EDITORIAL ESDEG

Revista
Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023
Bogotá, D.C, Colombia
ISSN: 2955-0270 • eISSN: 3028-3310
Página web: https://esdegrevistas.edu.co/index.php/rcit

Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento

Cybernetic and cognitive tools: two concepts that displaced conventional coping methods

Diego Ospina Quintana

CITACIÓN APA:

Ospina Quintana, D. (2023). Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento. *Ciberespacio, Tecnología e Innovación, 2*(3), 83-88.
https://doi.org/10.25062/2955-0270.4777

Publicado en línea: **Junio 30 de 2023**

Enviar un artículo a la Revista

Revista Ciberespacio, Tecnología e Innovación
Volumen 2, número 3, enero-junio 2023 (pp. 83-88)
Bogotá, D.C, Colombia

EDITORIAL ESDEG

Las herramientas cibernéticas y cognitivas: dos conceptos que desplazaron los métodos convencionales de enfrentamiento

Cybernetic and cognitive tools: two concepts that displaced conventional coping methods

DOI: https://doi.org/10.25062/2955-0270.4777

Diego Ospina Quintana
Escuela Superior de Guerra "General Rafael Reyes Prieto", Bogotá D. C., Colombia

Resumen

No resulta extraño escuchar sobre nuevos escenarios y tipos de guerras en los que las partes ya no se enfrentan en campos de batalla convencionales como los que se manifestaron en las dos guerras mundiales y durante la Guerra Fría, es necesario reconocer que existen una serie de medios, métodos y elementos que de la mano de tecnologías emergentes y disruptivas, como la Inteligencia Artificial, el aprendizaje automático, la automatización de plataformas de armas, los sistemas de vigilancia, el procesamiento de datos y los vehículos no tripulados, entre otros, han estructurado una dimensión de la guerra cada vez más difusa, etérea y difícil de clasificar.

Palabras Clave: Guerra; tecnologías; dominio.

Abstract

It is not strange to hear about new scenarios and types of wars in which the parties no longer confront each other on conventional battlefields such as those that occurred in the two world wars and during the Cold War, it is necessary to recognize that there are a series of means , methods and elements that, together with emerging and disruptive technologies, such as Artificial Intelligence, machine learning, the automation of weapons platforms, surveillance systems, data processing and unmanned vehicles, among others, have structured a dimension of war that is increasingly diffuse, ethereal and difficult to classify.

Key words: War; technologies; domain.

Artículo de reflexión
Recibido: 3 de marzo de 2023 • **Aceptado:** 10 de mayo de 2023
Contacto: Luis Renato Amórtegui Rodríguez lamorteg@ucm.es

Las herramientas cibernéticas y cognitivas

Las tecnologías resultan ser un fenómeno que ha sido explotado por actores estatales y no estatales al mismo nivel de otros actores reconocidos globalmente como potencias mundiales o con actores que mantienen alianzas de gran envergadura y en escenarios absolutamente asimétricos Lo característico, es que los mismos recursos financieros y materiales, los actores irregulares han logrado ocasionar daños y afectaciones de consideración, así como materializar sus propósitos y avanzar hacia la consecución de intereses políticos y económicos particulares.

Este documento pretende de manera breve argumentar como la combinación de herramientas cibernéticas, manejo de información y de elementos cognitivos, pueden impactar de manera decisiva en el desarrollo de conflictos de nivel mundial, tomando como ejemplo puntual, la estrategia Rusa de los últimos años.

Para tratar de contrarrestar la expansión de la ideología occidental a la cabeza de EE.UU, la Unión Europea y la OTAN, quienes considera una clara amenaza para su soberanía, se tiene la participación de Vladimir Putin, presidente de la Rusia, quien entendió que ya no era posible enfrentar de manera eficiente empleando métodos convencionales como los implementados hasta el fin de la Guerra Fría (1991).

Aunque Rusia en la actualidad, y especialmente luego del pasado 24 de febrero de 2022, cuando dio inicio a lo que ellos mismos denominaron *una operación especial* contra Ucrania, es considerado como una amenaza para buena parte de la comunidad europea y sus vecinos asiáticos, no es igualmente catalogado por otras naciones que, a pesar de esto, no le ven como su enemigo directo, sino más bien como un reto, que se debe vigilar y mantener en el radar con un seguimiento especial. Los antores antagonistas de occidente, ven a Rusia como un importante socio que les puede potencializar en la consecución de sus intereses nacionales (Sputnik Mundo, 2023).

Esta diferencia, al momento de definir lo que significa Rusia para una y otra nación, podría representar una muestra interesante de la estrategia del Kremlin para conseguir sus objetivos nacionales sin desatar una tercera guerra mundial o una reacción contundente de parte de occidente, haciendo uso de medios no militares, como su notable manejo de la información, una incontenible proliferación de dispositivos de comunicación de alta tecnología y el aumento exponencial de la conectividad.

> Desde la perspectiva de Putin, la continua rivalidad con el mundo occidental es una competencia de suma cero, lo que hace que el tipo de guerra nuevo, adaptable y flexible de Rusia, sea una respuesta lógica y relativamente barata a la superioridad occidental en el dominio convencional (Farkas, 2022, p. 3).

Un primer elemento que vale la pena señalar, es que los conceptos de guerra cibernética y ciberespacio, son propios de la terminología occidental, por lo que Rusia más

bien hace referencia al espacio de la información, el cual abarca tanto el dominio tecnológico como el psicológico; lo cual constituye el verdadero valor agregado de su estrategia, al acoplar los procesos informáticos y humanos en una misma balanza y regidos por una misma política nacional (Farkas, 2022, p.5).

Consecuente con lo anterior, la estrategia rusa en este ámbito se podría dividir en operaciones en la red y operaciones de información. Por un lado, y aunque ningún incidente hasta el momento ha podido ser atribuido oficialmente al gobierno ruso, numerosas hipótesis conducen a la contratación de empresas civiles por parte de los rusos para lanzar ataques cibernéticos, explotando precisamente la dificultad de atribución y, por lo mismo, la capacidad de respuesta del actor o activo atacado. Los rusos aún en conflictos convencionales o guerras proxy, citando al grupo Wagner como ejemplo, se consolidan en una punta de lanza de operaciones especiales prorrusas en Siria, África, Crimea y actualmente en Ucrania, solo para mencionar algunos ejemplos.

Por otro lado, Rusia le ha apostado al internet y a los medios de comunicación como una herramienta contundente para difundir sus ideas, controlar las narrativas que justifican sus operaciones militares y, finalmente, poder llegar a influenciar en los tomadores de decisiones y en los mismos ciudadanos de las naciones o alianzas objetivos, donde el propósito es alterar la cohesión, aumentar los niveles de incertidumbre e incluso afectar los sistemas políticos y económicos, dificultando una de las premisas clave para el ejercicio eficiente de alianzas internacionales como la OTAN, el consenso.

> Medidas tomadas recientemente por Rusia no son de naturaleza nueva. Los bolcheviques utilizaron el termino medidas activas cuando discutían métodos para influir en las acciones extranjeras hace más de un siglo. Desde entonces, Rusia ha utilizado este tipo de poder blando para imponer su propia voluntad a otros actores internacionales¨ (Farkas, 2022, p. 4).

Sobre esta dinámica en particular, Rusia tiene una habilidad enorme que se ha construido a lo largo de los años y de la experiencia, y es la sagacidad con que lleva a cabo campañas de desinformación y el empleo de propaganda y contrapropaganda para afectar a sus actores o naciones objetivo, los cuales generalmente corresponden a Estados con sistemas políticos democráticos occidentales que no tienen mayores restricciones a medios de comunicación ni redes sociales. De forma que, las operaciones informáticas tienen un costo relativamente bajo, pero con unos resultados que pueden llegar a resultar estratégicos si se llega a controlar la tendencia y la narrativa en escenarios internacionales, afectando elementos clave en la percepción del adversario y explotando sus vulnerabilidades ya identificadas en la conciencia y en la mente del público objetivo.

El resultado final de estas actividades informáticas, que hacen parte de la estrategia soviética en operaciones de información, de propaganda y contrapropaganda, se ve altamente potencializado mediante la explotación de campañas ejecutadas con el Ejército de trolls del Kremlin o a través de bots automatizados, que aceleran la consecución de los

objetivos en el marco psicológico y cognitivo, llegando a alterar y a hacer que se dude de la verdad misma por parte de las sociedades objetivo (Cunnighan, 2021).

De otro lado, pero en total sincronía y alineación con la política rusa de actividades en el espacio de la información, Putin y su círculo cercano, nunca han dejado de preocuparse por la carrera tecnológica y los avances en tecnologías emergentes y disruptivas, que puedan ser empleadas de manera contundente en el quinto dominio. Para lo cual, el desarrollo de semilleros de investigación y la infraestructura de innovación han sido pilares fundamentales para el Kremlin. Esta política, que incluye parques industriales, centros de ingeniería, instituciones de desarrollo financiero, así como prestigiosas universidades e institutos de investigación rusos, que, asociados con importantes fabricantes de armas y desarrolladores tecnológicos, tienen como principal pretensión fomentar la innovación en todos los campos, desarrollando nuevos sistemas de armas, pero también creando nuevos multiplicadores de fuerza basados en capacidades ya existentes.

> Por ejemplo, Rusia está experimentando con la integración de vehículos no tripulados para misiones nucleares (Proyecto Poseidón UUV), armas de precisión de largo alcance, incluidos misiles hipersónicos para disuasión no nuclear y explotar la Inteligencia Artificial en operaciones de zona gris (Zysk, 2022, p. 1).

Si bien es cierto que Rusia no atraviesa por su mejor momento para sostener un conflicto convencional, el espíritu de combate y el entrenamiento de sus fuerzas en tierra no es el mismo que el de hace dos décadas. Su economía se ha visto visiblemente golpeada por las sanciones implementadas desde antes de su invasión a Ucrania y, que, además, ha tenido que lidiar con la denominada fuga de cerebros, en la que jóvenes y mentes brillantes han decidido abandonar su país por la inestable situación económica y las condiciones complejas que se han agravado desde el inicio del conflicto.

No se debe subestimarse la capacidad de los rusos de sobreponerse, precisamente acudiendo a la implementación de estrategias híbridas en las que se combinen capacidades no convencionales, como el poder nuclear, las herramientas cibernéticas o las tecnologías emergentes disruptivas, con operaciones de información y propaganda, algo en lo que ya se había advertido, los rusos son expertos.

En ese mismo sentido, una eventual alianza estratégica con China, a pesar de que hoy en día no se vea tan factible, es un curso de acción que nunca puede descartarse, especialmente si EE.UU continúa con su ofensiva económica contra China y si la guerra en Ucrania termina involucrando a otros actores de manera directa, situación que llevaría a la integración y desarrollo de poderes, capacidades y tecnologías sin precedente, en un escenario que no solo se conciba en el imaginario, podría desencadenar el primer conflicto cibernético internacional, donde las herramientas y armas convencionales pasarían a un segundo plano y la supremacía se manifestaría en el dominio de lo tecnológico integrado con la explotación del elemento psicológico y cognitivo.

Conclusión

Para concluir, resulta imperativo afirmar que teniendo en cuenta las diferentes capacidades que se vienen desarrollando en tecnología, que involucran el ciberespacio como su principal medio, ninguna nación puede sentirse excluida de las amenazas que esto puede representar a su estabilidad, este no es un tema que exclusivamente deba preocupar a las grandes potencias o a las naciones con altos estándares en políticas cibernéticas, sino que, por el contrario, países como Colombia que hasta ahora se encuentran en una fase inicial en la estructuración de la protección de este dominio. Se deben encender alertas y trabajar fuertemente para posicionar esta capacidad con una política nacional lógica, clara y robusta, donde sin duda el primer paso debe ser la alfabetización tecnológica, de manera tal que el ciudadano promedio, sin necesidad de ser técnico o profesional en tecnología o informática, pueda entender y dimensionar la importancia de este campo.

De forma simultánea, la explotación de alianzas estratégicas regionales y globales, con naciones y organizaciones como la OTAN, que permitan potencializar tanto en conocimientos como en recursos e infraestructura la ciberdefensa nacional; serían dos escalones iniciales en la construcción de una política seria, y prospectiva, sustentada en el conocimiento, en el juicio estratégico y en la capacidad de adaptación para resolver problemas en escenarios cambiantes.

Declaración de divulgación

El autor declara que no existe ningún potencial conflicto de interés relacionado con el artículo.

Autor

Diego Ospina Quintana. Mayor del Ejército Nacional de Colombia. Candidato a Magíster en Ciberdefensa y Ciberseguridad, Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. Administrador de Empresas, Universidad Militar Nueva Granada, Colombia.

Orcid: https://orcid.org/0009-0008-8932-5157 Contacto: ospinadq@esdeg.edu.co

Referencias

Cunningham, C. (2021, Octubre). *A Russian Federation Information Warfare Primer.* The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/

Farkas, S. (2022, Abril). *Information warfare: Russia´s alternative, cheap solution to counter the conventional superiority of the west.* NDC Academic Portal. https://www.ndc.nato.int/download/downloads.php?icode=759

Forest, J. (2020, 16 Septiembre). *Globalization and transnational Crime.* E-International Relations. https://www.e-ir.info/2020/09/16/globalization-and-transnational-crime/

Gilli, A. (2021, Noviembre). *Future warfare, future skills, future professional military education.* NDC Academic portal. https://www.ndc.nato.int/download/downloads.php?icode=713

Smith, R. (2008). *The Utility of Force: The Art of War in the Modern World.* Van Haren Publishing.

Mundo, S. (2023, 2 febrero). El avance y los resultados de la operación militar rusa en Ucrania *Sputnik Mundo.* https://sputniknews.lat/20230202/mapa-como-avanza-la-operacion-especial-de-rusia-en-ucrania-1126329635.html

Zysc, K. (2022, mayo). Is Russia a threat in emerging and disruptive technologies?. *Sputnik Mundo.* https://sputniknews.lat/20230202/mapa-como-avanza-la-operacion- especial-de-rusia-en-ucrania-1126329635.html