G.E.O.



A2/AD Bubble in Russia

A2/AD nella Strategia Russa, Kaliningrad Bubble, Sistemi Missilistici Impiegati, Electronic Warfare

Redatto da:

Saverio Lesti - Senior Researcher Area Difesa & Sicurezza

Mondo Internazionale
Associazione culturale
Gallarate, Via Marco Polo 31
21013 - VA, Italia
C.F. 91071700123
P.IVA 03727710125

Mail: segreteria@mondointernazionale.com

INDICE

1 ORIGINE E DEFINIZIONE DEL TERMINE A2/AD

2 L'A2/AD NELLA STARTEGIA RUSSA

3 UN ESEMPIO DI A2/AD BUBBLE: KALININGRAD

4 SISTEMI MISSILISTICI DISPIEGATI A KALININGRAD

5 UN MOLTIPLICATORE DI FORZA IN CHIAVE A2/AD: L'ELECTRONIC WARFARE

6 CONCLUSIONI



ABSTRACT

Il concetto di Anti-Access/Area-Denial è diventato famoso nell'ultimo decennio in relazione alla categorizzazione da parte occidentale delle strategie che paesi come Russia e Cina hanno implementato in caso di scontro con gli Stati Uniti ed i loro alleati. La formulazione del termine e del relativo acronimo A2/AD è frutto della riflessione sulle sfide anche asimmetriche che le forze armate statunitensi avrebbero dovuto affrontare negli anni 2000.

È questo il caso della Russia che, dall'avvio del programma di riforma del suo strumento militare nel 2008, ha investito notevoli risorse nella creazione di capacità legate all'Anti-Access Warfare. Sebbene il termine A2/AD sia un costrutto del pensiero militare occidentale, è stato adattato alle esigenze della strategia russa dando vita ad una strategia che combina aspetti legati a misure militari di tipo offensivo e difensivo.

Tale approccio, basato sull'integrazione di diversi sistemi d'arma, è stato creato per difendere specifici obiettivi strategici, tra cui l'oblast di Kaliningrad dove ha sede la flotta russa del Baltico e la cui posizione geografica ha conseguenze dirette sulle operazioni statunitensi e NATO in caso di conflitto nella regione baltica.

Questo schieramento militare si compone di sistemi missilistici con capacità di deep strike, sistemi di difesa antiaerei integrati e capacità di condurre operazioni di guerra elettronica distruttive nei confronti dei sistemi d'arma e di comando e controllo dell'avversario. Tali dispositivi militari pongono una seria minaccia alle operazioni militari avversarie, in quanto si tratta di ostacoli non insormontabili ma con costi e tempi incerti in relazione al raggiungimento di questo obiettivo.

1. ORIGINE E DEFINIZIONE DEL TERMINE A2/AD

La *Anti-Access Warfare* è quella strategia, usata nel corso della storia, che cerca di opporsi o impedire il movimento delle forze avversarie. L'adozione di una simile strategia di difesa indica che l'aspetto primario del potenziale conflitto è il coinvolgimento di un avversario con maggiore potere militare, politico, diplomatico o economico. Per tale motivo, gli elementi principali della antiaccess warfare sono i seguenti[1]:

- La percezione della superiorità strategica di un avversario;
- Il primato della geografia, come l'elemento che più influenza il fattore tempo e facilita l'attrito in combattimento delle forze avversarie;
- La predominanza generale del dominio marittimo come spazio di conflitto;
- La criticità delle informazioni e dell'intelligence;
- L'impatto determinante di eventi estrinseci, a volte apparentemente non correlati, in altre regioni o a livello globale.

Nell'attuale dottrina militare statunitense, tale strategia si riferisce all'approccio che i potenziali avversari intendono attuare per negare o, almeno limitare, l'influenza degli Stati Uniti e la sua capacità di proiezione della potenza militare. Il dibattito sulla antiaccess warfare è stato dominato dall'acronimo *A2/AD*, che sta per *Anti-Access/Area-Denial*. Tuttavia, sin dalla sua origine, il termine è stato usato più come aggettivo per descrivere i tipi di sistemi d'arma e reti difensive usati in una campagna antiaccess, piuttosto che per riferirsi alla strategia sottostante. La creazione del termine A2/AD va ricercata nel documento "*Meeting the Anti-Access and Area-Denial Challenge*", redatto dal think tank Center for Strategic and Budgetary Assessments (CSBA) nel 2003.

[1] Sam J. Tangredi, "Antiaccess Warfare as Strategy", Naval War College Review, Volume 71, Number 1 Winter 2018, Article 4, pag. 4.

Il documento prende atto che esistono due tendenze da tenere in considerazione per lo sviluppo futuro delle forze armate statunitensi[2]; l'utilizzo da parte degli avversari di strategie e/o l'attuazione di minacce molto diverse da quelle affrontate in precedenza; la diffusione delle tecnologie militari e la rapida progressione delle tecnologie derivate dal settore della difesa. Particolare attenzione viene richiamata sulla crescente proliferazione ed accessibilità a servizi satellitari nazionali e commerciali ed alla tecnologia missilistica, quali strumenti per ostacolare la capacità di dispiegamento delle forze militari statunitensi. Secondo l'analisi, a tali tendenze si aggiungono i cambiamenti intervenuti nei seguenti contesti[3]:

- **Operational Realities**. Dalla conclusione della Guerra Fredda, il numero di forze statunitensi con sede all'estero è diminuito. Gli Stati Uniti basano le loro operazioni sulla capacità di proiettare le forze militari in teatri e su distanze intercontinentali;
- **Political Realities**. Il crollo dell'URRS ha spostato l'attenzione degli Stati Uniti verso lo svolgimento di operazioni militari a livello globale, mentre gli alleati si sono concentrati sulla partecipazione a missioni con un ampio mandato internazionale. Di conseguenza, non può essere dato per scontato il sostegno politico e militare degli alleati;
- **Geographic Realities**. Le forze armate statunitensi devono tenere conto che non saranno sempre disponibili strutture di supporto adeguate. A peggiorare le cose, molte potenziali aree di crisi sono contraddistinte dalla presenza di *choke point* che potrebbero rendere difficili le operazioni marittime.

In aggiunta a quanto appena riportato, anche l'evoluzione delle minacce militari aumenterà i limiti di cui dovrebbe tenere conto la capacità di proiezione degli Stati Uniti. I potenziali avversari stanno sviluppando o, sono già in possesso, di capacità militari che esporranno le forze statunitensi a rischi crescenti, quali l'utilizzo di missili con testate chimiche, biologiche, radiologiche, nucleari o ad esplosivo potenziato (CBRNE)[4].

[2] Andrew Krepinevich, Barry Watts & Robert Work, "Meeting the Anti-Access and Area-Denial Challenge", Center for Strategic and Budgetary Assessment, 2003, pag. 1.
[3] Ibid, pag. 1-3.
[4] Ibid, pag. 4.

Il generale Ronald Fogleman osservò nel 1996 che "Gli attacchi di saturazione con missili balistici contro le forze da sbarco, i porti, gli aeroporti, le strutture di stoccaggio e le aree di sosta potrebbero rendere estremamente costoso proiettare le forze statunitensi in un teatro conteso, tanto meno svolgere operazioni per sconfiggere un avversario ben armato. La semplice minaccia di tali attacchi missilistici nemici potrebbe dissuadere gli Stati Uniti e i partner della coalizione dal rispondere alla stessa aggressione"[5].

Se le strategie Anti-Access (A2) mirano a impedire alle forze nemiche di entrare in un teatro di operazioni, le operazioni di Area-Denial (AD) cercano invece di impedire la loro libertà di azione. Queste ultime includono un insieme di azioni in aria, terra e mare per contestare ed impedire operazioni militari all'interno del campo di battaglia[6]: una combinazione di operazioni aeree coordinate e difese contraeree integrate per mantenere un grado di parità aerea o superiorità locale; attacchi di artiglieria, razzi e missili a corto e medio raggio; campi minati; contaminazione di vaste aree con agenti CBRN; tattiche contro le operazioni speciali; l'uso di sottomarini; missili cruise e missili balistici antinave; campi minati in prossimità della costa; piccoli mezzi d'attacco. Gli Stati che stanno sviluppano strategie e strumenti di questo tipo potrebbero farlo in modo tale da rendere più problematico l'ingresso in un teatro di operazioni, negando alle forze statunitensi un'adeguata libertà di azione e degradare l'efficacia delle eventuali contromosse messe in atto. Citando i risultati di uno studio realizzato dal Defense Science Board (DSB), lo sviluppo di questo tipo di capacità A2/AD da parte di una potenza regionale nel periodo 2010-2020 era da ritenersi un'ipotesi plausibile[7]. A tal fine, vengono delineate le capacità essenziali che un avversario dovrebbe sviluppare in questo campo [8]:

- Political Access Denial: stringere alleanze o minacciare di attaccare nazioni vicine con l'obiettivo di negare l'accesso agli Stati Uniti;
- Geographic Access Denial: schierare forze nell'entroterra per mettere sotto stress la portata e le capacità di targeting delle forze statunitensi;

[5] Andrew Krepinevich, Barry Watts &Robert Work, "Meeting the Anti-Access and Area-Denial Challenge", Center for Strategic and Budgetary Assessment, 2003, pag. 4.
[6] Ibid, pag5.
[7] Defence Science Board, "Task Force on Globalization and Security Final Report", December 1999, pag. vi.
[8] Andrew Krepinevich, Barry Watts &Robert Work, "Meeting the Anti-Access and Area-Denial Challenge", Center for Strategic and Budgetary Assessment, 2003, pag. 6-7.

- Hardening of Fixed Targets: rafforzamento degli impianti di produzione e stoccaggio di armi di WMD, centri di comando e strutture collegate alla leadership nazionale;
- Sanctuaries: creare delle zone sicure posizionando forze militari in aree civili o vicino a punti di interesse culturali e l'utilizzo di jamming contro il segnale GPS;
- Mobility and Dispersion; l'utilizzo di lanciatori mobili per missili balistici e da crociera e di sistemi avanzati di difesa aerea;
- Stealth: utilizzare sistemi difficili da rilevare, come sottomarini diesel-elettrici, missili da crociera a bassa osservabilità e mine antinave avanzate;
- Deception: ricorrere a tecniche di mascheramento, come unità d'attacco costiere mascherate da navi mercantili;
- Predisporre attacchi informatici contro le reti statunitensi, in particolare quelle che supportano il graduale afflusso delle forze militari in un teatro operativo;
- Mettere in atto azioni di guerra non convenzionale contro punti di trasbordo, imbarco e sbarco sia aerei che marittimi.

Inoltre, dovendo necessariamente operare al di fuori della bolla A2/AD, le forze statunitensi dovranno anche gestire le tempistiche più lunghe legate alle attività di ricognizione, sorveglianza e acquisizione dei bersagli (RSTA), rendendo difficile eliminare i bersagli critici avversari. L'analisi del CSBA delinea all'inizio degli anni duemila il contesto in cui lo strumento militare degli Stati Uniti avrebbe dovuto operare e che ne avrebbe condizionato lo sviluppo quale forza con capacità di proiezione a livello globale, nell'ottica di un confronto contro avversari in un conflitto asimmetrico *near peer*.

Il concetto di strategia A2/AD per limitare ed annullare la capacità di proiezione degli Stati Uniti, è stata successivamente ripresa e definita nei suoi aspetti militari con la realizzazione del *Joint Operational Access Concept* (JOAC). Realizzato nel 2012, il JOAC introduceva il concetto della Cross-Domain Sinergy come strumento per garantire la libertà di azione alle forze combinate statunitensi nell'affrontare potenziali avversari dotati di capacità Anti-Access/Area-Denial.

Il documento traccia una chiara distinzione tra capacità A2 e AD[9]: per Anti-Access s'intendono azioni e capacità a lungo raggio, progettate per impedire a una forza avversaria di entrare in un'area operativa; invece, l'Area-Denial si riferisce ad azioni e capacità a corto raggio, ideate per limitare la libertà d'azione di un avversario all'interno di un'area operativa. Un importante innovazione rispetto alla precedente analisi del CSBA è l'inserimento tra le capacità di A2 della conduzione di azioni nel dominio spaziale e nel cyberspazio[10]. Inoltre, molte capacità militari possono essere impiegate per entrambi gli scopi: "lo stesso sottomarino che esegue una missione di negazione d'area nelle acque costiere può svolgere una capacità antiaccess quando impiegato in un pattugliamento a lungo raggio"[11].

Altri limiti al movimento e proiezione alle forze militari derivano da fattori quali[12]: la distanza dall'obiettivo; la presenza di basi avanzate; l'utilizzo di adeguate strutture di supporto; dall'esistenza di partner in grado di garantire supporto militare o politico. A questo riguardo, anche il JOAC delinea dei trend, più o meno in linea con quelli del CSBA, la cui evoluzione influirà sulle capacità di proiezione e la libertà d'azione delle forze armate statunitensi[13]:

- **Il miglioramento e la proliferazione di armi e altre tecnologie in grado di negare l'accesso o la libertà di azione all'interno di un'area operativa**;
- **Il cambiamento della postura difensiva degli Stati Uniti all'estero**;
- **L'emergere dello spazio e del cyberspazio come domini sempre più importanti e contestati**.

Sulla base dell'evoluzione dei trend citati e del loro impatto sulle tecnologie militari collegate allo sviluppo di strategie A2/AD, il JOAC procede a delineare le capacità Anti-Access chiave[14]:

- Varie tipologie di missili balistici e da crociera lanciabili da terra, aria e mare in grado di colpire con precisione a distanze superiori a 1.000 miglia nautiche;

[9] Department of Defense, "Joint Operational Access Concept (JOAC)", Version 1.0, 17 January 2012, pag. 6.
[10] Ibid, pag. 6.
[11] Ibid, pag. 6.
[12] Ibid, pag. 6-7.
[13] Ibid, pag. 9.
[14] Ibid, pag. 9-10.

- Sistemi di ricognizione e sorveglianza a lungo raggio, inclusi satelliti, aerei e radar terrestri e navali che forniscano informazioni per il targeting;
- Armi antisatellite (ASAT) cinetiche e non cinetiche che possono disabilitare i sistemi spaziali vitali per la proiezione delle forze statunitensi;
- Forze sottomarine in grado di interdire le linee di comunicazione marittime statunitensi e alleate sia in acque sovrane che internazionali;
- Capacità per condurre attacchi cibernetici per interrompere i sistemi di comando e controllo (C2) e colpire le infrastrutture critiche civili e militari;
- Terroristi disposti ad attaccare basi statunitensi o alleate;
- Forze capaci di compiere azioni dirette e di guerra non convenzionale.

Allo stesso modo vengono identificate le capacità chiave relative alle operazioni di Area-Denial[15]:

- Forze aeree e sistemi di difesa aerea, sia fissi che mobili, progettati per negare la superiorità aerea;
- Missili antinave a corto raggio e sottomarini che impiegano siluri avanzati per negare la superiorità marittima;
- Razzi, artiglieria, missili e mortai[16] con guida di precisione (G-RAMM) progettati per attaccare obiettivi con una precisione e una letalità maggiore rispetto al passato;
- L'uso di armi chimiche e biologiche per negare l'accesso all'area di operazioni;
- Capacità cibernetiche e di guerra elettronica (EW) per degradare, neutralizzare o distruggere le capacità di comando e controllo nell'area operativa;
- L'uso esteso di mine terrestri e navali;
- Schierare piccole imbarcazioni armate o cariche di esplosivi;
- Forze di manovra terrestri;
- Forze speciali capaci di condurre azioni dirette e operazioni di guerra non convenzionale;
- Sistemi senza pilota, sia aerei che sottomarini, con compiti di raccolta informazioni e targeting (ISTAR).

[15] Department of Defense, "Joint Operational Access Concept (JOAC)", Version 1.0, 17 January 2012, pag. 10.
[16] Small Arms Survey, "Guided Mortar Systems", Number 51, April 2015.

Come ricordato in precedenza, alcune delle capacità militari indicate sono impiegabili alternativamente sia nella sfera Anti-Access che in quella dell'Area-Denial, quali missili cruise e balistici, attacchi cyber, forze speciali e battelli sottomarini. Di seguito, nella Figura 1, una rappresentazione grafica delle capacità A2/AD in un sistema di difesa integrato.

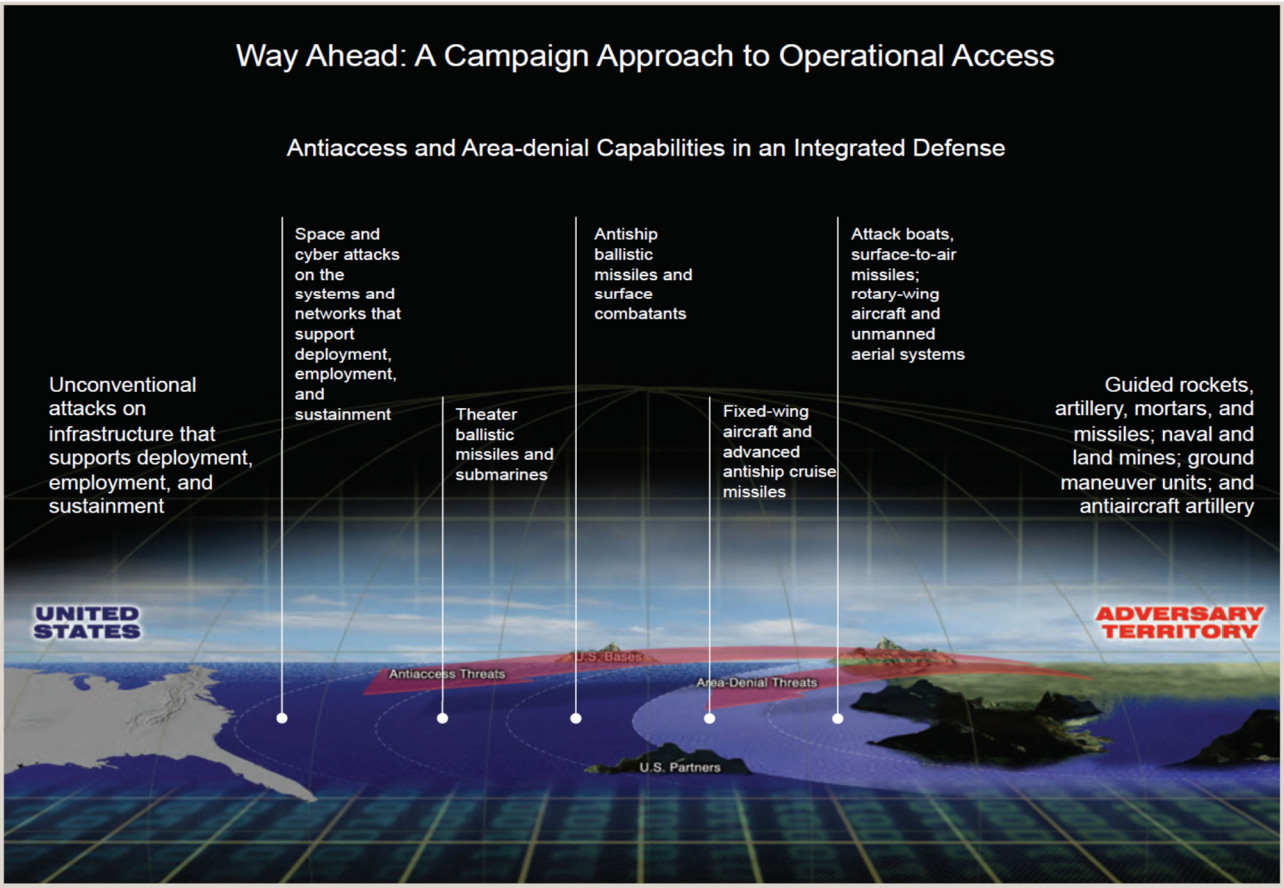


Figura 1, Antiaccess and Area-denial Capabilities in an Integrated Defense, Gregory Kreuder, "Lead Turning the Fight, The Joint Operational Access Concept and Joint Doctrine", National Defense University Press, Joint Force Quarterly 69, 2nd quarter 2013, pag. 104.

A seguito di questa dettagliata definizione del concetto di strategia Anti-Access/Area-Denial, viene messa in dubbio la capacità di condurre operazioni militari in un contesto operativo privo di ostacoli come nel periodo 1990-2010. Questo porterà gli Stati Uniti a confrontarsi con due tipi di scenari[17]: attori in grado di introdurre strategie A2/AD complesse ed integrate in più domini per tentare di negare del tutto l'accesso statunitense; attori con capacità meno solide e complete possono semplicemente tentare di infliggere perdite maggiori di quelle che gli Stati Uniti ritengono politicamente accettabili.

[17] Department of Defense, "Joint Operational Access Concept (JOAC)", Version 1.0, 17 January 2012, pag. 13.

Quanto illustrato permette di delineare il contesto dottrinale in cui è stato coniato il termine Anti-Aaccess/Area-Denial ed il relativo acronimo A2/AD, strettamente legato all'ambiente militare degli Stati Uniti. Con tale riflessione è stata definita la minaccia costituita dalle strategie di difesa integrata basate sul concetto di A2/AD, per contrastare e negare la capacità statunitense di condurre operazioni militari su larga scala ed a livello globale. Lo sviluppo di alcune tecnologie militari di punta e l'emergere di strumenti militari asimmetrici e non convenzionali hanno rafforzato le preoccupazioni in questo senso. L'aver osservato per anni come venivano condotte le operazioni militari statunitensi ha spinto i potenziali avversari a concentrarsi sullo sviluppo di dottrine operative e sistemi d'arma per colpire, in un confronto near peer ed in maniera asimmetrica, le capacità a sostegno della proiezione di potere globale degli Stati Uniti.

2. L'A2/AD NELLA STARTEGIA RUSSA

Secondo il Quadrennial Defense Review del 2014, "I conflitti futuri potrebbero variare tra scenari ibridi contro i gruppi di proxy che utilizzano mezzi asimmetrici, ad un conflitto ad alta intensità nei confronti di uno stato armato di WMD o capacità Anti-Access/Area-Denial tecnologicamente avanzate"[18].

Seguendo tale previsione, si dava per scontato che Stati con la capacità di utilizzare una combinazione di sensori e missili a lungo raggio per impedire agli avversari di operare in una zona di esclusione, o "bolla" adiacente al loro territorio, possiedano capacità A2/AD. A questo riguardo, molta attenzione è stata dedicata alle azioni della Cina nel Mar Cinese Meridionale e nello Stretto di Taiwan.

Tuttavia, in maniera graduale e silenziosa, anche la Russia ha sviluppato una propria capacità A2/AD, sfruttando soprattutto le entrate derivanti dalle vendite di materie prime energetiche sui mercati internazionali. La recente attività della Russia in questo settore ha attirato un'attenzione a causa della percezione dell'atteggiamento russo: imprevedibilità, irrazionalità e palese ostilità verso gli Stati Uniti[19].

[18] United States Department of Defense, "Quadrennial Defense Review 2014", March 2014, pag. VII.
[19] Keir Giles, Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, pag. 22.

Trattandosi di un termine coniato all'interno del sistema militare statunitense, l'Anti Access/Area Denial non esiste nel pensiero o nella dottrina militare russa, mentre è utilizzata per analizzate le capacità occidentali e per descrivere la percezione delle azioni militari occidentali. Come la guerra cibernetica e ibrida, l'A2/AD è un costrutto occidentale imposto al pensiero militare russo senza alcun valore intrinseco all'interno dell'analisi militare russa[20].

In tal senso, le capacità russe Anti-Access/Area-Denial sono da intendersi come parte di un più articolato sistema di strumenti. Il 2 marzo 2019, il capo di stato maggiore delle forze armate russe, Valery Gerasimov, in un discorso all'Accademia di Scienze Militari, ha presentato quella che ha definito una "strategia di difesa attiva", l'adattamento russo del concetto di A2/AD[21]. "La base della nostra risposta è la 'strategia di difesa attiva',...Dobbiamo agire rapidamente in modo da prevenire il nemico con le nostre misure preventive, identificare prontamente le sue vulnerabilità e creare minacce di danni inaccettabili. Ciò garantisce che l'iniziativa strategica venga acquisita e mantenuta "[22].

Per Gerasimov, cogliere e mantenere l'iniziativa strategica è diventato il fattore centrale. Il perseguimento di questa condizione comporta una serie di misure volte a scoraggiare strategicamente e neutralizzare preventivamente le minacce alla sicurezza nazionale russa. È importante sottolineare che l'azione preventiva è un elemento chiave e, inoltre, la dottrina russa prevede che le capacità di attacco di precisione vengano utilizzate per neutralizzare le risorse strategiche di un avversario, piuttosto che limitarsi esclusivamente all'interdizione strategica[23].

Il concetto parte dal presupposto che la fase iniziale della guerra sarà quella decisiva poiché i ritardi, l'attrito e la disorganizzazione impediranno alle forze armate avversarie di combattere una campagna basata sulla libertà di movimento verso ed all'interno di un teatro operativo. Un fallimento degli Stati Uniti nel raggiungere una rapida vittoria influenzerà in modo decisivo la volontà politica di proseguire il conflitto.

[20] Keir Giles Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, pag. 23.
[21] Valery Gerasimov, speech given at the Annual Meeting of the Academy of Military Science, Moscow, 2, MEMRI, 14 March 2019.
[22] Ibid, pag. 3.
[23] Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence", The RUSI Journal, 5 November 2020, pag. 72.

La linea di condotta è "ritardare, degradare, sopprimere o anticipare le azioni nemiche, al fine di distruggere la capacità dell'avversario di combattere come strumento integrato e, infine, vincere una guerra di logoramento"[24].

Per tale motivo, i pianificatori militari russi non si limitano a basare la difesa sulle sole capacità delle forze presenti sul campo ma, creando una rete di sistemi e capacità integrate per la difesa costiera, aerea e sottomarina e colmando eventuali lacune con l'uso estensivo di sistemi per la guerra elettronica[25]. La Russia ha recentemente implementato capacità A2/AD avanzate come; sistemi di difesa aerea a lungo raggio; sistemi di difesa costiera e ASW; sistemi missilistici mobili a medio raggio; nuove classi di sottomarini dotati di missili cruise; capacità di colpire il dominio spaziale ed il cyberspazio; sistemi per la EW[26].

L'ultimo programma di modernizzazione, attivo dal 2008, è riuscito in gran parte a rendere le forze armate russe più agili e aggiornate[27], mentre le principali innovazioni delle capacità A2/AD russe riguardano le seguenti sottocategorie[28]:

- Sistemi balistici avanzati e missili da crociera. Entrata in servizio del sistema missilistico tattico Iskander-M;
- Sistemi Difensivi Antinave. Lo schieramento, in combinazione o singolarmente, dei sistemi missilistici di difesa costiera K-300P Bastion-P e 3K60 Bal;
- Sistemi Difensivi Antiaerei. L'adozione dei sistemi S-300 nell'ultima variante S-300P- 300V e la versione imbarcata S-300 Fort. Ad essi si affianca il più moderno S-300PMU3 conosciuto come S-400 Triumf. Inoltre, i russi mantengono in servizio più di 30 reggimenti equipaggiati con vecchi sistemi S-300PS/PM;
- Sviluppo delle capacità EW. La Russia ha introdotto vari sistemi per le operazioni di guerra elettronica tra cui, per fare degli esempi: il complesso RB-341B Leer-3, l'RB-301B

[24] Michael Kofman, "IT'S TIME TO TALK ABOUT A2/AD: RETHINKING THE RUSSIAN MILITARY CHALLENGE", War on The Rocks, 5 Semptember 2019, pag. 5.
[25] Ibid, pag. 24.
[26] Aziz Erdogan, "Russian A2AD Strategy and Its Implications for NATO", Beyond the Horizon, 6 December 2018, pag. 11.
[27] Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence", The RUSI Journal, 5November 2020, pag. 70.
[28] Sergey Sukhankin, "David vs. Goliath: Kaliningrad Oblast as Russia's A2/AD 'Bubble'", Scandinavian Journal of Military Studies, 21 August 2019, pag. 101- 103.

Borisoglebsk-2, l'R-381T Taran, il sistema 1RL257 Krasucha-4;

- **Ripristino e Ampliamento del Potenziale Navale**. L'attuale strategia navale russa prevede di rafforzare flotta con navi di superficie più piccole come fregate e corvette[29] e sottomarini Project 636-M e636.3 Varshavyanka (nome in codice NATO: Improved Kilo), tutti con capacità di lancio del nuovo missile cruise 3M-14 Kalibr.

Con il Programma di Armamento Statale SAP-2027[30], la Russia continuerà ad investire nella produzione e schieramento di queste tipologie di equipaggiamenti militari in chiave Anti-Access/Area-Denial.

In Occidente un sistema così completo è definito Sistema Integrato di Difesa Aerea (IADS) o Sistema Integrato di Difesa Aerea e Missilistica (IAMD)[31]. La sovrapposizione di varie tipologie di sistemi missilistici con compiti diversi mostra la continuità con l'eredità sovietica dei "cerchi concentrici" per proteggere il proprio territorio e per condurre operazioni in ambienti marittimi contestati, creando al contempo la moderna capacità A2/AD della Russia.[32]Anche lo sviluppo delle forze sottomarine e dei sistemi di difesa costiera è una continuazione della strategia del 'bastione marittimo'[33] della Guerra Fredda, ovvero la creazione di siti marini fortemente difesi nelle aree costiere del paese per proteggere la flotta di sottomarini strategici.

L'obiettivo perseguito dai russi è quello di impedire lo svolgersi di una classica campagna militare statunitense basata sulla libertà di proiezione e movimento verso ed all'interno di una zona operativa. A tale riguardo, negli ultimi anni si è assistito alla creazione di bolle A2/AD nei fianchi orientale e meridionale della NATO. È fondamentale notare che in uno scenario in cui la Russia utilizza un approccio Anti-Access/Area-Denial, le forze occidentali dovrebbero essere disposte ad esporsi ad un alto livello di attrito per saturare sistemi difensivi russi[34].

[29] Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence", The RUSI Journal, 5 November 2020, pag. 76.
[30] Dan McCormick, "Allied A2AD in the Black Sea", Middle East Institute, 19 January 2021.
[31] Robert Dalsjö, Christofer Berglund, Michael Jonsson, "Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications", Swedish Defence Research Agency (FOI), March 2019, pag. 25.
[32] Keir Giles Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, pag. 24.
[33] Tomasz Smura, "Russian Anti-Access Area Denial A2AD Capabilities – Implications for NATO", Pulaski Policy Paper, 27 November 2016, pag. 2.
[34] Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence", The RUSI Journal, 5November 2020, pag. 73.

I dati attualmente disponibili, mostrano che la Russia concentra i suoi sistemi Anti-Access/Area-Denial nella zona di Mosca, nella Penisola di Kola, nel Mar Baltico, nel Mar Nero, in Crimea ed in Siria[35] come indicato nella Figura 2.

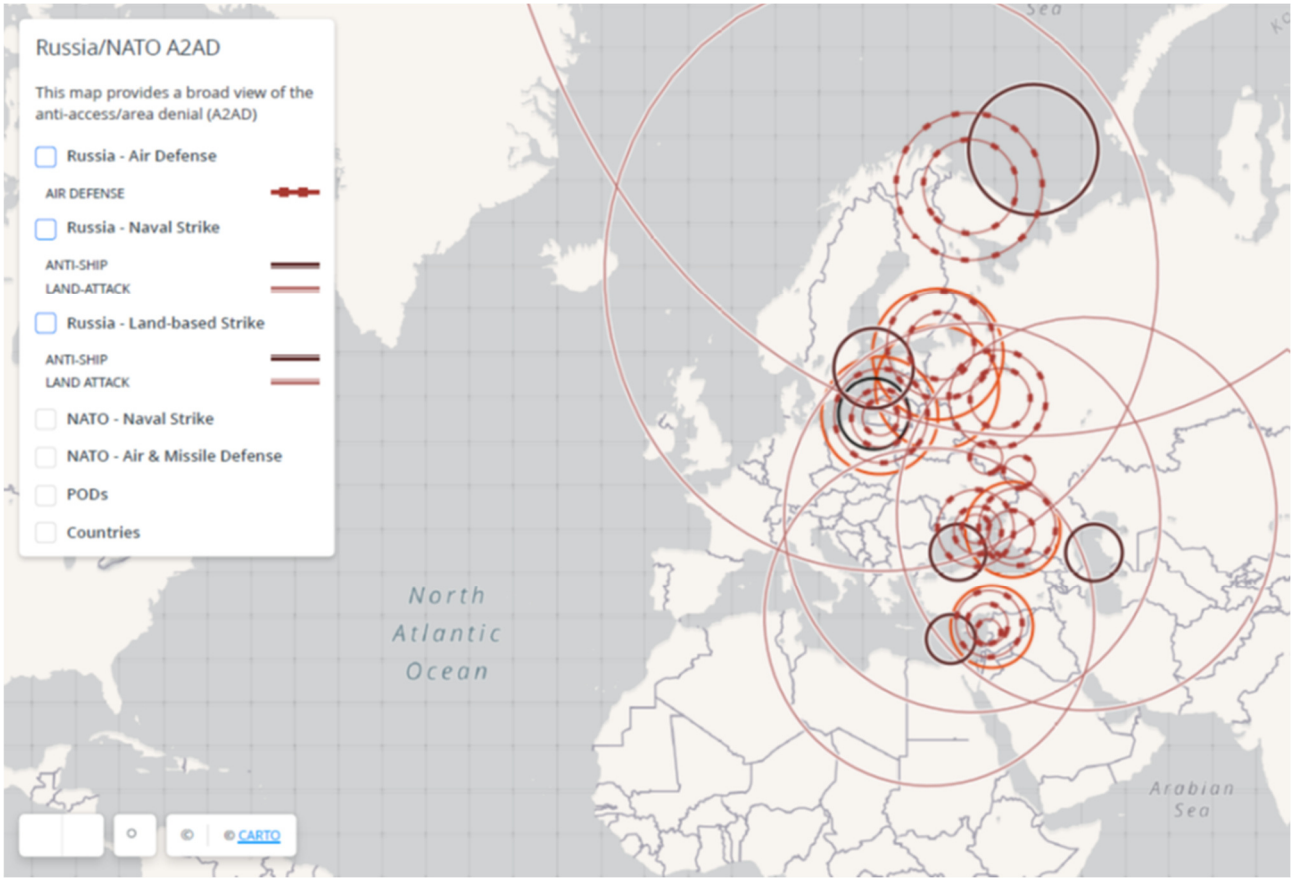


Figura 2, Russia/NATO A2/AD, "The Russia – NATO A2/AD Environment", Center For Strategic & International Studies, Missile Defense Project, 3 January 2017, Interactive Map By CARTO, 14/04/2021.

Queste capacità Anti-Access/Area-Denial consentono alla Russia di colpire parte dell'Europa orientale, oltre a contrastare le potenziali operazioni della NATO nelle regioni dell'estremo nord, del Baltico, del Mar Nero e del Mediterraneo orientale[36]. Quanto fin qui descritto, permette di avere un'idea di come la Russia abbia sviluppato un approccio alla strategia A2/AD, adattato al proprio background ed ambiente culturale ed operativo.

[35] Ionut Alin Cirdei, "A2AD Concept in the Modern Security Environment", 24th International Conference KNOWLEDGE-BASED ORGANIZZATION, Vol XXIV, 1 June 2018, pag. 54.
[36] Aziz Erdogan, "Russian A2AD Strategy and Its Implications for NATO", Beyond the Horizon, 6 December 2018, pag. 11.

L'approccio russo all'Anti-Access/Area-Denial si basa sull'uso coordinato e sovrapposto di strumenti di tipo asimmetrici per ostacolare, degradare o annullare le capacità del nemico in termini di comando e controllo del campo di battaglia, impedendogli di schierarsi ed operare in un determinato teatro operativo.

Tenendo conto della formulazione della Strategia di Difesa Attiva precedentemente descritta, l'obiettivo è colpire il nemico in termini di capacità di manovra e coordinamento nella fase iniziale del conflitto per poi usare una strategia di logoramento per minarne la volontà politica. La panoplia degli strumenti di A2/AD non andrebbe vista come limitata all'utilizzo per negare un'area geografica strategica ma in uno spettro di utilizzi molto più vasto, come impedire le operazioni nemiche colpendo punti di raduno, centri di comando, strutture di supporto e depositi, ossia le capacità a sostegno delle operazioni sul campo.

In quest'ottica il ricorso all'A2/AD in Russia si potrebbe anche declinare in questi termini "*non come Anti-Access/Area-Denial di uno spazio geografico ben definito e delimitato ma piuttosto come negazione all'accesso/utilizzo di capacità e strutture che agiscono come abilitatori del sistema di comando e controllo del nemico e della sua proiezione di potenza*".

Anzi, tale approccio ha in certi casi spinto i leader militari occidentali a prendere nota delle scelte russe, come riporta la seguente frase dell'Ammiraglio James G. Foggo "Per quanto riguarda le capacità difensive, come dico agli alleati e ai partner, se hai una quantità limitata di risorse e vuoi proteggere le tue coste, pensa a cosa fanno i russi e perseguiamo sistemi simili - mine intelligenti, missili da crociera antinave collegati a radar costieri "[37].

3. UN ESEMPIO DI A2/AD BUBBLE: KALININGRAD

L'exclave di Kaliningrad rappresenta un avamposto difensivo avanzato russo situato al centro della regione baltica e scandinava ed è fondamentale per l'architettura A2/AD regionale della Russia. La potenziale area di interdizione copre essenzialmente gli Stati baltici, un terzo della Polonia, la Scandinavia meridionale e il Golfo di Finlandia, nonché parti della Bielorussia. Kaliningrad rappresenta un ostacolo per le operazioni militari della NATO verso ed all'interno della regione a causa delle difese integrate Anti-Access/Area-Denial dell'oblast.

[37] Christopher Woody, "US allies worried about pricey weapons should look at what Russia's doing, the Navy's top officer in Europe says", Insider, 24 January 2020.

Il confine polacco-lituano, l'area del cosiddetto Suwalki Gap, è l'emblema del problema rappresentato da Kaliningrad: la Russia potrebbe impedire l'accesso terrestre agli Stati baltici in caso di conflitto bloccando le principali arterie stradali e ferroviarie nell'area di confine tra Kaliningrad, Lituania e Bielorussia, ricorrendo ad operazioni militari dirette o asimmetriche[38].

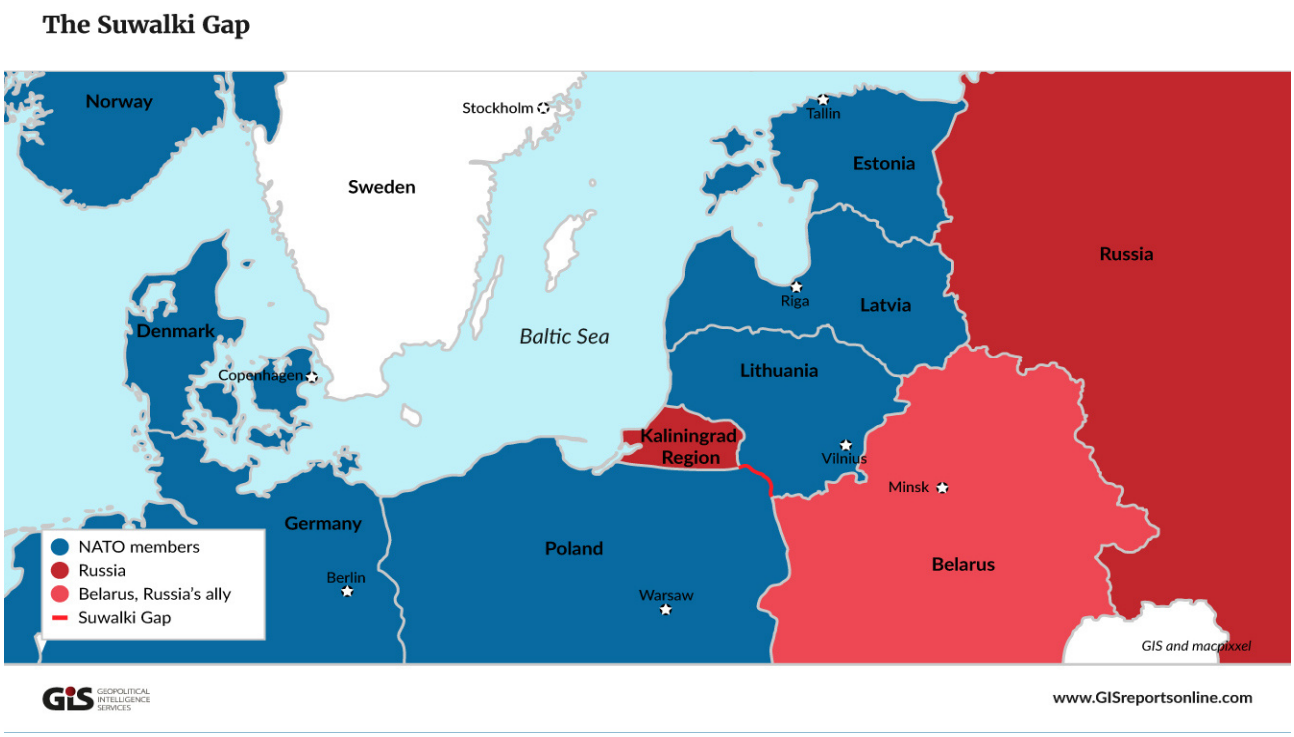


Figura 3, The Suwalki Gap, "Scenarios for Central and Eastern Europe in a Russia-NATO Conflict", Geopolitical Intelligence Services, 19 April 2017.

La posizione geostrategica di Kaliningrad presenta molti vantaggi per la Russia, consentendo il preallarme e la difesa aerea avanzata del territorio russo. La marina possiede basi che permettono il controllo del Mar Baltico centrale e l'accesso al Golfo di Finlandia, influenzando così anche la sicurezza e la libertà di manovra della Finlandia e della Svezia.

L'importanza di Kaliningrad è testimoniata dalle unità militari dell'esercito, della marina e dell'aviazione dislocate in questo piccolo angolo della Russia. La modernizzazione delle forze armate, avviata nel 2008, ha prodotto un significativo rafforzamento militare e investimenti in infrastrutture legate al settore militare[39].

[38] Keir Giles Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, pag. 27.

[39] Zdzislaw Sliwa, "KALININGRAD OBLAST AS THE FORWARD ANTI-ACCESS/ AREA DENIAL HUB", Baltic Defence College, Security Forum Volume 2, No 2, 2018, pag. 24.

La città Kaliningrad ospita il comando della flotta del Baltico, mentre la base navale si trova nel porto di Baltiysk. Tecnicamente, una base navale è "una formazione territoriale tattico-operativa responsabile di garantire condizioni favorevoli al lancio di operazioni navali"[40], ed include il 313° Distaccamento, un'unità con capacità di difesa costiera, per il dragaggio di mine, la guerra ASW ed il contrasto a forze speciali nemiche[41].

Complessivamente la flotta del Baltico comprende 227 unità di cui 131 dislocate nell'area di Kaliningrad, 52 delle quali sono unità da combattimento[42]. A Baltiysk sono acquartierate le seguenti unità della flotta[43]: la *36ª Brigata Navi Missilistiche*; la *64ª Brigata Navi di Protezione*; il *72° Squadrone Navi ELINT*; la *71ª Brigata Navi da Sbarco*; la *106ª Squadriglia Navi Missilistiche*; la *128ª Brigata Navi di Superficie*; il *342° Distaccamento SAR*.

La 128ª brigata costituisce la principale forza di superficie della marina russa nel Baltico[44], comprendendo un cacciatorpediniere, due fregate e quattro corvette[45]. La brigata ha ricevuto nuove unità navali, comprendenti quattro corvette della classe Steregushchy (Project 20380) ed una fregata classe Neustrashimy (Project 11540)[46].

A queste, si sono aggiunte tre navi lanciamissili della classe Karakurt (Project 22800)[47] e due della Bujan-M (Project 21631)[48], unità di nuova costruzione ed armate con il missile da crociera Kalibr e destinate alle divisioni di navi lanciamissili. Le unità navali appena descritte costituiscono la componente più moderna delle forze d'altura della flotta del Baltico.

[40] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 31.
[41] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 47.
[42] Ibid, pag. 32.
[43] Ibid, pag. 48.
[44] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 33.
[45] Ibid, pag. 72.
[46] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 48. Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 72.
[47] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 73.
[48] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 48.

La Figura 4 mostra il dislocamento della flotta del Baltico nell'oblast di Kaliningrad.

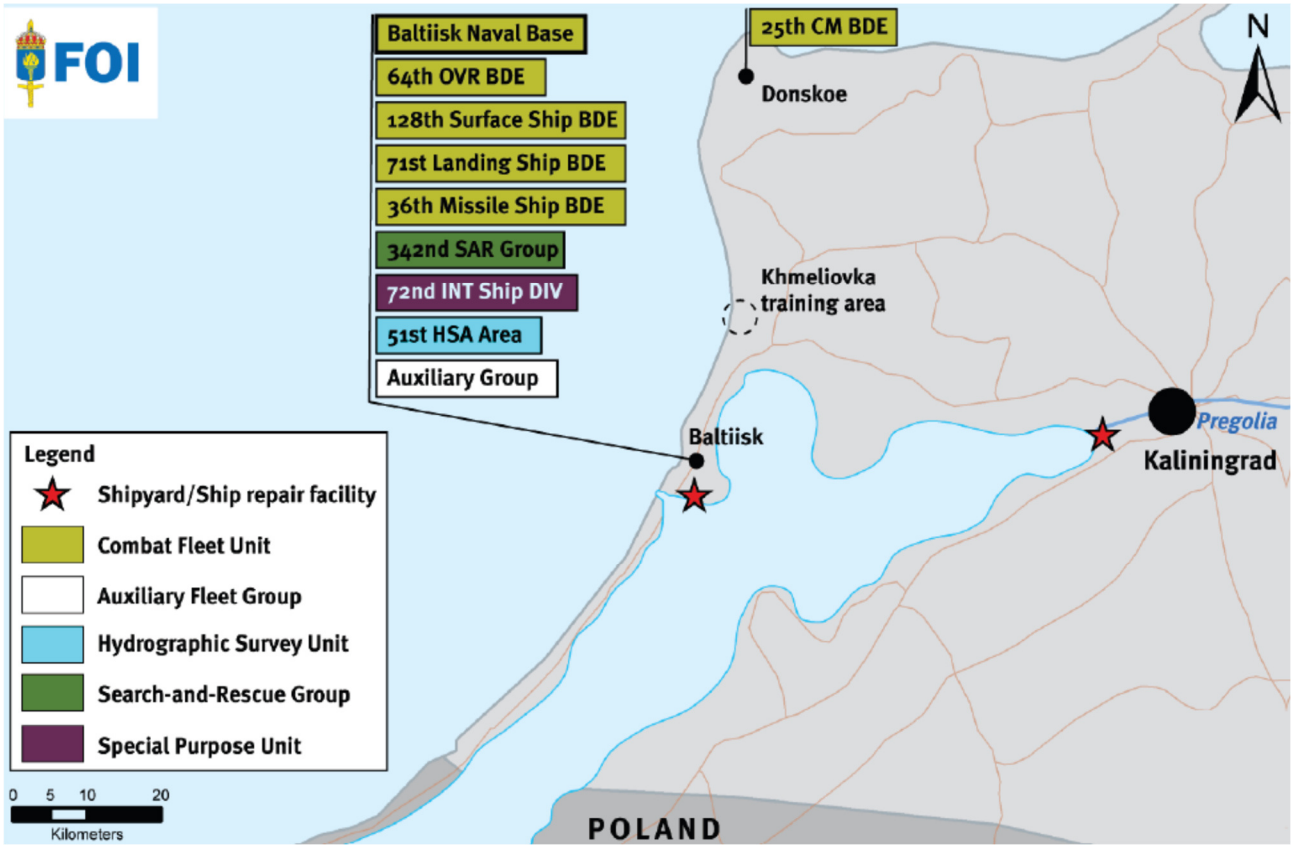


Figura 4, Baltiisk Naval Base, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 29. Notes: BDE – brigade; CM – coastal missile; DIV – division; HSA – hydrographic survey area; INT – intelligence; OVR – okhrana vodnogo raiona (water area protection); SAR – search and rescue.

Lele forze aeree presenti a Kaliningrad hanno sofferto di alcuni limiti organizzativi e logistici. Ciò è stato dovuto in maniera particolare ai lavori di ammodernamento della base aerea di Chkalovsk nel periodo 2013-18, oggi uno dei più grandi aeroporti militari russi[49]. Dal 2019 le forze aree presenti nell'oblast sono raggruppate nella 34ª *Divisione Aerea Combinata* formata da tre reggimenti che nel 2020 schieravano complessivamente dai 78 ai 104 velivoli[50]. I tre reggimenti[51] che compongono le forze aeree:

- *689° Reggimento dell'Aviazione da Combattimento della Guardia*. L'unità si compone di due squadrono dotati di Su-27P/UB[52], uno di UAV, ed uno da trasporto;

[49] OSW Team, "Fortress Kaliningrad", Centre for Eastern Studies (OSW), October 2019, pag. 72.
[50] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 43.
[51] Ibid, pag. 43.
[52] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 51.

- *4° Reggimento Combinato di Aviazione della Guardia*. Comprende uno squadrone di Su-24M[53] ed uno di Su-30M[54] con il compito di fornire il supporto aereo ravvicinato per la flotta,
- *396° Reggimento Combinato Elicotteri della Guardia*. Il reggimento comprende uno squadrone di elicotteri navali ASW Ka-27PS/PM/L, uno da trasporto su Mi-8 ed infine uno da attacco su Mi-24VP[55].

Alla modernizzazione della difesa aerea di Kaliningrad è stata una priorità molto alta, con l'introduzione in servizio di nuove unità dotate di sistemi antiaerei avanzati a lungo raggio. Le unità sono raggruppate sotto il comando della *44ª Divisione di Difesa Aerea* che risulta costituita da tre reggimenti[56]:

- *183° Reggimento Missilistico di Difesa Aerea della Guardia*. L'unità si compone di due battaglioni di S-400, due di S-300[57] ed uno di Pantsir-S1 per la difesa a corto raggio;
- *1545° Reggimento Missilistico di Difesa Aerea*. Originariamente equipaggiato con gli S-300 sostituiti nel 2019 con due battaglioni di S-400;
- *81° Reggimento Radiotecnico*. Sebbene i dettagli sulle attrezzature del reggimento siano scarse, si ritiene che includano i moderni radar mobili di sorveglianza, ricerca ed acquisizione a lungo raggio/alta quota della serie Nebo e Gamma[58].

Il dislocamento delle unità della 34ª divisione aerea combinata e della 44ª divisione di difesa aerea sono illustrate nella Figura 5.

[53] Tomasz Smura, "Russian Anti-Access Area Denial A2AD Capabilities – Implications for NATO", Pulaski Policy Paper, 27 November 2016, pag. 3.
[54] OSW Team, "Fortress Kaliningrad", Centre for Eastern Studies (OSW), October 2019, pag. 72.
[55] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 51.
[56] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 46.
[57] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 50.
[58] "Radiotekhnicheskie podrazdeleniia PVO Baltiiskogo flota provodiat ucheniia pod Kaliningradom", Tass, 26 March 2018, Consultato il 19/04/2021.

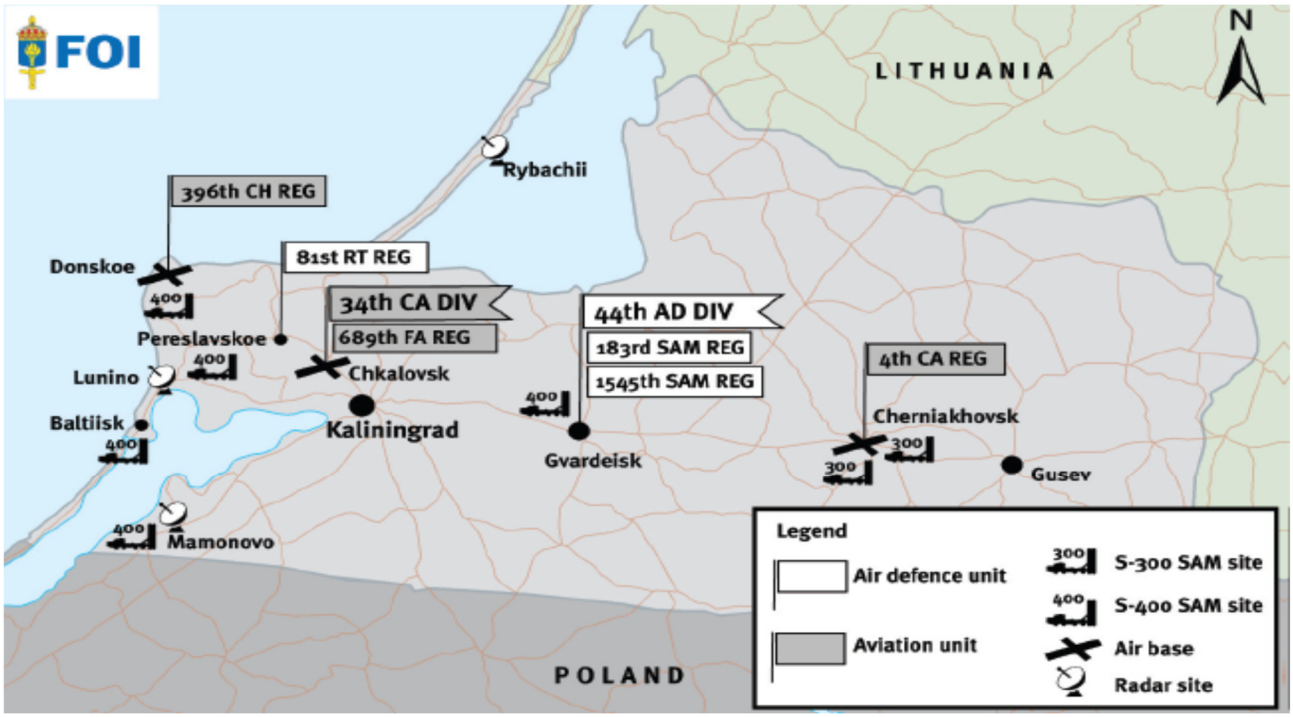


Figura 5, Units of the Baltic Fleet Naval Aviation and Air Defence, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 29. Notes: AD – air defence; CA – composite aviation; CH – composite helicopter; DIV – division; FA – fighter aviation; REG – regiment; RT – radio technical (radar); SAM – surface-to-air missile.

Il controllo delle unità terrestri nell'oblast è assicurato da parte dell'*11° Corpo d'Armata* istituito nel 2016[59] e a sua volta subordinato al comando della flotta del Baltico. Questo comprende una struttura di comando e supporto composta dal *40° Battaglione Comando* e dal *46° Battaglione da Ricognizione*[60], a cui si aggiunge il *148° Battaglione di Riparazione e Recupero*[61]. Ad esse si aggiungono tre unità di manovra[62]:

- *7° Reggimento Separato Fucilieri Motorizzati della Guardia* (APC BMP-2; SPG 2S3; MLRS BM-21; ATGM Shturm-S; SPAAG ZSU-23-4):
- *79ª Brigata Separata Fucilieri Motorizzati della Guardia* (APC BMP-2; MBT T-72B3; SPG 2S3; MLRS BM-21; ATGM Shturm-S; SPAAW Tunguska);
- *11° Reggimento Corazzato* (APC BMP-2; MBT T-72B3(M)[63]; SPG 2S19; ATGM Shturm-S).

[59] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 42.
[60] Ibid, pag. 49.
[61] Ibid, pag. 45.
[62] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 49-51.
[63] OSW Team, "Fortress Kaliningrad", Centre for Eastern Studies (OSW), October 2019, pag. 73.

Il supporto di fuoco è fornito dalla *244ª Brigata di Artiglieria* che ha in servizio anche i lanciarazzi BM-30 Smerch[64] (SPG 2A36/2S7; MLRS BM-27/BM-30; ATGM Khrizantema-S), mentre il *22° Reggimento di Difesa Aerea* fornisce la necessaria copertura antiaerea[65](SAM Tor-M1/M2). Infine, la *152ª Brigata Missili* composta da tre battaglioni dotati complessivamente di 24 sistemi missilistici SRBM Iskander-M[66] fornisce capacità di attacco terrestri di tipo deep strike.
A completare lo strumento terrestre schierato nell'area di Kaliningrad concorrono anche due unità dipendenti gerarchicamente dalla flotta del Baltico[67]:

- *336ª Brigata Separata di Fanteria Navale della Guardia*. I compiti principali della brigata sono condurre operazioni di guerra anfibia e combattere nelle zone costiere (APC BTR-82; 2S9 Nona; 2S1 Gvozdika);
- *25ª Brigata Missili Costieri*. Unità armata con due battaglioni missilistici costieri, uno con il Bal e uno con il Bastion-P. L'unità ha il compito di proteggere gli approcci marittimi e condurre attacchi contro le forze navali avversarie[68].

La flotta del Baltico dispone anche di una serie di unità per il supporto al combattimento:

- *742° Centro Trasmissioni della Guardia*. L'unità gestisce diversi i nodi di comunicazione che garantiscono il funzionamento della rete di comunicazione militare[69];
- *841° Centro per la Guerra Elettronica*. È composto da due battaglioni che forniscono capacità EW a livello tattico e strategico[70];
- *69° Reggimento Separato Ingegneri Navali*. Su tre battaglioni comprende unità di guastatori, genio pontieri ed una compagnia da sbarco[71];

[64] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 44.
[65] Tomasz Smura, "Russian Anti-Access Area Denial A2AD Capabilities – Implications for NATO", Pulaski Policy Paper, 27 November 2016, pag. 4.
[66] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 51.
[67] Ibid, pag. 51-52.
[68] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 46.
[69] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 53.
[70] Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 47.
[71] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 53.

- *9 Compagnia Separata di Protezione Chimica, Biologica e Radiologica*. Si tratta di una piccola unità con attrezzature per il contrasto ad attacchi CBR ed impiegata anche in attività di mimetizzazione come l'uso di cortine fumogene per mascherare mezzi militari[72];
- *561ª Stazione Navale per la Ricognizione*. Ogni flotta della Marina russa ha un'unità delle forze speciali navali note come Spetsnaz ed indipendenti rispetto al GRU (Glavnoe Razvedyvatel'noe Upravlenie - Direttorato Principale per l'informazione). L'unità della flotta del Baltico è di ridotte dimensioni e la sua composizione in termini numerici non è chiara oscillando tra le 50 e le 100 unità[73].

La Figura 6 rappresenta a livello grafico le unità precedentemente descritte.

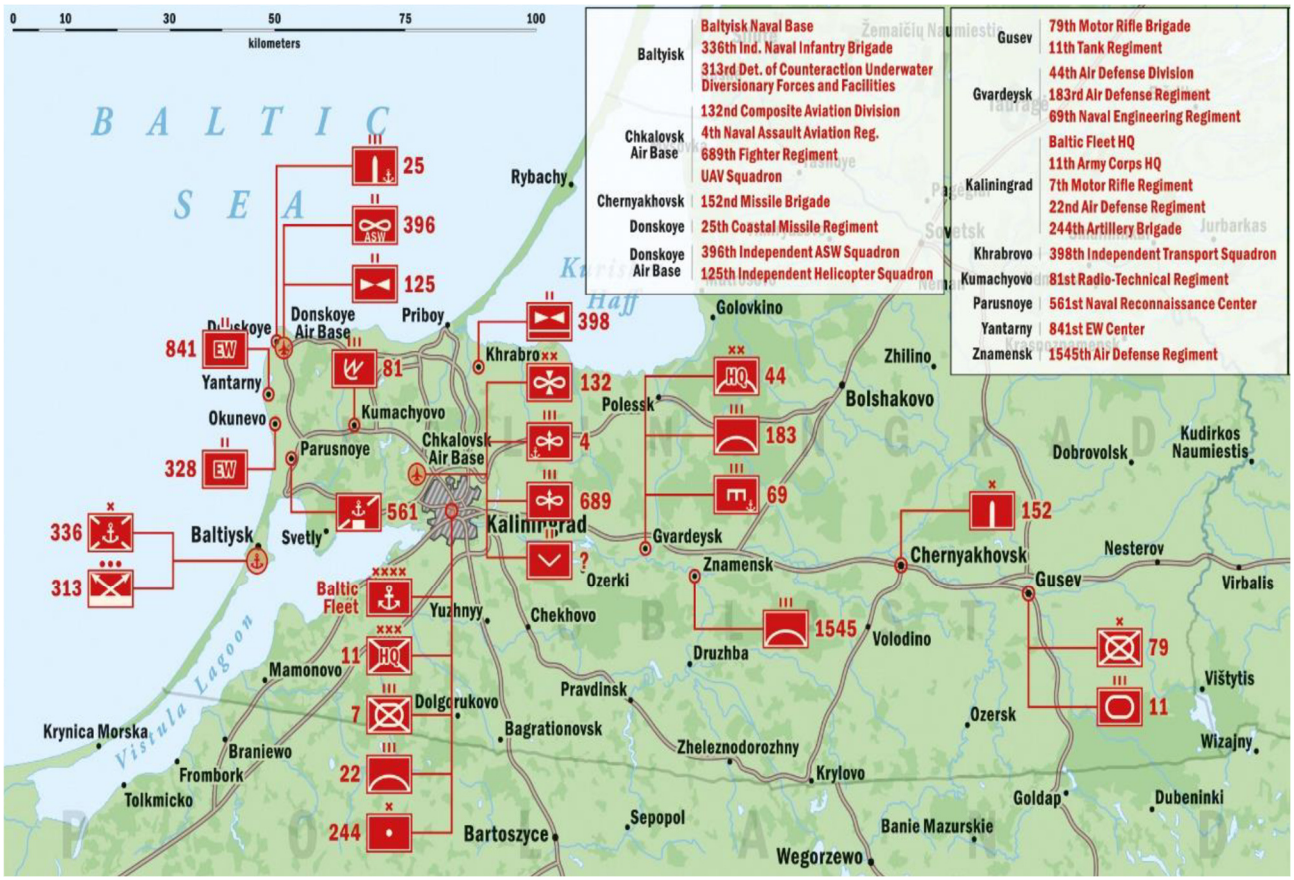


Figura 6, Russian forces in the Kaliningrad Oblast, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, pag. 43.

[72] Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, pag. 54.
[73] Ibid, pag 54.

Nell'ultimo decennio anche l'oblast sul Baltico ha beneficiato dei risultati della riforma dello strumento militare russo avviata nel 2008. La flotta del Baltico, la difesa antiaerea e costiera, le unità missilistiche dell'esercito hanno assistito all'introduzione di sistemi d'arma avanzati e con capacità di ingaggio ed attacco a lungo raggio.

Questo rientra nella strategia russa di creare aree in cui la presenza di differenti sistemi missilistici integrati permetta di costruire una difesa capace di impegnare a distanza l'avversario, ostacolandolo nella sua fase di avvicinamento e schieramento all'inizio di una campagna militare. In questa logica le forze russe operanti nell'area permettono di garantire l'assolvimento delle capacità di Anti-Access/Area-Denial previste dalla dottrina della Difesa Attiva per impedire il corretto svolgimento del piano d'azione nemico, degradando e/o negando le capacità critiche del nemico quali l'utilizzo di infrastrutture, delle rotte marittime, il supporto aereo e le attività di ISR.

4. SISTEMI MISSILISTICI DISPIEGATI A KALININGRAD

Attualmente, l'exclave di Kaliningrad quale sede della flotta baltica russa, ospita un notevole numero di risorse utilizzabili per una strategia Anti-Access/Area-Denial: sistemi SAM S-400, S-300 e Pantsir-S; sistemi di difesa costiera Bastion-P e Bal; missili balistici Iskander-M e da crociera Iskander-K; missile da crociera Kalibr in versione antinave e da attacco terrestre. Infine, va tenuto presente che le unità dell'esercito russo sono dotate di sistemi per la difesa aerea e di artiglieria missilistica che possono diventare rilevanti in un conflitto, come il Tor per la difesa aerea a corto/medio raggio e il sistema di artiglieria a razzo Smerch.

Complessivamente per la difesa antiaerea nell'oblast sono schierati quattro battaglioni di S-400, due di S-300, uno di Pantsir-S1 per la difesa ravvicinata, a cui si aggiunge un reggimento dell'esercito equipaggiato con il sistema Tor M1/M2. Vediamo nel dettaglio i sistemi missilistici antiaerei precedentemente elencati:

- **S-400 Triumph**. L'S-400 Triumf (nome in codice NATO: SA-21 Growler) è un sistema SAM a medio e lungo raggio mobile entrato in servizio nell'aprile 2007 con quattro reggimenti

a difesa dello spazio aereo nazionale nella regione di Mosca[74]. Il sistema impiega quattro modelli di missile intercettore[75]: il primo è il 48N6E3, una versione modificata del 48N6E2 utilizzata nei sistemi S-300P e con autonomia di 250 km ed una testata di 146 kg di esplosivo a frammentazione[76],il secondo è il 40N6 che ha l'autonomia estesa a 400 km; il terzo è il 9M96E che ha un'autonomia di 40 km; il quarto è il 9M96E2 che ha un'autonomia di 120 km. I missili 9M96E e 9M96E2 sono più piccoli e progettati per un impatto diretto con tecnologia *hit-to-kill*[77]. Un veicolo lanciatore per il sistema S-400 è in grado di trasportare 4-16 missili a seconda delle varianti impiegate, mentre un battaglione con otto veicoli di lancio schiera un totale di 32-128 missili[78]. Il sistema di comando e controllo 55K6E dell'S-400 Triumph si basa sul veicolo mobile del posto di comando Ural-532301[79]. Il radar di ricontrollo e tracciamento del bersaglio dell'S-400 è il 92N6E Gravestone, mentre Il radar 91N6E Big Bird per l'acquisizione e la gestione della battaglia dell'S-400 ha un raggio di azione di 600 km e può tracciare simultaneamente fino a 300 bersagli[80].

- S-300V. È un sistema SAM (nome in codice nato NATO: SA-23 Gladiator/Giant) a lungo raggio progettato con due diverse versioni che si distinguono per il missile che utilizza: l'SA-12A Gladiator viene utilizzato principalmente per mirare agli aerei, mentre l'SA-12B Giant è usato principalmente per contrastare i missili balistici tattici e da crociera[81]. L'S-300V utilizza missili 9M83 e 9M82, con una portata contro velivoli aerei rispettivamente di 75 e 100km, mentre contro vettori balistici è di soli 40 km[82]. Il sistema utilizza il veicolo lanciatore a quattro tubi 9A83ME per l'SA-23A Gladiator e il veicolo lanciatore a due tubi 9A84ME per l'SA-23B Giant, mentre tutte le varianti di missili trasportano testate a frammentazione da 150 kg con sistemi di guida inerziale e radar semi-attivi[83]. Il sistema si compone di un posto di comando 9S457ME, radar di sorveglianza 9S19ME per

[74] "S-400 Triumph Air Defence Missile System", Army Technology, Consultato il 21/04/2021.
[75] "S-400 Triumf Air Defense System", Missile Defense Advocacy Alliance, June 2016, Consultato 21/04/2021.
[76] "S-400 Triumf", Missile Threat, Center for Strategic and International Studies, 4 May 2017, Consultato 21/04/2021.
[77] "S-400 Triumph Air Defence Missile System", Army Technology, Consultato il 21/04/2021.
[78] "S-400 Triumf Air Defense System", Missile Defense Advocacy Alliance, June 2016, Consultato 21/04/2021.
[79] "S-400 Triumph Air Defence Missile System", Army Technology, Consultato il 21/04/2021.
[80] Ibid.
[81] "S-300V Air and Missile Defense System", Missile Defense Advocacy Alliance, December 2017, Consultato il 21/04/2021.
[82] "S-300", Missile Threat, Center for Strategic and International Studies, 4 May 2017, Consultato il 21/04/2021.
[83] Ibid.

tracciare e rilevare i bersagli e di radar di osservazione 9S15M2 per fornire dati di sorveglianza, preallarme e acquisizione bersagli[84].

- **Pantsir S-1[85]**. Lo sviluppo dell'SPAAW Pantsir (nome in codice NATO: SA-22 Greyhound) risale al 1989. Dopo il 1991, i requisiti per il sistema sono cambiati per fornire la difesa a corto raggio per le forze di terra russe e i sistemi SAM, entrando in servizio nel 2003. Il sistema incorpora missili e cannoni per intercettare aerei tattici, munizioni guidate di precisione e piccoli velivoli senza equipaggio. Utilizzando il suo radar di ricerca, il Pantsir può tracciare fino a 20 bersagli tattici delle dimensioni di un aeroplano a una distanza di 32-36 km. Sebbene il Pantsir sia in grado di funzionare in modo indipendente, in genere sono schierate batterie di sei veicoli di lancio occasionalmente accompagnate da un veicolo di comando e controllo separato. Il sistema è equipaggiato con un massimo di dodici missili 57E6 e due cannoni 2A38M da 30 mm. Il 57E6 è un missile a due stadi con guida radiocomandata e testata a frammentazione da 20 kg.
- **Tor-M1/M2**. Il sistema è stato progettato per difendere bersagli puntuali e unità corazzate contro aerei, elicotteri e munizioni a guida di precisione. La prima serie di produzione, il Tor-M (nome in codice NATO: SA-15 Gauntlet), è entrata in servizio nel 1991[86]. Il sistema di difesa aerea incorpora un radar di sorveglianza a scansione meccanica con un raggio di rilevamento di 25 km ed uno a guida elettronica con una portata massima di oltre 25 km[87]. Un'unità di lancio Tor-M1 ospita fino a otto missili 9M331con una portata massima di 15 km e con una testata a frammentazione di circa 15 kg[88]. La versione Tor-M2 può essere armata con 8 missili della serie 9M331 o 16 9M338, con sistemi radar, di rilevamento ed elaborazione del segnale migliorati[89]. Ogni batteria è composta da un comando batteria mobile, quattro veicoli da combattimento, due trasportatori/caricatori 9T224 e un veicolo di manutenzione[90].

[84] "S-300", Missile Threat, Center for Strategic and International Studies, 4 May 2017, Consultato il 21/04/2021.
[85] "Pantsir S-1", Missile Threat, Center for Strategic and International Studies, 4 May 2017, Consultato il 21/04/2021.
[86] "Tor (SA-15 Gauntlet)", Missile Threat, Center for Strategic and International Studies, 10 January 2020, Consultato il 21/04/2021.
[87] "Ibid.
[88] "9K330 Tor", WEAPONSYSTEMS.NET, Consultato il 21/04/2021.
[89] "Tor (SA-15 Gauntlet)", Missile Threat, Center for Strategic and International Studies, 10 January 2020, Consultato il 21/04/2021.
[90] "Tor M2 Surface-to-Air Missile (SAM) System", Army Technology, Consultato il 21/04/2021.

Nell'oblast di Kaliningrad sono schierati anche sistemi missilistici a medio raggio con capacità di attacco al suolo in funzione Anti-Access/Area-Denial, costituiti dai sistemi Iskander-M della 152ª Brigata Missili ed il missile Kalibr imbarcato sulle unità della flotta del Baltico:

- Iskander-M. Il sistema SRBM Iskander (nome in codice NATO: SS-26 Stone) entrò in servizio nel 2006. La designazione "Iskander" è tipicamente utilizzata per identificare sia il sistema di lancio che i missili balistici impiegati. Il missile 9M723 SRBM ha una portata massima di 500 km e può trasportare testate convenzionali e nucleari fino a 700 kg, impiegando un veicolo di rientro manovrabile (MaRV) oltre ad esche per sconfiggere i sistemi di difesa missilistica[91]. Le testate convenzionali includono quelle a grappolo, incendiarie, anti-bunker e testate elettromagnetiche (EMP)[92]. Il sistema utilizza il trasportatore TEL con due missili pronti al lancio, mentre i veicoli di ricarica, ciascuno con due missili e una gru, consentono operazioni prolungate sul campo di battaglia. Una brigata Iskander standard include 12 TEL ed i relativi veicoli di supporto[93] I missili utilizzano una combinazione di guida inerziale, GLONASS e radar, con un errore circolare probabile (CEP) stimato di 2-5 metri[94]. Negli anni 2000, la Russia ha dotato gli Iskander TEL di nuovi missili da crociera per impiego terrestre, il 9M728 (NATO SSC-7) anche indicato come sistema di combattimento "Iskander-K"[95].
- Kalibr. Il 3M-14T Kalibr (nome in codice NATO: SS-N-30A) è un missile da crociera russo per attacco terrestre (LACM), mentre il 3M54 è la versione antinave. Il missile ha una portata stimata di circa 1.500-2.500 km ed una testata da 450 kg di esplosivo, lanciato mediante celle di lancio verticali VLS[96]. Sebbene comunemente indicato come missile da crociera Kalibr, il 3M-14T è in realtà solo una parte della più ampia famiglia dei missili imbarcati in dotazione alla marina russa. La sua esistenza fu rivelata nel 2015 con il lancio di missili Kalibr dal Mar Caspio verso la Siria, con un volo di circa 1800 km[97].

[91] "Iskander-M (SS-26)", Missile Defense Advocacy Alliance, Consultato il 21/04/2021.
[92] Ibid.
[93] "SS-26 Iskander", Missile Threat, Center for Strategic and International Studies, 27 September 2016, Consultato il 21/04/2021.
[94] Ibid.
[95] Ibid.
[96] "3M-14 Kalibr (SS-N-30A)", Missile Defense Advocacy Alliance, May 2017, Consultato il 21/04/2021.
[97] Christopher P. Cavas, "Is Caspian Sea Fleet a Game-Changer?" Defense News, 11 October 2015.

A completare lo schieramento di sistemi missilistici in chiave A2/AD nell'oblast di Kaliningrad vanno riportati anche quelli preposti alla difesa costiera e schierati nell'ambito dei due battaglioni della 25ª Brigata missili costieri della flotta del Baltico:

- **Bastion-P**. Il 3K55 Bastion (nome in codice NATO: SS-C-5 Stooge) è un moderno sistema di difesa costiera sviluppato negli anni '90. Si basa sul missile P-800 Oniks utilizzabile a terra con due varianti: il Bastion-S fisso e il Bastion-P mobile. Una batteria tipica includerebbe quattro veicoli di lancio con due missili[98], un veicolo di comando, il veicolo radar e diversi veicoli di supporto[99]. Il P-800 Oniks (nome in codice NATO: SS-N-26 Strobile) è una famiglia di missili supersonici da crociera antinave russi, con tre varianti del missile per impiego navale, aereo e terrestre. Il raggio d'azione del missile è di 300 km, dotato di un sistema di navigazione inerziale attivo e passivo e con una testata perforante da 200 kg o esplosiva da 250 kg[100]. Nel 2002 è stato aggiornato il radar attivo ed aggiunto un cercatore di immagini a infrarossi[101]. Poiché il missile dipende dai dati radar, il raggio di ingaggio è limitato all'efficacia dei sistemi radar costieri. Utilizzando il radar Monolit-B l'ingaggio è da 150 a 200 km in versione del radar passiva e da 35 a 70 km in quella attiva[102]. In alternativa, il missile può anche ricevere dati di mira da droni, satelliti, aerei da pattugliamento marittimo ed elicotteri[103]. Il P-800 Oniks è principalmente un missile antinave, ma ha visto un maggiore utilizzo contro le forze di terra negli scontri che hanno coinvolto le forze militari russe in Siria[104].
- **Bal**. Il 3K60 Bal (nome in codice NATO: SSC-6 Sennight) è un sistema di difesa costiera meno sofisticato del Bastion. Una batteria Bal è composta da un veicolo di comando, due veicoli di lancio di missili e due veicoli di supporto. Un'unità di difesa costiera di solito è composta da due batterie ed i veicoli di lancio trasportano fino ad otto missili[105].

[98] Sebastien Roblin, "Why Russia's Bastion-P Truck-Launched Anti-Ship Missiles Could Be a Real Killer", The National Interest, 8 February 2020.
[99] "SS-N-26 "Strobile" (P-800 Oniks)/ Yakhont / Yakhont-M / Bastion (launch systems)", Missile Threat, Center for Strategic and International Studies, Consultato il 21/04/2021.
[100] Ibid.
[101] Ibid.
[102] "3K55 Bastion", Weaponsystems.net, Consultato il 21/04/2021.
[103] Sebastien Roblin, "Why Russia's Bastion-P Truck-Launched Anti-Ship Missiles Could Be a Real Killer", The National Interest, 8 February 2020.
[104] "P-800 Oniks (SS-N-26 Strobile)", Missile Defense Advocacy Alliance, June 2017, Consultato il 21/04/2021.
[105] "KH-35 (SS-N-25 Switchblade)", Missile Defense Advocacy Alliance, June 2017, Consultato il 21/04/2021.

Il sistema utilizza il Kh-35 (nome in codice NATO: SS-N-25 Switchblade), un missile da crociera subsonico antinave con un raggio di 120 km ed una testata esplosiva di 145 kg[106], mentre la versione aggiornata Kh-35U ha un raggio esteso a 260 km[107]. Il centro di comando è dotato di un radar di ricerca, mentre il missile Kh-35 utilizza una guida inerziale ed un radar attivo nella fase terminale[108]. Al posto del centro di comando per l'acquisizione dei bersagli può essere utilizzato anche il sistema di ricerca attivo e passivo associato al radar Monolit-B[109].

Per completare la rete di sistemi d'arma schierati a Kaliningrad in funzione A2/AD, vanno inclusi nell'analisi anche quei sistemi d'artiglieria che per gittata e potenza di fuoco concorrono alla strategia russa di Anti-Access/Area-Denial:

- BM-30 Smerch. Lo Smerch è entrato in servizio con le forze armate sovietiche nel 1987[110]. Il sistema è progettato per ingaggiare veicoli corazzati leggeri, artiglieria, missili tattici e unità di difesa aerea, elicotteri a terra, posti di comando, centri di comunicazione e installazioni militari-industriali[111]. I razzi trasportati sono da 300 mm con testata dal peso di 280 kg che può essere di varie tipologie: esplosiva a frammentazione; termobarica; incendiaria; cluster con submunizioni antiuomo e anticarro o munizioni anticarro autoguidate[112]. Il veicolo lanciatore è in grado di sparare a salve o lanciare singoli razzi, mentre la gittata dei razzi è compresa tra i 20 ed i 120 km[113]. Se il sistema è utilizzato per sparare una salva completa di 12 razzi, un singolo lanciatore copre un'area di circa 67 ettari[114]. Un'unità Smerch è composta da 6 veicoli lanciatori e 6 veicoli di ricarica, mentre il sistema di controllo del fuoco può funzionare automaticamente o in modalità di controllo manuale[115].

[106] "Kh-35", military-today.com, Consultato il 21/04/2021.
[107] Ibid.
[108] "3K60 Bal", Weaponsystems.net, Consultato il 21/04/2021.
[109] Ibid.
[110] Smerch Multiple Launch Rocket System, Military-Today.com, Consultato il 21/04/2021.
[111] "Smerch", ROSOBORONEXPORT, Consultato il 21/04/2021.
[112] Smerch Multiple Launch Rocket System, Military-Today.com, Consultato il 21/04/2021.
[113] Ibid.
[114] Ibid.
[115] Ibid.

Quanto fin qui descritto, in termini di sistemi missilistici e di artiglieria, permette di avere uno sguardo di insieme di quello che Kaliningrad costituisce nel sistema militare russo: un avamposto in cui i vari sistemi costituiscono un elaborato IADS/IAMD composto da differenti complessi missilistici a lungo raggio cui si affianca una robusta componente di artiglieria a lungo raggio e sistemi antiaerei a corto raggio.

Tali sistemi integrati rappresentano un complesso sistema che combina mezzi di attacco e difesa con capacità d'ingaggio a distanze variabili ed in ambiente terrestre, marino ed aereo. In questi termini l'oblast rappresenta una postazione militare perfettamente integrata nella strategia della Difesa Attiva precedentemente illustrata, utilizzando sistemi in grado di disabilitare o deteriorare le capacità critiche dell'avversario.

Da questo punto di vista Kaliningrad è un bastione avanzato dell'apparato militare della Russia la cui collocazione geografica lo rende un obbiettivo primario in caso di conflitto, mentre la densità dei sistemi difensivi presenti nella regione ne rendono laboriosa la soppressione.

5. UN MOLTIPLICATORE DI FORZA IN CHIAVE A2/AD: L'ELECTRONIC WARFARE

L'Electronic Warfare (EW) è stata descritta come "l'arte dell'invisibile"[116], riferendosi alle parti invisibili dello spettro elettromagnetico utilizzate per inviare i segnali. Essa ha diversi ruoli: proteggere e mantenere l'accesso allo spettro; degradare o negare l'accesso dell'avversario allo spettro; identificare e registrare le emissioni per proteggere l'accesso allo spettro o negarlo al nemico[117]. La Russia si è interessata all'EW in quanto è un modo relativamente economico per contrastare le capacità militari di un avversario. Con la riforma delle forze armate avviata nel 2008, alcuni strateghi russi hanno sostenuto l'attuazione della *Setetsentricheskaya Voyna* (network-centric warfare) come un "moltiplicatore di forza"[118] facendo della EW un elemento essenziale di questa riforma anche in chiave di capacità Anti-Access/Area-Denial.

[116] Patrick Smith, "Russian Electronic Warfare", American Security Project, April 2020, pag. 1.
[117] John R. Hoehn, "Defense Primer: Electronic Warfare", Congressional Research Service, 29 October 2020, pag. 1.
[118] Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 2.

Lo stato maggiore russo ha un alto livello di interesse nell'usare "moltiplicatori di forza e risposte asimmetriche per cercare di livellare il campo di gioco nei confronti di qualsiasi avversario dotato di sistemi ad alta tecnologie"[119]. In questo contesto, la Russia pensa che l'EW possa svolgere un ruolo fondamentale in un approccio olistico alla guerra, anche in chiave Anti-Access/Area-Denial dove "può trasformare le aree che rientrano nel [suo] raggio di azione in 'bolle' strategicamente e operativamente isolate"[120].

La definizione russa di EW è quella di *Radioelektronnaya Bor'ba* o REB[121], che sarà utilizzata nel proseguo del testo. Il maggiore generale Yuriy Lastochkin, che è a capo della forza di guerra radio-elettronica (REB) del Ministero della Difesa, ha dichiarato nel 2018 che gli uomini e le attrezzature destinati a tale scopo permetteranno alla Russia "di decidere il destino di tutte le operazioni militari"[122] nel prossimo futuro. In quest'ottica, l'utilizzo della REB serve ad ottenere l'effetto asimmetrico di disorganizzare la capacità di comando e controllo (C2) di un avversario. L'argomento della disorganizzazione è piuttosto prominente nella letteratura militare russa e, pertanto, si tratterebbe più di applicare alla strategia A2/AD il concetto di disorganizzazione del comando e controllo (C2D)[123], causano il caos nella pianificazione e nel coordinamento dell'avversario.

Come ha osservato il Lastochkin: "Non c'è niente di sorprendente che nelle circostanze attuali, la REB - come mezzo relativamente poco costoso e implementabile per interrompere il funzionamento del radar e di altri sistemi nemici e per difendere i propri sistemi dalle interferenze - stia emergendo come priorità ed obiettivo primario"[124].

[119] Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 2.
[120] Dominik P. Jankowski, Makysmilian Cziperski, "NATO's Strategic 'Six Pack' to Counter Russia's Anti-Access/Area Denial Capability", The National Interest, 22 September 2016.
[121] Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 1.
[122] Aleksandr Stepanov interview with Yuriy Illarionovich Lastochkin, MK Online, 15 April 2018, da Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", December 2019, pag. 62.
[123] Timothy Thomas, "RUSSIA'S ELECTRONIC WARFARE FORCE: BLENDING CONCEPTS WITH CAPABILITIES", MITRE Center for Technology and National Security, September 2020, pag. 5.
[124] Viktor Khudoleev, "Voyska dlya srazheniya v efire" [Troops for combat on airwaves], Krasnaya Zvezda, 14 April 2014, da Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 3.

Gli obiettivi primari delle forze REB sono le comunicazioni radio e cellulari, i radar, i sistemi elettronici e le capacità EW del nemico. Di conseguenza, il loro compito è di sopprime o protegge, a seconda che si tratti di attacco o difesa, i seguenti obiettivi[125]: C4ISR; i sistemi di identificazione e designazione dei bersagli; il controllo del fuoco; computer; sistemi di rete.

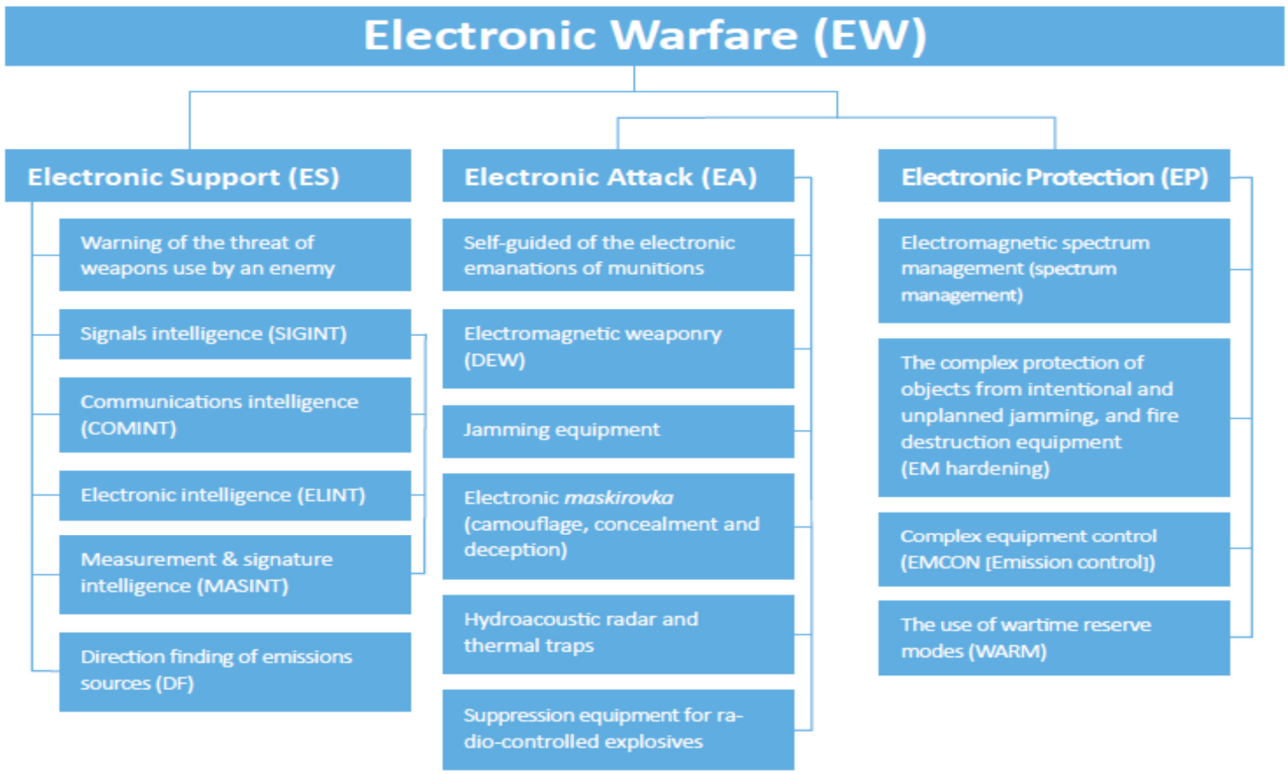
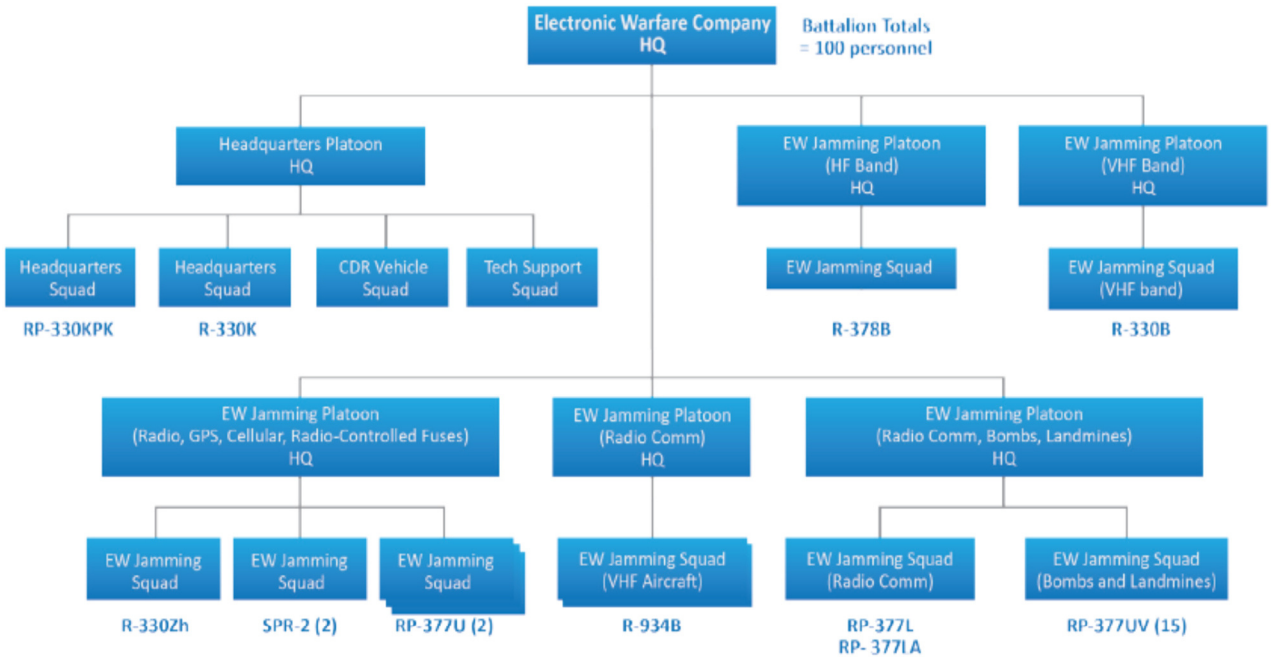


Figura 7, Electronic Warfare (EW), Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 4.

Le unità responsabili delle capacità REB russe sono disseminate in tutte le branche delle forze armate federali, con brigate indipendenti che sono state formate in tutti e quattro i distretti militari. Singole compagnie sono presenti in brigate e divisioni di carri armati, nonché nei ranghi delle truppe aviotrasportate. Inoltre, c'è anche una subunità simile nella brigata artica di fucilieri meccanizzati. Nella Marina, le forze REB di terra sono combinate in centri separati in tutte e quattro le flotte. Nelle forze aerospaziali, ci sono battaglioni REB indipendenti nelle unità di aviazione e di difesa aerea.

[125] Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 4.

Le attuali brigate di manovra russe sono state ristrutturate per contenere un'unità REB di livello compagnia[126], descritta nella Figura 7 nelle sue componenti e capacità operative.



Key to EW equipment

RP-330KPK: VHF Automated Command Post; RP-330K: Automated Control Station; R-378B: HF Automated Jamming Station; R330B: VHF Frequency Jammer linked to the *Borisoglebsk*-2 HF Automated Jamming System; R-330Zh: *Zhitel* Automated Jammer against INMARSAT and IRIDIUM satellite communication systems, GSM and GPS; SPR-2: VHF/ UHF Radio Jammer; RP-377U: Portable Jammer (against IEDs); RP-934B: VHF Automated Jamming Station against communications and tactical air guidance systems; RP-377L: IED Jammer; RP-377LP: Portable Automated Jammer; RP-377UV: Portable Automated Jammer.

Figura 8, EW Company, Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 7.

Lastochkin crede che la REB possa creare una 2bolla elettronica sul campo di battaglia, spegnendo e disabilitando gli occhi e le orecchie di un avversario"[127]. Una recente esercitazione russa[128] ha cercato di creare una bolla EW sulle truppe, ottenendo il risultato mediante l'uso di tre sistemi: il *Borisoglebsk* per la raccolta di informazioni; il *Krasukha* per sopprimere i radar degli aerei e i canali di controllo dei droni; lo *Zhitel* per bloccare le comunicazioni satellitari, i GPS e le comunicazioni cellulari in un raggio di 30 km.

[126] Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, pag. 5.
[127] Timothy Thomas, "RUSSIA'S ELECTRONIC WARFARE FORCE: BLENDING CONCEPTS WITH CAPABILITIES", MITRE Center for Technology and National Security, September 2020, pag. 6.
[128] Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", MITRE Center for Technology and National Security, December 2019, pag. 63.

Gli obiettivi e le capacità delle unità REB sono stati descritti in una serie di interviste rilasciate dal Generale Lastochkin nel corso degli ultimi anni. Ad esempio, nel 2014 notava che i sistemi radio-elettronici forniscono la base tecnica per la maggior parte degli armamenti e delle attrezzature militari ad alto contenuto tecnologico[129]. Per tale motivo l'impiego di strumenti di REB contro tali tecnologie rappresentava una misura asimmetrica per annullare la capacità di un avversario attraverso i seguenti approcci: individuare i sistemi di comando e controllo e di raccolta di informazioni come obiettivi prioritari; viluppo di nuovi modi per interrompere la propagazione delle onde radio; creazione di tecnologie per ridurre le emissioni dei sistemi d'arma; creazione di un ambiente REB ostile per le strutture di ricognizione tecnica e raccolta di informazioni dell'avversario[130].

In un successivo intervento del 2017, Lastochkin ampliava le competenze della REB ai seguenti settori[131]: costruzione di armi a radiazioni elettromagnetiche; sviluppare software in grado di interrompere l'accessibilità, l'integrità e la riservatezza delle informazioni degli avversari; applicare i mezzi per creare il falso ambiente elettromagnetico ed ingannare i sistemi avversari. In sintesi, il concetto espresso dal Generale Lastochkin è che le operazioni REB decideranno il destino di tutte le operazioni militari, attraverso un uso asimmetrico del concetto Anti-Access/Area-Denial applicato alla EW per colpire quello che la Russia considera una delle principali debolezze occidentali, l'eccessiva dipendenza derivante dall'utilizzo delle risorse spaziali in termini di comunicazioni e controllo del campo di battaglia.

La riforma delle forze REB russe ha anche beneficiato delle esperienze della guerra russo-georgiana del 2008, dove queste si dimostrarono inefficaci nel sopprimere le difese aeree georgiane, coprire le forze in avanzamento e creare zone di disturbo[132]. Dopo questa prova deludente, Mosca ha avviato un'ambiziosa campagna per modernizzare almeno il 70% dell'equipaggiamento EW in dotazione alle forze armate all' interno dello State Armaments

[129] Yuriy Lastochkin, interviewed by Viktor Khudoleyev, "Troops for the Battle in the Ether," Krasnaya Zvezda Online, 15 April 2014, da Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", MITRE Center for Technology and National Security, December 2019, pag. 66.

[130] Ibid, pag. 66.

[131] Oleg Falichev interview with Yuriy Lastochkin, "Dome over the Defense Ministry. Zaslon-REB System Blocks Any Channels of Information Leakage," VPK Voyenno-Promyshlennyy Kuryer Online, 26 April-2 May 2017, da Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", MITRE Center for Technology and National Security, December 2019, pag. 67.

[132] Roger McDermott, "Russia's Advances in Electronic Warfare Capability", The Jamestown Foundation, Eurasia Daily Monitor Volume: 16 Issue: 135, 2 October 2019.

Programme 2011-2020[133]. Di seguito sono descritti alcuni degli equipaggiamenti per la EW attualmente in dotazione alle unità REB delle forze terrestri della federazione russa[134]:

- Avotobaza. Sistema per disturbare i radar terrestri, svolgere intelligence elettronica e la ricognizione radio-tecnica;
- Brisoglebsk-2. Serve a sopprimere le componenti C2 del nemico, analizzando e raccogliendo informazioni sulle trasmissioni nemiche e generando interferenze radio;
- Dzyudoist. È in grado di bloccare i segnali dei proiettili radiocomandati, oltre a disturbare le comunicazioni cellulari ed i sistemi di navigazione;
- Filin. Jammer progettato per disabilitare i sensori ottici nemici, i telemetri laser ad infrarosso, i dispositivi di visione notturna e i sistemi di guida per i missili anticarro;
- Leer-3. Si basa su tre UAV Orlan-10 ed è dotato della capacità di disturbare le comunicazioni mobili 3G e 4G, condurre ricognizioni e trasmettere dati all'artiglieria;
- Leyer-3. Questo sistema sopprime le risorse elettroniche avversarie operanti nelle bande GSM-900 e GSM-1800;
- Lorandit-AD. Si tratta di un sistema aviolanciabile fornito alle forze aerotrasportate, con compiti di tracciamento e soppressione dei segnali di disturbo avversari;
- Krasukha-2.0. È un sistema progettato per identificare e bloccare radar terrestri e aerei, canali C2 per UAV e missili da crociera ad una distanza di 300 chilogrammi;
- Krasukha-S4. Il sistema contrasta i radar, le comunicazioni, i sistemi di trasferimento dati, radar aerei a lungo raggio ed i segnali satellitari per la guida dei missili;
- Moskva-1. Si tratta di sistema passivo per il tracciamento dei segnali radar e delle relative informazioni ad una distanza massima di 400 km, provvedendo alla loro analisi e trasmissione;
- Murmansk-BN. È utilizzato per ricognizioni elettroniche e il rilevamento di segnali radar terrestri ed aerei, disturbando i sistemi di comunicazione, navigazione e controllo a distanze comprese tra 5.000-8.000 km;

[133] "Sovremennym rossiyskim sredstvam REB pod silu 'vyrubit" tselyy polk" [Modern Russian EW means are capable of "switching off" an entire regiment], Voyennoye Obozreniye,10 December 2014.
[134] Timothy Thomas, "RUSSIA'S ELECTRONIC WARFARE FORCE", MITRE Center for Technology and National Security, September 2020, pag. 15-19.

- Palatin. Si tratta di un sistema in grado di sopprimere i sistemi di comunicazione, condurre ricognizioni elettroniche ed interrompere le comunicazioni cellulari;
- Pole-21. Il sistema dispone di moduli di soppressione e disturbo per contrastare droni e missili da crociera, oltre a sopprimere i segnali satellitari, inclusi GPS, Galileo e Beidou;
- Samarkand. Si tratta di un sistema progettato per generare interferenze e interrompere le comunicazioni e le armi di precisione dell'avversario come il Tomahawk statunitense;
- Serp. Questo sistema può contrastare sciami di piccoli droni utilizzando un sistema a microonde efficace anche contro le munizioni con sistema di guida di precisione;
- Solyaris-N. Il complesso è automatizzato e può coprire un'area di circa 80 km quadrati, attuando interferenze elettroniche contro le trasmissioni di dati ed i segnali GPS;
- Svet-KU. Questo è un sistema impiegato dalle truppe aerotrasportate ed in modalità automatica monitora i segnali radio-elettronici, li analizza e ne identifica le coordinate;
- Torn. Questo sistema è utilizzato dalle forze di pace russe. È un sistema di ricognizione mobile automatizzato che aiuta a raccogliere dati di intelligence nelle zone cuscinetto e tra le forze opposte;
- Zhitel. La stazione automatizzata disturba gli UAV a distanze superiori a 20 chilometri, bloccando anche i sistemi di guida di missili cruise e munizioni di precisione. È in grado di rilevare, tracciare e disturbare le stazioni di comunicazione satellitare e cellulare ed i sistemi di navigazione satellitare in un raggio di 20-30 chilometri.

Alla luce di quanto descritto in questo paragrafo, il divario tra le capacità russe e quelle statunitensi e della NATO nelle operazioni di REB/EW va preso seriamente. Dal 2008 Mosca ha investito notevoli risorse per ampliare le competenze e le dotazioni della specialità di nicchia costituita dalla guerra elettronica. La Russia ha inserito questo processo di sviluppo nell'ottica di avere un "abilitatore e "moltiplicatore di forza", inserendo la REB tra gli strumenti di tipo asimmetrico da impiegare per contrastare le capacità del blocco occidentale.
Lo stesso Lastochkin ha affermato l'importanza delle capacità REB per le operazioni militari russe, confermandone il ruolo di strumento asimmetrico in chiave A2/AD per colpire la critica dipendenza occidentale dalle risorse legate al dominio spaziale in termini di comunicazioni e capacità di controllo delle forze militari.

L'importanza delle forze REB russe ne fanno uno strumento dinamico che rientra nella strategia di difesa attiva, attraverso la disorganizzazione delle capacità di pianificazione e controllo del nemico, permettendo in questo modo alle forze russe di prendere l'iniziativa per contrastare e degradare la capacità avversaria di gestire efficacemente il proprio dispositivo militare.

6. CONCLUSIONI

Quando descritto all'interno di questa analisi, ha permesso di definire le origini del concetto di Anti-Aaccess/Area-Denial, da cui deriva l'acronimo A2/AD che tanto successo ha riscosso nella formulazione occidentale di una strategia di Anti-Access Warfare. Trattandosi di un'espressione scaturita dalla riflessione statunitense circa le sfide future per le forze armate statunitensi, essa si è concentrata sull'identificazione delle potenziali minacce piuttosto che sulla comprensione di come un ipotetico avversario avrebbe costruito una propria strategia di A2/AD. Il limite di questa formulazione sta appunto nel dicare molta attenzione all'analisi delle tecnologie applicabili a questa strategia piuttosto che a comprendere come tale concetto venisse adattato a contesti culturali e sociali diversi da quello statunitense.

L'approccio russo all'Anti-Access/Area-Denial, tenendo conto che tale termine non ha un suo omologo russo, non parte dal presupposto di creare una strategia A2/AD basata su di una risposta simmetrica. La formulazione di una Ant- Access Warfare parte dal presupposto che ci si sta confrontando con un avversario ritenuto superiore quantomeno in alcune specifiche capacità, una presa di coscienza che è una delle caratteristiche distintive alla base della formulazione di una simile strategia di difesa.

Da qui la formulazione da parte russa di una strategia di Difesa Attiva che, riprendendo anche alcuni concetti ed esperienze dell'epoca sovietica, non vuole precludere un determinato spazio geografico all'avversario, quanto piuttosto negargli la possibilità di condurre una campagna militare coordinata ed ordinata. L'uso coordinato di molteplici sistemi d'attacco e difesa missilistici, di artiglieria a lungo raggio e capacità di EW cerca di colpire in maniera asimmetrica le capacità critiche dell'avversario, degradando o annullando le sue capacità di C2 durante la fase di avvicinamento e schieramento.

Tale scelta deriva dall'analisi di come gli Stati Uniti e, in senso esteso anche la NATO, ha condotto negli ultimi vent'anni campagne basate sul controllo dello spazio aereo e delle rotte marittime per schierare rapidamente le truppe in un teatro operativo e fornendole di adeguato supporto di fuoco, sfruttando in maniera estesa l'accesso alle risorse spaziali per comunicazioni, raccolta informazioni e gestione del campo di battaglia.

L'oblast di Kaliningrad rappresenta un esempio di A2/AD Bubble, dato che nella piccola exclave si assiste ad una elevata concentrazione di sistemi missilistici, di artiglieria e di EW che creano un ambiente operativo esteso agli Stati baltici, alla Polonia ed al mar Baltico. Da un lato abbiamo sistemi a distanza, in profondità e con precisione infrastrutture critiche quali porti, strutture logistiche e aree di raccolta, dall'altro i sistemi SAM integrati assicurano la difesa di tali assetti pregiati, a cui si aggiunge l'uso intensivo della EW per ostacolare la rete di comando e intelligence avversaria agendo quale moltiplicatore di forze. Tale insieme di capacità offensive e difensive rappresenta un ostacolo non insuperabile ma certamente da non prendere alla leggera, la cui eliminazione richiede la presa di coscienza che si dovranno sostenere operazioni militari con tempi di esecuzione e costi incerti.

Tuttavia, l'effettiva efficacia dei sistemi missilistici e per la guerra elettronica su cui Mosca ha investito notevoli risorse nell'ultimo decennio, va affrontata con serietà ma senza sovrastimarla. Sebbene l'analisi delle capacità A2/AD russe dia l'idea di trovarsi di fronte a bolle impenetrabili ed estese per centinaia di chilometri, molti dei dati sono stimati o basati sull'analisi di fonti di parte. La portata effettiva stimata di un sistema missilistico antiaereo o antinave è spesso considerevolmente inferiore alla portata nominale massima propagandata dalla stampa[135]. Ad esempio, la differenza tra portata nominale e portata effettiva è più evidente nei sistemi SAM, specialmente contro piccoli bersagli operanti a basse altitudini. A questo va aggiunto lo scarso successo operativo di alcuni dei sistemi, ad esempio l'S-300[136] ed il Pansir-S1[137] durante l'impiego in Siria e Libia[138], mettendo in dubbio l'efficacia delle capacità russe di Anti-Access.

[135] Robert Dalsjö, Christofer Berglund, Michael Jonsson, "Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications", Swedish Defence Research Agency (FOI), March 2019, pag. 43-44.
[136] Arie Egozi, "Unanswered Israeli Air Strikes Against Syria Raise S-400 Questions", 9 June 2020.
[137] Daniel Brown, "Russian air defenses were caught on video getting beaten badly by Israeli forces in Syria - here are Russia's excuses", Business Insider, 14 May 2018, Sebastien Roblin, "Israel Kamikaze Drones are Destroying Syria's Air Defences", National Interest, 26 January 2019.
[138] Altan. A. Ozier, "Libya: A Catastrophe for Russia's Pantsir S1 Air Defense System", Real Clear Defense, 19 June 2020.

Quindi, si può affermare che la Russia attualmente non ha, in linea con la sua impostazione strategica della difesa attiva, una piena capacità A2 per negare l'accesso della NATO alla regione baltica, mentre dispone di una capacità AD per rendere pericoloso per un avversario approcciarsi, operare e rimanere nella regione compresa tra Kaliningrad e San Pietroburgo.

Gli Stati Uniti e la NATO devono predisporre e stanno implementando le opportune contromisure per difendere le capacità critiche legate alle funzioni di C2, ISR e di intelligence fornite dal dominio dello spazio, sia contro le minacce fisiche che contro quelle legate al cyber ed alla electronic warfare. Vanno anche predisposte tecnologie e modalità d'impiego delle stesse che permettano di contrastare i sistemi SAM integrati russi e la difesa contro i sistemi missilisti per attacco al suolo.

Per tale motivo, negli ultimi anni gli Stati Uniti e la NATO hanno introdotto misure per garantire una presenza militare permanente nell'Europa orientale, con particolare riferimento alla regione del Mar Baltico mediante il dislocamento di quattro battlegroups multinazionali[139], oltre alla riattivazione[140] della 41st Field Artillery Brigade in Germania nel 2018 che schiera ben 32 sistemi Multiple Launch Rocket System (MLRS)[141]. In aggiunta ai sistemi statunitensi, anche Romania[142] e Polonia[143] si doteranno di un totale di 74[144] sistemi High Mobility Artillery Rocket System (HIMARS). I Sistemi MLRS o HIMARS possono lanciare rispettivamente 12 o 6 razzi guidati nelle versioni GMLRS, GMLRS AW e ER GMLRS con una testata di circa 90 kg ad una distanza compresa tra 70 e 150 km a seconda delle versioni.[145]

In alternativa i due sistemi possono lanciare rispettivamente due o un solo razzo del tipo ATACMS, più pesante e con una testata di circa 227 km ad una distanza massima di 300km[146].

Inoltre, gli Stati Uniti stanno testando un nuovo razzo a lungo raggio compatibile con i sistemi MLRS e HIMARS, noto come Precision Strike Missile (PrSM)[147] ed accreditato di un raggio d'azione tra 60 e 499 km[148], mentre durante i test è stata raggiunta

[139] "NATO Enhanced Forward Presence", MINISTRY OF FOREIGN AFFAIRS OF THE REPUBLIC OF LATVIA, consultato il 21/05/2021.
[140] Lacey Justinger, "41st Field Artillery Brigade Returns to Germany", US Army, 30 November 2018.
[141] Brennan Deveraux, "ROCKET ARTILLERY CAN KEEP RUSSIA OUT OF THE BALTICS", War On The Rocks, 20 May 2021.
[142] Jen Judson, "Romania signs off on US deal to become first European HIMARS customer", Defense News, 28 February 2018.
[143] "Poland signs deal to buy HIMARS rocket systems from US", Radio Poland, 13 February 2019.
[144] Brennan Deveraux, "ROCKET ARTILLERY CAN KEEP RUSSIA OUT OF THE BALTICS", War On The Rocks, 20 May 2021.
[145] "Lockheed Martin's Next-Gen Precision Fires Rocket Aces Demo", Lockheed Martin, 25 March 2021.
[146] "Army Tactical Missile System", Lockheed Martin, 2020.
[147] "Precision Strike Missile (PrSM)", Lockheed Martin, 2020.
[148] Ibid.

una distanza di 400 km[149]. Con la fine del trattato INF è credibile che il sistema d'arma sarà sviluppato per incrementarne le capacità ed il raggio d'azione, mentre l'esercito statunitense prevede la sua immissione in servizio nel 2023[150]. Questi elementi devono far comprendere che in caso di conflitto aperto tra Stati Uniti e Nato da un lato e Russia dall'altro, non si deve dare per scontato che gli Stati baltici siano destinati a cadere in breve tempo, cioè in 60 ore di conflitto come ipotizzato in un wargames condotto dalla RAND Corporation[151].

Inoltre, negli Stati Uniti si sta lavorando allo sviluppo del Long Range Hypersonic Weapon (LRHW), con il primo test del missile compiuto il 19 marzo 2020[152] ed i primi elementi di una batteria sperimentale sono stati rivelati a marzo del 2021[153], mentre la gittata del nuovo missile dovrebbe essere di minimo 2,775 km [154]. Sviluppi ci sono anche nel campo della EW, dove lo stesso Armed Services Committee sostiene gli sforzi per colmare il divario accumulato in questo particolare settore[155].

Concludendo, l'approccio russo alla strategia A2/AD può essere preso da esempio per la difesa costiera e di obiettivi strategici in presenza di limitate risorse economiche, come affermato dall'Ammiraglio Foggo riguardo all'utilizzo di sistemi missilistici costieri[156]. Si tratta di una possibilità messa in atto dalla Svezia[157] e di recente attuata anche dalla Romania[158], mentre gli stessi Stati Uniti stanno svolgendo test di sistemi missilistici simili[159], che saranno adottati nei Marine Littoral Regiment (MLR)[160] e la cui entrata in servizio è prevista per il 2022[161].

---

[149] "Precision Strike Missile Completes Longest Flight to Date", Lockheed Martin, 12 May 2021.
[150] Jen Judson, "US Army's Precision Strike Missile breaks range record", Defense News, 12 May 2021.
[151] David A. Shlapak, Michael Johnson, "Reinforcing Deterrence on NATO's Eastern Flank Wargaming the Defense of the Baltics", RAND Corporation, 2016.
[152] Joseph Trevithick, "Army Shows First-Ever Footage Of New Hypersonic Missile In Flight And Impacting", The War Zone, 4 August 2020.
[153] Joseph Trevithick, "Army Delivers First Canisters To Its New Hypersonic Missile Battery But Won't Say Where It's Based", The War Zone, 19 March 2021.
[154] Joseph Trevithick, "The Army Has Finally Revealed The Range Of Its New Hypersonic Weapon", The War Zone, 13 May 2021.
[155] Mark Pomerleau, "Congress can't 'take foot off the gas' on DoD electronic warfare", C4ISRNET, 12 May 2021.
[156] Christopher Woody, "US allies worried about pricey weapons should look at what Russia's doing, the Navy's top officer in Europe says", Insider, 24 January 2020.
[157] Bruno Waterfield, "Sweden brings back Cold War weapons to deter Kremlin", The Times, 22 November 2016, "Saab unveils new anti-ship missile RBS15 Gungnir", Naval Today, 16 July 2018.
[158] Jaroslaw Adamowski, "Romanian government approves Naval Strike Missile buy", Defense News, 14 January 2021.
[159] Steven Stashwick, "US Marines Select an Anti-Ship Missile", The Diplomat, 9 May 2019.
[160] Megan Eckstein, "Marines Testing Regiment at Heart of Emerging Island-Hopping Future", USNI News, 4 june 2020.
[161] Mallory Shelbourne, "Marine Corps to Stand Up First Marine Littoral Regiment in FY 2022", USNI News, 20 January 2021.

BIBLIOGRAFIA

- Defence Science Board, "Task Force on Globalization and Security Final Report", December 1999, https://files.ethz.ch/isn13467/Globalization%20Security.pdf
- Andrew Krepinevich, Barry Watts &Robert Work, "Meeting the Anti-Access and Area-Denial Challenge", Center for Strategic and Budgetary Assessment, 2003, https://csbaonline.org/uploads/documents/2003.05.20-Anti-Access-Area-Denial-A2-AD.pdf
- Department of Defense, "Joint Operational Access Concept (JOAC)", Version 1.0, 17 January 2012, https://archive.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf
- United States Department of Defense, "Quadrennial Defense Review 2014", March 2014, https://digital.library.unt.edu/ark:/67531/metadc949810/m2/1/high_res_d/2014_Quadrennial_Defense_Review.pdf
- David A. Shlapak, Michael Johnson, "Reinforcing Deterrence on NATO's Eastern Flank Wargaming the Defense of the Baltics", RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1253.html
- Robert N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum", International Center for Defense and Security, September 2017, https://euagenda.eu/upload/publications/untitled-135826-ea.pdf
- Sam J. Tangredi, "Antiaccess Warfare as Strategy", Naval War College Review, Volume 71, Number 1 Winter 2018, https://digital-commons.usnwc.edu/nwc-review/vol71/iss1/4/
- OSW Team, "Fortress Kaliningrad", Centre for Eastern Studies (OSW), October 2019, https://www.osw.waw.pl/sites/default/files/Report_Fortress_Kaliningrad_net_0.pdf
- Robert Dalsjö, Christofer Berglund, Michael Jonsson, "Bursting the Bubble. Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications", Swedish Defence Research Agency (FOI), March 2019, file:///C:/Users/lesti/Downloads/FOIR4651%20(4).pdf
- Timothy Thomas, "Russian Combat Capabilities for 2020: Three Developments to Track", December 2019, https://www.armyupress.army.mil/Portals/7/Legacy-Articles/documents/Thomas-

Russian-Combat-Capabilities.pdf

- Timothy Thomas, "RUSSIA'S ELECTRONIC WARFARE FORCE: BLENDING CONCEPTS WITH CAPABILITIES", MITRE Center for Technology and National Security, September 2020, https://www.mitre.org/sites/default/files/publications/pr-19-2714-russias-electronic-warfare-force-blending-concepts-with-capabilities.pdf
- Konrad Muzyka, Rochan Consulting, "Russian Forces in the Western Military District", Center for Naval Analyses, December 2020, https://www.cna.org/research/2020
- Jonas Kjellén, "The Russian Baltic Fleet", Swedish Defence Research Agency (FOI), February 2021, https://www.foi.se/report-summary?reportNo=FOI-R--5119--SE

ARTICOLI

- "S-400 Triumph Air Defence Missile System", Army Technology, https://www.army-technology.com/projects/s-400-triumph-air-defence-missile-system/
- "9K330 Tor", WEAPONSYSTEMS.NET, https://weaponsystems.net/system/53-9K330+Tor
- "Tor M2 Surface-to-Air Missile (SAM) System", Army Technology, https://www.army-technology.com/projects/tor-m2-surface-to-air-missile-sam-system/#:~:text=The%20Tor%2DM2%20air%20defence,air%20defence%20in%20jamming%20environments.
- "Iskander-M (SS-26)", Missile Defense Advocacy Alliance, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/iskander-m-ss-26/
- "SS-N-26 "Strobile" (P-800 Oniks)/ Yakhont / Yakhont-M / Bastion (launch systems)", Missile Threat, Center for Strategic and International Studies, https://missilethreat.csis.org/missile/ss-n-26/
- "3K55 Bastion", Weaponsystems.net, https://old.weaponsystems.net/weaponsystem/DD06%20-%203K55%20Bastion%20(SS-C-5%20Stooge).html
- "Kh-35", military-today.com, http://www.military-today.com/missiles/kh_35.htm
- "3K60 Bal", Weaponsystems.net, https://weaponsystems.net/system/140-3K60+Bal

- "Smerch", ROSOBORONEXPORT, http://roe.ru/eng/catalog/land-forces/missile-systems-multiple-rocket-launchers-mrl-atgm-systems-and-field-artillery-guns/smerch-s-bm-9a52-2/
- Smerch Multiple Launch Rocket System, Military-Today.com, http://www.military-today.com/artillery/smerch.htm
- "Sovremennym rossiyskim sredstvam REB pod silu 'vyrubit" tselyy polk" [Modern Russian EW means are capable of "switching off" an entire regiment], Voyennoye Obozreniye,10 December 2014, https://topwar.ru/64421-sovremennym-rossiyskim-sredstvam-reb-pod-silu-vyrubit-celyy-polk.html
- Small Arms Survey, "Guided Mortar Systems", Number 51, April 2015, http://www.smallarmssurvey.org/about-us/highlights/highlights-2015/highlight-rn51.html
- Christopher P. Cavas, "Is Caspian Sea Fleet a Game-Changer?" Defense News, 11 October 2015, https://www.defensenews.com/naval/2015/10/11/is-caspian-sea-fleet-a-game-changer/
- "SS-26 Iskander", Missile Threat, Center for Strategic and International Studies, 27 September 2016, https://missilethreat.csis.org/missile/ss-26-2/
- "S-400 Triumf Air Defense System", Missile Defense Advocacy Alliance, June 2016, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/russia-anti-access-area-denial/s-400-triumf-air-defense-system/
- Dominik P. Jankowski, Makysmilian Cziperski, "NATO's Strategic 'Six Pack' to Counter Russia's Anti-Access/Area Denial Capability", The 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
- Bruno Waterfield, "Sweden brings back Cold War weapons to deter Kremlin", The Times, 22 November 2016, https://www.thetimes.co.uk/article/sweden-puts-cold-war-missiles-back-into-service-w8sl9hsgf
- Tomasz Smura, "Russian Anti-Access Area Denial A2AD Capabilities – Implications for NATO", Pulaski Policy Paper, 27 November 2016, https://pulaski.pl/en/russian-anti-access-area-denial-a2ad-capabilities-implications-for-nato/

- "3M-14 Kalibr (SS-N-30A)", Missile Defense Advocacy Alliance, May 2017, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/ss-n-30a-kalibr/
- "S-400 Triumf", Missile Threat, Center for Strategic and International Studies, 4 May 2017, https://missilethreat.csis.org/defsys/s-400-triumf/
- "S-300", Missile Threat, Center for Strategic and International Studies, 4 May 2017, https://missilethreat.csis.org/defsys/s-300/
- "Pantsir S-1", Missile Threat, Center for Strategic and International Studies, 4 May 2017, https://missilethreat.csis.org/defsys/pantsir-s-1/
- "P-800 Oniks (SS-N-26 Strobile)", Missile Defense Advocacy Alliance, June 2017, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/16962-2/
- "KH-35 (SS-N-25 Switchblade)", Missile Defense Advocacy Alliance, June 2017, https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/kh-35-ss-n-25-switchblade/
- "S-300V Air and Missile Defense System", Missile Defense Advocacy Alliance, December 2017,
- https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/russia/russia-anti-access-area-denial/s-300v-air-and-missile-defense-system/
- Zdzislaw Sliwa, "KALININGRAD OBLAST AS THE FORWARD ANTI-ACCESS/ AREA DENIAL HUB", Baltic Defence College, Security Forum Volume 2, No 2, 2018, https://www.baltdefcol.org/?id=1569
- Jen Judson, "Romania signs off on US deal to become first European HIMARS customer", Defense News, 28 February 2018, https://www.defensenews.com/land/2018/03/01/romania-signs-off-on-deal-to-become-first-european-himars-customer/#:~:text=WASHINGTON%20%E2%80%94%20Romania%20signed%20a%20letter,the%20first%20European%20HIMARS%20customer.
- "Radiotekhnicheskie podrazdeleniia PVO Baltiiskogo flota provodiat ucheniia pod Kaliningradom", Tass, 26 March 2018, https://tass.ru/armiya-i-opk/5067688

- Daniel Brown, "Russian air defenses were caught on video getting beaten badly by Israeli forces in Syria - here are Russia's excuses", Business Insider, 14 May 2018, https://www.businessinsider.com/russia-explains-why-its-air-defenses-were-beaten-by-israel-in-syria-2018-5?IR=T
- Ionut Alin Cirdei, "A2AD Concept in the Modern Security Environment", 24th International Conference KNOWLEDGE-BASED ORGANIZZATION, Vol XXIV, 1 June 2018, file:///C:/Users/lesti/Downloads/A2ADConceptintheModernSecurityEnvironment%20(1).pdf
- "Saab unveils new anti-ship missile RBS15 Gungnir", Naval Today, 16 July 2018, https://www.navaltoday.com/2018/07/16/saab-unveils-new-anti-ship-missile-rbs15-gungnir/
- Lacey Justinger, "41st Field Artillery Brigade Returns to Germany", US Army, 30 November 2018, https://www.army.mil/article/214491/41st_field_artillery_brigade_returns_to_germany
- Aziz Erdogan, "Russian A2AD Strategy and Its Implications for NATO", Beyond the Horizon, 6 December 2018, https://behorizon.org/russian-a2ad-strategy-and-its-implications-for-nato/
- "Poland signs deal to buy HIMARS rocket systems from US", Radio Poland, 13 February 2019, http://archiwum.thenews.pl/1/12/Artykul/406288,Poland-signs-deal-to-buy-HIMARS-rocket-systems-from-US#:~:text=Poland%20on%20Wednesday%20signed%20a,of%20a%20military%20modernisation%20drive.
- Sebastien Roblin, "Israel Kamikaze Drones are Destroying Syria's Air Defences", National Interest, 26 January 2019, https://nationalinterest.org/print/blog/buzz/israel-kamikaze-drones-aredestroying-syria%E2%80%99s-air-defenses-42592
- Keir Giles Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, https://press.armywarcollege.edu/parameters/vol49/iss1/4/
- Valery Gerasimov, speech given at the Annual Meeting of the Academy of Military Science, Moscow, 2, MEMRI, 14 March 2019, https://www.memri.org/reports/russian-

first-deputy-defense-minister-gerasimov-our-response-based-active-defense-strategy

- Keir Giles Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined", United States Army War College Press, 1 March 2019, https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2860&context=parameters
- Steven Stashwick, "US Marines Select an Anti-Ship Missile", The Diplomat, 9 May 2019, https://thediplomat.com/2019/05/us-marines-select-an-anti-ship-missile/
- Sergey Sukhankin, "David vs. Goliath: Kaliningrad Oblast as Russia's A2/AD 'Bubble'", Scandinavian Journal of Military Studies, 21 August 2019, https://sjms.nu/articles/10.31374/sjms.20/
- Michael Kofman, "IT'S TIME TO TALK ABOUT A2/AD: RETHINKING THE RUSSIAN MILITARY CHALLENGE", War on The Rocks, 5 Semptember 2019, https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/
- "Army Tactical Missile System", Lockheed Martin, 2020, https://www.lockheedmartin.com/content/dam/lockheed-martin/mfc/documents/business-area-landing/mfc-Fast-Facts-ATACMS.pdf
- "Precision Strike Missile (PrSM)", Lockheed Martin, 2020, https://www.lockheedmartin.com/content/dam/lockheed-martin/mfc/documents/prsm/mfc-prsm-fact-sheet.pdf
- "Tor (SA-15 Gauntlet)", Missile Threat, Center for Strategic and International Studies, 10 January 2020, https://missilethreat.csis.org/defsys/tor/
- Christopher Woody, "US allies worried about pricey weapons should look at what Russia's doing, the Navy's top officer in Europe says", Insider, 24 January 2020, https://www.businessinsider.com/foggo-allies-worried-about-weapons-should-look-at-russia-a2ad-2020-1?IR=T
- Sebastien Roblin, "Why Russia's Bastion-P Truck-Launched Anti-Ship Missiles Could Be a Real Killer", The National Interest, 8 February 2020, https://nationalinterest.org/blog/buzz/why-russia%E2%80%99s-bastion-p-truck-launched-anti-ship-missiles-could-be-real-killer-121551

- Patrick Smith, "Russian Electronic Warfare", American Security Project, April 2020, https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf
- Megan Eckstein, "Marines Testing Regiment at Heart of Emerging Island-Hopping Future", USNI News, 4 june 2020, https://news.usni.org/2020/06/04/marines-testing-regiment-at-heart-of-emerging-island-hopping-future
- Arie Egozi, "Unanswered Israeli Air Strikes Against Syria Raise S-400 Questions", 9 June 2020, https://breakingdefense.com/2020/06/unanswered-israeli-air-strikes-against-syria-raise-s-400-questions/
- Altan. A. Ozier, "Libya: A Catastrophe for Russia's Pantsir S1 Air Defense System", Real Clear Defense, 19 June 2020, https://www.realcleardefense.com/articles/2020/06/19/libya_a_catastrophe_for_russias_pantsir_s1_air_defense_system_115394.html
- Joseph Trevithick, "Army Shows First-Ever Footage Of New Hypersonic Missile In Flight And Impacting", The War Zone, 4 August 2020, https://www.thedrive.com/the-war-zone/35369/army-shows-first-ever-footage-of-new-hypersonic-missile-in-flight-and-impacting
- John R. Hoehn, "Defense Primer: Electronic Warfare", Congressional Research Service, 29 October 2020, https://fas.org/sgp/crs/natsec/IF11118.pdf
- Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence", The RUSI Journal, 5 November 2020, https://rusi.org/publication/rusi-journal/missiles-vessels-and-active-defence-what-potential-threat-do-russian-armed
- Jaroslaw Adamowski, "Romanian government approves Naval Strike Missile buy", Defense News, 14 January 2021, https://www.defensenews.com/global/europe/2021/01/14/romanian-government-approves-naval-strike-missile-buy/
- Dan McCormick, "Allied A2AD in the Black Sea", Middle East Institute, 19 January 2021, https://mei.edu/publications/allied-a2ad-black-sea

- Mallory Shelbourne, “Marine Corps to Stand Up First Marine Littoral Regiment in FY 2022”, USNI News, 20 January 2021, https://news.usni.org/2021/01/20/marine-corps-to-stand-up-first-marine-littoral-regiment-in-fy-2022
- Joseph Trevithick, “Army Delivers First Canisters To Its New Hypersonic Missile Battery But Won't Say Where It's Based”, The War Zone, 19 March 2021, https://www.thedrive.com/the-war-zone/39851/army-delivers-first-canisters-to-its-new-hypersonic-missile-battery-but-wont-say-where-its-based
- “Lockheed Martin’s Next-Gen Precision Fires Rocket Aces Demo”, Lockheed Martin, 25 March 2021, https://www.lockheedmartin.com/content/dam/lockheed-martin/mfc/documents/guided-mlrs-unitary-rocket/ER-GMLRS-Flight-Test-March-25-2021-fast-fact-3.pdf
- Mark Pomerleau, “Congress can’t ‘take foot off the gas’ on DoD electronic warfare”, C4ISRNET, 12 May 2021, https://www.c4isrnet.com/electronic-warfare/2021/05/12/congress-cant-take-foot-off-the-gas-on-dod-electronic-warfare/?utm_medium=social&utm_campaign=Socialflow+C4&utm_source=facebook.com&fbclid=IwAR2N5c-hy1O3xncPL9h-Ltdxv-48TzsYY4a_HneiZoe6fo_QfNdbaBFcK10
- Jen Judson, “US Army’s Precision Strike Missile breaks range record”, Defense News, 12 May 2021, https://www.defensenews.com/land/2021/05/12/armys-precision-strike-missile-breaks-range-record/?utm_source=twitter.com&utm_campaign=Socialflow+DFN&utm_medium=social&fbclid=IwAR1ikEadGkgvOPaF19mi4rJ6p5GEOv8HKOciVDPzk45v3Ncr7P6KrydngsU
- “Precision Strike Missile Completes Longest Flight to Date”, Lockheed Martin, 12 May 2021, https://news.lockheedmartin.com/precision-strike-missile-completes-longest-flight-to-date?_ga=2.200546926.1995867400.1621630601-1406311823.1621630601

- Joseph Trevithick, “The Army Has Finally Revealed The Range Of Its New Hypersonic Weapon”, The War Zone, 13 May 2021, https://www.thedrive.com/the-war-zone/40584/the-army-has-finally-revealed-the-range-its-new-hypersonic-weapon?fbclid=IwAR3WF0MrCjYfQRLcWQJ-XDUvCi8MgMknFwffls3hZ0VD6ayf8f7hltPIn78
- Brennan Deveraux, “ROCKET ARTILLERY CAN KEEP RUSSIA OUT OF THE BALTICS”, War On The Rocks, 20 May 2021, https://warontherocks.com/2021/05/rocket-artillery-can-keep-russia-out-of-the-baltics/?fbclid=IwAR1nqzKp9OauoK3tTnlScJjkjzvrSnAnd9iFmMNrlqtkv8AGpYBfVnXJOVo
- “NATO Enhanced Forward Presence”, MINISTRY OF FOREIGN AFFAIRS OF THE REPUBLIC OF LATVIA, https://www.mfa.gov.lv/en/policy/security-policy/nato-enhanced-forward-presence#:~:text=USA%20%E2%80%93%20in%20Poland.-,NATO's%20enhanced%20Forward%20Presence%20in%20the%20Baltic%20States%20and%20Poland,of%20Ukraine%20and%20the%20increased