Moscow's emerging electronic warfare capabilities: a dangerous jammer on U.S./NATO-Russian relations?

by Anya Loukianova[1]

1. Introduction

Ongoing conflicts in Ukraine and the Middle East have given Russia an opportunity to test the employment of electronic warfare (EW) capabilities that it has developed over the last decade in order to deter and counter military threats from the West. News reports suggest that pro-Russian separatists in Ukraine have utilized Russian systems and concepts for electronic warfare in their operations against Ukrainian government forces.[2] In that conflict, jamming technologies have hindered the operations of monitoring drones flown by the Organization for Security and Cooperation in Europe.[3] Moscow also has touted that capabilities deployed in Russia's area of operations in Syria could "blind" NATO radar systems.[4]

Western analysts have foreseen the emergence of Russia's anti-access/area denial capabilities, including advanced electronic counter measures (ECM), for over a decade.[5] What arguably came as a surprise is the demonstrative nature of Russia's use of these capabilities. Since 2014, Moscow has provocatively operated EW systems in close proximity to U.S. forces and widely publicized these developments in state-run media organizations.[6] In response to these actions, U.S. and NATO officials have expressed concerns with regard to implications for Western military operations, especially those conducted in close quarters with Russian forces.[7]

Russia's actions suggest a growing sense of optimism in Moscow with the nascent ability to challenge the U.S. military's post-Cold War "command of the commons."[8] Unfortunately, they also hint at Moscow's overconfidence and a lack of regard for the concomitant rise of escalation dangers between U.S./NATO and Russian forces. While these dynamics could arguably be ameliorated only by cooperative activities, Russia's

[1] Anya Loukianova is a PhD candidate, School of Public Policy, University of Maryland, College Park and a graduate fellow at the Center for International and Security Studies at Maryland (CISSM).

[2] Joe Gould, "Electronic warfare: what U.S. Army can learn from Ukraine," *Defense News*, August 4, 2015, http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/.

[3] Paul McLeary, "Russia's winning the electronic war," *Foreign Policy*, October 21, 2015, http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

[4] "Russian jamming system blocks all NATO electronics over Syria," Sputnik, October 29, 2015, http://in.sputniknews.com/world/20151029/1016211289/russian-jamming-system-syria-nato.html.

[5] See Eric V. Larson, Derek Eaton, Paul Elrick, Theodore Karasik, Robert Klein, Sherrill Lingel, Brian Nichiporuk, Robert Uy, John Zavadil, *Assuring Access in Key Strategic Regions: Toward a Long-Term Strategy* (RAND Arroyo Center, 2004), pp. 11-12, http://www.rand.org/pubs/monographs/MG112.html.

[6] See Sputnik, op. cit., and Paul D. Shinkman, "More 'Top Gun': Russian jets buzz U.S. Navy destroyer in Black Sea," *U.S. News and World Report*, June 1, 2015, www.usnews.com/news/articles/2015/06/01/more-top-gun-russian-jets-buzz-us-navy-destroyer-in-black-sea.

[7] Andrew Tilghman and Oriana Pawlyk, "U.S. vs. Russia: what a war would look like between the world's most fearsome militaries," *Military Times*, www.militarytimes.com/story/military/2015/10/05/us-russia-vladimir-putin-syria-ukraine-american-military-plans/73147344/.

[8] The concept is from Barry Posen, "Command of the Commons: The Military Foundations of U.S. Hegemony," *International Security* 28/1 (summer 2003), pp. 5-46.

demonstrative employment of EW technologies may worsen the prospects of that cooperation.

This paper begins with a broad discussion of the role of EW in defensive and offensive operations.[9] It then uses coverage in Russian-language media, including interviews from military publications, to present an overview of Russia's discussion of its capabilities. The paper then focuses on concerns about escalation in a conflict involving Western and Russian forces and the impact of the EW dimension on escalation dynamics. It concludes with a discussion of the implications of these issues for future U.S./NATO-Russia cooperation.

2. EW and escalation issues

Denial of information to or deception of radar sensors (jamming) is perhaps the most well-known way to employ EW. ECM are devices intended to deceive or disrupt an adversary's communications and sensor systems such as radar or infrared. At their most basic, these devices are designed to emit radio frequency signals that interfere with the reception or degrade the quality of information that sensors detect or relay. ECM-enabled activities include jamming that disrupts communication among individuals, sensors, and systems; thwarts their ability to connect to satellites in order to geolocate; and facilitates the denial or distortion of targeting data to weapon systems. ECM can be mounted on trucks, aircraft, or vessels and employed in both offensive or defensive operations.

Radar detection affords states the opportunity to see outside of their borders and into their territorial waters or their neighbors' airspaces. Since World War 2, radar-detected information could allow states to mount an organized defense against an airborne threat with artillery or scramble interceptor aircraft. The development of offensive EW technologies and stealth sought to counter defensive detection and engagement technologies. And, the only way to acquire air superiority over a state with an effective and coordinated system of radar, air defense, and EW involved the destruction and disablement of these systems. On the flip side, the increased incorporation of information processing and distribution systems into warfare planning and implementation have also contributed to the vulnerability of these systems to disruption. These days, both attackers and defenders require EW tools for successful operations.

Since the end of the Cold War, the United States has led multiple conventional campaigns with an extensive use of airpower for reconnaissance and strike. Military operations, including during the Gulf War, in former Yugoslavia, Afghanistan, and Iraq showcased an increase in the effectiveness and precision of U.S. airpower.[10] While the United States performed a supporting, yet key, role in the 2011 campaign in Libya, those operations were praised for NATO's ability to exercise command and control over aerial

[9] Electronic warfare is a broad concept that is generally recognized as having three components: electronic warfare support, electronic protection, and electronic attack. This paper does not focus on cyber issues.

[10] However, see the discussion of problematic air power effectiveness narratives during the Gulf War in Daryl G. Press, "The Myth of Air Power in the Persian Gulf War and the Future of Warfare," *International Security*, Vol. 26, No. 2 (Fall 2001), pp. 5–44.

strike operations that required a high degree of coordination among allies and partners.[11]

In the first salvos of air operations, attacking forces seek to disable and destroy elements of the defender's networked radar and air defense systems in order to establish air superiority and enable effective air operations.[12] Since the attacker's targeting occurs with the help of aircraft-mounted sensors that are able to track electronic emissions, a defender has to be able to deny the attacker the acquisition of targeting data. A defender can be a "cooperative target" if the components of its air defense systems are enabled, thus revealing their locations to the attacker's sensors. These sensors then communicate targeting data to the attacker's aircraft and standoff platforms launching missiles designed specifically to home in on the defender's emitting radar and surface to air missile systems. However, the defender's mobile air defense systems can also operate with their radar sensors turned off. In this "uncooperative target" scenario, these systems present a challenge for the attacker to locate and suppress—especially if they are geographically dispersed and well hidden.[13]

In both "cooperative" and "uncooperative" scenarios, the attacker's primary goal is to deny the defender the ability to detect, track, and lock onto the attacker's strike assets, as well as to destroy the defender's integrated air defense system. For a defender, the networking of sensors, shooters, and command and control allows the elements of its air defense system to be more survivable and less "cooperative" targets that can also deny the attacker (confidence in achieving) air superiority. For an attacker, effective networking allows for more effective and diverse reconnaissance and strike capabilities, especially in a coalition environment. However, a network can also be vulnerable since its various elements can be disrupted. In air operations, EW tools are used by the attacker to prevent the defender's air defense system's elements from detecting, tracking, and targeting the attacker's reconnaissance or strike assets. In turn, EW tools are also used by the defender in order to deny or deceive the attacker's aerial reconnaissance and strike assets. In both air and ground operations, both sides use EW tools to disrupt and intercept one another's command, control, and communications. The development of offensive cyber capabilities enables further non-kinetic solutions for disabling networked systems. To this end, a defender is faced with the need to plan to defend and counter both kinetic and cyber attacks.

One of the dangers with these types of combat engagements is their unpredictability. As Keir Lieber and Daryl Press have presciently argued, "the nature of conventional warfare in the information age is highly escalatory."[14] This is in large part because both attackers and the defenders seek to gain advantage by disrupting one another's networks of

[11] Ivo H. Daalder and James G. Stavridis, "NATO's Victory in Libya," *Foreign Affairs*, March/April 2012, https://www.foreignaffairs.com/articles/libya/2012-02-02/natos-victory-libya.

[12] For a useful discussion of operations to suppress air defense, see Christopher Bolkcom, "Military Suppression of Enemy Air Defenses (SEAD): Assessing Future Needs," CRS Report for Congress, May 11, 2005, www.fas.org/sgp/crs/weapons/RS21141.pdf.

[13] On experiences from Yugoslavia and Iraq, see Benjamin S. Lambeth, "Kosovo and the Continuing SEAD Challenge," *Aerospace Power Journal*, Summer 2002, www.ausairpower.net/APJ-Lambeth-Mirror.html and Posen, op. cit., pp. 24-30.

[14] Keir Lieber and Daryl Press, "Conventional War and Escalation," permission needed, January 3, 2014, https://www.princeton.edu/politics/about/file-repository/public/Lieber_Press_Article_Esc_030114.pdf.

command, control, communications, computers, intelligence, surveillance, and reconnaissance [C4ISR].[15] In addition, U.S. military planners have a propensity to target an adversary's strategic assets.[16] The implication of all of this is a dynamic of instability in crises in which U.S./NATO forces are faced with a conventionally-inferior adversaries with nuclear weapons. These adversaries also have a high political stake in the outcome of the crisis. In such crises, the power of U.S. conventional counterforce capabilities and their demonstrated effectiveness pushes adversaries to rely on strategies of coercive escalation, including potentially to nuclear weapons.[17]

A common perception is that the probability of a U.S.-Russian strategic nuclear exchange stabilizes the relationship at the strategic level. However, as Forrest Morgan has argued, "escalation dynamics in a conflict between NATO and Russia would not hinge on the risks of a strategic nuclear exchange, at least not initially, rather, they would build from the bottom up."[18] And, given longstanding concerns in Moscow about an inability to detect and counter a U.S./NATO attack on Russia's integrated air defense elements and command and control nodes, such an attack could raise the pressure for Moscow to de-escalate the conflict with the use of tactical nuclear weapons.[19]

Thus, conflict in which U.S. forces are faced with a conventionally-inferior and nuclear-armed adversary, like Russia, could be very prone to escalatory dynamics. However, a layer of escalation dangers is added to this when Russia is overconfident about its ability to challenge U.S. forces in certain domain. The section that follows discusses Russia's development and recent employment of EW technologies.

3. Russia and EW developments

Russia prides itself on being the first country to employ EW in a combat environment. This employment was somewhat in accident, and occurred when telegraphy stations at Port Arthur and Russia's battleships prevented radio coordination by a group of Japanese military vessels during the Russo-Japanese war. [20] This incident took place on

[15] "First, military forces now derive their effectiveness, more than ever before, from their ability to function as part of a network. Sensors, data processing facilities, commanders, and shooters are often widely dispersed; increasingly, generating combat power depends on a military's ability to integrate information from multiple sources, make effective decisions, and then coordinate the actions of widely dispersed forces. Second, and following directly from the first point, the payoffs from disrupting an adversary's "command and control" network have soared. Third, powerful states now have an unprecedented capacity to degrade an enemy's "command and control" system: thanks to long-range precision weapons, and possibly also through unconventional means (e.g., offensive cyber attacks). It would be an exaggeration to say that warfare is now entirely about degrading enemy command and control; rather, those operations typically open the door for decisive force-on-force engagements. But the efforts to gather and utilize information, coordinate actions among many units, and deny that intelligence and coordination to others, is a bigger part of modern warfare than ever before." Ibid.

[16]Keir Lieber and Daryl Press, "The New Era of Nuclear Weapons, Deterrence, and Conflict," *Strategic Studies Quarterly*, Spring 2013, pp. 3-14.

[17] Ibid., pg. 6.

[18] Morgan suggested a Russia-Baltic conflict or a conflict between Poland and Belarus, which would put comparable escalatory pressures on NATO and Russia, respectively. Forrest E. Morgan, *Dancing with the Bear: Managing Escalation in a Conflict with Russia*, IFRI proliferation paper, Winter 2012, pg. 37.

[19] Ibid., pg. 38.

[20] "111 let pomekh," Lenta.ru, April 15, 2015, http://lenta.ru/articles/2015/04/15/ew/.

April 15, 1904, and thus April 15 is celebrated as a professional holiday of EW operators in the Russian forces. [21]

The steady development and deployment of primarily ECM technologies followed suit. Soviet forces used employed ECM during World War 2, and they were viewed as integrated element of Soviet planning and operations during the Cold War.[22] Soviet forces used ECM during their involvement in Afghanistan, where jamming systems were primarily designed to reduce the threat to aircraft and helicopter from shoulder-fired, man-portable air defense missiles.[23] Russian sources also note that the 1982 Bekaa Valley battle that saw the engagement between Soviet-supplied Syrian air defense and ECM systems and U.S.-supplied Israeli aerial reconnaissance and strike systems gave the Soviet military a glimpse of the role of EW in future warfare.[24]

The increasing importance of EW began to sink in as Soviet and Russian military officials assessed Western aerial operations during the Gulf War.[25] A U.S. analyst described Russian thinking in 1992 regarding a defensive fire-strike operation in which Russian forces would survive repel enemy precision weapons and aircraft.[26] Despite the repudiation of its “no-first-use” commitment in the 1993 military doctrine, Moscow also set a course for the development of conventional systems that could prevent the need to resort to nuclear weapons.[27] In addition, Russia would seek to develop EW measures in order to disrupt enemy command, control, and communication systems in defensive and offensive operations.[28]

Russian military planners view U.S./NATO-led aerial campaigns as effective in suppressing and defeating enemy air defenses through a combination of EW, use of aerial and satellite reconnaissance for targeting strike systems, and firepower. [29] In a discussion of operations Desert Storm and Desert Shield, a Russian EW professional noted that “a radio-electronic strike allowed [Western forces] to create positive conditions for the sudden use of air and ground forces and high-precision weapons, facilitating a superiority in command and control.”[30] In addition, in both Yugoslavia and

[21] Evgeniy Lisanov, "Perebivaya iskroy telegrammy," *Krasnaya Zdezda*, April 15, 2004, http://old.redstar.ru/2004/04/15_04/1_02.html.

[22] Ibid. However, see also Matthew M. Hurley, "The BEKAA Valley Air Battle, June 1982: Lessons Mislearned?" *Airpower Journal*, Winter 1989, www.airpower.maxwell.af.mil/airchronicles/apj/apj89/win89/hurley.html.

[23] "111 let pomekh," Lenta.ru, April 15, 2015, http://lenta.ru/articles/2015/04/15/ew/.

[24] Ibid.

[25] It may be an interesting question as to whether the Russian military overestimated the effectiveness of Western airpower, much like many Western analysts, did at the time.

[26] Mary C. FitzGerald, “The Russian Military’s Strategy for ‘Sixth Generation’ Warfare,” *Orbis* 38:3 (Summer 1994).

[27] See Alexei Arbatov, *The Transformation of Russian Military Doctrine: Lessons Learned from Kosovo and Chechnya*, The Marshall Center Papers, no. 2, July 2000, pp. 15-20.

[28] FitzGerald, op. cit.

[29] In Russian, EW is *radio-elektronnaya bor’ba (REB)* and EW measures are *stredstva REB*. It should be noted, though, that *bor’ba* in Russian is better understood as “combat” as opposed to “war” or “warfare.”

[30] “По сути, впервые в практике ведения РЭБ была реализована форма «радиоэлектронного удара», в результате чего удалось создать благоприятные условия для внезапного применения авиации и сухопутных группировок войск (сил), высокоточного оружия и добиться в целом превосходства в управлении.” Viktor Khudoleev, "Voiska dlya srazheniya v efire," *Krasnaya Zvezda,*

Iraq 2003, Western forces also were able to destroy those governments' abilities to broadcast information regarding the conduct of the war to their populations.[31]

The watershed role for Russian military planners of the 1999 NATO attacks on Yugoslavia has been widely discussed and noted.[32] However, Russia had been developing anti-access/area denial capabilities, including EW measures, since the mid-1990s, and accelerated those developments with the improvement in its economy in the early 2000s. In debates about developments in response to U.S. missile defense infrastructure deployments to Europe, even moderate analysts like Alexey Arbatov posited that ECM and point-defense of high-value targets was a cost-effective way to counter perceived aerial threats from the West.[33] However, at the time, Arbatov also noted that the scenario of a Western aerial attack on Russia was unrealistic, especially because the West understood that such an attack would be highly escalatory. [34]

Today, Russian military officials view EW and ECM as an inexpensive, yet key determinants in the conduct and outcome of combat.[35] They posit that "new developments allow to achieve information dominance over the adversary by the suppression of its [C4ISR] systems, achieve air superiority by neutralization of enemy radar, and deal with many other tasks." [36] As a Russian EW officer explained:

> "There is nothing surprising that in the current circumstances, EW—as a relatively inexpensive and easily implemented means to disrupt the functioning of an enemy's radar and other systems and to defend one's own analogous systems from interference—is emerging as a priority and a focus for development. In certain circumstances, use of EW approaches can be viewed as asymmetric measures that negate the benefits of an adversary's highly sophisticated systems and means of armed combat."[37]

Despite stated efforts keep pace with the developments in Western strike systems, Russia's domestic development of ECM was faced with difficulties until 2009. During

April 14, 2014, www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire.

[31] Ibid. Additional concern raised by Russian military officials from the latter campaign centers on the Western ability to deny information operations to the government of Serbia.

[32] But, again, it's not known whether Russia overstated the effectiveness of the operation as a whole.

[33] Alexey Arbatov, "Strategicheskii surrealism somnitelnykh kontseptsiy," *Nezavisimoye Voyennoe Obozreniye*, March 5, 2010, http://nvo.ng.ru.

[34] Ibid. But he also noted that Russia's tactical nuclear weapons could provide a deterrent since they could target U.S./NATO forward-deployed forces.

[35] Viktor Khudoleyev, "Na sluzhbe bezopasnosti efira," *Krasnaya Zvezda*, April 15, 2010, http://old.redstar.ru/2010/04/15_04/2_01.html.

[36] Oleg Grozny, "Splav opyta i novykh tekhnologyi," *Krasnaya Zvezda*, April 14, 2015, http://www.redstar.ru/index.php/news-menu/vesti/iz-vvs1/item/23087-splav-opyta-i-novykh-tekhnologij-i-boevogo-primeneniya-vojsk-reb.

[37] "Нет ничего удивительного в том, что в сложившихся условиях именно радиоэлектронная борьба как относительно малозатратный и достаточно легко реализуемый метод дезорганизации работы отдельных РЭС и систем на их основе у противника и защиты своих аналогичных систем от воздействия выходит на первый план и получает приоритетное развитие. При определённых условиях именно применение методов РЭБ можно рассматривать как асимметричные меры, нивелирующие достоинства высокотехнологичных систем и средств вооружённой борьбы противника." Viktor Khudoleev, "Voiska dlya srazheniya v efire," *Krasnaya Zvezda*, April 14, 2014, www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire.

that year, over a hundred of companies involved in EW design and production aspects underwent vertical integration. This resulted in the creation of KRET (Kontsern Radioelektronnyye Tekhnologii), a state-owned enterprise tasked with managing the design and production process of radar and EW technologies. KRET has apparently been effective in managing projects across the sector and lobbying the government for funding. The recent emergence of EW systems is also thus the result of efforts to integrate this sector of Russia's defense industry and properly fund research and development.

Russia's EW capabilities include land, air, and sea-based systems to jam communications, radar, and command-and-control networks.[38] The domestic deployment of these systems is not discussed in great detail in the Russian media. It can be said that they are deployed in the Western military district, in Kaliningrad, and now in Crimea. They provide support for locations in which air defense assets are present in great numbers, including likely to cover Russia's strategic assets. The overall plan is to upgrade up to 70 percent of EW equipment through all of the forces by 2020.[39] Some areas, such as South Ossetia and Crimea, these upgrades have been prioritized. Military operators at the Black Sea fleet suggest that most of their equipment is not older than 2012.[40]

The Russian Ministry of Defense has sought to professionalize EW in the Russian armed forces. More recently, they have sough to integrate young technical experts and create specially-organized units focused on EW issues.[41] These units have been frequently exercised on their own as well as in combination with other forces in order to increase readiness.[42] Reports suggest that, more recently, there has been improved coordination between development centers in the industry and their ability to have their new systems field tested by these specially-organized units.[43]

Russian officials appear to have made a very deliberate choice to publicize EW developments in domestic media. The head of KRET, for example, frequently brags

[38] See a basic overview of systems in Russian at http://www.rusarmy.com/pvo/reb-rtr.html.

[39] "V Rossiiskoi armii idet masshtabnoye pereosnascheniye voisk sovremennoi tekhnikoi radioelectronnoy bor'by," *Krasnaya Zvezda*, April 15, 2015, www.redstar.ru/index.php/news-menu/vesti/tablo-dnya/item/23118-v-rossijskoj-armii-idet-masshtabnoe-pereosnashchenie-vojsk-sovremennoj-tekhnikoj-radioelektronnoj-borby

[40] Pavel Zavolokin, "Na linii elektronnogo fronta," *Krasnaya Zvezda*, September 17, 2015, www.redstar.ru/index.php/syria/item/25764-na-linii-elektronnogo-fronta

[41] "Proizvodstvennaya rota REB nachnet rabotu v Tambovskoi oblasti," RIA Novosti, October 26, 2015, http://ria.ru/defense_safety/20151026/1308281580.html and "Okolo 70 prizyvnikov otpravyatsya sluzhit v tri nobye nauchnye roty," RIA Novosti, October 27, 2015, http://ria.ru/defense_safety/20151027/1308673716.html.

[42] Viktor Khudoleev, "Voiska dlya srazheniya v efire," *Krasnaya Zvezda*, April 14, 2014, www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire. RF ispytayet sisemu bor'by so sredstvami vozdushno-kosmicheskoi ataki," RIA Novosti, August 25, 2015, http://ria.ru/defense_safety/20150825/1205686148.html.

[43] Oleg Grozny, "Splav opyta i novykh tekhnologyi," *Krasnaya Zvezda*, http://www.redstar.ru/index.php/news-menu/vesti/iz-vvs1/item/23087-splav-opyta-i-novykh-tekhnologij-i-boevogo-primeneniya-vojsk-reb.

about capabilities that are currently under development.[44] Recently, he announced that the company intends to initiate state testing of a “principally new system of EW, intended for electronic suppression of the most modern means and systems of air-space attack. This would mean the development of a whole family of multi-functional systems and complexes of reconnaissance, EW, and command and control, which would have new capabilities to combat air-space reconnaissance, targeting, the employment of highly-precise weapons, and navigation.”[45] This public relations campaign, however, pales in comparison to the domestic coverage of Russia’s employment of EW systems abroad.[46]

4. EW use in Syria and Ukraine

During operations in Chechnya and the North Caucasus during the 1990s and 2000s, Russian forces employed EW to disrupt and defeat communication networks among militant groups—reportedly a challenging endeavor in a highly mountainous terrain. ECM systems also allowed Russian forces to thwart the use of radio-controlled explosive devices by the militants.[47] In the 2008 conflict with Georgia, Russian forces reportedly also used ECM for jamming of Georgia’s unmanned aerial systems (UAS).[48] However, Russia’s deployment and employment of EW systems during the ongoing conflicts in Ukraine and Syria have perhaps been most noted in Western and Russian media alike.

The mobile Krasuha series of systems is arguably the most widely discussed in Russian media. Designed in the mid-1990s, the system entered production in 2011.[49] According to *Jane’s*, Krasuha-4 is “designed to neutralize Low-Earth Orbit (LEO) spy satellites such as the U.S. Lacrosse/Onyx series, satellites, ground-based radars, airborne surveillance radars, and radar-guided ordinance.”[50] The system is reportedly able to protect an object from radar detection at the distance of 150-300 kilometers as well as inflict electronic disruption to adversary's radar electronic warfare and communications system.[51] The system, generally employed in coordination with air defense elements in

[44] For example, “KRET v 2015 godu peredal Vooruzhennym silam 9 kompleksov REB Moskva-1, RIA Novosti, December 25, 2015, http://ria.ru/defense_safety/20151225/1348750286.html.

[45] "RF ispytayet sisemu bor'by so sredstvami vozdushno-kosmicheskoi ataki," RIA Novosti, August 25, 2015, http://ria.ru/defense_safety/20150825/1205686148.html. He also has touted KRET’s development of radio-optical phased array antenna (ROFAR), slated for unveiling in 2018.See KRET, “Radio photos and future technologies,” November 11, 2015, http://kret.com/en/news/4057/.

[46] See "Russian jamming system blocks all NATO electronics over Syria," op. cit.

[47] Viktor Khudoleev, "Voiska dlya srazheniya v efire," *Krasnaya Zvezda*, April 14, 2014, www.redstar.ru/index.php/news-menu/vesti/iz-sukhoputnykh-vojsk/item/15511-vojska-dlya-srazheniya-v-efire.

[48] Anton Valagin, “Chto napugalo amerikanskii esminets,”*Rossiiskaya Gazeta*, April 30, 2014, www.rg.ru/2014/04/30/reb-site.html.

[49] “Krasuha series radar jammers,” *Jane’s C4ISR & Mission Systems/IHS.com*, December 17, 2015.

[50] Ibid.

[51] "V Siirri zamecheny noveishiye sistemy radiolelektronnoi bor'by Krasuha-4," *Lenta.ru*, October 5, 2015, http://lenta.ru/news/2015/10/05/krasuha/.

order to increase their survivability, is in service with the Russian military and will also reportedly be deployed in the Arctic in the near future.[52]

The Krasuha-4's deployment in October 2015 at Latakia airfield in Syria perhaps caused the most concern to U.S./NATO and Israeli military forces. Presumably, its deployment was necessary in order to be able to jam ISIL and rebel communication systems. However, deployed in close proximity to other militaries engaged in counter-ISIL operations, the system also had an ability to disrupt radar, communications, and signals intelligence systems. Russia and Israel created a mechanism to deconflict their operations in Syria, including in "the electromagnetic arenas" in the fall of 2015.[53] A deconfliction mechanism has also been worked out with the United States.[54] Presumably, these deconfliction mechanisms should have explicitly prohibited the jamming of one another's radar systems, but this is unknown since Russia has apparently asked that the final texts of these agreements not be made public.

This Western discreetness has arguably helped Russia's domestic narrative about its nascent ability to challenge U.S./NATO forces. Krasuha's deployment has been widely reported in Russian media, even if its capabilities to "blind" NATO systems had been overstated.[55] Russian servicemen have bragged that Krasuha-4 can neutralize AWACS reconnaissance and surveillance. "The adversary's aircraft loses its ability to precisely fire weapons, employ navigation, and receive targeting data. They can only "eyeball" their targets and operate at lower altitudes, where they are vulnerable to air defense systems," they note.[56]

Russia's deployment of EW systems in Ukraine has been extensive, as discussed in Western publications.[57] Russia has also reinforced the Black Sea fleet base in Crimea with heavy EW capabilities. [58] Despite Ukrainian requests, the United States has not

[52] "V Siirri zamecheny noveishiye sistemy radiolelektronnoi bor'by Krasuha-4," Lenta.ru, October 5, 2015, http://lenta.ru/news/2015/10/05/krasuha/ and"PVO v Arktike poluchat kompleksy radioelektronnoi bor'by Krasuha," RIA Novosti, April 2, 2015, http://ria.ru/defense_safety/20150402/1056209751.html.

[53] Yaakov Lappin, "No progress reported from first Israel, Russia deconfliction meeting," *Jane's Defense Weekly*, October 8, 2015; Barbara Opall-Rome, "Russia, Israel To Broaden Defense Coordination in Syria," *Defense News*, December 1, 2015, www.defensenews.com/story/defense/air-space/2015/11/30/russia-israel-broaden-defense-coordination-syria/76576390/.

[54] Neil MacFarquhar, "U.S. Agrees With Russia on Rules in Syrian Sky," *New York Times*, October 20, 2015, www.nytimes.com/2015/10/21/world/middleeast/us-and-russia-agree-to-regulate-all-flights-over-syria.html?_r=0.

[55] "Russian jamming system blocks all NATO electronics over Syria," Sputnik, October 29, 2015, http://in.sputniknews.com/world/20151029/1016211289/russian-jamming-system-syria-nato.html.

[56] Мы можем сделать так, что современный боевой самолёт будет вынужден летать как во время Великой Отечественной войны – по бумажной карте на коленке пилота и по наземным ориентирам, – рассказывает врио командира отдельной роты РЭБ с самолётными средствами старший лейтенант Сергей Наймушин. Pavel Zavolokin, "Na linii elektronnogo fronta," *Krasnaya Zvezda*, September 17, 2015, www.redstar.ru/index.php/syria/item/25764-na-linii-elektronnogo-fronta

[57] See, for example, C.J. Chivers, "Is That an R-330Zh Zhitel on the Road in Crimea?," *New York Times*, April 2, 2014, www.nytimes.com/2014/04/03/world/europe/instagram-catalogs-new-russian-weaponry.html?_r=2.

[58] Deployed at the Black Sea fleet base in Crimea, the Murmansk is touted as the "strategic bomber" of Russian EW. This system reportedly can "cover up to 5,000 kilometers and suppress over 20 frequencies simultaneously." The system substantially lacks in mobility since it has to be based on six vehicles. Pavel

supplied EW systems or systems to counter Russian-ECM to Ukraine, potentially due to concerns of escalation.[59] Pro-Russian separatists have used Russian UAS for reconnaissance and targeting purposes.[60] In a February 2015 report, former U.S. officials called for U.S. provision of ECM equipment for Ukraine that could counter Russian UAS activities.[61] In addition to their use in countering Ukrainian government forces, ECM have also hindered the operations of conflict monitoring drones flown by the OSCE.[62] In response to this, OSCE UAS had to be fitted with a system to counter jamming.[63]

U.S. military officials have indicated that Russia's use of UAS and EW systems has had implications for the "long-held [U.S.] presumption of air superiority."[64] Western forces did not encounter ECM in Iraq and Afghanistan to this great extent, and Russia's use of these systems in Ukraine has involved a learning curve for U.S. forces assisting Ukrainian government forces.[65] U.S. officials have noted that, based on some of these experiences, there was a need to increase interoperability, especially with regard to the security of communications among allies in NATO and other partners, so that Western systems would be less susceptible to interception and disruption.[66]

Finally, Russian news websites have been all too happy to re-translate English-language reports that note a U.S./NATO surprise with Russian EW capabilities.[67] Arguably, one wouldn't care about this if it weren't a part of an emerging Russian narrative about its ability to challenge Western forces. Worse, after the Turkish air force downed the Russian jet in November 2015, Russian analysts have also raised the specter of

Zavolokin, "Na linii elektronnogo fronta," *Krasnaya Zvezda*, September 17, 2015, www.redstar.ru/index.php/syria/item/25764-na-linii-elektronnogo-fronta.

[59] Reuben Johnson, "Ukrainian requests for EW equipment go unanswered," *Jane's Defense Weekly*, July 24, 2014.

[60] Adam Rawnsley, "Ukraine scrambles for UAVs, but Russian drones own the skies," War is Boring, February 20, 2015, https://medium.com/war-is-boring/ukraine-scrambles-for-uavs-but-russian-drones-own-the-skies-74f5007183a2#.sk4mnbuos.

[61] Ivo Daalder, Michele Flournoy, John Herbst, Jan Lodal, Steven Pifer, James Stavridis, Strobe Talbott and Charles Wald, "Preserving Ukraine's Independence, Resisting Russian Aggression," Atlantic Council, Brookings, and Chicago Council on Global Affairs report, Februay 2015, pg. 4, www.thechicagocouncil.org/sites/default/files/UkraineReport_February2015_FINAL.pdf

[62] Paul McLeary, "Russia's winning the electronic war," *Foreign Policy*, October 21, 2015, http://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

[63] Huw Williams, "Find and fix: counter-UAV solutions emerge to tackle new challenges," *Jane's International Defence Review*, January 6, 2016.

[64] Andrew Tilghman, "Advanced Russian air power, jammers are focus of U.S. troops," *Military Times*, December 10, 2015, www.militarytimes.com/story/military/pentagon/2015/12/10/advanced-russian-air-power-jammers-focus-us-troops/77090544/

[65] Daniel Wasserbly, "AUSA 2015: Lessons learned from Ukraine added to training at Hohenfels," *Jane's International Defence Review*, October 14, 2015.

[66] Daniel Wasserbly, "Amid Russian EW threat, U.S. Army seeks greater European interoperability," *Jane's International Defence Review*, July 15, 2015.

[67] The echo chamber has been especially interesting with regard to pieces in the National Interest. See Dave Majumdar, "The Russian Military's 5 Next Generation Super Weapons," *The National Interest*, November 8, 2015, http://nationalinterest.org/blog/the-buzz/the-russian-militarys-5-next-generation-super-weapons-14276 and "Brutalnaya rossiya: top superoruzhiya novogo pokoleniya," Vesti.lv, November 9, 2015, http://vesti.lv/news/brutalynaya-rossiya-top-superoruzhiya-novogo-pokoleniya.

escalation, arguing that Krasuha-4 could also be used to protect Russian aircraft in Syria from Western forces.[68]

5. Associated escalation dangers

Managing escalation has been a difficult enough task for U.S./NATO policy makers and military officials in light of the security environment in Europe and the Middle East. Now, Russia's emerging EW capabilities also need to be factored into hypothetical scenarios of U.S./NATO-Russian conflicts in the Euro-Atlantic region, especially ones which have escalation potential. In addition, Moscow's newfound confidence in its conventional abilities may also challenge past notions about escalation and potentially shift the understanding of Russia's escalation thresholds.

States (can and do) choose to escalate political-military conflicts for various reasons.[69] One useful example from 2004 of how U.S. planners perceived escalation issues in the Euro-Atlantic is a RAND report that explored a hypothetical conventional conflict involving Russia and the Baltics. The report offered a rare unclassified example of U.S./NATO perception of threats from Moscow in 2004 by detailing an anti-access scenario in which Moscow utilized coercion in an attempt to "separate the three Baltic states [...] from NATO."[70] In the scenario, Russia utilized its mobile air defense systems and elements of the Russo-Belarusian air defense network to aid in a rapid ground offensive. With help from ECM and short-range ballistic missiles, Russia would create an integrated air defense system to cover the Baltic states in order to prevent access by U.S./NATO air forces.[71] With its key assumption that Russia's threat to use nuclear weapons would deter large scale operations by U.S./NATO forces, the report also judged that Russia's ability to deny access was "protracted" at best due to "the chronic and difficult-to-reverse weaknesses of the Russian military."[72]

[68] "Jamming Systems to Protect Its Pilots in Syria," Sputnik, November 24, 2015, http://sputniknews.com/middleeast/20151124/1030665306/russia-syria-electronic-warfare.html#ixzz3xLGP1wVz,

[69] Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Polipeter, Roger Cliff, *Dangerous Thresholds: Managing Escalation in the 21st Century*, RAND Project Air Force study (MG-614-AF), 2008., pg. xii. In instrumental escalation, "the combatant deliberately increases the intensity or scope of an operation to gain advantage or avoid defeat." In suggestive escalation, the combatant wishes to "send signals, [...] punish enemies for earlier escalatory deeds, or warn them that they are at a risk of even greater escalation if they do not comply with coercive demands."

[70] Eric V. Larson et al., op. cit., pg. 65. The scenario envisioned Russian involvement in the Baltic states on the pretense of separatists sentiments in the Baltics. The involvement triggered a strong NATO response which, in turn, provoked a political crisis in Russia. The scenario presumed that, in an attempt to "save face," the Russian government would order the mobilization of forces to launch an attack that would isolate and overrun the Baltic states. While also preparing for a potential NATO counterattack, Russia would "present NATO with a fait accompli that will lead to a negotiated settlement acceptable to Russia." The scenario also assumed a month-long mobilization effort on part of the Russian military that gave ample warning time and preparation to U.S. and NATO. However, arguably, in a crisis, the restraint and ample warning time criteria would not hold as effectively. Larson et al, pp. 67-68.

[71] Larson et al, pg. 81.

[72] Larson et al, pg. 72. The report judged that a strategically meaningful Russian anti-access strategy could be used with[information operations and psychological operations in order to separate the United States from its key NATO allies: Germany, Belgium, the Netherlands, and Poland. Larson et al, pp. 75-77.

More than ten years later, Russia's access-denial capabilities have developed to the extent that Russia feels comfortable using them in military operations. Worse, the demonstrative nature of Russia's use of its EW arguably what arguably came as a surprise to Western analysts. In the spring of 2014, a Russian Su-34 aircraft devices provocatively buzzed USS Don Cook, an Arleigh Burke-class guided missile destroyer.[73] After the incident, Russian media outlets reported that the fighter aircraft was equipped with the Khibiny EW system that was able to turn off radar, targeting, and information transmission on the naval vessel "as one would turn off the television by pressing a remote button."[74] To be sure, the U.S. Navy had dismissed this story, arguing that it is untrue. [75] However, it's not likely that this denial sufficiently challenged the internal Russian narrative or registered in Russian policy making circles.

In addition to Moscow's stated reliance on tactical nuclear weapons to offset NATO's conventional advantages, Russia is developing increasing confidence in its anti-access/area denial capabilities. The deployment of these capabilities suggests that Russia is increasing its reliance on deterrence by denial. Russia's adventurism in Ukraine, however, points to deterrence by punishment insofar as Moscow is willing and able to get involved and stick it out in an asymmetrical conflict in a neighboring state. And, while Russia chose creative uses of airpower in Ukraine, relying on air defense and UAS-enabled targeting of artillery, it has also attempted to demonstrate its prowess with strike systems in Syria. Analysts have argued, however, that Russia's capabilities are still "brittle" and thus, their demonstrative use is provocative and risky—to say the least.[76]

The most effective way to manage deliberate escalation is through deterrence. In situations with escalation potential, there is some consensus that "a more reliable strategy for deterring deliberate escalation is one that buttresses threats of punishment with visible capabilities for denial."[77] And, "if conventional deterrence fails, a force designed for deterrence by denial is more able to engage in conventional conflict, control escalation, and exercise a winning strategy."[78] Thus, U.S./NATO strategies need to seek to counter Russia's anti-access capabilities, but also take care to deter Russia from adventurism.

In a conflict with Russia, greater dangers lie in the prospect of inadvertent and accidental escalation. Inadvertent escalation is essentially an unexpected outcome of a

[73] Anton Valagin, "Chto napugalo amerikanskii esminets," *Rossiiskaya Gazeta*, April 30, 2014, www.rg.ru/2014/04/30/reb-site.html.
[74] Anton Valagin, "Pochemu NATO boitsya Russkikh ucheniy," *Rossiiskaya Gazeta*, November 3, 2014, www.rg.ru/printable/2014/11/03/uchenia-site.html.
[75] David E. Meadows, "Blog: Electronic warfare is the teeth-clenching defense of the last mile," AFCEA Signal, September 16, 2015, https://www.afcea.org/content/?q=Blog-electronic-warfare-teeth-clenching-defense-last-mile.
[76] See, for example, Pavel K. Baev, "Russian Air Power is Too Brittle for Brinksmanship," PONARS policy memo, November 2015, www.ponarseurasia.org/memo/russian-air-power-too-brittle-brinksmanship.
[77] Morgan, et al., op. cit., pg. xiii and also pp. 20-23.
[78] Michael Gerson, "Conventional Deterrence in the Second Nuclear Age," *Parameters*, Autumn 2009, pg. 38, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/09autumn/gerson.pdf.

deliberate action.[79] In this dynamic, “large-scale conventional operations [...] produce patterns of damage or threat to the major elements of a state’s nuclear forces.”[80] Managing inadvertent escalation is a more challenging task for policy makers since it requires mutual understanding with regard to thresholds of escalation. But, in an environment where Russia is overly confident about its anti-access capabilities, and U.S./NATO and Russia hardly, if at all, engage on military issues, the prospect of gaining understanding with one another’s thresholds is daunting. In addition, Russia’s domestic public relations efforts link the Putin administration’s legitimacy to its ability to challenge Western forces and thus may push its policy makers to mistakenly decide to escalate.

In accidental escalation, “operators make mistakes or leaders fail to set appropriate rules of engagement or maintain adequate discipline over forces under their command.”[81] There are persistent dangers of accidental escalation, as recent examples from both Ukraine and Syria show. In Ukraine, Russia’s apparent transfer of a high-altitude air defense system to inexperienced separatists led to the downing of a civilian airliner. In Syria, Turkey decided to down a Russian fighter aircraft that made repeated incursions into its airspace. Thus, building on the Russian leadership’s propensity to flaunt the ability to challenge Western forces, Russian theater-level operators are at a risk of making bad decisions that lead to significant complications for Russian and U.S./NATO leaders alike.

6. Conclusions

Russia is extremely proud of its nascent EW capabilities. Employed to increase the survivability of Russia’s air defense and strike systems, these cost-effective capabilities will pose challenges for U.S./NATO policy makers and military planners with their ability to disrupt C4ISR of Western forces. Domestically, Russia uses these systems as a part of its public relations effort to reverse narratives about its past conventional military weakness and vulnerability vis-à-vis the West. Their provocative demonstration against Western forces is a key component of this effort, and the West needs to find ways to effectively counter it.

Russia and the West are also involved in unfortunate proxy conflicts in Ukraine and Syria—perhaps unwittingly to the West. These allow Russia to field-test its new conventional capabilities and U.S./NATO to learn more about Russian systems and concepts. In the summer of August 2015, the U.S. Army carried out a war game that tested its new air and missile defense command system in an environment of Russian

[79] Morgan, et al., op. cit., pp. 23-25. As the RAND study defines, this type of escalation “engages when a combatant deliberately takes actions that it does not perceive to be escalatory but are interpreted that way by the enemy.”

[80] In his work on inadvertent nuclear escalation, Barry Posen warned that “Direct conventional attacks on critical nuclear forces, attacks that degrade strategic early warning or command and control systems, or even attacks on general-purpose forces that protect strong nuclear forces, could all produce strong reactions from the party on the receiving end.” Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Cornell University Press, 1989), pg. 3.

[81] Morgan et al, op. cit., pp. 26-28.

EW systems.[82] Similarly, in Ukraine, U.S. forces learn from their Ukrainian counterparts with regard to effective means to recognize and counter Russian EW capabilities.

To date, U.S./NATO forces have carefully sought to manage escalation, but it's unclear how long these efforts are going to be successful. One can argue that the time in which U.S./NATO and Russian forces are trying to figure out the shifts in their respective thresholds can be rather dangerous. Repeated incidents have illustrated escalation dangers in Europe and the Middle East. The lack of effective military engagement between Russia and NATO, as many have argued, will only contribute to these dangers.[83] As a first step, these dangers need to be addressed through dialogue.

In a plot twist, KRET has expressed its interest in exporting some of its new EW developments to states in the Middle East and South Asia.[84] They have also noted the possibility of exporting some systems to Iran.[85] Russian officials have highlighted that operators from Armenia, Algeria, and China are among students undertaking training at a Russian EW center.[86] While KRET is unlikely to be exporting the most cutting edge Russian EW systems, these exports will have implications for U.S./NATO and allied forces as well as crisis stability dynamics in those regions.

[82] Sydney J. Freedberg Jr., "U.S. wargame pits army missile defenses against Russian jamming," *Breaking Defense*, August 14, 2015, http://breakingdefense.com/2015/08/us-wargame-pits-army-missile-defenses-against-russian-jamming/.

[83] Thomas Frear, Lukasz Kulesa, Ian Kearns, "Dangerous Brinkmanship: Close Military Encounters Between Russia and the West in 2014," European Leadership Network policy brief, November 2014, http://www.europeanleadershipnetwork.org/medialibrary/2014/11/09/6375e3da/Dangerous%20Brinkmanship.pdf.

[84] Systems have been marketed to India at India Airshow and to Middle Eastern states in Dubai Airshow in 2015. KRET officials have noted that their airborne EW systems could be installed on Western aircraft. See Gareth Jennings, "Dubai Airshow 2015: Russian electronics concern KRET to grow international revenues," *Jane's Defence Weekly*, November 9, 2015.

[85] "KRET mozhet predlozhit Iranu postavki nazemnykh stantsii REB," RIA Novosti, November 9, 2015, http://ria.ru/defense_safety/20151109/1316921724.html. "Currently, KRET is offering its foreign partners the Rychag, Krasukha, President-S, Rtut, and Moskva series of electronic warfare systems, as well as the export version of the Khibiny airborne system for individual protection." See KRET, "Radio photos and future technologies," November 11, 2015, http://kret.com/en/news/4057/

[86] Oleg Grozny, "Splav opyta i novykh tekhnologyi," *Krasnaya Zvezda*, http://www.redstar.ru/index.php/news-menu/vesti/iz-vvs1/item/23087-splav-opyta-i-novykh-tekhnologij-i-boevogo-primeneniya-vojsk-reb.