ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

85/2019 27 de septiembre de 2019

*David García Cantalapiedra**

Hacia un nuevo concepto de seguridad en un espacio multidominio: complejidad, guerra y seguridad transdominio

Hacia un nuevo concepto de seguridad en un espacio multidominio: complejidad, guerra y seguridad transdominio

Resumen:

En un escenario de transformación del Estado westfaliano y el concepto de la guerra, cada vez más influida por las amenazas híbridas y la guerra ilimitada; la integración de la seguridad interior y exterior, y un espacio de multidominio y competitivo, la concepción de la seguridad no parece ya la que se ha mantenido hasta ahora, sino buscando el objetivo del control de los dominios, sobre todo de los no físicos, en un concepto de seguridad transdominio. No obstante, ni la comunidad estratégica europea, los estudios de seguridad o las instituciones europeas han dado aún una clara respuesta teórica, estratégica o política a este transcendental cambio.

Palabras clave:

Seguridad, defensa, guerra, dominios, orden internacional.

Toward a new security concept in a multi-domain space: Complexity, War and Cross-domain Security

Abstract:

Due to a transformative scenario in the Westphalian State system and the concept of War, influenced by hybrid threats and Unrestricted Warfare; the integration process between Security and Defence, and a competitive and multi-domain space, the conception of Security is under a changing process, focused on the control of domains, above all regarding to the non-physical, toward a trans-domain security. Nevertheless, the European strategic community, Security Studies or EU institutions are not be able to offer a clear response to this transcendent process at any theorical, strategic or political level.

Keywords:

Security, defence, war, domains, international order.

Cómo citar este documento:

GARCÍA CANTALAPIEDRA, David. *Hacia un nuevo concepto de seguridad en un espacio multidominio: complejidad, guerra y seguridad transdominio.* Documento de Opinión IEEE 85/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción: orden internacional, guerra y seguridad

El concepto de seguridad está cambiando más rápido de lo que piensan los políticos, militares y académicos. Así, la separación entre la seguridad interior y exterior se ha estado difuminando progresivamente y los ataques del 11 de septiembre de 2001 confirmaron esta dinámica. La seguridad comprehensiva ya se había utilizado desde principios de la década de 1990: «La seguridad es liberarse de la amenaza y ser capaz, bien sean los Estados y las sociedades de mantener su independencia en lo que se refiere a su identidad, y a su integridad funcional, frente a las fuerzas de cambio consideradas hostiles»[1]. La lógica de la ampliación de este concepto de seguridad tras la Guerra Fría, mientras que sufrió un proceso de desmilitarización, paradójicamente, introdujo una extensa variedad de áreas para «securitizar», algunas de ellas apenas relacionadas con la seguridad «clásica» y que cerró la etapa de los estudios estratégicos. Sin embargo, abriría un intenso debate en los ámbitos político y académico debido a la problemática de esas nuevas amenazas y desafíos y provocaban en la estructura de la concepción general de ese modelo de seguridad. Esto impulsaría la creación del llamado «enfoque integral», y más tarde el uso de la resiliencia. Por lo tanto, una concepción que habría funcionado lo suficientemente bien después de la Guerra Fría fue duramente afectada cuando los ataques del 11 de septiembre produjeron una progresiva remilitarización de la seguridad llevada a cabo por Estados y actores no estatales. Sin embargo, esta remilitarización significaba evitar la «guerra convencional» con la mayoría de estos actores actuando bajo el nivel del concepto legal de guerra. Las lecciones de la guerra del Golfo, pero también las de Somalia o Kosovo, entre otras, habían quedado claras para ambos tipos de actores. Por un lado, para Rusia, China y otros Estados autoritarios y, por otro, para Al Qaeda, Talibán, ISIS y otras insurgencias. Pero también para otros como los poderosos grupos del crimen organizado transnacional. Esto provocaría un número importante de debates conceptuales, pero otros conceptos como la «guerra ilimitada» o sin restricciones (*Unrestricted Warfare*) y la «Estrategia de las

[1] BUZAN, Barry. “New Patterns of Global Security in the Twenty-First Century”. International Affairs, Vol. 67, No. 3, July 1991. pp. 431-451

Tres Guerras» (*Three Warfare Strategy)*[2], o la Insurgencia Criminal[3] no recibieron suficiente atención. Lo cierto es que ninguno de estos conceptos generó respuestas en la comunidad estratégica occidental. Además, las dinámicas y amenazas más «clásicas» como las armas nucleares también han recuperado un papel principal nuevamente en este escenario, pero sin el marco de «reglas» de la Guerra Fría. Este escenario sería aún más complejo debido al impacto de la militarización del espacio, la irrupción transversal del ciberespacio, la biotecnología y de la Inteligencia Artificial[4]. A pesar de ello, la comunidad académica de estudios de seguridad, la comunidad estratégica de la UE o hasta las instituciones de la UE apenas han abandonado o modificado sus enfoques principales. Incluso se han mantenido en posiciones ideológicamente bastante atrincheradas a pesar del fin del orden de seguridad europeo post-Guerra Fría tras el abandono del Tratado sobre Fuerzas Convencionales en Europa por Rusia en 2007, la ruptura del Principio III del Acta Final de Helsinki (inviolabilidad de las fronteras) con la invasión de Georgia (2008) y Ucrania (2014), y la denuncia y fin del Tratado INF de 1987 en 2019. Solo tras la crisis de 2014 en Ucrania, hubo pasos tímidos centrados en cómo responder a la guerra de nueva generación de Rusia a través de las definiciones de la OTAN sobre la guerra híbrida. Finalmente, instituciones y organismos de la UE ofrecerían respuestas a estas dinámicas, pero no ofrecían un análisis sobre el impacto de la guerra ilimitada, ni una revisión real y profunda sobre nuestra concepción de la seguridad. El pensamiento estratégico europeo no ha reconsiderado seria y profundamente nuestra concepción de la seguridad respecto a una serie de temas clave, como son la relación concepto de la guerra-orden internacional liberal en declive; la incertidumbre como el problema central en un proceso de solapamiento entre seguridad y defensa; así como la gran estrategia a largo plazo en un contexto de competición[5] y guerra ilimitada[6]. Sumado

[2] QIAO Liang and WANG Xiangsui. “Unrestricted Warfare”. PLA Literature and Arts Publishing House, Beijing February 1999; Office of the Secretary of Defense. Military and Security Developments Involving the People’s Republic of China 2011, Annual Report to Congress. 16 August 2011.

[3] SULLIVAN, J. & BUNKER, R “Rethinking insurgency: criminality, spirituality, and societal warfare in the Americas”, Small Wars & Insurgencies, 22:5, 2011. p. 742-763;

[4] KISSINGER, H. et al. ”The Metamorphosis”. The Atlantic. August 2019. Disponible en: https://amp-theatlantic-com.cdn.ampproject.org/c/s/amp.theatlantic.com/amp/article/592771/ Fecha de consulta 25.08.2019

[5] BRANDS, Hal. “The Lost Art of Long-Term Competition”. The Washington Quarterly. vol 41, 4, Winter 2019. pp. 31–51; CSIS. “Rebuilding Strategic Thinking”. A Report of the CSIS Transnational Threats Project. October 2018.

[6] Véase FERCHEN, M. Assessing China’s Influence in Europe through Investments in Technology and Infrastructure. Four Cases. LeidenAsiaCentre. Leiden University. December 2018; TOBIN, Liza.

a todo lo anterior, y coexistiendo con esta realidad (o interrelacionada con ella), la existencia de una red global de redes donde se juega, no a través de la negociación, sino mediante la construcción de conexiones y relaciones y en la dinámica de los sistemas no jerárquicos[7].

Un nuevo sistema internacional, un nuevo concepto de seguridad

Viniendo del impulso del «fin de la historia», de un momento en que todavía parecía fácil establecer la diferencia entre guerra y paz, y entre la seguridad interior y la exterior, también fue fácil establecer un concepto de seguridad modular y una idea de complejo de seguridad en el que la seguridad de los Estados y los individuos estaban intrínsecamente vinculados como estableció la Escuela de Copenhague durante la década de los 90[8]. Esta aproximación partía de cierta idea de orden, realmente basada en un sistema Westfaliano y un orden internacional liberal. Sin embargo, Hedley Bull ya establecía en su seminario *The Anarchic Society* de 1977, los cambios que podrían tener lugar en la estructura del sistema internacional donde los Estados, ese sistema de Westfalia, comenzaran a perder su dominio a través de una reducción progresiva de soberanía a favor de los actores no estatales que provocaría la aparición de la violencia privada y la pérdida de un monopolio sobre el uso de la fuerza, incluida la influencia de los actores transnacionales y la tecnología que podrían hacer desaparecer progresivamente las fronteras. Bull argumentó que, si ocurriera esta dinámica, entre otros, el sistema internacional podría volver a una situación *prewestfaliana* y que habría una serie completa de actores no estatales que no solo competirían con el Estado como entidades principales del sistema internacional, sino que incluso podrían reemplazarlo[9]. Así, la guerra consistía en violencia organizada entre Estados soberanos por normas o reglas, ya fueran legales o no, de los Estados. Sin embargo, si el sistema evolucionara a esa situación *prewestfaliana* que planteó Bull, ¿sería solo la violencia organizada de

"Underway. Beijing's Strategy to Build China into a Maritime Great Power," Naval War College Review: Vol. 71: No. 2, Article 5. 2018; una postura especialmente realista y dura es la de Stephen Walt, "Europe's Future Is as China's Enemy". Foreign Policy. January 22, 2019.

[7] Véase la obra del profesor Robert Jervis, "System Effects". Princeton,1999.

[8] BUZAN, B., WAEVER, O. & WILDE, Jaap de. "Security: A New Framework for Analysis". Lynne Rienner Publishers. 1998.

[9] BULL, Hedley. "The Anarchical Society. a study of order in world politics". Columbia University Press, New York, 1977.

las unidades políticas llevadas unas contra otras lo que consideraríamos guerra, o este concepto se ampliaría? ¿Qué pasaría si hubiera unidades políticas no estatales, o incluso unidades no políticas, desde el punto de vista de la definición de guerra? ¿Sería posible la guerra entre ellos y los Estados? Además, ¿sería posible la guerra en un sistema *prewestfaliano*? Bull articuló su concepto de guerra a través de la diferencia entre la guerra en el sentido material, es decir, las hostilidades reales; y la guerra en el sentido legal o normativo. Por ejemplo, si se habla de la guerra en el sentido legal, la distinción entre guerra y paz es absoluta. Por otro lado, la guerra en el sentido material es a veces difícil de distinguir de la paz. Pero Bull reconoció la imposibilidad de separar los dos conceptos, ya que la dinámica de las hostilidades a veces juega en contra de esa separación. Así, las «amenazas híbridas» o la «zona gris» siempre han existido en diferentes formas, pero una falta de conciencia histórica también ha contribuido a nuestra falta de preparación conceptual[10]. Rosa Brooks afirma: «En un mundo donde presionar un botón puede permitir, en cuestión de segundos, la muerte de una persona determinada a más de 10 000 kilómetros de distancia, ¿es posible definir «guerra» con claridad? Más aún cuando los límites referidos al ámbito de lo militar y de la guerra son cada vez más borrosos, ¿pagaremos un precio por ello?»[11].

[10] ECHEVERRIA, A. J. “Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy”. United States Army War College Press. Carlisle Barracks, Pennsylvania. April, 2016.

[11] BROOKS, R. “How Everything Became War and the Military Became Everything”. Simon and Schuster, 2016. p. 8

La necesidad de un nuevo marco de análisis multidominio: amenazas híbridas, *guerra ilimitada* y un concepto de seguridad transdominio

Frank Hoffman[12], las Fuerzas Armadas de EE. UU.[13], la UE[14], el Centro de Excelencia sobre Amenazas Híbridas (HybridCoE)[15] o la OTAN[16] hacen aproximaciones y definiciones diferentes sobre las amenazas híbridas, y otros usan el término para describir la llamada doctrina Gerasimov[17]. Esta situación plantea una falta de consenso doctrinal y la existencia de grandes diferencias sobre el alcance material del concepto. Aurel Sari estima que establecer que las amenazas híbridas son actividades producidas por debajo del umbral de una guerra legalmente declarado sería, hasta cierto punto, ingenuo, y socavaría cualquier intento de definición claro, ya que estas «guerras» son ya una rareza[18]. Brooks declara: «De igual forma, luchamos para establecer la diferencia entre "civiles" y "combatientes". ¿Cuál sería entonces un objeto civil protegido en el ciberespacio? ¿Cuándo puede un hacker, un financiero o un propagandista ser considerado un combatiente?»[19]. Cada vez más se difumina la distinción entre lo que es y lo que no es un campo de batalla: los llamados «espacios comunes» (*Global Commons*) son todos campos de batalla potenciales, pero también los espacios no físicos. Así, parece que no hay consenso sobre qué es un campo de batalla y qué no lo es, entre qué es paz y qué es guerra, cuál es el estado «normal» y cómo definiremos la seguridad. La doctrina ha debatido sobre la naturaleza y el impacto de estas amenazas, pero no existe un debate sobre el impacto de estas categorías en los estudios de

[12] HOFFMAN, F. "Hybrid Warfare and Challenges". *Joint Forces Quarterly*, nº 52, 2009. Disponible en: http://smallwarsjournal.com/documents/jfqhoffman.pdf Fecha de consulta 20.07.2019

[13] ADRP 3-0. Army Doctrine Reference Publication. No. 3-0. Headquarters Department of the Army. Washington, DC, 6 October 2017. pp. 1-3

[14] European Commission, Joint Framework on Countering Hybrid Threats: A European Union Response, JOIN (2016) 18 final (Apr. 6, 2016). Secretary-General of the European Commission, Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats 'EU Playbook' 11034/16 (July 7, 2016).

[15] Hybrid CoE. Countering Hybrid Threats 2019. Disponible en: https://www.hybridcoe.fi/hybrid-threats/ Fecha de consulta 20.07.2019

[16] NATO. Hybrid thr. Disponible en: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en Fecha de consulta 20.07.2019

[17] GALEOTTI, Mark "The 'Gerasimov Doctrine' and Russian Non-Linear War," Moscow's Shadow (blog), July 6, 2014.

[18] SARIA, A. "Hybrid Warfare, Law and the Fulda Gap". Law School. Exeter. pp.14-15.

[19] BROOKS, R. "Rule of Law in the Grey Zone". Modern War Institute. July 2, 2018.

seguridad, ni un intento real de ofrecer nuevos enfoques y la definición del concepto de seguridad[20]. Sin embargo, las concepciones anteriores al primer enfoque de Hoffman suponían ya un desafío incluso más importante: los coroneles del Ejército Popular de la RPC, Qiao Liang y Wang Xiangsui, definieron la guerra, en su libro de 1999, como «el uso de todos los medios, incluidas las fuerzas armadas o no armadas, militares y no militares, y medios letales y no letales para obligar a un enemigo a aceptar sus intereses»[21]. Así, la idea de limitar la guerra como concepto y objetivo no funcionaría tal y como ya fue desarrollado por Hedley Bull. Paradójicamente, a pesar de que las características y los medios de la guerra han evolucionado, esta sigue siendo, a la Clausewitz, «un acto de fuerza para obligar a nuestro enemigo a hacer nuestra voluntad», donde «para la aplicación de esa fuerza no hay límite». Sin embargo, no cabría pensar en esa aplicación desde el punto de vista de fuerza material y militar incremental, sino en la búsqueda de la expansión de los dominios de la guerra. Esto hace posible la expansión exponencial del concepto del campo de batalla más allá del dominio físico al eliminar sus restricciones geográficas, funcionales, políticas y legales permitiendo que se vuelva omnipresente. En respuesta a la pregunta «¿dónde está el campo de batalla?». Liang y Xiangsui responden simplemente que ahora está «en todas partes». Por lo tanto, esta aplicación podría ser cualitativa y no necesariamente cuantitativa en términos de escalada en el uso de la fuerza cinética militar, como se interpreta comúnmente. Esta expansión de los medios se hace a los diferentes dominios: todos estos actores, todas estas capacidades diferentes, significan extenderse a todos los dominios. Paradójicamente, al apuntar al control de estos dominios, esto también podría significar una tendencia a su «militarización», sobre todo por el impacto transversal del ciberespacio y la pérdida de diferencia entre lo civil y lo militar. Es sintomático este uso y la búsqueda de control de los dominios, sobre todo del ciberespacio, por parte de algunas grandes potencias[22]. Este proceso está en directa

[20] Excepto por algunos pocos intentos. Véase BARKAWI, T. “From War to Security: Security Studies, the Wider Agenda and the Fate of the Study of War”. Millennium: Journal of International Studies. Vol. 39, nº 3, 2011. pp. 701–716.

[21] QIAO Liang and WANG Xiangsui. “Unrestricted Warfare”. PLA Literature and Arts Publishing House, Beijing February 1999. P. 7; HAROLD, S. “Defeat, Not Merely Compete. China's View of Its Military Aerospace Goals and Requirements in Relation to the United States”. RAND. 2018. Disponible en: https://www.rand.org/pubs/research_reports/RR2588.html Fecha de consulta 20.07.2019.

[22] Véase, por ejemplo, BEHA, Patrick. “Civil-Military Integration in China: A Techno-Nationalist Approach to Development”. American Journal of Chinese Studies, Vol. 18, No. 2, octubre 2011, pp. 97-111; LASKAI, L. “Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise”. Net Politics

relación con el otro aspecto que Bull señaló como una causa para el fin del sistema de Westfalia. La Cuarta Revolución Industrial-Tecnológica, el ciberespacio, la Inteligencia Artificial (IA) y la relación con los humanos, no solo en el Internet de las Cosas, sino en el Campo de Batalla de las Cosas (*Battlefield of Things*). Como Alexander Kott establece: «¿Qué va a ocurrir en el campo de batalla del futuro cuando humanos y maquinas luchen unos contra otros, pero "piensen "de manera diferente? Esto va a hacer el campo de batalla más duro de comprender y manejar. Los combatientes humanos tendrán que enfrentarse a un mundo impredecible mucho más complejo donde las cosas tendrán su propia mente y llevarán a cabo acciones que puedan parecer inexplicables a los humanos»[23].

¿Cómo será la relación humano-IA? ¿Será una fuerza humana prescindible tácticamente para sostener estratégicamente una máquina-robot autónoma/IA, que ofrecerá la victoria en un enfrentamiento, batalla, guerra o conflicto general? En este sentido las expectativas para una IA podrían ser diferentes a las de los humanos. Al mismo tiempo, como los niveles de incertidumbre serán más y más altos en el campo de batalla, también lo serán en el ámbito de la seguridad: ¿quién entonces va a identificar una amenaza existencial y un objeto o ideal para proteger? ¿Será necesario persuadir a una audiencia? Más aún, ¿habrá un proceso situación normal-securitización-desecuritización de acuerdo con los parámetros de la Escuela de Copenhague?

Este nuevo «campo de batalla» está tan lleno de incertidumbre que hace casi imposible reconocer amenazas, objetos protegidos, estrategias claras o «actos discursivos». Esa incertidumbre nos empujaría a buscar el control de los dominios tanto como podamos para reducirla. En el campo de la defensa parece que esta situación conduce al campo

and Digital and Cyberspace Policy Program. CFR. January 29, 2018. También en el uso de las fuerzas armadas en la lucha contra el crimen organizado transnacional, véanse los estudios publicados por el Real Instituto Elcano y el Centro de Estudios Estratégicos del Ejército de Perú. En otro sentido, pero referido también a la "militarización" véase SCHLZKE, Marcus. "Necessary and surplus militarization: rethinking civil-military interactions and their consequences". European Journal of International Security. Vol. 3 part 1. 2017. pp. 94-112.

[23] KOTT, A. "Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments". 2018 AAAI Spring Symposium Series. p.147. Disponible en: https://www.researchgate.net/publication/324150694_Challenges_and_Characteristics_of_Intelligent_Autonomy_for_Internet_of_Battle_Things_in_Highly_Adversarial_Environments Fecha de consulta 20.07.2019

de batalla y operaciones multidominio[24]. Realmente nos acercamos a otro espacio de seguridad y, por ende, a un nuevo concepto. Estas dinámicas así podrían favorecer una convergencia en la «militarización» de la seguridad, y tal como advierte Lydia Kostopoulus, en una búsqueda de *predictive policing in Defense*[25], terminando definitivamente con la división entre seguridad interior y exterior. Sin embargo, los objetivos para la seguridad no parecen ser aquellos en los que se haya centrado hasta ahora. En primer lugar, ya no está claro el significado del Estado y, junto a las sociedades y los seres humanos, cómo compiten como receptores de esta protección, aunque haya una tendencia a priorizar la seguridad nacional de nuevo. En segundo lugar, la tecnología no es inherentemente civil o militar y hace que todos los conflictos sean conflictos multidominio/civil-militar. Y, por último, todos los dominios no tienen la misma importancia y no está claro que exista un «dominio» de cada dominio[26]. La característica más importante de este nuevo espacio de seguridad transdominio es su naturaleza integrada, aunque asimétrica, con una tendencia que parece apuntar a controlar los dominios como objetivo principal: físico (tierra, mar, aire, espacio), información/ciber, cognitivo, moral y social[27]. Los Estados y otros actores buscarán ese dominio, en función de sus capacidades, y no parece que todos tengan como objetivo la protección de las personas, sino su control. En este sentido los Estados, en general, tenderán hacia la seguridad nacional y los Estados autoritarios hacia la supervivencia del partido o grupo en el poder. En este caso la incertidumbre no tendrá como respuesta la resiliencia, sino una expansión del control interno por parte del Estado[28]:

---

[24] See SHMUEL, Shmuel. "Multi-Domain Battle: AirLand Battle, Once More, with Feeling". War on the Rocks. 20 June 2017. Disponible en: https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling Fecha de consulta 20.07.2019. Sin embargo, el US JOE 2035 excluye a propósito el ciberespacio de los *global commons* para darle un tratamiento exclusivo. Véase JCS. Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World. July 14, 2016

[25] "Predictive Policing: From Data to Actionable Intelligence", en KOSTOPOULUS, Lydia. The Role of Data in Algorithmic Decision-Making. A Primer. United Nations Institute for Disarmament Research (UNIDIR). 2019. p. 2.

[26] HEFTYE, E. "Multidomain confusion: all domains are not created equal". The Bridge. May 26, 2017.

[27] REED, D. "Beyond the War on Terror: Into the Fifth Generation of War and Conflict". Studies in Conflict & Terrorism, vol. 31. n. 8, 2008. pp. 684-722.

[28] Véase la tendencia a la militarización en la policía china, ahora se ocupan de la seguridad interior, la marítima y apoyo al ejército en tiempos de guerra. BOYD, H. "China's People's Armed Police: reorganized and refocused". Military Balance Blog. IISS. June 21, 2019; "China spending puts domestic security ahead of defense Budget rise highest in western regions of Xinjiang and Tibet". Nikkei Asian Review. March 14, 2018; LIANG, F. et al. "Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure". Policy & Internet, Vol. 10, No. 4, 2018. pp. 415-53.

- Dominio(s) físico(s): son los dominios de tierra, mar, aire y espacio.
- Dominio de información: donde se crea, manipula y comparte la información. Se extiende por el dominio cibernético.
- Dominio cognitivo: donde residen la intención, la doctrina, las tácticas, las técnicas y los procedimientos.
- Dominio social: donde se interactúa, se intercambia información, se forma conciencia, comprensión compartida y setoman decisiones: *social media/networks are the foundation of commercial, political and civil life*[29].

Así, la seguridad[30] no parece que esté dividida en dimensiones espaciales globales, regionales o locales, sino en el dominio físico, sobre todo debido a la desaparición de la seguridad interior y exterior, y a que las «identidades» de los actores (Estados o actores no estatales) tampoco están claramente definidas. La incertidumbre y esta difusión en la identidad de los actores (en el fondo, de la soberanía) hace complicado el establecimiento de objetos referentes ya sean Estados, principios o personas, debido a la fuerte influencia que generaría el dominio social, con muchos actores entre población, empresas, gobiernos y otros actores no estatales; los sectores se establecerán en función de los dominios de información y cognitivo. Las dimensiones espaciales, sectores, identidades y la naturaleza de los objetos de referencia servirán para crear un marco que estudia los temas que «son representados como amenazas existenciales a los objetos de referencia por un actor de seguridad que genera el respaldo de las medidas de emergencia más allá de las reglas obligatorias legales del sistema de gobierno democrático»[31]. ¿Quién va a identificar una amenaza existencial y un objeto o ideal por proteger? ¿Será necesario persuadir a una audiencia? Más aún, ¿habrá un proceso securitización-desecuritización, de acuerdo con los parámetros de la Escuela de Copenhague? Este nuevo «campo de batalla» está tan lleno de incertidumbre que hace muy difícil reconocer amenazas, establecer objetos protegidos y crear estrategias claras.

[29] SINGER, P. and BROOKING, E. “LikeWar. The Weponization of Social Media”. HMH. NY. 2018. P. 262.

[30] Según Buzan, Waever y Wide, la Seguridad estaba dividida en varias dimensiones definidas por caracteristicas espaciales (local, regional, y global), sectores (militar, político, económico, cultural, and medioambiental), identidades (estados, actores sociales, organizaciones internacionales), y la naturaleza de los objetos de referencia (estados, naciones, principios, naturaleza). BUZAN, B., WAEVER, O. & WILDE, Jaap de. “Security: A New Framework for Analysis”. Lynne Rienner Publishers. 1998.

[31] BUZAN et al, p.5

Conclusiones: consecuencias para la seguridad, la defensa y la disuasión

Siguiendo la conceptualización que nos da la guerra ilimitada y a su extensión, a todos los ámbitos y dominios, tal como vemos las dinámicas actuales, paradójicamente parece que estas empujan realmente a una «militarización» de todos los dominios y, por ende, de la seguridad, como estamos viendo en la lucha contra los cárteles en Latinoamérica o contra las sinergias terrorismo-crimen organizado. En principio, la dinámica marcada en esta definición, junto con el uso de medios y actores no militares, parecería contradecir esa tendencia; sin embargo, el conflicto se mueve en todos los ámbitos y la pérdida de separación entre seguridad interior y exterior empuja a una fusión seguridad-defensa. Cuestiones como el tratamiento legal de acciones bajo el umbral de la guerra, la atribución de los ataques cibernéticos, ataques transdominios, la convergencia de crimen e insurgencia, hibridación, áreas desgobernadas y subgobernadas junto con la difusión de poder desde el Estado westfaliano hace que debamos replantearnos nuestra visión sobre la seguridad, la defensa y sobre la disuasión. ¿Cómo considerar un ciberataque que inutilice las centrales nucleares y eléctricas de un país? ¿Cómo saber qué tipo de objetivo o beneficio hay tras él? La atribución sería básica, pero saber las intenciones sería fundamental[32], aunque ¿cómo reconocerla? Y responder con un ataque militar cinético a un ciber-ataque ¿sería una respuesta incremental o una opción alternativa y aceptable?[33] ¿Sería esto un aumento de la beligerancia o sería un acto proporcional de respuesta y opcional en este escenario transdominio?[34] En este sentido, este paso de un dominio a otro apunta a dicho espacio de seguridad transdominio. Por extensión, la disuasión será también transdominio, lo que implica el uso de capacidades de un tipo para contrarrestar amenazas o combinaciones de amenazas de otro tipo, a fin de evitar ataques inaceptables. En realidad, este tipo de disuasión también se producía durante la Guerra Fría, pero lo que ha cambiado es que la respuesta a un ataque

[32] Véase por ejemplo ROSATO, Sebastian. The Inscrutable Intentions of Great Powers. *International Security*. vol. 39, n.3, 2015, pp. 48-88.

[33] What Israel's strike on Hamas means for Cyberwar. *Wired*. May 6, 2019. Disponible en: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/ Fecha de consulta 8.08.2019.

[34] GARCIA CANTALAPIEDRA, David. Incertidumbre, "militarización" y un nuevo espacio de seguridad: Seguridad multi/transdominio y defensa comprehensiva". Análisis. Pensamiento estratégico en seguridad y defensa. Centro de Estudios Estratégicos del Ejército de Perú. 3 de junio de 2019. Disponible en: https://ceeep.mil.pe/2019/06/03/incertidumbre-militarizacion-y-un-nuevo-espacio-de-seguridad-seguridad-multi-trans-dominio-y-defensa-comprehensiva/ Fecha de consulta 8.08.2019.

cibernético destructivo no tiene por qué limitarse al dominio cibernético, sino que también puede incluir represalias «convencionales» o incluso nucleares. De acuerdo con Erik Gartzke y Jon Lindsay, esto cambia completamente el marco general y las implicaciones estratégicas de las acciones y sus consecuencias en cuanto al potencial de escalada, la interpretación de las señales, incluso los efectos de las operaciones[35]. En este sentido, cuanto mayor sea la robotización (por ejemplo, *swarms*), los incentivos para tomar la ofensiva rápidamente y atacar primero aumentarán[36]. No obstante, ni la comunidad estratégica europea, ni los estudios de seguridad, ni las instituciones europeas han dado aún una clara respuesta teórica, estratégica o política. Esto exigiría una revisión de la *Estrategia Global de Seguridad* de 2016 en profundidad, creando una gran estrategia más que una estrategia de política exterior o de seguridad[37]. Lo que sí parece claro es que en este espacio multidominio y de competición, la concepción de la seguridad no parece ya la que se ha venido manteniendo hasta ahora. El tema central quizá ahora no es solo la incertidumbre o la AI, sino que el sector central vuelva a ser el aspecto militar de la seguridad como fue principalmente durante la Guerra Fría. El problema podría pasar a ser la expansión de lo militar en una búsqueda de control en todos los dominios. Paradójicamente, los estudios de seguridad, tal y como los conocemos, podrían sufrir un proceso de erosión que lleve de nuevo a la reaparición de unos nuevos estudios estratégicos redefinidos para este nuevo contexto.

*David García Cantalapiedra**
Departamento de RR. II. e Historia Global
Facultad de Ciencias Políticas, Universidad Complutense de Madrid

[35] GARTZKE, Erik and LINDSAY, Jon. "Cross-Domain Deterrence: Strategy in an Era of Complexity". Office of Naval Research Grant N00014-14-1-0071 and the Department of Defense Minerva Research Initiative. 15 July 2014. Véase también GARTZKE, Erik and LINDDSAY, Jon. "*Cross-Domain Deterrence: Strategy in an Era of Complexity"*. Oxford University Press. 2019;

[36] WORK, Robert and BRIMLEY, Shawn. "20YY Preparing for War in the Robotic Age". CNAS. January 2014. P.34

[37] GARCIA CANTALAPIEDRA, David. "Realism, International Order and Security: time to move beyond the 2016 EUGS"**,** en CONDE, E. "EU Handbook on law and security". Routledge, 2019.