La Ciberdefensa ofensiva y la Inteligencia Artificial

Oscar Niss
(UNDef)
oscarniss@gmail.com

Resumen: La Ciberdefensa es un Área de Capacidad nueva dentro de las Fuer zas Armadas. A diferencia de los dominios tradicionales donde se desarrollan los conflictos armados – tierra, mar y aire - el *Ciberespacio* posee, además de su anclaje territorial, una importante componente de configuración que le da las características propias de la virtualidad. No por ello exento de efectos producidos en el mundo físico ante una operación iniciada en ese dominio.

En el estado del arte actual, la protección del *Ciberespacio* es mayoritariamente defensiva, por lo que no requeriría de elementos ofensivos para el cumplimiento del objetivo, sin embargo el devenir conceptual y tecnológico está migrando hacia sistemas proactivos y no reactivos, impulsados por tecnologías disruptivas como la Inteligencia Artificial (IA).

En ese sentido, el uso dual – civil y militar - de tecnologías para la protección cibernética, conllevaría el riesgo de la propagación de ataques automatizados mediante armas dotadas de IA y posibles efectos indirectos en el mundo físico, por lo que es necesario explorar el aspecto normativo de su desarrollo y empleo.

Este artículo pretende plantear interrogantes e inquietudes frente al desafío de la irrupción de esta nueva tecnología y su empleo de uso dual, civil y militar.

Palabras Clave: Ciberdefensa; Ciberarmas; Inteligencia Artificial

1 Introducción

Sin duda, aunque no sin esfuerzo, podemos encontrar paralelismos o puntos de contacto entre el mundo físico y el ambiente creado por el hombre denominado *Ciberespacio*.

A diferencia del ambiente puramente simbólico imaginado por el autor *William Gibson*, que luego encontró anclaje en las Tecnologías de la Información y la Comunicación (TIC), el resultante tiene un enorme componente físico, siendo en gran parte contenedor del lógico o intangible. Ese componente físico tiene un claro anclaje territorial, por ende, podemos delimitar un adentro y un afuera incluso de las fronteras tradicionales, desde donde podemos inferir cuestiones de soberanía. Estas características no hacen sino manifestarnos un ambiente tensionado y atravesado incluso por aspectos vinculados a la geopolítica, cuando se ha convertido en un activo de importancia estratégica para el desarrollo de cualquier sociedad. Así lo entiende la normativa argentina cuando expresa, en su segunda propuesta de Estrategia Nacional de Ciberseguridad, que el *Ciberespacio* está concurrido por "servicios esenciales para la vida de las personas y para la economía […] con una fuerte dependencia de las redes informáticas. (República Argentina PEN, 2023).

De acuerdo a lo expresado por nuestro país, que va en línea con lo que entienden la mayoría de las naciones, se puede decir que el *Ciberespacio* atañe al quehacer de los gobiernos y al deber ser de los Estados, tanto que la Organización de las Naciones Unidas (ONU) publicó en uno de sus informes que "el derecho internacional, y en particular la Carta de las Naciones Unidas, es aplicable y esencial para mantener la paz y la estabilidad y para promover un entorno de TIC abierto, seguro, estable, accesible y pacífico." (ONU, 2021)

En ese contexto, las naciones no tardaron en poner en cuestión el tema de la soberanía en el *Ciberespacio*, por lo que comprender su naturaleza real es necesario para poder abordar cuestiones de interés nacional, como son las regulaciones sobre los asuntos de índole soberana[1] y de defensa del territorio, extendiéndolo desde los dominios tradicionales tierra, mar, aire y espacio, al *Ciberespacio*.

En ese sentido, se están perfeccionando los usos militares de las tecnologías robóticas, cibernéticas, de inteligencia artificial y de sensores remotos, llevando a los sectores de defensa de varios países a ensayar estrategias de protección ante potenciales ataques. "En casos específicos, esas innovaciones se han traducido en capacidades militares ofensivas." (ARG DCTO-2021-457-APN-PTE, p 39)

2 Desafíos

Sin duda la IA agrega un componente harto complejo a la problemática conceptual y de uso de las *Ciberarmas* dotadas de autonomía. Pero, para poder avanzar en sus aproximaciones es necesario plantearnos algunas preguntas, ¿De qué trata una Ciberarma y qué características la dotan de automatismo? ¿Cuándo existe uso de la fuerza en el espacio Cibernético? ¿Podría una Ciberarma autónoma distinguir objetivos militares de objetivos civiles? ¿De quién sería la responsabilidad de un Ciberataque autónomo?

Una definición sencilla de Ciberarma, que exige una profundización, nos la proporciona la Junta Interamericana de Defensa (JID): "Software específicamente diseñado para causar un daño o efecto perjudicial a un elemento del *Ciberespacio* pudiendo tener consecuencias físicas en los ámbitos de operaciones convencionales" (Junta Interamericana de Defensa, p. 13).

La complejidad adicional aparece cuando a la Ciberarma la dotamos de automatismo, con algoritmos de IA y Maching Learning (IA/ML). Aparecen así sistemas de *Ciberarmas* Autónomos (SCA), que son empeñados en Operaciones Multidominio[2] desde el ambiente Cibernético, en sus capas Lógica y/o TIC. Si bien los SCA pueden

[1] En la primera versión de la Estrategia Nacional de Ciberseguridad del año 2019 se expresa que "Internet representa un dominio global e intangible y un flujo infinito de datos sobre el cual no se ejerce dominio ni soberanía". Nótese las distintas concepciones acorde al posicionamiento del país en ese espacio. Incluso es notable que esa definición vaya en contra de lo expresado por la comunidad internacional en el seno de la ONU, en los distintos informes del GEG.

[2] El foco de las Operaciones Multi-dominio "se centra en todas las dimensiones del campo de batalla y no en una amenaza determinada" (Fuente - Johnson, 2018, p.6).

influir en la maniobra operacional a través de efectos kinéticos, estos siempre tienen su origen en la dimensión Cibernética y su empeño se complejiza ya que la pieza puede permanecer en estado latente hasta que se decide su activación, tal es el caso de las Amenazas Persistentes Avanzadas (APT)[3].

Resumiendo, los SCA, buscan, identifican y defienden / atacan objetivos de manera independiente, sin intervención humana, produciendo efectos primarios en el ambiente Ciberespacial o efectos kinéticos secundarios, utilizando técnicas de IA/ML.

Partiendo de ese concepto, debemos indagar sobre el *uso de la fuerza* en el *Ciberespacio*. Noruega hizo una contribución en un informe de la ONU, apoyada por muchos países miembros, donde entiende que "una Ciberoperación[4] puede constituir el uso de la fuerza o incluso un ataque armado si su escala y sus efectos son comparables a los del uso de la fuerza o de un ataque armado por medios convencionales." (Sentencia de 27 de junio de 1986, ICJ Rep., 1986, p. 14)

En ese sentido, las Operaciones Multi-Dominio[5], al integrar el espacio físico y el *Ciberespacio* como dimensiones del campo de batalla de carácter no lineal y sin límites físicos ni geográficos convencionales, presentan un gran desafío para la medición de efectos no kinéticos y fuegos no letales, por cuanto son extremadamente difíciles de dimensionar en forma cuantitativa y física[6]. Vemos así la problemática para determinar si hubo o no uso de la fuerza.

Es importante destacar que la ONU reconoció la aplicación del Artículo 2 de la Carta de Naciones Unidas, instando a los países miembros a: respetar la jurisdicción de los Estados sobre el territorio, incluida la infraestructura de TIC que se encuentra allí; la prohibición del uso de la fuerza; la prohibición de la intervención interna de la intervención interna de otros Estados; la obligación de respetar el territorio soberano de otros Estados; la obligación de no permitir a sabiendas que su territorio sea utilizado para actos contrarios a los derechos de otros Estados; y la obligación de respetar los derechos humanos. Es claro que el cómo aplicar estos principios a la dimension Ciberespacial justifica una clara línea de investigación o debate, más aun considerando que la IA/ML atraviesa cada una de ellos.

Si bien nos estamos centrando en el uso de *Ciberarmas* por parte de los Estados, debemos considerar que la mayoría de ellas están diseñadas para uso dual, esto es civil y militar. También, como en lo convencional, existe apropiación de *Ciberarmas* diseñadas para uso exclusivo militar, comercializada y utilizada en operaciones civiles por parte de individuos o grupos para estatales. Además, a diferencia de las armas convencionales, debemos tener en cuenta que su diseño y producción está al alcance

[3] APT por su denominación en Ingles *Advanced Persistent Threats*, se trata de un Ciberataque que se prolonga en el tiempo y dirigido por un proceso de *Mando y Control* en el que el atacante obtiene acceso a una infraestructura y permanece sin ser detectado por un período indefinido.

[4] Las Ciberoperaciones son acciones militares planificadas, organizadas, coordinadas y llevadas a cabo por unidades de ciberdefensa con la finalidad de lograr efectos en el ciberespacio, así como en los otros ámbitos de operaciones.

[5] En esencia hablamos de operaciones que se desarrollan en los dominios físico y cibernético.

[6] Adaptación del texto OPERACIONES MULTI-DOMINIO: SOLUCIONES TÁCTICAS PARA DESAFÍOS ESTRATÉGICOS Y OPERACIONALES de Osvaldo Alaniz Miranda.

de un personas con los conocimientos necesarios, con bajísimos costos y además con ayuda hoy, de la IA. Capítulo aparte es el uso de la IA para el diseño de armas, que ameritaría un proyecto de investigación, donde sería interesante preguntarse sobre la regulación de la IA para estos casos. Un elemento estrechamente vinculado al concepto y diseño de un SCA está relacionado a la obligación del sistema de distinguir objetivos militares de civiles. Recordemos los Convenios de La Haya de 1907, cuya finalidad primordial consiste en limitar la guerra a ataques contra objetivos necesarios para el resultado de las operaciones militares distinguiendo objetivos civiles de militares. Aquí, otra complejidad que se presenta, es que existen infraestructuras civiles que podrían ser subsidiarias al Sistema de Defensa, constituyendo un objetivo en momentos de una operación militar. En estos casos la supresión de ese objetivo podría ser necesario para el cumplimiento de una misión militar. Queda abierto el interrogante ¿quién tomaría esa decisión en el caso del empleo de un SCA?¿sería responsabilidad de la capa de diseño o de la operación?.

3 Conclusión

La complejidad presentada por las tecnologías de IA/ML aplicadas a la Ciberdefensa Ofensiva en operaciones militares, exceden al análisis que pueda hacerse desde una sola dimensión y requieren de un abordaje multidisciplinario.

Las *Ciberarmas* con IA/ML o SCA - si bien su empleo debiera estar restringido al uso militar - se venden en mercados de la Deep o Dark Web al que puede acceder una organización civil sin ningún control estatal. Es claro que el diseño y programación de este tipo de armas deben minimizar el sesgo en los datos y en el algoritmo, para garantizar que las decisiones que tome la *Ciberarma* sean ajustas al derecho y las normas, esto implica la necesidad de implementar procesos rigurosos de verificación y validación por parte de los Estados u organismos a traves de tratados específicos entre las naciones. Como se dijo al comienzo, las tecnologías disruptivas se llevan por delante las normas, corren delante de ellas. Aún no se canceló el debate sobre la Paz y Seguridad en el *Ciberespacio*, dado en el seno de la ONU y ya se le agrega una complejidad más con la irrupción de la IA/ML.

Otra dimensión de la IA/ML para uso militar, que excede este trabajo, es la generación de información falsa para interferir en la maniobra del oponente. Basta citar el informe del United States Special Operations Command (USSOCOM) donde propone el uso de estas nuevas tecnologías para desarrollar "operaciones de influencia, engaño digital, interrupción de la comunicación y campañas de desinformación en el borde táctico y los niveles operativos" (Agency: United States Special Operations Command, 2020, pág. 16). Se abre aquí una línea de investigación que llega a los límites de la convivencia entre naciones, si se quiere. “Es una tecnología peligrosa”, dijo Rizzuto, investigador del Atlantic Council. “No se puede moderar esta tecnología de la misma manera que abordamos otros tipos de contenido en Internet”, dijo. “Los deepfakes como tecnología tienen más en común con las conversaciones sobre la no proliferación nuclear”.

Esta tecnología de la IA/ML, disruptiva por excelencia, plantea nuevos paradigmas en el desarrollo de la Ciberdefensa Ofensiva y los conflictos armados, que deben ser abordados con la suficiente antelación que otras tecnologías disruptivas también requerían y no tuvieron. El aspecto legal, las normas y las leyes del derecho internacional, y la diplomacia para el mantenimiento de la seguridad y la paz en el *Ciberespacio* están nuevamente tensionadas con el avance acelerado de la IA/ML.

Referencias

1. Agency: United States Special Operations Command. (2020). BROAD AGENCY ANNOUNCEMENT USSOCOM-BAAST-2020.
2. ARG DCTO-2021-457-APN-PTE. (s.f.). Directiva de Política de Defensa Nacional2021.
3. ICRC. (2014). Report of the ICRC Expert Meeting on ‘Autonomous weapon systems.
4. Junta Interamericana de Defensa. Guía de Ciberdefensa.
5. Ministerio de Defensa RESOL-2023-105-APN-MD. (2022). Política de Ciberdefensa. Argentina.
6. Miranda, O. A. OPERACIONES MULTI-DOMINIO: SOLUCIONES TÁCTICAS PARA DESAFÍOS ESTRATÉGICOS Y OPERACIONALES.
7. ONU A/65/201. (2010). Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones .
8. ONU A/70/174.
9. ONU. (2021). Informe de las Naciones Unidas A/76/135.
10. República Argentina PEN. (02 de 1 de 2023). https://www.argentina.gob.ar. Recuperado el 28 de 02 de 2023, de https://www.argentina.gob.ar/normativa/nacional/resolución-1-2023-377806/texto
11. Sentencia de 27 de junio de 1986, ICJ Rep. (1986).