Russian Electronic Warfare

A Growing Threat to U.S. Battlefield Supremacy

ASP

American Security Project

Perspective

Patrick Smith

April 2020

BOARD OF DIRECTORS

The Honorable Gary Hart, Chairman Emeritus

Senator Hart served the State of Colorado in the U.S. Senate and was a member of the Committee on Armed Services during his tenure.

Governor Christine Todd Whitman, Chairperson

Christine Todd Whitman is the President of the Whitman Strategy Group, a consulting firm that specializes in energy and environmental issues.

Brigadier General Stephen A. Cheney, USMC (Ret.), President of ASP

Brigadier General Cheney is the President of ASP.

Matthew Bergman

Matthew Bergman is an attorney, philanthropist and entrepreneur based in Seattle. He serves as a Trustee of Reed College and on the Board of Visitors of Lewis & Clark Law School.

Ambassador Jeffrey Bleich

The Hon. Jeffrey Bleich heads the Global Practice for Munger, Tolles & Olson. He served as the U.S. Ambassador to Australia from 2009 to 2013. He previously served in the Clinton Administration.

Alejandro Brito

Alejandro Brito is President of Brito Development Group (BDG), LLP. In the last twenty years, Mr. Brito has overseen the design, construction, development and management of over 1,500 luxury housing units in Puerto Rico.

The Honorable Donald Beyer

Congressman Donald Beyer is the former United States Ambassador to Switzerland and Liechtenstein, as well as a former Lieutenant Governor and President of the Senate of Virginia.

Lieutenant General Daniel Christman, USA (Ret.)

Lieutenant General Christman is Senior Vice President for International Affairs at the United States Chamber of Commerce.

Robert B. Carver

Robert B. Carver is a Partner of Nelson Mullins Riley & Scarborough in its Boston and Washington, DC offices. He is co-chair of the firm's Government Relations practice.

Lee Cullum

Lee Cullum, at one time a commentator on the PBS NewsHour and "All Things Considered" on NPR, currently contributes to the Dallas Morning News and hosts "CEO."

Nicholas Clark

Nicholas Clark is the former CEO and Executive Director of Alenton International. He is also co-founder and Managing Partner at Vinticus Capital.

Nelson W. Cunningham

Nelson Cunningham is President of McLarty Associates, the international strategic advisory firm headed by former White House Chief of Staff and Special Envoy for the Americas Thomas F. "Mack" McLarty, III.

Admiral William Fallon, USN (Ret.)

Admiral Fallon has led U.S. and Allied forces and played a leadership role in military and diplomatic matters at the highest levels of the U.S. government.

Scott Gilbert

Scott Gilbert is a Partner of Gilbert LLP and Managing Director of Resco LLC.

Vice Admiral Lee Gunn, USN (Ret.)

Vice Admiral Gunn is Vice Chairman of the CNA Military Advisory Board, Former Inspector General of the Department of the Navy, and Former President of the Institute of Public Research at the CNA Corporation.

The Honorable Chuck Hagel

Chuck Hagel served as the 24th U.S. Secretary of Defense and served two terms in the United States Senate (1997-2009). Hagel was a senior member of the Senate Foreign Relations, Banking, Housing and Urban Affairs and Intelligence Committees.

Lieutenant General Claudia Kennedy, USA (Ret.)

Lieutenant General Kennedy was the first woman to achieve the rank of three-star general in the United States Army.

The Honorable John F. Kerry

John Kerry is a distinguished fellow for global affairs at Yale University. In 2013, Kerry was sworn in as the 68th secretary of state of the United States. Kerry served for more than twenty-five years as a U.S. senator from Massachusetts.

General Lester L. Lyles, USAF (Ret.)

General Lyles retired from the United States Air Force after a distinguished 35 year career. He is presently Chairman of USAA, a member of the Defense Science Board, and a member of the President's Intelligence Advisory Board.

Dennis Mehiel

Dennis Mehiel is the Principal Shareholder and Chairman of U.S. Corrugated, Inc..

Stuart Pilich

Stuart Pilich is the Co-Founder and Managing Director of Cambridge Advisory Group, an actuarial and benefits consulting firm based in Philadelphia.

Ed Reilly

Edward Reilly is Global Chief Executive Officer of the Strategic Communications practice of FTI Consulting.

LtGen Norman Seip, USAF (Ret)

Lieutenant General Norman R. Seip, USAF (Ret) served in the Air Force for 35 years. His last assignment was Commander of 12th Air Force.

David Wade

David Wade is a consultant helping global corporations and organizations with strategic advice, public affairs and thought leadership, crisis communications, political intelligence gathering, and federal and legislative strategy.

U.S. Russia-Relationship

In this Report:

Acknowledging shortcomings in its performance during the 2008 Russo-Georgian War, Russia has concentrated on ways to improve its capabilities. Russia's military modernization after the conflict effort has prioritized areas where Russia can attain an asymmetric advantage over potential foes, including electronic warfare.

Russia's electronic warfare capabilities are already being used to degrade the performance of American forces in Syria. America's focus on counterterrorism operations has allowed American capabilities in the field of electronic warfare to atrophy. In the face the increased threat posed by Russia, the United States must focus on improving its electronic warfare capabilities.

Interact:

Join our discussion on Twitter with the hashtag #ASPRussia
Discuss electronic warfare with the author on Twitter at @PatrickJMSmith
Learn more about ASP at @amsecproject

IN BRIEF

- Following failures of Russian electronic warfare efforts during the 2008 Russo-Georgian War, Russia has concentrated on sharpening its capabilities in the electromagnetic spectrum. Today, many observers and defense officials stated Russia's ability to engage in electronic warfare is superior to that of the United States.
- After the Cold War, the United States military largely discontinued its electronic warfare programs. In recent years the United States has been involved in conflicts where its mastery of the electromagnetic spectrum is largely uncontested.
- The conflicts in Ukraine and Syria have demonstrated the importance of electronic warfare in Russian military operations. During these conflicts, American supplied equipment and U.S. forces are being challenged on the electromagnetic spectrum by Russia.
- In response to the challenge posed by Russian forces, the United States has begun to pursue its own efforts to enhance its electronic warfare capabilities. Both the Department of Defense and Congress have identified electronic warfare as an area where America needs to improve.
- Enhancing America's electronic warfare capabilities will be a long-term project that will require more than just increased enthusiasm. Making progress in the field will require a concerted and deliberate effort.

About the Authors

Patrick Smith is a Master's Student at the Josef Korbel School of International Studies. He studied European History during his undergraduate education at Trinity University. He is interested in Russia and its relationship to the United States.

What is Electronic Warfare?

Electronic Warfare (EW) has been described as the "art of the invisible," since it utilizes the invisible parts of the electromagnetic spectrum that are used to send signals that are detected by machines.[1] EW has several roles. EW consists of protective measures designed to maintain access to the spectrum, offensive measures that degrade or deny an adversary's access to the spectrum, and supportive measures that identify and store emissions to protect access to the spectrum or develop plans to deny access to the enemy.[2] The reliance on the electromagnetic spectrum by modern militaries to communicate, provide situational awareness, disrupt, and coordinate means that access to it is critical to the operation of modernized militaries.

A Changing World

The evolution of Russian EW is especially important as the United States turns to deal with new threats. For nearly twenty years, the U.S. military has been largely involved in conflicts against terrorists and non-state groups. However, this focus on countering violent extremism is beginning to change. The Summary of the 2018 National Defense Strategy declared that, "[i]nter-state strategic competition, not terrorism, is now the primary concern in U.S. national security."[3] The 2017 National Security Strategy (NSS) signaled this change of focus when it stated, "after being dismissed as a phenomenon of an earlier century, great power competition has returned."[4] In particular, the NSS acknowledged Russia is seeking to regain its great power status.[5] These statements reflect a fundamental shift in the strategic priorities of the United States.

The shift to an emphasis on great power competition will require substantive changes in how the U.S. military operates. In the most recent conflicts, the United States has found itself largely fighting groups of non-state actors. These groups generally lack the resources, technology, and personnel available to the types of large states involved in great power competition. The United States has become accustomed to conflicts in which its superiority in these areas was assured. However, in the event of great power conflict these advantages can no longer be assumed.

The NSS is not alone in drawing attention to Russia. In 2016 Major General Walter Piatt, the Army's Rapid Capabilities Office (RCO) operations director at the time, identified Russia as a more pressing threat than China because of its aggressive behavior.[6] In its preparations to compete as a global power, Russia has developed several niche capabilities to provide it with an asymmetric edge.[7] According to a 2019 RAND report, air defense, electronic warfare, and indirect fire capabilities are areas where Russia's military has emphasized quality and quantity.[8]

A Brief History of Russian EW

According to Russia, it has engaged in EW for more than a century. The Russian term, radioelektronnaya borba (literally translated as "radio-electronic combat [or struggle]," reflects the period during which the phrase originated in the beginning of the 20th century.[9] Russia's modern EW forces trace their roots back to the Russo-Japanese War. The "Day of Radioelectronic Warfare" is held on April 15th, the date Russia first used EW in 1904 to disrupt communications of the Japanese Navy forces coordinating the shelling of Russian targets.[10] Russia's early adoption of electronic warfare was followed by continued interest in developing the military's capability to use the electromagnetic spectrum.

Over the course of the century, EW became an increasingly integral part of the military. In 1956, the Soviet Union activated its first communications and radar jamming battalions in branches throughout the Armed Forces, and in the 1970s Soviet EW became a force used to suppress enemy assets and systems.[11] EW continued to occupy Russian military thinkers even after the fall of the Soviet Union. The use of EW by the U.S. military during the First Gulf War helped heighten Russian interest in the field. Indeed, during the 1990s, American EW usage during the conflict became a "recurring theme" in studies by Russian General Staff officers.[12]

However, despite this interest, Russia's EW capability and effectiveness were found wanting when tested in combat. When Russia's EW was used during the 2008 Russo-Georgian War, its capabilities were limited.[13] In the conflict, Russia's electronic warfare was not sufficiently effective to suppress Georgian air defenses, cover advancing forces, and create jamming zones.[14] These failures were a wakeup call for Russia, making it aware of the shortcomings within its forces and how they were employed. Following the war, Moscow pursued an ambitious campaign to reform and modernize its forces. It committed to a target of 70% new or modern content within its military inventory.[15]

Rumors of Russian Capabilities

Much has been made of Russian electronic warfare (EW) capabilities. For instance, in 2014 a Russian SU-24 aircraft made repeated passes near the USS Donald Cook.[16] According to Russian media, during this encounter with American forces the pilot of the Su-24 demonstrated the prowess of Russian EW. Russian reporting claimed that once spotted, the pilot "switched on the equipment, and powerful radio-electronic waves deactivated the whole ship's systems."[17] The reporting assigned fantastical abilities to Russian EW, which would allow it to prevail in a conflict without even shooting. The story, however, was nothing more than propaganda. Even the manufacturer of the equipment allegedly used has admitted it is a "nothing but a newspaper hoax."[18]

The *USS Donald Cook* was the alleged target of a Russian EW attack, but no evidence of electronic warfare against the ship is apparent. U.S. Navy photo.

While Russian claims about its EW capabilities in this instance were untrue, it doesn't mean the U.S. can write off the threat posed by Russian EW. On the contrary, there is plenty of credible evidence that the U.S. should take the threat quite seriously. Western experts acknowledge Russia has developed "killer capabilities" in the field of EW.[19] Recent events demonstrate that EW plays a critical role in how the Russian military operates. Russia has seriously invested in its EW capabilities, and its use of EW seems to indicate that much of this investment yielded practical advantages. Russian EW capability in Ukraine has been described as "eye-watering" by the former commander of U.S. Army Units in Europe.[20] Indeed, some note Russian EW weapons are superior to American ones in several respects.[21]

Why is Russia so Interested in EW?

One reason that Russia is so focused on EW is that it is a relatively cheap way of diminishing an adversary's capabilities. The United States has a very capable military, but through EW, Russia can counter some of the capabilities that make the U.S. military so effective. EW can target communications the U.S. uses to coordinate operations in multiple domains, or it can disrupt or degrade the navigation systems used by U.S. forces to locate themselves and identify targets for precision guided munitions (PGMs). In addition to making it harder to fire on them, EW could also allow Russian forces to identify targets for its rocket artillery batteries. This is an important capability as Michael Kofman, a research scientist at CNA, has noted, "The Russian military is incredibly good at killing things if it can find them, but it always historically struggles at seeing on the battlefield"[22]

Russia views its array of EW systems as "force enablers and multipliers."[23] In a struggle against a highly advanced foe like NATO, EW could help to level the playing field. Indeed, Russia's interest in boosting its capabilities originated in an effort to asymmetrically challenge the more vulnerable member states on the alliance's periphery and maximize the chances of success in an operation against eastern NATO members before the alliance could organize a coordinated response.[24] Based on its recent experiences, Russia believes EW assets could double land forces' combat potential, diminish the air force's losses by six-times and naval losses by three-times.[25] If these estimates are correct, EW could act as a potent asymmetric tool.

EW also appeals to the Russian military because it believes it has applications not only for air defense, but also psychological operations and cyber warfare.[26] The Russian military perceives war today as becoming increasingly driven by the information modern militaries require to operate. The adage holds that armies march on their stomachs, but, today, modern militaries rely just as much on data feeds. In this environment, Russia thinks EW can play an integral role in a holistic approach to warfighting. EW can also play a role in Russian anti-access/area denial efforts (A2/AD), where EW can be used as a "stand-off weapon" that "can turn areas falling within [its] range into strategically and operationally isolated 'bubbles.'"[27] In these roles, EW can become a significant tool. Strategically, the deterrent value of EW could convince foes to not engage in combat against Russia due to the prospect of a degraded communication environment or other complications.

Modernization Efforts

EW has occupied an important position within the broader modernization of Russia's military. Laurie Moe Buckhout, a retired Army colonel with a specialization in electronic warfare, observed that Russia has "redone and reengineered [its] entire EW fleet in the last 20 years," and poured millions into upgrading its EW capabilities after the conflict with Georgia.[28] Through this investment, Russia aimed to create "a total package" of EW capabilities able to cover a broad frequency range.[29] During this process, more than a dozen systems were tested and evaluated.[30] Now, Russia has deployed a diverse array of EW systems including the Krasukha, Leer-3, Moskva, and Murmansk-BN.[31]

The Krasukha system is one of the EW platforms Russia has developed. Photo source: Russian Ministry of Defense.

Russia's development of its EW capabilities hasn't been confined to research and procurement. There were sweeping changes in how this equipment was produced, integrated within the Russian military, and how EW specialists are trained. In 2009, production of the equipment was changed when a loose collection of domestic companies involved in the manufacturing of EW systems were integrated into the holding company known as Concern Radio-Electronic Technologies (Kontsern Radioelektronnye Tekhnologii—KRET).[32] In terms of force structure, Russian EW has a more organic presence within the military. For instance, Russian EW battalions have been added to combined-arms brigades.[33] In addition to changing production and force structure, emphasis was also placed on training personnel to engage in EW. Efforts to transform EW educational and training systems are expected to include simulators, Magniy-REB training complexes, and an Integrated Training and Learning System.[34]

Russian EW on Display: Ukraine and Syria

Ukraine has provided a proving ground for the EW capabilities Russia developed. An International Centre for Defence and Security report on Russian EW lists ten different Russian EW systems deployed in Donbas, such as the RB-341V Leer-3, RB-301B Borisoglebsk-2, R-330zh Zhitel, Torn, and R-318T Taran.[35] These systems have been put to use in both kinetic and non-kinetic operations.[36] Russia has employed its EW assets in a myriad of ways. For instance, Russia has been applying EW to psychological warfare by identifying Ukrainian soldiers and sending text messages saying things like "Leave and you will live."[37] While the effectiveness of this tactic is unclear, it demonstrates that Russia is using EW to do more than just jam the enemy.

The Leer-3 is one of the Russian EW systems that has been deployed in Syria. Photo credit: Vitaly V. Kuzmin. CC License Attribution-Share Alike 4.0

Russian EW has also been used to support kinetic operations in Ukraine. Using its EW capabilities, Russia has managed to disrupt the Ukrainian military's communications equipment. This has led Ukrainian soldiers to rely on their cellphones to communicate. While Russia uses EW to jam some communication, it also used EW tools to intercept enemy communications and triangulate Ukrainian forces to target them with rocket artillery.[38] Russian EW efforts also managed to turn some technology used by the Ukrainians against them. Due to jamming and hacking, Ukrainian forces found U.S. supplied Raven RQ-11B drones more of a liability than an asset. An advisor to the Ukrainian military noted the drones were no longer in use on the front lines because, among other things, they allowed the enemy to see Ukrainian military positions.[39]

Syria has also been a showcase of Russian EW capabilities. For instance, a drone swarm attack provided an example of how Russia can use its EW assets to effectively deal with the threat posed by the militarization of small drones. In January of 2018, a swarm of 13 drones carrying explosive fragmentation munitions was directed at Russian forces, and Russia's Ministry of Defense claimed EW systems forced at least six of these drones to land at certain locations.[40] The ability of Russia to neutralize these drones shows how effective Russian GPS spoofing attacks can be. There are indications GPS spoofing is being used more broadly in the country. Russian EW equipment, which can send out false GPS signals 500 times stronger than genuine ones, also appears to be disrupting the GPS of civilian flights in Israel.[41]

Russian supplied EW tech in Ukraine turned the Raven RQ-11B into a liability. U.S. Army photo.

Since both the United States and Russia have been active in Syria, the country has also provided the opportunity to see the relative strength of Russia's EW. The Syrian conflict zone has been described as "the most aggressive EW environment on the planet" by Gen. Raymond Thomas, the former commander of United States Special Operations Command.[42] Operating in close proximity to the Russians, American forces found themselves continually tested in the electromagnetic spectrum. Gen. Thomas noted that everyday Russia is "knocking our communications down."[43] So far, events indicate Russian EW is somewhat effective against the U.S. military. Russia has successfully jammed some U.S. drones, even some with encrypted signals and anti-jamming receivers.[44]

The Atrophy of U.S. EW Capabilities

Unlike Russia, until recently the United States allowed its EW capabilities to atrophy in the wake of the Cold War. After the Cold War, much of the U.S. military's EW forces were disbanded.[45] Since then, the United States largely hasn't had to operate in a demanding EW environment. The role of EW in the wars in Afghanistan and Iraq has been limited. The use of EW has also been largely defensive. The majority of U.S. EW activity in these conflicts has been directed at interfering with IEDs to protect American troops. The U.S. didn't engage in offensive EW until recently. Efforts to shut down enemy radios to prevent communication only began later in the conflicts.[46] A notable exception has been in conflicts with state level actors. For instance, in the 2011 military intervention in Libya EW played a crucial role in jamming Libyan air defense radar to give "free rein" to NATO fighters and bombers.[47]

EA-18G Growler aircraft played a key electronic warfare role in the Libya war. U.S. Navy photo.

Since the involvement of EW in the conflicts in Afghanistan and Iraq was limited, there didn't seem to be much need to further develop American capabilities in the spectrum. This changed, however, when the United States began to see what Russia was doing in EW. After witnessing the effectiveness of Russian EW in Ukraine and Syria and its integral role within Russian forces, U.S. officials became alarmed at the surge in Russia's capabilities. Recognition of the EW capabilities of near-peer adversaries like Russia sparked a critical examination of America's own. James Faist, Director of Defense Research and Engineering for Advanced Capabilities at the Department of Defense, acknowledged that "we've just lost so much capability."[48] A more dire assessment by Alan Shaffer, now Deputy Under Secretary of Defense Acquisition & Sustainment, stated the U.S. had "lost the electromagnetic spectrum."[49]

Charting a New Path Forward

The prospect of conflict in the electromagnetic spectrum with a near-peer adversary like Russia requires some change in the way the U.S. military operates. Now that we are aware of the potential gulf between Russian and American capabilities, we can work to address the issue. Unfortunately, working to regain dominance in the spectrum may require substantial effort. William Conley, former Director of EW, remarked that we have found ourselves in this situation due to "25 years of inattention," and that we "will get out of it with 25 years of attention."[50] That seems like a long time, but rebuilding U.S. EW is an endeavor that will require serious effort and attention. Despite trying to move quickly to address EW disparities, a report found that at the current pace the DoD will need at least a decade to address the gap between American capabilities and those of Russia and China.[51]

Since the United States is embarking on an undertaking that may last a decade, it is important not let the urgency overtake efforts to deliberately move toward the goal of achieving parity or dominance. Thankfully, the idea of advancing American EW capabilities has been met with "a groundswell of enthusiasm."[52] But, in a decades-long process, achieving the desired outcome will take more than enthusiasm. While the DoD increased funding for EW in fiscal year 2017, one report forecasts funding of the sector will stagnate in budgets after fiscal year 2020.[53] In order to properly address the issue the U.S. needs to clearly understand where it wants to be, and needs a sustained effort to get there.

Deciding what forms EW should take and how it will be used plays a major role in shaping an American effort to advance in the field. America's adversaries believe EW "is an important part of their offensive and defensive arsenal," while the U.S. has tended to treat it "as a combat enabler."[54] The United States needs to decide whether it is going to adopt its adversaries' perspective of EW, which focuses on it as an offensive and defensive tool, in order to know where it is trying to go with EW. The United States needs doctrine and strategy to inform its modernization efforts. It is important to acknowledge mainstays of American thinking, such as attaining air or naval superiority depend on the electromagnetic spectrum (EMS). Rep. Don Bacon, an advocate of EW, has said that "EMS is a physical domain that we have to have superiority [in] just like we do with air, sea, ground and space and cyber."[55] That seems like a good objective the United States can use to direct its efforts.

It seems like the various parts of the DoD are working toward achieving a consensus along those lines. While bureaucratic issues may preclude the DoD from acknowledging the electromagnetic spectrum as an independent domain, leaders have made clear leveraging the spectrum "is a priority for every department and every platform."[56] Individual branches of the military seem to be on the same page there. Unfortunately, the statements about the prioritization of the EMS do not always seem to indicate leaders are pursuing the spectrum's full potential. Although Laurence Mixon, of the Army's Program Executive Office for Intelligence, Electronic Warfare and Sensors, indicated the EMS operations would range "from strategic down to tactical," his statement emphasizes these operations would work to "enable all of our forces to communicate and maneuver effectively."[57] As the United States moves toward a consensus on the importance of the EMS, it must not pigeonhole EW into a role that is entirely supportive.

The U.S should not neglect the process between envisioning the type of EW capabilities to which it aspires and how these plans are to be actualized. While the United States should urgently work toward superiority in the EMS, it shouldn't let that force us to work haphazardly. Fortunately, in 2015 the Pentagon created a new high-level council to direct its EW programs.[58] This should help direct the shape of the growing EW programs and the spending on them.

However, things aren't working as well as one might hope. A report found that while spending increased, additional funding was not focused "on the most important new technologies and programs needed to gain an advantage in the EMS."[59] This indicates the United States hasn't been using its resources properly. In the FY20 budget request, the Army requested nearly $2.4 billion more than it had planned to spend during the period according to budget documents from spring 2018.[60] Proper planning should have prevented such an unexpected increase in requests from occurring.

Transforming America's Approach to EW

Getting American EW capabilities where they need to be will also require changes in how the DoD conducts R&D, how equipment is procured, how force structure is organized, and how U.S. military forces operate. Again, all these changes should have their roots in America's EW strategy. Therefore, it is important the United States continually work on this strategy and keep it up to date. In October, Congress asked the Pentagon to update its EW strategy, which at that point was two years old.[61] Considering the expense and effort that are involved in modernizing the United States' EW arsenal, the DoD should be updating its strategy on its own instead of responding to requests from Congress. The expense and scope of change involved in modernizing the DoD's EW requires the help of Congress, and it should be working more proactively to maintain that body's support.

In terms of research, development, and acquisition, the U.S. seems to be moving in the right direction. The neglect of EW means that developing and procuring EW systems is a priority. It's tempting to try to answer the problem using massive and long-term investments in a limited number of systems. So far, however, there has been some resistance to this typical approach. Instead, there has been a push for a more flexible approach. The defense industry has been advised to prepare for rapid-prototyping that would allow for progress.[62] Alan Shaffer, deputy undersecretary of defense for acquisition and sustainment, spoke of resisting a "one-size-fits-everything" approach and getting away from "linear large scale" acquisitions.[63] The U.S. should strive to follow this course of development so it can develop a variety of assets capable of addressing several different situations and reacting to further developments in Russian EW.

The U.S. needs to follow the Russian example and more deeply integrate its EW forces across the different branches. Fortunately, this is also an area where the U.S. has made significant progress. Recent efforts to grow American EW forces in the Army brought the number of troops assigned to the spectrum from 813 in 2015 to 940 in 2018, a 15 percent increase.[64] While this increase in the number of EW troops is important, so is the way these troops are being deployed within the force structure. These EW troops are being integrated into the army at every echelon, from brigades to divisions and corps.[65] Similar developments can also be found in the other branches. Gen. James "Mike" Jones, Commander, Air Combat Command, described restructuring within the service as pursuing a "distributed electronic warfare strategy."[66]

Finally, U.S. forces will need to change how they operate in the field. The U.S. military can no longer to afford to operate the same way it did in Afghanistan and Iraq. American superiority in all domains can no longer be taken for granted. Russia's ability to challenge and disrupt operations in Syria has proven American forces will be required to operate on battlefields where superiority in all domains is contested. Our forces need to become sensitive to their footprints in the EMS. Russia's ability to use American-supplied drones against the very Ukrainian forces operating them demonstrates that we need to be wary of how some of our less defended assets can be used against us. The Ukrainian conflict has also shown that American troops need to be aware of the vulnerability created by something as simple as carrying their cellphones.[67]

To become accustomed to the additional challenges created by an environment where the EMS is contested, the U.S. military needs further training. Major training exercises should realistically portray how EW can be used against American forces. In our exercises, "[w]e've got to stop wishing it [our EW shortcomings] away" according to a Marine at US Strategic Command.[68] In order to deal with things like the potential failure of modern navigational devices during EW, sometimes training will need to restore a knowledge of more antiquated skills. Efforts to return to teaching skills like celestial navigation to Navy officers are valuable and need to be continued and expanded.[69]

Conclusion

The threat posed by Russian EW isn't as dire as it is portrayed by Russian propaganda, but the gap between Russian and American operations in the EMS needs to be taken seriously. In the wake of its conflict with Georgia, Russia engaged in a concerted effort to modernize its forces, especially in niche areas like EW. The success Russia enjoyed in the EMS recently has been the result of a determined campaign to advance capabilities in an area where they can be strategically valuable. Russia viewed EW as a "force enabler" and "force multiplier," and it used these concepts to advance EW in ways to asymmetrically challenge the U.S. and NATO. While American EW atrophied following the fall of the Soviet Union, this situation can be rectified. Russia's ability to turn from its failures in Georgia to its position of relative strength shows such an effort can succeed. The United States must articulate a clear vision of where it wants to go in terms of EW, and the efforts it is making to modernize its EW arsenal need to continue.

Endnotes

1. Atherton, Kelsey D. "What's the Frequency, Putin? 5 Questions about Russia's EW Capability." C4ISRNET. 4 June 2018. https://www.c4isrnet.com/electronic-warfare/2018/06/04/whats-the-frequency-putin-5-questions-about-russias-ew-capability/
2. Hoehn, John R. (2019). Defense Primer: Electronic Warfare (CRS Report No. IF11118). Retrieved from Congressional Research Service website: https://crsreports.congress.gov/product/pdf/IF/IF11118. p. 1.
3. Summary of the 2018 National Defense Strategy of The United States of America. p.1.
4. National Security Strategy of the United States of America. 2017. p. 27.
5. Ibid. p 25.
6. Freedberg, Sydney J. "Red Electrons: Army Rapid Capabilities Office Fights Russian GPS Jamming, Cyber, EW." Breaking Defense. 22 Nov. 2016. https://breakingdefense.com/2016/11/red-electrons-army-rapid-capabilities-office-fights-russian-gps-jamming-cyber-ew/
7. McDermott, Roger. "Russia's Evolving Electronic Warfare Capability: Unlocking Asymmetric Potential." Jamestown. 17 Apr. 2018. https://jamestown.org/program/russias-evolving-electronic-warfare-capability-unlocking-asymmetric-potential/?mc_cid=d53a936cf1&mc_eid=4b516b0c01
8. Crane, Keith; Olga Oliker; and Brian Nichiporuk. Trends in Russia's Armed Forces: An Overview of Budgets and Capabilities. RAND Corporation. 2019. https://www.rand.org/pubs/research_reports/RR2573.html p 65.
9. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf p. 4.
10. Dura, Maksymilian. "Electronic Warfare: Russian Response to the NATO's Advantage? [ANALYSIS]." Defence24.Com. 5 May 2017. https://www.defence24.com/electronic-warfare-russian-response-to-the-natos-advantage-analysis

11. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf p 9.
12. Ibid. p 9.
13. Creery, Madison. "The Russian Edge in Electronic Warfare." Georgetown Security Studies Review. 26 June 2019. https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/
14. McDermott, Roger. "Russia's Advances in Electronic Warfare Capability." Jamestown. 2 Oct. 2019. https://jamestown.org/program/russias-advances-in-electronic-warfare-capability/
15. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. p 13.
16. Garamone, Jim. "Russian Aircraft Flies Near U.S. Navy Ship in Black Sea." United States Department of Defense. 14 Apr. 2014. https://archive.defense.gov/news/newsarticle.aspx?id=122052
17. "Electronic Warfare: How to Neutralize the Enemy Without a Single Shot." Vesti.ru, Вести.Ru. 17 Apr. 2017. https://www.vesti.ru/doc.html?id=2878732&cid=4441
18. KRET. "Top 5 Russian Radio Electronic Warfare Systems." 26 Feb 2015. http://archive.is/NDE7r
19. Clark, Colin. "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria." Breaking Defense. 24 Apr. 2018. https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/
20. Gould, Joe. "Electronic Warfare: What US Army Can Learn From Ukraine." Defense News. 2 Aug. 2015. https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine/
21. Kube, Courtney. "Russia Has Figured out How to Jam U.S. Drones in Syria, Officials Say." NBCNews.com. 10 Apr. 2018. https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931
22. Freedberg, Sydney J. "Electronic Warfare Trumps Cyber For Deterring Russia." Breaking Defense, 1 Feb. 2018, https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/
23. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. p IV.
24. Ibid.
25. Dura, Maksymilian. "Electronic Warfare: Russian Response to the NATO's Advantage? [ANALYSIS]." Defence24.Com. 5 May 2017. https://www.defence24.com/electronic-warfare-russian-response-to-the-natos-advantage-analysis
26. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. p V.
27. Jankowski, Dominik P.; Cziperski, Makysmilian. "NATO's Strategic 'Six Pack' to Counter Russia's Anti-Access/Area Denial Capability." National Interest. 22 September 2016. https://nationalinterest.org/blog/the-buzz/natos-strategic-%E2%80%98six-pack%E2%80%99-counter-russias-anti-access-area-17798
28. Clark, Colin. "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria." Breaking Defense. 24 Apr. 2018. https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/
29. Ackerman, Robert K. "Russian Electronic Warfare Targets NATO Assets." SIGNAL Magazine. 1 Nov. 2017. https://www.afcea.org/content/russian-electronic-warfare-targets-nato-assets
30. Bendett, Samuel. "America Is Getting Outclassed by Russian Electronic Warfare." The National Interest. 19 Sept. 2017. https://nationalinterest.org/feature/america-getting-outclassed-by-russian-electronic-warfare-22380

31. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. p 7.

32. Ibid. p 7.

33. McDermott, Roger. "Moscow Deploys Latest Electronic Warfare Systems in Kaliningrad." RealClearDefense. 12 Dec. 2018. https://www.realcleardefense.com/articles/2018/12/12/moscow_deploys_latest_electronic_warfare_systems_in_kaliningrad_114022.html

34. McDermott, Robert N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. International Center for Defense and Security. 2017. https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf p 8.

35. Ibid. p 24.

36. Ibid. p IV.

37. "Sinister Text Messages Reveal High-Tech Front in Ukraine War." Voice of America. 11 May 2017. https://www.voanews.com/europe/sinister-text-messages-reveal-high-tech-front-ukraine-war

38. Freedberg, Sydney J. "Electronic Warfare Trumps Cyber For Deterring Russia." Breaking Defense. 1 Feb. 2018. https://breakingdefense.com/2018/02/electronic-warfare-trumps-cyber-for-deterring-russia/

39. Stewart, Phil. "Exclusive: U.S.-Supplied Drones Disappoint Ukraine at the Front Lines." Reuters. 21 Dec. 2016. https://www.reuters.com/article/us-usa-ukraine-drones-exclusive-idUSKBN14A26D

40. "Above Us Only Stars." C4ADS, 26 Mar. 2019, https://www.c4reports.org/aboveusonlystars. Pg. 48.

41. Egozi, Arie; Freedberg, Sydney J. "Why Would Russia Spoof Israeli GPS? F-35 & Iran." Breaking Defense. 28 June 2019. https://breakingdefense.com/2019/06/if-russia-is-spoofing-israeli-gps-then-why-iran-f-35/?fbclid=IwAR3UIVjaJT72jH7zQqqmit9KFeLS2ixDmZkrN6COARXTpP87OnrmTbm4smg

42. Clark, Colin. "Russia Widens EW War, 'Disabling' EC-130s OR AC-130s In Syria." Breaking Defense. 24 Apr. 2018. https://breakingdefense.com/2018/04/russia-widens-ew-war-disabling-ec-130s-in-syria/

43. Trevithick, Joseph. "American General Says 'Adversaries' Are Jamming AC-130 Gunships in Syria." The Drive. 25 April 2018. https://www.thedrive.com/the-war-zone/20404/american-general-says-adversaries-are-jamming-ac-130-gunships-in-syria

44. Kube, Courtney. "Russia Has Figured out How to Jam U.S. Drones in Syria, Officials Say." NBCNews.com. 10 Apr. 2018. https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931

45. Freedberg, Sydney J. "Red Electrons: Army Rapid Capabilities Office Fights Russian GPS Jamming, Cyber, EW." Breaking Defense. 22 Nov. 2016. https://breakingdefense.com/2016/11/red-electrons-army-rapid-capabilities-office-fights-russian-gps-jamming-cyber-ew/

46. Creery, Madison. "The Russian Edge in Electronic Warfare." Georgetown Security Studies Review. 26 June 2019. https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/

47. Hennigan, W.J. "U.S. is using electronic warfare to attack in waves" Los Angeles Times. 11 July 2011. https://www.latimes.com/archives/la-xpm-2011-jul-11-la-fi-electronic-warfare-20110711-story.html

48. Freedberg, Sydney J. "Pentagon Jumpstarts Hypersonic Targeting, Electronic Warfare, C2." Breaking Defense. 22 May 2019. https://breakingdefense.com/2019/05/pentagon-jumpstarts-hypersonic-targeting-electronic-warfare-c2/

49. Freedberg, Sydney J. "US Has Lost 'Dominance In Electromagnetic Spectrum': Shaffer." Breaking Defense. 3 Sept. 2014. https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/

50. Freedberg, Sydney J. "Electronic Warfare 'Growing'; Joint Airborne EW Study Underway." Breaking Defense. 23 June 2017. https://breakingdefense.com/2017/06/electronic-warfare-growing-joint-airborne-ew-study-underway/

51. Pomerleau, Mark. "How Far behind Is the Pentagon in Electronic Warfare?" C4ISRNET. 19 Nov. 2019. https://www.c4isrnet.com/electronic-warfare/2019/11/19/how-far-behind-is-the-pentagon-in-electronic-warfare/

52. Freedberg, Sydney J. "Pentagon Jumpstarts Hypersonic Targeting, Electronic Warfare, C2." Breaking Defense. 22 May 2019. https://breakingdefense.com/2019/05/pentagon-jumpstarts-hypersonic-targeting-electronic-warfare-c2/

53. Pomerleau, Mark. "How Far behind Is the Pentagon in Electronic Warfare?" C4ISRNET. 19 Nov. 2019. https://www.c4isrnet.com/electronic-warfare/2019/11/19/how-far-behind-is-the-pentagon-in-electronic-warfare/

54. Freedberg, Sydney J. "Work Elevates Electronic Warfare, Eye On Missile Defense." Breaking Defense. 17 Mar. 2015. https://breakingdefense.com/2015/03/raid-breaker-work-elevates-electronic-warfare-eye-on-missile-defense/

55. Pomerleau, Mark. "A Strategy for Electronic Warfare May Be More Important than Money." C4ISRNET. 1 Nov. 2019. https://www.c4isrnet.com/electronic-warfare/2019/11/01/a-strategy-for-electronic-warfare-may-be-more-important-than-money/

56. Strout, Nathan. "Should the Military Treat the Electromagnetic Spectrum as Its Own Domain?" C4ISRNET. 6 Nov. 2019. https://www.c4isrnet.com/electronic-warfare/2019/11/06/should-the-military-treat-the-electromagnetic-spectrum-as-its-own-domain/

57. Ibid.

58. Freedberg, Sydney J. "Work Elevates Electronic Warfare, Eye On Missile Defense." Breaking Defense. 17 Mar. 2015. https://breakingdefense.com/2015/03/raid-breaker-work-elevates-electronic-warfare-eye-on-missile-defense/

59. Clark, Bryan; McNamara, Whitney Morgan; Walton, Timothy A. "Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum." Center for Strategic and Budgetary Assessments. 20 November 2019. https://csbaonline.org/research/publications/winning-the-invisible-war-gaining-an-enduring-u.s-advantage-in-the-electromagnetic-spectrum

60. Gruss, Mike. "Congress Wants to Improve Electronic Warfare Capabilities." C4ISRNET. 15 Oct. 2019. https://www.c4isrnet.com/show-reporter/ausa/2019/10/15/congress-wants-to-improve-electronic-warfare-capabilities/

61. Ibid.

62. Keller, Jared. "After Experiencing Russian Jamming up Close in Syria, the Pentagon Is Scrambling to Catch Up." Business Insider. 3 June 2019. https://www.businessinsider.com/pentagon-focus-on-electronic-warfare-after-russian-jamming-in-syria-2019-6

63. Pomerleau, Mark. "Can Pentagon Acquisition Keep up with Electronic Warfare?" C4ISRNET. 28 Oct. 2019. https://www.c4isrnet.com/electronic-warfare/2019/10/28/can-pentagon-acquisition-keep-up-with-electronic-warfare/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB 10.29.19&utm_term=Editorial - Military - Early Bird Brief

64. Freedberg , Sydney J. "Army Boosts Electronic Warfare Numbers, Training, Role." Breaking Defense. 7 Aug. 2018. https://breakingdefense.com/2018/08/army-boosts-electronic-warfare-numbers-training-role/

65. Ibid.

66. Tirpak, John A. "Air Force Explains Electronic Warfare Restructure Following ECCT Review." Air Force Magazine. 16 Apr. 2019. https://www.airforcemag.com/air-force-explains-electronic-warfare-restructure-following-ecct-review/

67. Freedberg, Sydney J. "Turn Off That IPhone, Commandant Tells Marines." Breaking Defense. 9 Aug. 2016. https://breakingdefense.com/2016/08/turn-off-that-iphone-commandant-tells-marines/

68. Freedberg, Sydney J. "US Forces Untrained, Unready For Russian, Chinese Jamming." Breaking Defense. 30 Oct. 2019. https://breakingdefense.com/2019/10/us-forces-untrained-not-ready-for-russian-jamming/

69. Brumfiel, Geoff. "U.S. Navy Brings Back Navigation By The Stars For Officers." NPR. 22 Feb. 2016. https://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers

The American Security Project (ASP) is a nonpartisan organization created to educate the American public and the world about the changing nature of national security in the 21st Century.

Gone are the days when a nation's security could be measured by bombers and battleships. Security in this new era requires harnessing all of America's strengths: the force of our diplomacy; the might of our military; the vigor and competitiveness of our economy; and the power of our ideals.

We believe that America must lead in the pursuit of our common goals and shared security. We must confront international challenges with our partners and with all the tools at our disposal and address emerging problems before they become security crises. And to do this we must forge a bipartisan consensus here at home.

ASP brings together prominent American business leaders, former members of Congress, retired military flag officers, and prominent former government officials. ASP conducts research on a broad range of issues and engages and empowers the American public by taking its findings directly to them via events, traditional & new media, meetings, and publications.

We live in a time when the threats to our security are as complex and diverse as terrorism, nuclear proliferation, climate change, energy challenges, and our economic wellbeing. Partisan bickering and age old solutions simply won't solve our problems. America – and the world - needs an honest dialogue about security that is as robust as it is realistic.

ASP exists to promote that dialogue, to forge that consensus, and to spur constructive action so that America meets the challenges to its security while seizing the opportunities that abound.

ASP

American Security Project

www.americansecurityproject.org