

# Countering Electronic Warfare Undermatch in the European AOR

---

CW4 Jeff Elwell (United States Army Special Operations Command)

\* The views expressed are the authors' and do not represent official NDU, DOD, or USG positions.

The overall classification of this presentation is **UNCLASSIFIED**

# Overview

- With return of great power competition, SOF must adapt after decades of conducting CT/COIN to compete with near-peer adversaries like Russia and China.
  - This is *not* a suggestion that SOF divest of the CT/COIN mission
- Russian advances in electronic warfare (EW) and anti-access and area denial (A2AD) create a capability overmatch
  - Demonstrated will to employ = deterrence (Syria, E. Europe)
  - One factor in a multi-domain/multi-threat world
  - Place U.S. and our allies at a disadvantage in event of conflict
- To regain competitive edge, SOF must adapt to guarantee communications surety in conflict with Russia

# Agenda

- Electronic warfare (EW) definitions
- How we got here: U.S. vulnerabilities
- Russian EW/A2AD
- Implications for USSOF
- Countering EW Undermatch

# Electronic Warfare

- Defined as: “military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.”

*DoD Dictionary of Military and Associated Terms*

- Three Categories:
  - Electronic Attack- degrade, neutralize, or destroy enemy combat capability (ex: counter-IED, jamming, GPS spoofing, antiradiation missiles)
  - Electronic Protection- protection of friendly forces from enemy electronic attack (ex: spectrum management, TTPs)
  - Electronic Warfare Support- identifying and locating sources of enemy electromagnetic emissions (ex: direction finding)

# How we got here

- Absence of near-peer threats following the end of the Cold War
  - U.S. considerable technological advantage: dominance of airspace and electromagnetic spectrum
  - Focus on CT/COIN: VEOs and rogue regimes lack sophisticated EW caps = divestment of EW caps
- DoD developed comms system utilizing SATCOM as its backbone: data transfer rate, difficulty in disrupting the signals.
  - C4ISR largely satellite-based due to a lack of threats
  - Mission command systems: DCIGS, FBCB2



Source: coloradospacenews.com



Source: Army.mil

# U.S. Vulnerabilities

- Over-reliance on SATCOM = strategic vulnerability
  - Easily exploited in a conflict with near-peer adversary
- Overall loss of institutional knowledge in electronic protection—IEDs, FOBs
- Reliance on GPS for navigation, blue force tracking, and precision-guided munitions
- Return of great-power competition: re-focus on EW



Source: [gdmisionsystems.com](http://gdmisionsystems.com)



Source: Nat'l AF Museum

# Modernization of the Russian Armed Forces

- EW a key component of Soviet military doctrine—atrophied following the end of the Cold War
- In 2004, the Russian military began to modernize after years of neglect
  - Investing in technologies that exploit U.S. weaknesses: EW, anti-satellite weapons, and anti-access and area denial (A2AD)
  - 2008 Russia-Georgia War highlighted importance of EW in a combined arms fight
  - Integration of EW down to the brigade-level
- Anti-satellite technology (missiles, lasers, and jammers) = ability to deny U.S. SATCOM

# Russian EW

- Component of “hybrid warfare”
  - Disrupted Ukrainian comms in Crimea (radio and cell)
- Employment
  - Eastern Ukraine- ISO Russian-separatists
  - Syria- ISO Syrian Regime
  - Against NATO aircraft and exercises
- Tactics
  - Geolocate forces for delivery of fires
  - Deny communications
  - Delivery of messaging ISO influence operations (cellular network)
  - Jamming of SATCOM
  - GPS spoofing: NATO Exercise TRIDENT JUNCTURE 2018

Shipovnik-AERO EW System



Source: Kienthuk.net

Leer-2 EW System



Source: defense.pk

Orlan-10 UAV



Source: eng.mil.ru



# Component of A2AD

- Integrated with Air defense, intermediate range ballistic missiles, and anti-ship missiles
- Protect critical assets
  - Jamming radar
  - Geolocate enemy emissions
  - Spoofing GPS to protect against guided munitions
- All of Baltics, half of Poland, and most of the Baltic Sea under the A2AD “bubble”
- Difficult to penetrate by all but 5<sup>th</sup> Gen aircraft
- **Cannot guarantee air superiority, let alone air dominance!**



Source: CSBA

# Proliferation of EW

- Russia is exporting its advanced A2AD technology to other countries
  - China, India, **Turkey**, **Saudi Arabia**
  - Implications of **strategy to undermine U.S. allies and NATO Alliance?**
  - Relative importance to strategic approach is changing!
- Propagates this capability to other potential adversaries as well.
- Military cooperation with China: potential for collaboration in development of EW

# The limits of Russian EW overmatch

- Robust capability; however, Russian EW is often over-emphasized or exaggerated
  - Can't jam everything: they must communicate as well
  - Jamming exposes the jammer, making it vulnerable to attack
  - There are a finite number of EW systems— well protected
- Potential to create a comms degraded environment, but not denied
  - Loss of SATCOM would be a considerable hinderance, but would only occur in conventional war
    - Attack U.S. strategic asset = Vertical escalation
    - Need to manage escalation is still there
  - Irregular Warfare against Russian-backed forces: expect similar experience to Syria – significant impact on ops, but U.S. forces developed work arounds (PACE plan)
- The more Russia is employing EW in Ukraine and Syria, the more we learn about their capability: develop counters

# Implications for SOF

- With a return of great-power competition, SOF is integral in countering Russian aggression and will play a critical role in any future conflict
  - Irregular Warfare or a conventional fight
- SOF cannot continue to operate under the same assumptions that its communications are guaranteed
- Impact on C4ISR/ Mission Command
  - Jamming, geolocation, GPS spoofing, cyber attacks
  - Loss of SOF enablers (ISR)
  - Targeting of SOF teams

# Irregular Warfare

- Russian-backed or equipped proxy forces possess the capability to affect SOF communications, and to impede **partner comms**
  - Ex: Russian-Separatists in E. Ukraine, Syrian Regime Forces
- Impact on SOF Ops
  - RF and GPS jamming
  - Disruption of UAVs
  - Geolocation for kinetic strike/delivery of IO
  - SATCOM could experience jamming = minimal impact on mission command

# SOF support to a conventional fight with Russia in Eastern Europe

- Because of the potential for any conflict w/ Russia to escalate to a nuclear exchange, this is a **worst-case scenario**
  - SOF must be prepared for that eventuality
  - SOF role will involve full spectrum of SOF operations in support of the greater conventional fight
  - Support to resistance and enabling joint fires to degrade Russian A2AD
- SOF will be expected to operate forward of the front lines, potentially deep in Russian-controlled rear areas for extended periods
  - In these denied areas, Russian security forces will likely dominate the EW environment with the ability to jam communications or geolocate SOF teams.
  - Significant threat to SOF C4ISR with the loss of SATCOM and the integration of EW across Russian military formations
  - Lack of support: A2AD will severely impact delivery of precision fires, logistical support, and MEDEVAC



Source: dailymail.co.uk



# Changing the Mission Command paradigm

- Expectation management
- Changing the paradigm developed conducting CT/COIN in GWOT to contend with rapidly changing battlefield of future
  - Detailed planning, mission orders, and commander's intent
- Reflected in training/exercises
  - **Content:** Less = more = less vulnerable
    - Fixed text formats
    - Push-pull, DOWNREP
  - **Competency:** acquisition training → collective tng → major exercises
  - **Training modules:** develop muscle memory/institutional knowledge



Source: army.mil



Source: afcea



# Conclusion

- Russia currently enjoys an overmatch regarding EW
- Modernizing current C4ISR, employing good TTPs, and incorporating EW into SOF will reduce U.S. undermatch
  - Demonstrate U.S. caps: exercises and messaging
  - Undermine Russian confidence in deterrence effect of A2AD
  - Bolster U.S./Allied confidence of ability to operate w/in Russian A2AD
- Provide a more level playing field to counter Russian aggression

