DOI: 10.53477/2668-2001-21-09

RUSSIAN ELECTRONIC WARFARE CAPABILITIES AND THEIR IMPLICATIONS FOR EUROPEAN STRATEGIC STABILITY: A CASE STUDY OF THE SYRIAN CONFLICT

Cristina Marzal[1]
General Gutiérrez Mellado Institute, UNED, Spain
Guillem Colom-Piella
Pablo de Olavide University, Seville, Spain

Abstract

The Russian intervention in Syria, as well as the associated deployment of electronic warfare systems, generated alarm among NATO members linked to the possibility that a strengthening of electronic warfare capabilities by Russia could reduce the current technological asymmetry in favor of NATO. Such reduction would come from the use of electronic warfare systems to hamper the command and control capacity of attack and defense systems. This paper analyses the Russian intervention in Syria in order to define whether it can be understood that there is an increasing risk to Euro-Atlantic security stemming from Russian advances in electronic warfare.

Keywords: Syria; Russia; electronic warfare; NATO; military strategy.

INTRODUCTION[2]

Despite the relevance of the electromagnetic spectrum and its importance for modern warfare, during the last 20 years it has been sidelined by the consolidation of cyberspace as the fifth domain of warfare. This, however, changed in April 2014, when a Russian *SU-24 Fencer* fighter equipped with a sophisticated Electronic Warfare (EW) system conducted a series of low altitude flights over USS *Donald Cook*, an *Arleigh Burke* destroyer, allegedly jamming all of its electronic sensors and communication systems (it was later confirmed that this information, widely reported at the time by Russian media, was false) (DRFLab 2017). However, Russian intervention in eastern Ukraine and Syria, as well as the operation of EW systems close to NATO and EU countries (including the jamming of GPS signals) showed both the extent of Western reliance in the radioelectric domain (particularly between 9 KHz and 3000 GHz) and the significant advances made by Russia in EW capabilities.

Unlike during operations in the Ukraine, where the Russian EW was aimed at supporting the ground forces and combined cyber, information and electromagnetic capabilities, in Syria the Russian forces have focused on the use of drones to collect electronic intelligence and jam the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities (McCrory 2021; Turunen 2020, 16). Although Russia has focused on thwarting the command and control of the anti-Assad fighters as means to degrade their capacity to communicate and therefore coordinate their operations, it has also used its EW capabilities to diminish the intelligence gathering efforts (from low-orbit surveillance satellites, reconnaissance aircraft or drones) from the US and NATO via spoofing the GPS signals (Kofman et al. 2017; C4ADS 2019). These tactics have generated a certain degree of concern among foreign militaries also present in the conflict, particularly the US military, who were able to realize their own limitations regarding electronic protection capabilities (Stupples 2015; Seligman 2018). We could consider that this realization, added to the use of EW that was reported in the Ukrainian and Syrian conflicts, its potential use both in grey-

[1] Corresponding author: mmarzal13@alumno.uned.edu.com
[2] This contribution is part of the research project *Ciberataques y gobernanza global* (DER2017-85612-R) (Ministerio de Economía, Industria y Competitividad) (2018-21).

zone scenarios and as an integral part of Anti-Access/Area-Denial (A2/AD) strategies, and its military reliance to the electronic spectrum for waging the “American way of war”, is likely to have fueled the renewed US interest in increasing their EW research and development projects. An example of such growth in interest from US policymakers can be drawn from the topics covered by Congressional Research Papers. These have increased tangibly the number of papers dedicated to EW, reaching a record of 5 EW-specific CRS reports published in 2020.

RUSSIAN EW CAPABILITIES

Despite the recent publicity, Russian EW has a long history dating back to the early 20th century (Kjellén 2018, 19). However, the basis of the current approach was laid during the Cold War with the development of the Radio-Electronic Combat (REC) doctrine. The REC doctrine brought the previously dispersed techniques and disciplines under one conceptual umbrella, integrating them into a concept of operations and developed a wide range of means to operate in the electromagnetic spectrum (Turunen 2020, 14). Although the end of the Cold War led to a significant loss of EW capabilities, the military modernisation process that began in the mid-2000s revitalised the Russian EW industry and brought new materials into service (Radin et al. 2019, 187-88; Denisentsev 2014). Despite this, the war in Georgia (2008) highlighted the immaturity and limitations of Russian EW (Collins 2018). However, lessons learned from this campaign – such as its apparent fiasco in the information domain (Beehner 2018) – also served to mature capabilities that could be observed in Ukraine or Syria.

Broadly speaking, the current Russian REC doctrine combines the traditional electronic attack and protection functions with activities such as technical reconnaissance countermeasures or radio electronic information support measures (Ramm 2015a, 2015b). Similar to the West, with the progressive consolidation of *Cyber Electro Magnetic Activities* (CEMA)[3] due to the increasing convergence between cyberspace and radio-electric domains, the Russian doctrine also envisages the use of a wide range of information actions to protect, exploit, degrade or deny the use of electromagnetic space. Unlike the West, however, Russian doctrine also envisages the use of conventional means – such as anti-radiation missiles – to degrade adversary electronic systems. While these kinetic means would be employed in open conflict, all other tools of information warfare - from EW to degrade adversary radio communications or spoofing GPS signals to psychological operations, propaganda or cyber-attacks[4] – could also be used in the grey zone. In this case, as with other information weapons, EW operations make it difficult to attribute responsibility while degrading the adversary's civilian and military capabilities, reducing resilience and contributing to escalation dominance. In any case, EW can be regarded as a force multiplier capable of being used in any scenario and contingency for offensive or defensive activities and supporting operations on land, sea, air, space and cyberspace. This is why Russian EW is not limited to the tactical level, but can also be used at the operational and strategic levels across the entire spectrum of conflict and fully integrated with actions in other domains.

Despite the lack of a detailed and structured reporting from Russian authorities in regards to its current EW weaponry and tactics, there is a significant degree of exposure of such systems in both State-backed media, such as official Army publications, and Russian press. The validity of these publications should be questioned, as it has been shown that a certain degree of exaggeration is occasionally added to such reports. A prominent case is found in the news reports about the USS Cook incident previously mentioned. Other, subtler enhancements also make their way into publications about successful military operations in conflicts such as the Syrian civil war, as well as into reports signed by commanders about the capabilities and progress made by their own areas of responsibility. This is enhanced by the extended use of EW capabilities within a wider trend of State propaganda about the military might of the Russian armed forces.

[3] It is important to point out that, in general terms, EW has three components: electronic warfare support, electronic protection, and electronic attack.

[4] Strictly speaking, these are informational weapons focused on achieving informational-technical effects on adversary infrastructures and systems and informational-psychological effects on the perceptions of their population.

Having said this, Russian EW capabilities can be better structured based on their capacity to support military operations in the land, air and sea domains:

Regarding ground forces, the participation of EW resources on ground operations and planning underwent significant change during the structural reform of Russian Armed Forces in 2008. Such reform embedded EW units in the organic structure of tank and motorised rifle manoeuvre brigades (McDermott 2017, 5). These units consist mainly of electronic attack systems, but also capabilities for anti-air protection for ground forces and automated command and control systems which are integrated with those of the ground forces they accompany. As noted by McDermott (McDermott 2017) this represents a significant difference between Russian and Western organization of EW resources, since Russian ground units are not deployed without an EW support component.

Such systems have also been reported to support psychological operations. For example, multiple reports emerged during the Ukrainian conflict about text messages being received by Ukrainian civilians containing demoralizing messages and encouraging them to surrender. Although this could never be proved by research, it is believed that the Russian Army launched these operations using the *Leer-3* system. This tactic, as reported by Kjellén, was tried in exercises at the Prudboi range in the Southern Military District (Kjellén, 2018, 70). The *Leer-3* system consists of a mobile platform and an attached small UAV, which have the ability to create virtual cell tower (spoofing) and intercept or alter, as proven in Ukraine, the data received by mobile phones in the area.

Regarding the Russian Air Force, EW support to air operations is far less intense as in the case of ground forces, at least in what refers to the diversity of EW technology being embedded in aircraft. As such, the main support consists of electronic countermeasure (ECM) pods in the systems of specific aircraft such as the *Su-34 Fullback*. This is the case of the L-175V *Khibiny* pods, among others (i.e., the *SAP-518* usually mounted in the *Su-27/Su-30/Su-35 Flanker* fighters), which provide protection against guided missiles[5]. Reportedly, a more sophisticated version of the *Khibiny* technology, referred to as Tarantul, is currently being tested, potentially providing electronic protection for a larger group of aircraft (Kjellén, 2018, 57). Another key task and capability of Russian airborne EW system is SIGINT. In this regard, deployment in environments where NATO aircraft conduct operations provides the benefits of collecting such signals, which can then be reported back and analysed (C4ISR intelligence cycle) to reinforce the possibilities of their own EW systems in a potential standoff against NATO forces.

As for EW in the Russian navy, as reported by McDermott, EW forces are represented in naval fleets as well as in battalions in the respective Military Districts. Both support structures pursue a largely protective goal against potential enemy strikes. In this regard, as an example of ongoing technological developments, the *5P-42 Filin* electro-optic countermeasure can be cited. This system, embedded in at least two frigates since 2019 (McDermott, 2019) generates strong beams of light which impede attackers to correctly see the platform and aim any fire towards it. As reported by McDermott citing Russian media outlets, the Russian Navy claims this system attacks the optic nerves of enemy forces, creating temporary blindness and even hallucinations.

As a conclusion of this brief overview of Russian EW capabilities, it can be observed that the Russian military are investing resources in EW research and development to obtain strategic advantages derived from negating enemy technology. Additionally, although we can assume that any lacks or issues presented by the current program will unlikely surface to open sources, this program seems to count with a high level of endorsement and institutional support, tangible not only in the investments made but in the structural changes made to accommodate EW as a crucial component of military operations and protection of critical infrastructure.

[5] Needless to say that those systems can also detect traces and discriminate targets, so they may provide an additional layer of Identification Friend or Foe (IFF) capacity. In any case, the Russian doctrine prioritises land-based control of aircraft and hence, IFF interrogation may be accessory.

RUSSIAN EW DEPLOYMENT IN THE SYRIAN CONFLICT

As could possibly be expected based on the summary of Russian EW capabilities, EW capabilities and personnel were largely present and active during the Russian intervention in the Syrian conflict.

In this regard, the Syrian intervention saw both the use of EW as combat support and as protection for critical infrastructure or equipment. Due to the heavy use of UAVs as compared to previous Russian deployments, such as the east Ukraine conflict, discussions about the implications of Russian EW measures in Syria are largely centered about UAV-borne EW capabilities and protecting their critical infrastructure against UAV-based airstrikes.

Due to the symbolism and impact it has had on the military planning and exercises carried out during 2019-2020 (Sukhankin, 2019), the most relevant example can be found in the protection of the Khmeimim airbase, located in Western Syria and key for Russian deployment in the country. In Khmeimim, a series of electronic protection systems containing at least one *Krasukha-4* jammer was deployed, providing coverage against UAV airstrikes. However, such coverage was continuously tested by Syrian rebels between 2017 and 2019, when they managed to inflict minor damage on the base by conducting massive drone attacks (reaching 80 UAVs) or exploiting temporary de-activations of the electronic protection measures to attack the base (Urcosta, 2020, 51). Whether the finding of these "opportunity windows" was accidental or based on an advanced EW collection plan is an open question that could provide significant implications for the analysis of the Syrian conflict.

Apart from the evident benefits gained from EW as a support and protection force multiplier, it is noted that the Kremlin has also found it possible to use the Syrian conflict as a great maneuvering ground in which to improve its newest technology in real situations (Turunen, 2020, 16). As noted by Turunen, the scope of such tests has differed in the Syrian conflict in comparison to the deployment in east Ukraine. In this regard, the deployment in Syria has represented a testing ground for EW capabilities linked to UAV deployment, signals intelligence and protection against reconnaissance.

This testing strategy not only allows Russia to acquire greater experience and training in the use of this equipment, but also to deepen the general training of their troops and detect possible improvements or failures that may be found in specific systems or tactics. However, it should be noted that, as McDermott (2017, 21) points out, the scope of the Syrian deployment in terms of the volume and novelty of tested equipment is not comparable to the volume of testing that took place in the eastern Ukraine intervention.

IMPLICATIONS FOR EUROPEAN STRATEGIC STABILITY

While some commentators see the Russian EW as one of the Kremlin's "silver bullets" - along with hypersonic weapons or nuclear torpedoes - against Washington's military superiority, others consider it as another piece of Russia's deterrence strategy (or so called A2/AD) in Europe. Both positions are partly right: the US has maintained its military dominance for decades thanks to its information superiority. However, its reliance on the ability to collect, process, disseminate and exploit more information, faster and better than its opponents, has also become its main weakness. Therefore, it is not surprising that countries like Russia, unable to symmetrically compete with the US, are exploiting this dependence asymmetrically. One of the many responses put forward by Moscow is the enhancement of its EW capabilities. On the other hand, this development is also part of the A2/AD with which Moscow threatens the strategic balance in Eastern Europe[6]. In this sense, EW capabilities can be regarded as another layer - along with long-range radars, multi-layered air defences and long-range precision attack systems - that may contribute to altering NATOs strategic calculus. By its nature, EW can also contribute to escalation dominance and, above all, be used in the grey-zone to

[6] However, this concept originally used to depict the Chinese strategies to ensure the control of its first island chain does not fully grasp the Russian approach. Strictly speaking, what Moscow has developed is a Reconnaissance-Strike Complex (*Razvedyvatel no-Udarnyy Kompleks* – RUK). Conceived by the USSR in the 1980s, it consisted of a broad range of sensors and vectors capable of identifying enemy forces and launching long-range precision strikes. A RUK was sited within a (mostly anti-air) bubble to prevent the adversary from hitting its most precious components. In addition, it is important to bear in mind that what might be termed an advanced *Integrated Air Defence System* (IADS) is but one component - together with the air defences of land-based units and the air force – of Russia's air defence (Kofman 2020).

exploit the electromagnetic dependence of advanced societies. In this case, they would unlikely be used in isolation, but as part of information warfare in the context of multidimensional (hybrid) strategies.

In this sense, it is important to analyze in greater depth whether the currently known or public Russian EW capabilities really respond to or justify this social alarm about an increased risk on European security. On the basis of what has been described above, and following the conclusions reached by the main studies and sources analyzed, it can be stated that we are in an intermediate situation between the total absence of risk for NATO and the situation of serious risk perceived from some sectors, due to a series of reasons:

First, one of the arguments frequently detected when denouncing the dangerousness and risk involved in Russian investment in EW capabilities is conditioned by the alleged novelty of such systems. From this point of view, Russia would be investing large sums of money in the development of electronic warfare capabilities that would be groundbreaking with the current technology at its disposal. Not only that, but it would be doing so with sufficient efficiency and speed to have significant updates in its systems to be able to test some of them in the conflict in eastern Ukraine and other different and more evolved ones in the Syrian conflict.

While it is true that Russia is making a clear commitment to the development of its electronic warfare capabilities, it is not so evident, based on the systems whose deployment in Ukraine and Syria has been made public, that the pace of technological development and production of these systems is so high and efficient. In fact, as Kjellén states, there is no known case of a novel electronic warfare system deployed in Syria that had not already been tested before in Ukraine, although those sent to Syria probably included improvements derived from lessons learned from previous deployments (Kjellén 2018, 62). An exception would have been the *Tarantul* devices mentioned previously, which so far have not been sighted in Syria.

Likewise, from the point of view of advancement in the technologies underlying such systems, Kjellén also warns that no major advances are perceived between one generation of systems and the next from the point of view of the technology behind them, so this argument would lose force when it comes to justifying a possible Russian competitive advantage from major technological advances in the short-medium term.

As the main exception to this fact, and with the aim of offering a balanced view of the analysis carried out, it is worth mentioning the existence of specific cases in which progress is being made and which present relevant innovations in the field of electronic warfare, such as the enabling of radars on drones or research and development to suppress or hinder satellite detection, reconnaissance, command and control capabilities. Likewise, Kjellén highlights the efforts being made to generate systems to protect troops and facilities against guided missiles, as well as the development of specific command and control systems for electronic warfare, which allow for better coordination of operations while transmitting valuable situational awareness information in the electromagnetic spectrum (Kjellén 2018, 62).

Secondly, it is noted that alarm about Russian electronic warfare capabilities has largely been driven by assumptions or claims, many of them coming from unreliable media, about the capabilities of such systems. The clearest example is the incident in which, allegedly, a single aircraft equipped with *Khibiny* systems, intended to protect the aircraft itself, would have inhibited the USS Donald Cook's communications completely, leaving it "blind" (Kjellén 2018, 56) to what was happening in its vicinity. Similarly, contradictory and differently ranging versions have been detected about the real capability of the *Krasukha* family of systems, claiming that they would be able to blind NATO command, control and reconnaissance systems completely and in a very high radius.

Faced with this possibility, two clear tendencies of response to the question have been observed, conditioned by the specific source that is consulted. While non-specialized press, especially those media that could be classified as having less technical rigor or knowledge, (for example, The Huffington Post, with headlines such as “NATO would be totally outmatched in a conventional war against Russia” (Ritter, 2017) tend to affirm that, indeed, Russian electronic warfare systems can generate a significant advantage over NATO forces. However, academic reports

stemming from institutions specialized in Defense matters coincide in their affirmations that, at a technological level, the current threat posed by Russian EW technology is definitely not as strong as portrayed in the press. McDermott, who makes a clear comparison between NATO's capabilities and those possessed, for example, by the Ukrainian army in the Donbas during the conflict, states this categorically.

At this point, it is interesting to stop and think about the implications of this statement. In a context of frequent proxy conflicts, where the involvement of rival powers is not always easy to determine (as was, formally speaking, Russia's involvement in Ukraine), should the existence of neighboring countries with a clear technological disadvantage vis-à-vis Russia not be a source of concern, even if NATO countries are not nearly as vulnerable themselves? Is this not, in practice, a "proxy" capability gap, allowing Russia to advance and promote its interests? These questions have predictably already made their way into NATO's strategic planning, and have possibly been weighed against the dilemma of escalating tensions that would be generated by any perceived attempt by NATO to develop Ukraine's or other non-member's military capabilities. What is worth noting at this point is the distinction between a conventional conflict and a nuclear conflict. While in the nuclear realm, as Dalsjö, Berglund and Jonsson (2019, 52) point out, an overmatch of EW Russian capabilities against US EW is highly unlikely both offensively and defensively. However, we do observe a clear risk in the case of employing such systems against less prepared militaries of countries in Russia's immediate sphere of influence, as was the case in Ukraine.

This leads us to the following statement by McDermott, in which he considers that, although he categorically denies that Russia has sufficiently powerful systems to, in their current size, be highly disruptive for Allied capabilities, it is capable, with its current dimensions, of using them to generate serious disruptions to the operations of its enemy. Thus, we could consider that half of the initial Russian objective has been achieved, being the generation of an asymmetric advantage at the tactical level through the application of a specific technology. Kjellén goes so far as to predict that, in a scenario of direct conflict between NATO and Russia, the first signs of ongoing conflict would manifest themselves in the electromagnetic spectrum, since, for the Kremlin, this domain is where NATO is perceived to be weakest (Kjellén 2018, 28).

In particular, McDermott points to the urgency of providing such capabilities to the states most affected by this threat, such as the Baltic countries. Specifically, the author points to the existence of a key challenge for NATO. According to him, the organization bases an important part of its military superiority on the development of highly complex and effective command and control systems, which make it possible to coordinate operations through the simultaneous communication of all the actors involved. Thus, the possibility that, by means of electronic warfare systems, these command and control systems would see their effectiveness reduced, would lead to a situation in which one of NATO's main strategic advantages could be seriously affected.

REFERENCES

Beehner, Lionel et al. 2018. *Analyzing the Russian Way of War Evidence from the 2008 Conflict with Georgia*. West Point: Modern War Institute.

Bērzinš, Jānis. 2020. "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria". *The Journal of Slavic Military Studies* 33 (3): 355-380 http://www.doi.org/10.1080/13518046.2020.1824109

C4ADS. 2019. *Above Us Only Stars. Exposing GPS Spoofing in Russia and Syria*. Washington DC: The Center for Advanced Defense Studies.

Collins, Liam. 2018. "Russia Gives Lessons in Electronic Warfare". *Association of the United States Army*. Last modified July 26, 2018 https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare Accessed 5 March 2021.

Dalsjö, Robert, Christofer Berglund and Michael Jonsson (eds.). 2020. *Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction*. Stockholm: FOI.

Denisentsev, Sergey. 2014. “Okno vozmozhnostey dlya REB”. *Voyenno-Promyshlennyy Kuryer* 23 (541) http://www.vpk-news.ru/articles/20874 Accessed 2 March 2021.

Defense Intelligence Agency [DIA]. 2017. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, DC: Defence Intelligence Agency.

DFRLab. 2017. Russia’s Fake “Electronic Bomb”. How a fake based on a parody spread to the Western Mainstream. Last modified May 9, 2017 https://medium.com/dfrlab/russias-fake-electronic-bomb-4ce9dbbc57f8 Accessed 4 March 2021

Hamilton, Robert; Chris Miller and Aaron Stein (eds.). 2020. *Russia’s War in Syria. Assessing Russian Military Capabilities and Lessons Learned*. Philadelphia: Foreign Policy Research Institute.

Jones, Seth (ed.). 2020. *Moscow’s War in Syria*. Washington DC: CSIS.

Kjellén, Jonas. 2018. *Russian Electronic Warfare. The Role of Electronic Warfare in the Russian Armed Forces*. FOI-R-4625-SE. Stockholm: FOI.

Kofman, Michael. “Russian A2/AD: It is not overrated, just poorly understood”. *Russia Military Analysis*. Last modified January 25, 2020https://russianmilitaryanalysis.wordpress.com/2020/01/25/russian-a2-ad-it-is-not-overrated-just-poorly-understood/ Accessed 7 March 2021.

Kofman, Michael et al. 2017. *Lessons from Russia’s Operations in Crimea and Eastern Ukraine*. Santa Monica: RAND Corporation.

McCrory, Duncan. 2021. “Russian Electronic Warfare, Cyber and Information Operations in Ukraine.” *The RUSI Journal*, http://www.doi.org/10.1080/03071847.2021.1888654

McDermott, Roger. 2017. *Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallinn: International Centre for Defence and Security.

McDermott, Roger. 2019. *Russian Navy Procures New Electronic Warfare Capabilities*. Washington DC: The Jamestown Foundation, https://jamestown.org/program/russian-navy-procures-new-electronic-warfare-capabilities/ Accessed 7 March 2021.

Radin, Andrew et al. 2019. *The Future of the Russian Military: Russia’s Combat Capabilities and Implications for U.S.-Russia Competition*. Santa Monica: RAND Corporation.

Ramm, Alexei. 2015a. “Elektronnaya vojna, mify i pravda (part I)”. *Voyenno-Promyshlennyy Kuryer* 37 (603) https://vpk-news.ru/articles/27272 Accessed 3 March 2021.

Ramm, Alexei. 2015b. “Elektronnaya voyna, mify i pravda (part 2)”. *Voyenno-Promyshlennyy Kurye*r 38 (604) http://vpk-news.ru/articles/27410 Accessed 3 March 2021.

Seligman, Lara. 2018. “Russian Jamming Poses a Growing Threat to U.S. Troops in Syria”. *Foreign Policy,* 30 July https://foreignpolicy.com/2018/07/30/russian-jamming-poses-a-growing-threat-to-u-s-troops-in-syria/ Accessed 27 February 2021.

Sukhankin, Sergey. 2019. “Syrian Experience Provides New Impetus for Russia’s UAV Strategy (Part Two)”. Washington DC: The Jamestown Foundation, https://jamestown.org/program/syrian-experience-provides-new-impetus-for-russias-uav-strategy-part-two/ Accessed 7 March 2021.

Stupples, David. 2015. “How Syria is becoming a test zone for electronic warfare”. *CNN*. 9 October. https://edition.cnn.com/2015/10/09/opinions/syria-electronic-warfare-russia-nato/index.html Accessed 3 March 2021

Thomas, Timothy. 2014. “Russia’s Information Warfare Strategy: Can the Nation Cope in Future Conflicts?”. *Journal of Slavic Military Studies* 27 (1): 101-130. http://www.doi.org/10.1080/13518046.2014.874845

Turunen, Andreas. 2020. “The Broader Challenge of Russian Electronic Warfare Capabilities”. In *Improvisation and Adaptability in the Russian Military*, edited by Jeffrey Mankoff, 13-21. Washington DC: CSIS.

Urcosta, Ridvan Bari. 2020. “The Revolution in Drone Warfare: The Lessons from the Idlib De-Escalation Zone”. Air Force Journal of European, Middle Eastern & African affairs 3 (2): 50-65.