ieee.es
Instituto Español de Estudios Estratégicos

Opinion Paper

85/2019 27 September 2019

*David García Cantalapiedra**

Toward a new security concept in a multi-domain space: complexity, war and cross-domain security

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.

How to quote:

GARCÍA CANTALAPIEDRA, David. *Toward a new security concept in a multi-domain space: complexity, war and cross-domain security*. Documento de Opinión IEEE 85/2019. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

***NOTE:** The ideas contained in the Opinion Papers shall be responsibility of their authors, without necessarily reflecting the thinking of the IEEE or the Ministry of Defense

.

> "If an entity uses robots to conduct a massive offensive and destroys the opponent's entire robot army, does the war end? Or did a naïve population just realize they would have to fight the war themselves? Are they ready? What is the legal justification of the casus belli and enmity animating their will?"[1]

International order, war and security[2]

The concept of security is changing faster than politicians, military and academics could suspect. Thus, the gap between internal and external security has progressively been closing since 9/11 attacks confirmed this process. Meanwhile, Comprehensive Security has been used as the main security conception since early 1990s: "Security is taken to be about the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change, which they see as hostile"[3]. The logic of enlarging the security concept after the end of the Cold War, while it suffered a process of de-militarization, paradoxically, introduced extensive panoply of areas to securitize, some of them hardly related to "classical" security, closing the era of Strategic Studies. This was to create a harsh debate in political and academic realms due to the problematic those new threats, challenges and new responses provoked in the structure of that security's general conception. These also pushed toward the creation of a comprehensive approach, and later Resilience as follow-up concept. Thus, a conception that would have work good enough after the Cold War was really shocked when the 9/11 attacks produced a progressive re-militarization of security, not only by the GWOT, but by a quietly process carried out by States and Non-State actors. However, this re-militarization meant to abandon "conventional war", and

[1] EUHUS, Brandon T. "A Clausewitzian Response to "Hyperwarfare". *Parameters*, 2018.

[2] Some arguments in this article showed up first in GARCIA CANTALAPIEDRA, David y PULIDO, Julia "El nuevo espacio de seguridad trans/multi-dominio. Las amenazas híbridas y la insurgencia criminal: la evolución del concepto de sociedad anárquica de Hedley Bull", en GRASA, R. y GARCIA, C. "Cambios en la naturaleza de la Diplomacia y de la Guerra en los cuarenta años de la Sociedad Anárquica de Hedley Bull". Tirant lo Blanch. 2019. Págs. 211-220. Also in GARCIA CANTALAPIEDRA, David (ed.) "The Greater Maghreb. Hybrid threats, strategy and policy for Europe". Lexington books, Rowan & Little Ed, 2019

[3] BUZAN, Barry. "New Patterns of Global Security in the Twenty-First Century". *International Affairs*, Vol. 67, No. 3, Jul., 1991. pp. 431-451

most of these actors were to act under the level of the concept of "legal" war: the lessons of the Gulf War, but also those of Somalia and Kosovo among others, were crystal clear for both kinds of actors: in one hand, for Russia, China and other authoritarian states, and on the other hand, for AQ, Taliban, ISIS and other insurgencies, but also for others as powerful groups of transnational organized crime. Nevertheless, there were different concepts which did not catch enough attention as *Unrestricted Warfare* and the *Three Warfare Strategy*[4], or *Criminal Insurgency*[5]. The reality was that any of these concepts generated proper responses in the Western strategic community. Besides, more "classical" dynamics and threats as nuclear weapons also were recovering a main role again in this scenario, but without the "rules framework" of the Cold War. This scenario is still more complex than previously thought due to the impact of the militarization of space, the transversal irruption of cyberspace, biotechnology and AI[6]. However, academic Security Studies community, the EU Strategic Community or even the EU institutions have hardly abandoned or modified their main approaches. They have even maintained ideologically entrenched positions despite of the end of the Post-Cold War European Security Order when Russia unilaterally abandoned the 1990 CFE Treaty in 2007, broke the Principle III Helsinki Final Act (Inviolability of the frontiers), and the Russian non-compliance and US withdrawn ended the 1987 INF Treaty in 2019. Only after the 2014 Ukraine invasion, there were timid steps focused on how to respond the Russian's "New Generation Warfare" through NATO definitions on Hybrid War. Finally, EU institutions and organizations started to offer answers to these developments, however without the lightest approach or serious review about Unrestricted Warfare, or a real and deep review about our conception of Security. European strategic thought has not faced a serious and in-deep reconsideration of our security conception regarding a set of key issues: how to manage the relation between War and the declining International Liberal Order; uncertainty as the most import problem in the process of security-defense overlapping;

[4] QIAO Liang and WANG Xiangsui. "Unrestricted Warfare". PLA Literature and Arts Publishing House, Beijing February 1999; OSD. Military and Security Developments Involving the People's Republic of China 2011, Annual Report to Congress. 16 August 2011. Washington D.C.

[5] SULLIVAN, J. & BUNKER, R. "Rethinking insurgency: criminality, spirituality, and societal warfare in the Americas", Small Wars & Insurgencies, vol. 22, nº 5, 2011. págs.742-763.

[6] KISSINGER, H. et al.The Metamorphosis. The Atlantic. August 2019. Available at: https://amp-theatlantic-com.cdn.ampproject.org/c/s/amp.theatlantic.com/amp/article/592771/ fecha de consulta 25.08.2019

long term grand strategy in a context of competition[7] and Unrestricted Warfare[8]; finally, and co-existing to this reality (or interrelated with it), there is a global web of networks where games are played not through bargaining but by building connections and relationships and in the dynamics of nonhierarchical systems[9].

A new international system, a new security concept

Coming from "the end of history" momentum and from a time when still seemed easy to establish the difference between peace and war, and interior-external security, it was also easy to face a modular security concept and an idea of security complex, in which the security of states and individuals were intrinsically linked, as the Copenhagen School established during the 1990s[10]. But these notions departed from certain idea of order and were really based mainly in a Westphalian state system and an International Liberal Order. For instance, Hedley Bull already established in his 1977 seminal *The Anarchic Society* the changes that could take place in the structure of the international system where the States, that Westphalian system, begin to lose their dominance: a progressive loss of sovereignty in favor of non-state actors, which would provoke the emergence of private violence and the loss of a monopoly on the use of force, including the influence of transnational actors and technology could progressively make borders disappear. Bull argued that if these dynamics occurred, among others, the international system could return to a pre-Westphalian situation and that there would be a whole series of non-state actors that would not only compete with the state as main entities of the international

[7] BRANDS, Hal. "The Lost Art of Long-Term Competition". The Washington Quarterly. vol 41, nº 4, Winter 2019. págs. 31–51. CSIS. "Rebuilding Strategic Thinking". A Report of the CSIS Transnational Threats Project. October 2018.

[8] For instance, see FERCHEN, M. et al. Assessing China's Influence in Europe through Investments in Technology and Infrastructure. Four Cases. LeidenAsiaCentre. Leiden University. December 2018; TOBIN, L. "Underway. Beijing's Strategy to Build China into a Maritime Great Power," Naval War College Review: Vol. 71, nº. 2, Article 5. 2018. Available at: https://digital-commons.usnwc.edu/nwc-review/vol71/iss2/5; by an even tougher position, see Stephen Walt's article, "Europe's Future Is as China's Enemy". Foreign Policy. January 22, 2019. Fecha de consulta 20.07.2019.

[9] See for instance JERVIS, Robert. "System Effects". Princeton,1999;

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

system, but they could even replace it[11]. Paradoxically, an institution that Bull considered inseparable from that system of States was the War as organized violence carried out by political units against each other. He also considered the development of the modern concept of war as organized violence among sovereign states as the result of a process of limiting or confining violence. Thus, in any real hostility to which we can give the name of "war", norms or rules, whether legal or otherwise, invariably play a role. However, if the system of States would evolve to that pre-Westphalian situation that Bull posed, is it only the organized violence of political units carried against each other what we would consider War, or would this concept be extended? What would happen if there were non-state political units, or even non-political units, from the point of view of the definition of War? Would War between them and States be possible? Moreover, would War, as Bull understood it, be possible in a pre-Westphalian system? Bull articulated his concept of War through the difference between war in the material sense, that is, real hostilities, and war in the legal or normative sense, a theoretical state created by the satisfaction of certain legal or normative criteria: talking about war in the legal sense, the distinction between war and peace is absolute. On the other hand, war in the material sense is sometimes difficult to distinguish from peace. But Bull recognized the impossibility of separating the two since the dynamics of hostilities sometimes play against that separation. This lack of historical awareness also contributes to our lack of conceptual preparation[12]. As Rosa Brooks affirms: “In a world in which the push of a button can lead, within seconds, to the deaths of a specific man more than eight thousand miles away, is it possible to define “war” with clarity? Most of all: As the boundaries around war and the military grow ever blurrier, will we all pay a price?”[13].

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

[12] 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.

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

Toward a new analysis framework: hybrid threats, unrestricted warfare and a new cross-domain security concept

Frank Hoffman[14], the United States Military[15], the European Union[16], the HybridCoE[17], and NATO[18] maintain significant differences over the material scope of the concept, and others use the term to describe the so-called Gerasimov Doctrine[19]. This lack of doctrinal consensus means a problematic theorical and practical approach to tackle efficiently these dynamics. According to Aurel Sari, to stipulate that hybrid threats are activities which remain below the threshold of formally declared warfare would be naïve, and undermine a clear understanding and definition, as "formally declared wars are something of a rarity in international relations"[20]. For instance, as Rosa Brooks establishes: "Similarly, we struggle to tell the difference between "civilians" and "combatants." What counts as a protected civilian object in cyberspace? When can a hacker, a financier, or a propagandist be considered a combatant?"[21]. It is distinctive that there is no longer a clear distinction between what is and is not a battlefield: physical spaces (Global Commons) are all potential battlefields, but social spaces such as political, economic, and cultural spheres, cyberspace, and even the psyche are also at risk. It seems there is no consensus on what is battlefield or not, between what is peace or war, what is the "normal" status" and how will we define Security? Authors as Frank Hoffman, Peter Singer, Colin S. Gray, Max Boot, David Kilcullen, Antullio Echeverria or John Arquilla have debated about the nature and impact of these threats. However, there is neither a debate about the impact of these categories in Security Studies nor a real attempt of delivering new

[14] HOFFMAN, F. "Hybrid Warfare and Challenges", Joint Forces Quarterly, nº 52, 2009.

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

[16] 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.

[17] Hybrid CoE. Countering Hybrid Threats. Available at: https://www.hybridcoe.fi/hybrid-threats/ fecha de consulta 20.07.2019.

[18] NATO. Hybrid threats. Available at: https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en fecha de consulta 20.07.2019

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

[20] SARI, A."Hybrid Warfare, Law and the Fulda Gap". Law School. Exeter. Pp.14-15.

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

approaches and definition of the concept of Security[22]. However, it seems there are conceptions even previous to Hoffman's first approach: PLA Colonels Qiao Liang and Wang Xiangsui defined war in their 1999 book "Unrestricted Warfare" as "using all means, including armed force or non-armed force, military and nonmilitary, and lethal and non-lethal means to compel an enemy to accept one's interests"[23]. Certainly, the idea of limiting War as a concept and goal is not working as it was previously developed by Hedley Bull. Paradoxically, even though the characteristics and means of War have changed, War still is *á la Clausewitz*, "an act of force to compel our enemy to do our will", and "to the application of that force there is no limit". However, this dynamic would be related to enlarging war domains, not regarding material military incremental force. This expansion of the domains of war makes possible the exponential expansion of the concept of the battlefield beyond the physical domain by removing its geographical and political constraints and allowing it to become omnipresent. In response to the question, "Where is the battlefield?" Liang and Xiangsui answer simply that it is now "everywhere". Thus, this application could be qualitative and not necessarily quantitative in terms of escalation in the use of kinetic force as commonly is interpreted. This expansion of means could be translated to the different domains: all these actors, all these different capabilities, spread to all the domains. Paradoxically, in aiming the control of these domains, this could also mean a trend to the militarization of domains, above all due to the crossing impact of cyberspace and the civil-military diffusion, although it is symptomatic the use and search of control of domains (mainly cyberspace) by some great powers[24]. This process is directly related to the other aspect Bull pointed out as a cause

[22] Except for a few attempts. See for instance 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.

[23] QIAO Liang and WANG Xiangsui. "Unrestricted Warfare". PLA Literature and Arts Publishing House, Beijing February 1999. pág. 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. Available at: https://www.rand.org/pubs/research_reports/RR2588.html Fecha de consulta 20.07.2019.

[24] See 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 and Digital and Cyberspace Policy Program. CFR. January 29, 2018; also the use of armed forces in the fight against transnational organized crime. See research and studies by Real Instituto Elcano/ Centro de Estudios Estratégicos del Ejército de Perú; from other point of view see SCHIZKE, M. "Necessary and surplus militarization: rethinking civil-military interactions and their consequences". European Journal of International Security. Vol. 3 part 1. 2017. págs. 94-112.

for the end of the Westphalian system: the 4th Tech Revolution, the cyberspace, the Artificial Intelligence (AI) and the relation with humans, not only in Internet of Things (IoT), but in the Battlefield of Things (BoT). As Alexander Kott establishes:

"What happens on the future battlefield when humans and machines battle each other yet "think" very differently? "it… makes the battlefield harder to understand and manage. Human warfighters have to face a much more complex, more unpredictable world where things have the mind of their own and perform actions that may appear inexplicable to the humans."[25].

How will be the relation human-AI? Will a human force be tactically expendable in order to sustain an Autonomous/AI machine-robot strategically, which will offer victory in an engagement or battle? At the same time, as the levels of uncertainty will be higher and higher in the security realm, who is going to identify an existential threat and an object or ideal to be protected? Will it be necessary to persuade an audience? More, will there be a process of securitization-desecuritization according to Copenhagen School's parameters? This new "battlefield" is so full of uncertainty that makes almost impossible to know threats, protected objects, clear strategies or "speech acts". That uncertainty would push us to seek the control of the domains as much as we can to reduce it and, however, the expectations for an AI could be different from that of the humans. In the field of Defense this situation leads to the Multi-domain Battlefield and Operations[26]. These dynamics could converge leading to a "militarization" of Security and according to Lydia Kostopoulus, the search of "predictive policing" in Defense[27], blurring definitively the division and differences between interior and external security. However, the goals for

[25] KOTT, A. Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments. The 2018 AAAI Spring Symposium Series. 2018. pág. 147. Available at: 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

[26] See SHMUEL, S. "Multi-Domain Battle: AirLand Battle, Once More, with Feeling". *War on the Rocks*. 20 June 2017. Available at: https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling Fecha de consulta 20.07.2019; Still, the US JOE 2035 purposefully excludes cyberspace from the global commons context, instead giving it an exclusive context. See JCS. Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World. July 14, 2016

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

Security does not seem mainly those have been focusing on until now: first, since it is not clear the meaning of State, and how State, societies and human beings compete as receptors of this protection (although it seems there is a trend toward national security); second, technology is not inherently civilian or military, and makes all conflict multi-domain conflict; third, all the domains are not equal in importance and it is far from clear that it exists a clear "dominance" of every domain[28]. The most important characteristic of this new multi-domain security space is his integrated and cross-domain nature of Security, with a trend that seems aimed to control the domains: physical (land, sea, air, space), Information/Cyber, Cognitive, Moral and Social[29]. States and other actors will try to dominate, according their capabilities, but they do not seem encouraged to protect population but to control it. In this vein, the main trend in States will be national security and the authoritarian states will look for the survival of the party o power elite: in this case, uncertainty will not probably result in resilience approach but an expansion of internal control by state apparatus[30]:

- Physical Domain(s). The traditional domain of warfare. It spans the traditional land, sea, air, and space domains.
- Information Domain. The domain where information is created, manipulated, and shared. It spans the cyber domain.
- Cognitive Domain. Here doctrine, tactics, techniques, and procedures reside. It is the domain where decisive concepts emerge.
- Social Domain. It is where humans interact, exchange information, form shared awareness and understandings, and make collaborative decisions: "social media/networks are the foundation of commercial, political and civil life"[31].

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

[29] 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.

[30] Chinese police force has been turning toward militarization probably since 2011. Currently it takes care of interior security, maritime security and Armed Forces support in war times. See for instance. 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. Págs. 415-53.

[31] SINGER, P. and BROOKING, E. "LikeWar. The Weaponization of Social Media". HMH. NY. 2018. Pág. 262.

Security[32] will be not divided or focused on several dimensions defined by spatial characteristics (local, regional, and global), but in the Physical Domain (above all in an internal-external security mix and a "identity" actors' diffuse status); uncertainty makes very complicated to identify security reference objects (states, principles or people) because of the impact of social domain generate by multiple actors(as people, companies, governments or other NSAs); security sectors really will respond to cognitive and information domains. Spatial dimensions, sectors, identities and the nature of reference objects served to create a framework in order to study issues which are represented as existential threats for reference objects by a security actor that generates support to the emergency measures beyond legal mandatory rules in the democratic government system[33]. Who is going to identify an existential threat and an object or idea to protect? Will it be necessary to persuade an audience? And according to the Copenhagen School's parameters, will it proceed a securitization-de-securitization process? In this so uncertain new "battlefield" it will be very complicated to know threats, to establish protected objects and clear strategies.

Final thoughts: consequences for security, defense and deterrence

After this general context, expanded to all domains, the main trend paradoxically seems to push toward a "militarization" in the security realm as it is already happening in the fight against drug cartels and transnational organized crime in Latin-America. Even though this idea could be counterintuitive according the characters and parameters described above, the spread of conflict to every domain and the fusion of internal-external security is overlapping security and defense. The legal treatment of cyber-attacks, cross-domain attacks, crime-insurgency convergence, hybrid dynamics in one hand, and the diffusion of power from the Westphalian state system (and ungoverned and under-governed spaces) in the other hand, should initiate a complete review of our vision about Security, Defense and Deterrence. Plenty of questions are opened in this context: what kind of

[32] Security is divided or focused on several dimensions defined by spatial characteristics (local, regional, and global), sectors (military, political, economic, cultural, and environmental), identities (states, societal actors, international organizations), and the nature of the referent objects (states, nations, principals, nature). BUZAN, B., WAEER, O. & WILDE, Jaap de. "Security: A New Framework for Analysis". Lynne Rienner Publishers. 1998.

[33] BUZAN et al, pág.5.

attack would be a cyber-attack to nuclear and electric installations in a country? What is the goal or benefit of such attack? Attribution would be a key issue but knowing intentions would be even more important[34], but how to know? A kinetic counterattack would be a valid and acceptable alternative option to a cyber-attack?[35] ¿Would it be an increase in belligerence or a normal optional response in cross-domain scenarios?[36]

In this regard, these cross-domain actions establish a cross-domain security space, in which Deterrence would move using different kind of capabilities to deter threats or combined threats in order to avoid unacceptable actions or attacks. This kind of Deterrence was already used during the Cold War, but a major change occurs threatening or responding to a cyber-attack, not only in the cyber domain, but through "conventional" o even nuclear retaliation. According to Erik Gartzke and Jon Lindsay, this completely changes the general framework and the strategic implications of these actions and consequences regarding potential escalation, signaling interpretation, and even operational effects[37]. In this vein, the more the robotization (for instance swarms) the larger will be the incentives toward Offense and first strikes[38]. Thus, this evolution in Deterrence would respond to the transformative general scenario described above. Nevertheless, neither European strategic community, Security Studies nor EU institutions moved toward a steady and clear theorical, strategic and political response. Such endeavor would require a full review of the 2016 EU Global Strategy and key basic arguments, moving beyond a foreign policy or security strategy toward a real grand

[34] See for instance ROSATO, Sebastian. "The Inscrutable Intentions of Great Powers". International Security, vol. 39, n.3, 2015, págs.48-88

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

[36] GARCIA CANTALAPIEDRA, D. Incertidumbre, "militarización" y un nuevo espacio de seguridad: Seguridad multi/trans-dominio y defensa comprehensiva". Centro de Estudios Estratégicos del Ejército de Perú. 3 de junio de 2019. Available at: 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 10.08.2019

[37] 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. Also GARTZKE, Erik and LINDSAY, Jon. "*Cross-Domain Deterrence: Strategy in an Era of Complexity"*. Oxford University Press. 2019;

[38] WORK, R. and Shawn BRIMLEY, S. 20YY Preparing for War in the Robotic Age. CNAS. January 2014. Pág.34

strategy[39]. What it seems crystal clear in this competitive multi-domain security space is an unavoidable change of the concept of Security. Moreover, uncertainty and AI are not the only challenges in this transitional moment, but a trend toward the militarization of Security in order to control every domain, moving military sector to the center of the process as it was during the Cold War. Paradoxically, this process would produce that the Security Studies as we know now could be eroded and transformed in such way that a refined and renewed Strategic Studies could reborn in this new context.

*David García Cantalapiedra**
Department of International Relations and Global History
Faculty of Political Sciences, Complutense University of Madrid

[39] 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.