esa decisión en manos de un algoritmo determinado y de un hardware asociado.

La expresión que se utiliza en la academia sajona es "in the loop", donde la decisión humana es el "loop" sobre el cual corren el *in*, el *on* y *out*, básicamente la diferencia se encuentra en dónde se ubica la decisión humana en la cadena de decisión de disparo. El *(in) the loop* está presente en el 80% de los sistemas militares de los países que poseen sistemas autónomos. En el resto de los sistemas se considera que el humano se encuentra sobre la cadena de decisión de disparo (*on*) en funciones de verificación y, finalmente, un número ínfimo de los mismos, en especial en el campo de los sistemas aéreos, los humanos han sido dejados afuera de la decisión de disparo (*out*) (29).

Sumado a los robots, aparecen sistemas que buscan integrar humanos con máquinas, conformando una idea de mundo post-humano que el aparato de Hollywood ha popularizado como *cyborgs*. Al respecto, dos sistemas de armas comienzan a probarse efectivamente en el campo de batalla actual. El primero es aquel que se relaciona con los llamados "humanos aumentados", ya sea por modificaciones genéticas, nuevas drogas que mejoran el estado de alerta de los soldados, la capacidad de recuperación de las heridas, la construcción de exoesqueletos o la implantación de chips para saber el estado de los soldados monitoreando sus reacciones corporales. Asimismo, y eventualmente, ir reduciendo los efectos del síndrome postraumático.

Los exoesqueletos son una innovación en la forma de equipar al ser humano asistiendo a los soldados de infantería cargando más municiones y otro equipamiento como drones portátiles. La unidad mínima de combate como un pelotón esta aprendiendo a utilizar esta nueva capacidad junto con robots que los acompañan como exploradores adelantados, evacuación de heridos o carga de equipamiento. La idea que rige esta innovación es la creciente capacidad para fusionar el cuerpo humano con máquinas (*cyborgs*), aunque estos ingenios se encuentran recién en etapas de implementación operativa, estudiando la viabilidad de los mismos en el campo de batalla (30). Estos avances se los conoce como primera ola de integración y son una realidad. El campo médico es el que mayor avances presenta, sobretodo en temas de prótesis, pero también en drogas que asisten el combate del PTSD o stress pos traumático.

La llamada segunda ola es aquella relacionada con los cambios genéticos, principalmente modificando la genética corporal y eventualmente la modificación del cuerpo humano brindando

atributos que no se tenían o resistencias a determinados ambientes, lo cual está en plena etapa de desarrollo con investigaciones de alteración de genes con fines determinados como mayor inteligencia, fortaleza, la eliminación de genes defectuosos mediante el desarrollo de una herramienta de alteración del ADN conocida como CRISPR-CAS9. Este es el futuro de los humanos aumentados, una suerte de "X-men" sin super poderes pero con capacidades mayores a las de un humano nacido en condiciones normales (31).

Finalmente, en el campo de las armas aparece la realidad aumentada y la realidad virtual como complemento al equipamiento del hombre. La realidad aumentada tiene como función permitir al soldado el conocimiento total de una situación a sus alrededores mejorando la información que posee del entorno en el que combate, brindando más chances de supervivencia a los soldados, especialmente en los ambientes urbanos los cuales siguen siendo complejos y mortales para la infantería. Esa misma realidad aumentada ofrece la oportunidad de mejorar a la capacidad de los tiradores individuales, para descubrir lugares de ocultamiento de fuerzas oponentes.

La integración futura entre equipos, implantes, robots y soldados debería constituir una suerte de imparable máquina de combatir a una unidad tan pequeña como puede ser un pelotón. Por otra parte, la realidad virtual ya es el presente de los campos de entrenamiento de las fuerzas armadas occidentales y orientales sin importar cuán poderosas o limitadas sean.

La necesidad de plantear esquemas donde los soldados puedan entrenarse en entornos relativamente seguros pero al mismo tiempo exigentes ha motivado el desarrollo de todo tipo de programas destinados a simular diversos ambientes y condiciones de operaciones permitiendo a un pelotón tener la experiencia de ser desplegados en terrenos (simulados) similares a los que van a operar, lo cual facilita recortar la ventaja que poseen los locales en relación a su propio espacio de combate. Las simulaciones aéreas, las submarinas y los combates urbanos simulados son actualmente parte del entrenamiento militar obligatorio de las fuerzas occidentales. La capacidad de recrear calles, geografías y entornos en softwares que faciliten la creación de entornos virtuales pone en perspectiva dejar circular libremente el auto de Google que toma las fotos para su aplicación *street view*, ya que todos estos ingenios pueden tener implicancias para la seguridad nacional. Estados Unidos es quien con mayor rapidez se está moviendo a sumarlas en función de aquello que se conoce en el Pentágono como estrategias de compensación. En el presente estamos presenciando la tercera estrategia de compensación. Esta idea supone el desarrollo de los sistemas que permiten a ese país mantener sus ventajas militares, creando nuevas tecnologías que revisten carácter de transformacionales mediante la innovación (32).

El advenimiento de una estrategia que apunte a la superioridad tecnológica es el resultado de los problemas derivados de la asimetría existentes en el espacio terrestre, la modalidad de combate de guerra de guerrillas, y la proliferación tecnológica, mediante la cual hay una mejora en los sistemas de defensa aire-aire, mejores capacidad de reconocimiento del terreno, una mayor capacidad de detección de las tecnologías de invisibilidad y el creciente final de los espacios comunes como santuarios desde donde poder lanzar ataques con relativa tranquilidad. Esta situación nos recuerda una premisa de los años noventa cuando comenzaban a tomar forma los efectos del ciberespacio: "las relaciones políticas que toman lugar en el espacio virtual generan efectos muy reales en las sociedades" (Keohane y Nye 1998). En este sentido, el Departamento de Defensa de Estados Unidos ha decidido llevar adelante la integración efectiva de los sistemas militares y obligar a los comandantes que se encargan de los procesos de adquisiciones militares a que justifiquen aquellas incorporaciones de equipamiento militar que no sea robótico, dando lugar a un creciente peso de estos sistemas en la estrategia militar norteamericana. A un mayor peso del equipamiento aéreo, naval y terrestre no tripulado, se le van a sumar las mejoras en las

operaciones aéreas y la llamada "proyección de poder mediante capacidades alternativas", lo cual es un eufemismo para hablar de las cibercapacidades.

Cabe destacar que todas estas tecnologías descriptas están en distintas etapas, ya sean en expansión o en pleno desarrollo, pero lo cierto es que abandonan cada vez más el componente de ficción. Esta es la actualidad del campo militar y, en un futuro cercano, estaremos viendo la profundización de un camino que ya presenta trazos reconocibles en las capacidades militares de los países que disponen de estos sistemas.

## Del futuro al pasado: Consideraciones sobre la defensa argentina

Argentina se ha insertado en este proceso de manera limitada en algunos aspectos de esta revolución tecnológica, principalmente desde sus capacidades civiles y comerciales y con algún esfuerzo en el campo de la aviación no tripulada, el cual ha presentado resistencias por quienes siguen planteando la defensa de manera anacrónica y desde un desconocimiento del tema han elevado cartas de preocupación por la posibilidad de que estos ingenios se armen o se los utilice para violentar los derechos humanos. Casi con su lógica abolicionista deberíamos dejar de trabajar con las computadoras por la dualidad de las mismas (Dinatale 2014).

Resulta redundante señalar que Argentina no está preparada para estos cambios que se están produciendo a nivel internacional, y el nivel de conocimiento varía entre académicos, desarrolladores y eventualmente quienes tienen interés en que esta industria y su componente para la seguridad tanto doméstica como internacional se desarrollen. Aun cuando se habla del tema y existen ingentes trabajos sobre cuestiones del ciberespacio, robots y sistemas no tripulados, en el mundo militar recién ahora comienza a tomarse algún tipo de conciencia en relación a tecnologías que están en el mundo desde hace más de 35 años. A ello se suma una mentalidad crítica a todo aquello que se relacione con desarrollar de manera activas estas capacidades porque, ciertamente, son más difíciles de controlar para aquellos que tienen que desarrollar mecanismos que efectivamente ayuden a trabajar con las mismas. Por lo tanto, no tenemos una capacidad que permita armar un complejo tecnológico-civil y militar en este campo ni tampoco somos afectos a la asociación público- privada, generando las condiciones para que se creen sistemas militares propios con aquellas empresas que se dedican a generarlos desde el ámbito civil.

En estos temas estamos huérfanos de ideas y de acciones mas allá de las declaraciones y de la creación de un cibercomando creado bajo la órbita del Estado Mayor Conjunto con algunas capacidades para cumplir con la misión encomendada que es la protección del ciberespacio argentino (33). Al no ser un país que genera tecnología de punta aplicada al campo militar, los avances que se producen en este campo quedan marginados del pensamiento nacional, lo cual provoca que las discusiones se realicen a partir de obras y autores que tienen que lidiar con la realidad de los problemas de los sistemas de armas que generan y su integración en el campo de batalla moderno. La diferenciación de defensa y seguridad también debe aplicarse al ciberespacio. Por lo tanto, aunque una agresión provenga del exterior, el criterio de involucramiento debería estar relacionado con la infraestructura atacada, lo cual genera dudas entre quién tiene competencias y si el acto cometido contra los intereses argentinos está vinculado al ámbito de la seguridad o el de la defensa.

Asimismo la postura mal llamada defensa defensiva pregonada por los otrora intelectuales de la defensa argentina genera problemas en el ámbito del ciberespacio como consecuencia de que las capacidades que en este se desarrollan tienen componentes activos de búsqueda y penetración de sistemas enemigos, y pasivos que hacen a la defensa de las penetraciones de la voluntad oponente. Esta situación también genera claroscuros desde el enfoque que todavía distingue a la defensa nacional, en términos retrógrados con aquello que sucede en el mundo. Penetrar en sistemas enemigos permite conocer que poseen y

prepara mejor la defensa. Sin embargo, la penetración puede ser considerada un hecho hostil, lo cual es un sacrilegio en la comunidad de pensadores posmodernos de la defensa.

Una fuerza militar que combina resabios mentales del siglo XIX y XX con capacidades militares muy limitadas y ciertamente sin un gran protagonismo futuro en este campo nos enfrenta a nuestra primer pregunta: ¿desde dónde podemos pensar la integración tecnológica en el campo de batalla de manera tal que sea útil para nuestro país? Sabemos que los desarrollos robóticos orientados al campo militar aéreo son realizados por cada una de las fuerzas y existen una serie de modelos de aviones pilotados por control remoto desarrollados por el Ejército, la Fuerza Aérea y la Armada, conocido como Sistema Aéreo Robótico Argentino o SARA, contrato firmado entre el Ministerio de Defensa e Invap en 2015, intentando unificar los distintos proyectos existentes entre las fuerzas.

Esta voluntad de producción de sistemas no tripulados se la unió a la idea de industria de la defensa y todos estos anuncios todavía no han desembocado en la producción en serie de estos artefactos ni se conocen órdenes de compra para la provisión de los mismos a las fuerzas armadas. Estos desarrollos se orientan principalmente a los modelos de baja y media altitud, lo cuales son desarrollos comunes en todos los países que han destinado recursos para esta finalidad. Se supone que la industria argentina en este caso es líder en la región, pero al no existir datos fidedignos salvo informaciones de la web, poco puede profundizarse al respecto.

Otro tema sensible es el desarrollo de software con aplicaciones militares. Existen informaciones dispersas sobre desarrollos relacionados con la realidad aumentada aplicados para las fuerzas armadas y producidos por CITEDEF, al igual que simuladores de disparo que reemplazan los costos de ejercitarse en determinados espacios con munición de entrenamiento. El llamado RAIOM o Realidad Aumentada para Información de Objetivos Militares anunciado en el 2014, no tiene estado operativo y todo quedó en los planes (34). Al igual que otros proyectos en el área militar, la gran mayoría queda en la etapa de desarrollo o evaluación pero no llegan a ser producidos en serie. La antigüedad de sus sistemas de armas provoca que tampoco puedan llevarse a cabo la etapa de mejorar sus capacidades operativas mediante la integración con el mundo digital.

El campo de ciberdefensa sigue el mismo destino que la defensa. Una baja atención por parte del poder político, más allá de los clisés argumentativos conocidos, fondos que se destinan sin una gran capacidad de rendición de cuentas, donde los anuncios rimbombantes dan lugar luego a un silencio en el campo de la transparencia y concreción de esos eventos dejándonos en el peor de los mundos, ya que se sabe que se necesita la capacidad, pero que poco o nada se hizo al respecto.

Se supone que de las tres ramas existentes en las fuerzas armadas, y a pesar de que el Estado Mayor Conjunto debería ser el encargado de llevar a cabo los programas de ciberdefensa, ha sido el Ejército el mayor beneficiado como consecuencia de los abundantes presupuestos recibidos por parte de la gestión Fernández de Kirchner para el entonces jefe de la inteligencia de esa fuerza, quien destinó una gran parte de los mil doscientos millones de pesos a desarrollar estas capacidades realizando acuerdos con Alemania, Brasil, Rusia y, algunos señalan, China.

La nueva administración ha intentado recuperar cierto control sobre toda esta estructura y junto con el área de modernización del Estado se encuentran tratando de articular una política de ciberdefensa que realce las capacidades del Estado de manera integral poniendo énfasis en la dimensión público-privada. Asimismo, la nueva administración ha estrechado lazos con la administración Obama, a los efectos de poner en marcha el grupo de trabajo en tecnologías digitales con el fin de crear capacidades y mejorar la conexión gubernamental a la red junto con su infraestructura crítica. Con el cambio de autoridades en Estados Unidos es de esperar que se mantengan las relaciones en este campo, aunque como todo inicio las prioridades pueden variar en función de

las necesidades de la ahora administración Trump.

Todas estas iniciativas se encuentran alineadas con lo que sucede en otros países del mundo, pero como su implementación implica tiempo, recién cuando finalice la gestión podrán comenzar a evaluarse los resultados de la misma. Toda pérdida de tiempo en este aspecto significan penalidades perceptibles (y otras no tanto) que pagarán tanto la actual generación de argentinos en oportunidades perdidas, así como también las futuras.

## Conclusiones

Mientras que en el mundo, y principalmente en los países que lideran la revolución en curso, se están preguntando cuánto falta para llegar ya sea a la panacea tecnológica prometida de algunos científicos o a la distopía augurada por otros, en nuestro país todavía no tenemos en claro a dónde queremos ir y, en el mejor de los casos, somos desarrolladores de determinadas capacidades. Pero en este campo estamos lejos de sentarnos a la mesa de quienes discuten la orientación y el alcance de la política, como sucede por ejemplo en el campo nuclear.

En esta revolución somos, en el mejor de los casos, desarrolladores auxiliares o espectadores de primera fila, pero no actores principales. Es en el terreno militar donde esto se ve muy bien. Nuestras fuerzas armadas responden a parámetros de mediados del siglo XX y los debates alrededor de ellas no conllevan a ninguno de estos campos que hemos mencionados. En el mejor de los casos, seguimos con los clisés. Por suerte, el campo comercial y económico se adapta más rápidamente a estas transformaciones, lo cual hace que no quedemos tan desfasados, al menos en las discusiones.

Como se desarrolló extensamente en este trabajo, los cambios que se están dando en el terreno militar y político están en distintas etapas, algunos más avanzados y otros se encuentran en etapas embrionarias. Estos cambios impactan en una estructura internacional mas jerárquica, el fin de la estabilidad estratégica entre los Grandes Poderes pasada que caracterizó a la bipolaridad y a la unipolaridad posguerra fría, volviendo a estos actores más osados, usando canales directos e indirectos para operar y, finalmente, estas tecnologías proliferan. Como se ha visto, hasta el momento, la ausencia de consensos para limitar su expansión, junto con una dificultad efectiva para regularla, refuerza el sentido de inestabilidad estratégica.

Las armas son muy variadas y la sección dos solo fue una especie de repaso rápido sobre aquello que existe hoy y que estamos desplegando en los campos de batalla. La ciencia continúa empujando los límites, haciendo realidad aquello que la ciencia ficción crea. Si la frase "la imaginación al poder" tiene algún sentido, es en este campo donde lo podemos apreciar.

## Bibliografía


Buchanan, Ben: "The Life Cycles of Cyber Threats", Survival, Vol.58. No.1, February March 2016.

Carr, Nicholas: Atrapados: Como las maquinas se apoderan de nuestras vidas, Ed.Taurus, 2014.

Coker, Christopher: Warrior Geeks: How 21st Century Technology is Changing the Way We fight and Think About War, Oxford University Press, 2013.

Clancy, Tom (2003): El Oso y el Dragon, Ed. Sudamericana.

Charap, Samuel: "The Ghost of Hybrid War", Survival Global Politics and Strategy, December 2015- January 2016, Vol.57 No.6.

Dinatale, Martin: Defensa, Avanza en el país la fabricación de sofisticados drones, La Nación, 2 de Julio de 2014.

Dick, Philip K. (2005), *La Segunda Variedad*, en Cuentos Completos Vol.2, Ed. Minotauro

Franklin, Bruce H. (2010): War Stars: Guerra, ciencia ficción y hegemonía imperial, Ed. Final Abierto.

Greenwald, Glenn (2014): Sin un lugar para esconderse, Ediciones B.

Greengard, Samuel: The Internet of Thing, MIT Press, Essential Knowledge Series, 2015.

Dick, Philip K.: La Segunda Variedad, en Cuentos Completos Vol.2, Ed. Minotauro, 2005.

Keohane, Robert & Nye, Joseph jr.: "Power & Interdependence in the Information Age", Foreign Affairs, Vol.77 No.5, September-October 1998.
Lipton, Eric & Sanger, David & Shane Scott: The Perfect Weapon: How Russian Cyberpower Invaded the U.S., New York Times, December 13, 2016.
Mahnkem, Thomas: Technology and The American Way of War Since 1945, Columbia University Press, 2008.
Rid, Thomas y Ben Buchanan (2015), "Attributing Cyber Attacks", *Journal of Strategic Studies* 38(1)
Shaw, Ian G.R. (2016): Predator Empire: Drone Warfare and Full Spectrum Dominance, University of Minnesota.
Singer, P. W. Wired for War: The Robotics Revolution and Conflict in the 21St Century, Penguin Books, 2009.
Singer, P.W. & Cole August: Ghost Fleet: A novel of the next world war, Houghton Mifflin Harcourt Publishing, 2015.
Toffler, Alvin & Toffler, Heidi: Las Guerras del Futuro: La supervivencia en el Alba del Siglo XXI, Plaza & Janes, 1994.
Van Creveld, Martin: The Age of Air Power, Public Affairs, 2011.
Whitaker, reg: El Fin de la Privacidad: Como la Vigilancia total se esta convirtiendo en realidad, Paidos Comunicación, 1999, Barcelona

## Artículos online

Berman, Dennis (2015), "Adm Michael Rogers on the Prospect of a Digital Pearl Harbor", The Wall Street Journal, 26 de octubre de 2015, disponible en https://www.wsj.com/articles/adm-michael-rogers-on-the-prospect-of-a-digital-pearl-harbor-1445911336
Center for New American Security: Autonomous Weapons Program. https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk
Club Valdai (2016), "John Mearsheimer discusses global order and great power politics at Valdai Club", Club Valdai, 18 de octubre de 2016, disponible en http://valdaiclub.com/events/posts/articles/john-mearsheimer-discusses-global-order
Davenport, Christian: Robots, Swarming drones and "iron man": Welcome to the new arms race, June 17, 2016, Washington Post. https://www.washingtonpost.com/news/checkpoint/wp/2016/06/17/robots-swarming-drones-and-iron-man-welcome-to-the-new-arms-race
Dinatale, Martin (2014), "Defensa, Avanza en el país la fabricación de sofisticados drones", La Nación, 2 de Julio de 2014, disponible en http://www.lanacion.com.ar/1706379-avanza-en-el-pais-la-fabricacion-de-sofisticados-drones
Gorman, Siobhan y Julian Barnes (2011), "Cyber combat and Act of War: Pentagon Sets Stage for US Response to computer sabotage with military force", *The Wall Street Journal*, 31 de mayo de 2011, disponible en http://www.wsj.com/articles/SB10001424052702304563104576355623135782718
Hammes, T. X. (2013), "Offshore Control vs. AirSea Battle: Who Wins?", *The National Interest*, 21 de agosto de 2013, disponible en http://nationalinterest.org/commentary/offshore-control-vs-airsea-battle-who-wins-8920
Harrison, Adam Jay, Christopher Zember y Jawad Rachami (2014), "Innovation warfare: technology domain awareness and America's military edge", *War on the Rocks*, 29 de octubre de 2014, disponible en https://warontherocks.com/2014/10/innovation-warfare-technology-domain-awareness-and-americas-military-edge
Lin, Jeffrey & Singer Peter: China Army Hosts an Auntonomous Robots Contest, Called Overcoming Obstacles 2016, Popular Science October 26, 2016. http://www.popsci.com/chinas-army-hosts-an-autonomous-robots-contest
Nakashima, Ellen (2013), "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies", *The Washington Post*, 27 de mayo de 2013, disponible en https://www.washingtonpost.com/world/national-

security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html

Ragan, Steve (2015), "Cyber Pearl Harbor: A date that will live in infamy, and the marketing machine that hijacked it", CSO, 7 de diciembre de 2015, disponible en http://www.csoonline.com/article/3012257/techology-business/cyber-pearl-harbor-a-date-that-will-live-in-infamy-and-the-marketing-machine-that-hijacked-it.html

Schmidt, Michael y Erik Schmitt (2016), "Pentagon Confront New Threats from ISIS: Exploding Drones", *The New York Times*, 11 de octubre de 2016, disponible en http://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html

Stout, Mark: "The Danger of Inadvertent War in the Next Four Year", War on The Rocks, November 16, 2016. http://warontherocks.com/2016/11/the-danger-of-inadvertent-war-in-the-next-four-years

Xin, Hao: China to create its own DARPA http://www.sciencemag.org/news/2016/03/china-create-its-own-darpa

## Referencias

(1) El cine capturó la esencia de los temores y problemas de las armas nucleares. En las pantallas el mundo ha peleado innumerables guerras nucleares. Clásicos como "Dr. Strangelove" (1964), de Stanley Kubrick, "El día después" (1983), de Nicholas Meyer; "The War Game" (1965) de Peter Watskin y a principios de los ochenta en clave juvenil la temprana combinación de ciberespacio con las armas nucleares en la película "Juegos de Guerra" (1983) de John Badham, entre varias otras.

(2) En su libro Atrapados (*The Glass Cage*) Nicholas Carr, nos demuestra nuestra creciente dependencia de la pantalla y los efectos que ello tiene sobre nuestras habilidades humanas. Virtual y real aparecen fusionados, al tiempo que surgen debates sobre la conveniencia de responder un ataque cibernético mediante una respuesta cinética, y si es que eso debe ser considerado un acto de Guerra (Gorman y Barnes 2011).

(3) Todo liderazgo militar conoce que una vez que la contienda comienza, aquello que sucede en el campo de batalla es difícil de discernir de ahí el concepto de niebla de la guerra, no obstante y sobretodo en EE.UU. desde los anos ochenta pero efectivamente desde la primera guerra del golfo se viene trabajando en el concepto de Conocimiento total de la situación o "Total Domain Awarness", a los efectos de poder responder en tiempo real y con precisión a los avatares del campo de batalla (Harrison et al 2014).

(4) Quienes trabajan en el campo de la ciberseguridad suelen señalar que el liderazgo político, que decide, traba, o empuja una determinada línea de acción sobre determinadas tecnologías, proviene en el mejor de los casos de la transición analógica a la digital, lo cual hace que no puedan comprender el alcance de la revolución que opera en el campo tecnológico. El grado de complejidad técnica que involucra a varios de estos desarrollos, el surgimiento de un mundo gobernado por algoritmos cada vez mas complejos y la subsiguiente castas de algorimistas, provoca dos situaciones: una desinterés en la sociedad, y en especial en el liderazgo político, lo cual puede provocar líneas de trabajo ya sea por parte de gobierno o de actores privados contraproducentes y que a la larga tenga consecuencias negativas para el ser humano. La segunda consecuencia es que al no apreciar las virtudes de dichos desarrollos se traben, limiten o discontinúen líneas de investigación necesarias e importantes para el desarrollo humano.

(5) El debut del Teledyn Ryan BQM-34 fue en 1964 y su despliegue operacional fue limitado. Recién en 1991 después de la Guerra del Golfo es que la nueva generación de drones fue aceptada como parte integral del campo de batalla. Poner armas en los drones es algo inclusive mas reciente que data del año 2006 cuando aparecieron los primeros predators armados, luego conocidos como Reapers (Mahnkem 2008).

(6) En las conclusiones de su libro, "Going Down 1945-?", pone de manifiesto que el advenimiento de los misiles intercontinentales y los Drones marcan el final del poder aéreo, las variaciones de funciones y el desarrollo de aviones

para tareas especificas, declinando en variedad, como en números para ser reemplazados por estos ingenios no tripulados (Van Creveld 2011).

(7) Argentina al final de la IIGM desarrolló -en una escala menor- capacidades similares y convergentes con aquellas que desarrollaban las grandes potencias. Este momento de frontera tecnológica en el campo de la aviación a reacción, la cohetería y la energía nuclear, el liderazgo político supo ver e integrar dichos avances a su idea de crecimiento y eventualmente de potencialidad para el país. Lamentablemente algunos desarrollos fueron terminados, como el de la aviación a reacción, otros desvirtuados como el de cohetería, y solo se salvó la energía nuclear y sus proyectos civiles que hoy dan a la Argentina un lugar en la mesa de los países poseedores de tecnologías sensibles. Las restricciones para desarrollar robots, nano y otros desarrollos todavía no son tantas aunque indudablemente irán apareciendo a medida que se aumenten los usuarios y temores sobre estas tecnologías cerrando la ventana de oportunidad para potencias medias de desarrollar estas capacidades, las cuales además deberán contar con una clara idea de colaboración transnacional y además vinculando al sector privado con el público. Esa necesidad de una estrategia de inserción en este campo todavía no es evidente para los decisores mas allá de algunos clisés discursivos.

(8) Noruega, Suiza y Suecia también han alcanzando un importante desarrollo de aplicaciones militares con tecnologías disruptivas pero, en estos casos, en cooperación con los países mencionados.

(9) La idea de control total del espacio geográfico no es nueva en si misma, y la historia de la humanidad puede ser definida en términos del esfuerzo que se ha realizado para desarrollar capacidades primero para acceder a determinados espacios, luego para obtener ventajas de los mismo y para ejercer control, sobre el entorno y quienes están en el. La combinación del poder de computación y análisis está permitiendo llevar a cabo esta aspiración de control por parte de los grandes poderes, en especial de occidente. Ian G.R. Shaw (2016) expone estas ideas. Una buena referencia cinematográfica de esta situación se encuentra en la película "Battleship" (2012) donde se utiliza el sistema de boyas del servicio oceanográfico norteamericano, como sistema de ubicación alternativa en caso de que Estados Unidos u otra potencia anulara los sistemas de posicionamiento de los destructores de la armada japonesa. En la fantasía se lo utiliza contra unos alienígenas invasores, pero el mensaje queda en evidencia de cuan monitoreados están, inclusive, los aliados. Asimismo, la película "Control Total" (Eagle eye -2008) muestra como una versión avanzada del sistema IBM Watson que está en el Departamento de Defensa planeando una acción terrorista para empujar una agenda de seguridad que permita a Estados Unidos alcanzar un grado de seguridad mayor en la guerra contra el terrorismo, eliminando a una serie de actores políticos relevantes.

(10) El problema del control y los excesos que ello puede provocar se ha traducido en un sonoro debate en relación a las capacidades de distintos actores en el ciberespacio. En este sentido, las posiciones optimistas señalan que las oportunidades que brinda el ciberespacio flexibilizan las fronteras logrando que los regímenes autoritarios, los líderes políticos que tengan una agenda oculta sientan su amenaza, como se puede observar en los casos de Anonymus y otros notables grupos de hackers. Wikileaks ha jugado un rol central en estropear la posición internacional de Estados Unidos y recientemente en boicotear la carrera presidencial de Hillary Clinton, al punto tal que la candidata llego a identificar a este grupo con Rusia. Posiciones más pesimistas ponen de manifiesto que será imposible competir contra la creciente acumulación de activos de poder por parte de actores privados que pondrán en juego la propia privacidad individual a favor de aquel que pueda solventar dicha empresa. Las agencias de inteligencia con estas capacidades podrán constituirse en el poder detrás del poder. Nuevamente los casos de Wikileaks y Edward Snowden, muestran que ambas posiciones se dan en simultáneo. La idea de un panóptico internacional sobre el que no hay capacidad de rendición de cuentas es opaco y, además, crece de manera poco contralada, toma forma (Whitaker 1999). Finalmente, la tensión existente entre anonimidad e identificación está provocando una fuerte pulseada entre el Estado y los actores no estatales que buscan cubrir sus rastros

en el ciberespacio y aquellos que quieren identificarlos para poder realizar las tareas de atribución, sobre todo si provienen del campo estatal y de esa forma castigar a quien corresponda (Rid y Buchanan 2015). Estas tecnologías generan la discusión creciente sobre el riesgo de una guerra inadvertida, como se puede apreciar (Stout 2016).

(11) El Pentágono ha publicado varios reportes que evidencian un incremento del robo de información por parte de hackers chinos, suponiendo que quienes están detrás de dichas operaciones es el propio estado chino. Hasta el momento se sabe que China ha tenido acceso a sistemas de armas de todo tipo, desde aquellos que forman parte del escudo antimisiles como el THAAD o el Patriot PAC-3, hasta el avión de combate mas sofisticado del mundo el F-35. Asimismo los UAV chinos tienen un parecido para nada casual con los Predator, Reapers, y Global Hawk norteamericanos. También se cree que el helicóptero hibrido V-22 Osprey ha caído en manos de los ingenieros chinos. Las consecuencias de esas acciones es que China ha reducido la brecha tecnológica con Estados Unidos rápidamente según ha puesto de manifiesto el Asesor de Seguridad Nacional Tom Donilon (Nakashima 2013).

(12) El combate a la llamada ruta de la seda en la llamada dark web o la internet oculta muestra la lógica de hidra de múltiples cabezas, que presenta la seguridad en este campo y sin embargo el Estado en el uso de sus capacidades puede ir afectando sus operaciones. Aun cuando parezcan conflictos de nunca acabar, las disrupciones aprendizajes y medidas de respuesta hará cada vez mas difícil operar en un espacio que aun cuando es fluido tiene lógicas de funcionamiento restrictivas, básicamente para el lector que no posee conocimientos sobre este tema, bien podría decirse que navegar por internet no significa ser un ciberguerrero y no todos los que tienen computadoras o servers forman un cibercomando.

(13) Hasta el momento se conocen solo seis países con la capacidad de poner misiles a sus UAV. Cinco son productores (Estados Unidos, Reino Unido, Israel, Rusia y China). Irán, Irak y Pakistán los utilizan con misiles guiados de manufactura china; Francia utiliza los vendidos por Estados Unidos y el Congreso norteamericano autorizó la venta de armados a Arabia Saudita. En el campo de los actores no estatales se encuentra bien documentado el uso de UAV civiles por parte de Heezbollah contra las IDF israelíes, y a mediados de octubre se informó que se sospecha que drones de manufactura civil fueron modificados y artillados por ISIS contras las peshmergas con cierto éxito (Schmidt y Schmidt 2016).

(14) Para conocer quienes y que tipo de drones se están desarrollando se recomienda la siguiente página http://securitydata.newamerica.net/world-drones.html

(15) Defense Research Advance Project Agency, dicha agencia no tiene un laboratorio en si, pero dispone de casi cuatro mil millones de U$S para distribuir en distintas competencias de tecnología para que las universidades e investigadores industriales desarrollar "ciencia al limite".

(16) El PLA realiza el mismo tipo de competencia la cual recibe el nombre en castellano de "sobrepasando grandes obstáculos" (Lin y Singer 2016). Este tipo de competencia dependía del Comité de Armamentos Generales del PLA, el cual seria disuelto y se crearía una comisión mixta entre el PLA y la Academia China de Ciencias. (Xin s/f). Rusia por su parte tiene ha creado una nueva agencia en función de sus retrasos tecnológicos. Conocida en inglés como *Russian Foundation for Advance Research Project in the Defense Agency*.

(17) Es por ello que hoy vemos como diarios como el New York Times o el Washington Post se avienen a hablar de una virtual ciberguerra entre todos los grandes poderes ya que ninguno escapa a las intrusiones del otro gran poder.

(18) Stephen Van Evera desarrolla estos conceptos en su libro Causes of war (1999), el cual sirve actualmente de base para discutir en que situación deja a los estados los crecientes desarrollos de capacidades en el ciberespacio, las cuales no son fácilmente discernibles si son parte de una estructura ofensiva o de la defensa de un país. Entre otros por los serios problemas que tienen los países para llevar a cabo el ejercicio de atribución –esto es de quien es el responsable– de un ataque cibernético.

(19) Existen lógicas mas conservadoras al interior del propio pentágono, donde se señala que el existo del futuro para lidiar con china es la capacidad de bloquearle las líneas de comunicación físicas y virtuales, sin tener que desarrollar

un dispositivo ofensivo complejo como el combate aero-naval. La iniciativa conocida como offshore control encuentra adeptos en el pentágono, sobretodo en épocas de recortes presupuestarios, pero no muchos oficiales navales que apoyen este tipo de estrategia (Hammes 2013).

(20) La idea de Cole y Singer no es del todo original, aunque logran bajar a nuestros días el mismo mensaje que la serie Battlestar Galáctica realiza en el año 2004. Cuando en una reinvención del universo creado en 1978, una guerra de aniquilación comienza entre la humanidad y una raza de robots mejorados conocidos como cylones. Su ataque es una combinación de un letal virus informático que anula las defensas de las doce colonias para luego lanzar una serie de ataques nucleares simultáneos. Como consecuencia de dicha acción, la prolífica humanidad queda reducida a 50.000 hombres, mujeres y niños y una sola nave de combate la cual da el título a la serie.

(21) Algunos ejemplos de dichas ideas son Ragan (2015) y Berman (2015).

(22) Se ha discutido el concepto de guerra hibrida el cual supone la utilización de medios convencionales y tácticas no tradicionales para alcanzar objetivos políticos y militares a los efectos de desestabilizar a los países. En el caso de Ucrania incluyo la capacidad para usar subversión, ciber, proxies, operaciones convencionales para ejercer coerción y disuadir, todas ellas conducidas bajo el paraguas nuclear (Charap 2016). Con respecto a la posibilidad de un conflicto entre Estados Unidos contra Rusia y China existen visiones disidentes, ya que varios creen que el mayor problema de seguridad lo tiene Rusia en función del ascenso de China. En una reciente conferencia en Rusia en el llamado Club de Valdai, John Mearsheimer señaló las razones por las cuales existen más incentivos estructurales para cooperar con Rusia y no seguir empujándola a China (Club Valdai 2016). En este sentido, el libro de Cooper y Singer también tienen implícitos los errores cometidos por las administraciones norteamericanas antecesoras.

(23) Cuando se escribió la novela de Orson Scott Card, El Juego de Ender (1985), los videojuegos estaban entrando en su etapa de expansión planetaria. La reina de dicha época era la consola Atari y los juegos eran parte del ocio. Scott Card se animó a pensar en ellos como la base de entrenamiento militar de chicos reclutados a partir de los seis años para enfrentar a una raza de alienígenas conocida como los insectores. En un mundo simulado y controlado a distancia, Ender da fin a una civilización, pensando que solo es un juego. Hoy cientos de juegos que llegan a las consolas de videos son usados al mismo tiempo por las fuerzas armadas o grupos insurgentes para entrenar a sus combatientes en un ambiente relativamente seguro, pero también para estimular y condicionar reflejos producto de dicho entrenamiento. Hoy los juegos se readaptan y presentan nuevos niveles de dificultad y la incorporación de la realidad virtual da un espacio nuevo a los entrenamientos simulados.

(24) Cada vez con mayor frecuencia se acumulan los debates sobre el rol del ser humano en la Guerra moderna. Existen dos trabajos que valen la pena ser leídos: Singer (2009) y Coker (2013).

(25) El ciclo de vida una amenaza cibernética bien puede separarse en una serie de etapas bien definidas. La primera etapa es el descubrimiento y desarrollo de una vulnerabilidad; la segunda etapa es la de introducción de la misma en un sistema comprometido y comenzar el ataque por una determinada APT. Conocidos como "ataques de día cero" (Zero Day Attack) son fallas solo conocidas por el operador atacante, y no por el defensor. En este caso es donde el ataque reporta los mayores beneficios. La tercera etapa es la del crecimiento de acciones relacionadas con dicha capacidad, donde se busca explotar al máximo las vulnerabilidades corriendo contra el reloj antes de que sea descubierta por otro o por el mismo fabricante de software. Hasta ese momento el conocimiento de las vulnerabilidades están relativamente confinadas a los atacantes y a un número limitado de sistemas. Hasta este momento el atacante tiene ventaja. Sin embargo, dicho ciclo ofensivo comienza a declinar cuando aparece la llamada etapa de la maduración, de día cero, y el defensor comienza a actuar de manera tal de cerrar la brecha de ventaja con el atacante. La etapa final es la de difusión de la amenaza donde las ventajas del ataque se reducen a medida que la misma es conocida y los sistemas son mejor defendidos, producto de los desarrollos que se realizan. Finalmente, la última eta-

pa, llamada de declinación, donde solo pueden atacarse, usando la misma APT, sistemas que quedan exclusivamente vulnerables y aquellos que no fueron debidamente actualizados (Buchanan 2016).

(26) En la nueva edición (remake) de la película Robocop (2014), los sistemas que se emplean como "pacificadores urbanos" son los robots antropomorfos, mientras los soldados cumplen un rol de verificadores pasivos de la conducta de los robots, mediante sus pantallas táctiles. Los insurgentes que deben enfrentar a estos ingenios tienen que superar el escollo de las capacidades derivadas de la analítica de grandes datos para –si llegan a sobrevivir– pelear con los soldados, ciertamente las apuestas no estarían a favor de ellos. Toda la operación es presentada como la respuesta occidental a limitar las bajas de ambos bandos y a proteger a los soldados. El robot en sí mismo es presentado como un eje fundamental para la política exterior de ese país.

(27) Esta idea no es otra mas que la amplificación de los portaviones como plataformas de lanzamiento de ataques. Películas como "El Día de la Independencia" (1996), series como Battlestar Galactica (2004). Estas imágenes se constituyen posiblemente en la forma que se va a operar militarmente en los próximos años.

(28) ¿Cuáles son las chances de una abeja o avispa contra un ser humano? ¿Cuáles son las chances de un ser humano contra un enjambre? Esta es la lógica del *swarming*. Ya Philip K. Dick había anticipado este tipo de ataque por parte de los robots en su cuento la segunda variedad (Dick 2005). Para leer más acerca de las técnicas de enjambre, se recomienda leer a Singer (2009).

(29) En este sentido, los sistemas robóticos se vuelven autónomos en relación al grado de independencia que tienen de la decisión humana y al grado de inteligencia que se le asigna. Existen distintos niveles o grados de autonomía que van desde sistemas automáticos, semiautónomos y aquellos que son independientes de la decisión humana o autónomos. Esto tiene que ver con el grado de inteligencia artificial que poseen, en especial en su condición de adaptativa y la ejecución de procesos. CNAS Autonomous Weapons Program https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk

(30) Al igual que en otras partes del presente trabajo, el cine es quien nos permite aproximarnos conceptualmente a la implementación que estos equipos podrían tener en el campo de batalla. En la película *Al filo del mañana* (The Edge of Tomorrow), los humanos son capaces de vencer a una entidad invasora de mente colectiva utilizando estos ingenios militares que permiten aumentar el poder de fuego y de carga a los soldados en un asalto militar relativamente convencional. Con respecto a las modificaciones genéticas, las mismas las estamos realizando sobre nuestros cultivos para hacerlos más resistentes a determinadas plagas o al clima. Esa manipulación puede tener fines perversos también. Al respecto se recomienda mirar una serie corta de dos temporadas que se llama *Helix* (2014).

(31) La versión cinematográfica de dichas alteraciones genéticas se puede ver en una película de mediados de los años 90 conocida como "Soldier" (1998). Su argumento justamente trata sobre la posibilidad de que niños que fueron separados de sus familias y entrenados desde chicos para ser super-soldados, son reemplazados por un conjunto de nuevos super-soldados modificados genéticamente. Los predecesores son relegados a tareas de descarte y uno de ellos eventualmente se rebela a partir de su condición humana.

(32) En este sentido, las estrategias de compensación que precedieron a la presente fueron: La Primera Estrategia de Compensación (First offset Strategy) que tomó lugar entre 1950 y mediados de los años 70, la cual se relacionó con el desarrollo de armas nucleares de diversos tipos junto con sus plataformas asociadas pensadas para sobrevivir a un conflicto nuclear masivo, castigando a los potenciales enemigos con el pleno desarrollo integral de las capacidades nucleares. La Segunda Estrategia de Compensación tomó lugar para enfrentar a países convencionalmente poderosos y aquellos que dependieran su forma de combatir de manera convencional, produciendo un dislocamiento de las fuerzas defensivas similar al que podrían provocar un ataque nuclear que desarmara al oponente de la opción del contragolpe sin los efectos de la radiación. La misma contemplaba

la munición de precisión, la invisibilidad y la integración de los sistemas de vigilancia y reconocimiento (Technology and future Conflict, Strategic Survey, 2016).

(33) Resolución de Jefatura Gabinete de Ministros, Nro.580/2011: Creación del Programa Nacional de Infraestructuras Criticas de Información y de Ciberseguridad, bajo la Oficina Nacional de Tecnologías de la Información. A su interior tienen los siguientes grupos de trabajo: ICIC-CERT (Computer Emergency Response Team), ICIC- GAP (Grupo de Acción Preventiva), ICIC-GICI (Grupo de Infraestructuras Criticas y de Información), ICIC- Internet SANO. En el espacio del Estado Mayor Conjunto de las Fuerzas Armadas, la Resolución Nro. 343/MD establece la creación de un comando conjunto de ciberdefensa en Mayo del 2014.

(34) "Argentina desarrolla el proyecto Realidad Aumentada para la identificación de objetivos Militares", http://www.infodefensa.com/latam/2012/06/14/noticia-argentina-desarrolla-el-proyecto-realidad-aumentada-para-la-identificacion-de-objetivos-militares.html

Para citar este artículo:
Battaleme, Juan. (2016), "El campo de batalla en la actualidad", [disponible en línea desde marzo 2017], Grupo de Trabajo sobre la Inserción de la Argentina en el mundo. Consejo Argentino para las Relaciones Internacionales. Dirección URL: http://www.cari.org.ar/pdf/campo_batalla.pdf