JINSA
The Jewish Institute for National Security of America

U.S. Should Invest In Electronic Warfare As Adversaries Advance

Yoni Tobin
Policy Analyst

Ari Cicurel
Assistant Director of Foreign Policy

U.S. adversaries—China, Russia, and Iran—have recently demonstrated that they are developing and using increasingly more sophisticated electronic warfare (EW) capabilities. As "our most advanced adversaries have done their best to rapidly evolve," according to Chairman of the Joint Chiefs of Staff General Charles Q. Brown, the military has "lost some muscle memory" in the EW domain. To regain the advantage in this important form of warfare, the United States should explore including Israel, a world leader in electronic warfare research and development, in existing and new initiatives to bridge the capabilities gap. As part of these initiatives, the United States should also attempt to integrate other Middle East partners seeking to enhance their own electronic warfare readiness.

What Happened?

- On September 27, vessels belonging to Iran's Islamic Revolutionary Guard Corps Navy pointed lasers, a form of electronic warfare (EW), at a U.S. Marine Corps AH-1Z Viper operating in the Arabian Gulf, which the U.S. military called "unsafe, unprofessional, and irresponsible." The last known case of Iranian naval forces directing lasers at a U.S. helicopter was in 2017.

- On August 25, Russia claimed it used EW to bring down thirty-three Ukrainian drones at once, an unverified figure on par with Ukrainian assessments.

- Also on August 25, Iran announced it was conducting an EW drill, among the only such drills it has held, involving its ground, naval, and air forces, and air defense systems.

    - The drills consisted of domestically produced manned and unmanned fighter aircraft, drones, miniaturized drones, and radars, and simulated EW capabilities against mock targets such as combat drones, fighter aircraft, and helicopters.

- China reportedly engaged in a large-scale EW campaign during U.S. Speaker of the House Nancy Pelosi's visit to Taiwan last August, including conducting EW surveillance and signals monitoring of Pelosi's aircraft.

Why Is It Important?

- U.S. adversaries' growing capabilities in the EW domain pose an increasing threat to the United States, as control of the electromagnetic spectrum—which is used to transmit radio communications and satellite data—impacts virtually all components of military operations. According to the Defense Department's inaugural Electromagnetic Spectrum Superiority Strategy, a lack of U.S. dominance in the EW domain "jeopardizes the U.S. military's ability to sense, command, control, communicate, test, train, protect, and project force effectively."

  - » Enhanced EW capabilities are almost certain to embolden an increasingly provocative China, an actively expansionist Russia, and an ever-more belligerent Iran on the precipice of a nuclear weapons capability.

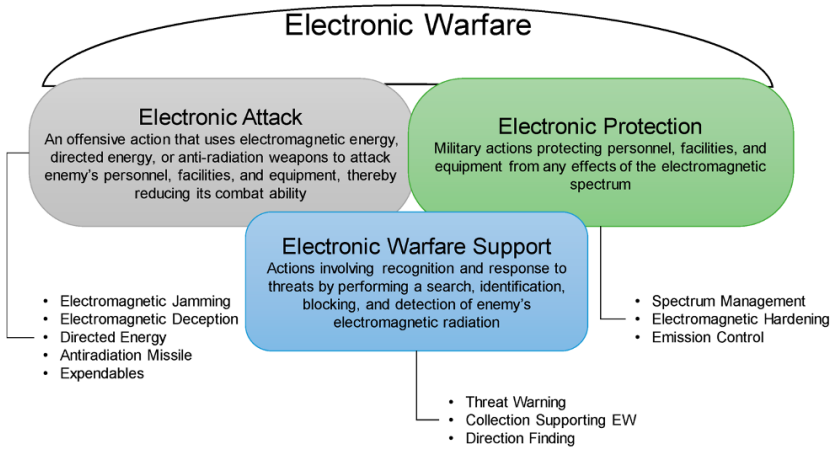
  - » U.S. investment in high-end EW reportedly waned after the end of the Cold War, with renewed attention to the subject only having arisen in recent years due to increasing tensions with Russia and China and an erosion of U.S. EW readiness.

- Chairman of the Joint Chiefs of Staff General Charles Q. Brown stated in July that EW is often conceptualized "as a supporting effort" but "in modern warfare, [EW] may be the main effort to achieve the desired strategic effects."

  - » The U.S. Electromagnetic Defense Task Force wrote in a 2019 report that unless the United States and its allies dominate in the EW domain, the United States "faces almost impossible odds of winning" future wars.

  - » The applications of EW are wide-ranging, but typically involve the use of the electromagnetic spectrum to either interfere with an adversary's radars and drones, and potentially other platforms including air defense systems, computer networks, communications systems, and projectiles, or to defend one's own assets from EW sabotage.

  - » The use of EW also frequently includes spoofing signals to deceive the adversary, and the disruption or manipulation of internal adversary communications.



Source: Department of Defense, Joint Publication 3-13.1, Electronic Warfare, February 2012.

- EW plays an increasingly important role in China's regional expansionism and competition with the United States.
  - » China's efforts to surveil U.S. leaders with EW are aimed at boosting "deterrence" against the United States, according to a PLA general.
  - » According to Taiwanese defense analysts, China has heavily utilized EW aircraft to try to interfere with Taiwan's air defense systems and feed them erroneous information.
    - – Of the 544 PLA air intrusions into Taiwan's Air Defense Identification Zone between January and September 2021, 99 of them, or 18 percent, were EW aircraft including the J-16D and the Y-8 and Y-9 aircraft, according to Taiwan's Institute for National Defense and Security Research (INDSR).
    - – China's EW flights purportedly are aimed at neutralizing or spoofing Taiwan's radar systems and would almost certainly be utilized in a Chinese invasion.
  - » China also has stationed EW platforms on its various outposts in the South China Sea, allowing it to intercept radio and satellite communications of U.S. regional partners across a broad swathe of the Indo-Pacific, including reportedly as far south as Malaysia and Indonesia.
- Iran, the most dangerous adversary in the Middle East for the United States and its regional partners, has an increasingly sophisticated EW program.
  - » Iran's August EW drills were the first dedicated exclusively to EW since 2017 and reportedly involved advanced tactics such as simulating radar detection and data disruption.
  - » Iran is one of only a handful of non-NATO countries, including China, North Korea, and Russia, with the capacity to spoof GPS data, and has demonstrated these capabilities to trick commercial vessels into traveling into Iranian waters and allegedly to capture a U.S. military drone.
- Russia has deployed advanced EW capabilities in the ongoing war in Ukraine, complicating the Ukrainian counteroffensive.
  - » The Ukrainian air force's spokesperson, Yuriy Ignat, stated in July that Russia was "far ahead" of Ukraine in the EW domain, and Russia has reportedly used its EW systems to send Ukraine's Joint Direct Attack Munition glide munitions and other projectiles off course.
  - » As of May, according to high-ranking Ukrainian military officials, Russia has been downing an average of 10,000 Ukrainian drones a month and has stationed EW systems every six miles along the war's frontline.
- The United States has also developed platforms that use cutting-edge EW technologies.
  - » Earlier this month, the U.S. Air Force unveiled the new EC-37B Compass Call EW aircraft, capable of jamming adversary communications, radar, navigation, and air defense systems. The EC-37B can operate at approximately double the altitude and speed of its predecessor, the decades-old EC130 EW aircraft.

  - The U.S. Navy has plans to incorporate large, unmanned vessels with EW capacities across its fleet, likely including the Fifth Fleet's area of responsibility and Task Force 59.

- However, the U.S. military's own EW preparedness has eroded relative to the growing threats, and Gen. Brown testified in July that the U.S. military had "lost some muscle memory" in the EW domain.
  - Russia utilized EW in 2018 during the Syrian Civil War to successfully jam U.S. surveillance and tactical drones, rendering them inoperable and possibly even causing them to crash.
    - U.S. officials revealed that Russian EW jamming was very sophisticated, and overrode the drones' electronic countermeasures, including signal encryption.
  - In 2021, in part to address the growing EW threat from pacing challenge China, the Pentagon created the 350th Spectrum Warfare Wing, responsible for Air Force EW readiness.
    - However, its unit commander said in April that the unit has a shortage of civilian and military personnel, talent, and facilities.
  - Under Secretary of the Army Gabe Camarillo remarked in July 2022 that a lack of EW readiness "keeps me up at night."
- Meanwhile, Israel has developed innovative EW capabilities in addition to looking to purchase U.S.-made platforms.
  - Israel has agreed to purchase KC-46A aircraft from the United States, which would provide significantly greater EW capabilities over its current fleet of Ram tankers that are over fifty years old. However, it is not set to receive its first KC-46A until 2025.
    - The Air Force's KC-46A aircraft refueling tankers utilize spoof-resistant MAGR2K positioning systems to counter electromagnetic interference, which could potentially alter or neutralize its communications and radar systems.
  - Israel's state-owned Israel Aerospace Industries (IAI), in 2021, unveiled its suite of Scorpius EW platforms, which have potential applications in the West's efforts to stymie Russia's offensive in Ukraine as well against other adversaries.
    - The Scorpius-G is a mobile, ground-based EW system capable of non-kinetically intercepting combat drones, such as the Iranian-supplied Shahed combat drones that have featured prominently in Russia's campaign against Ukraine.
    - Importantly, the Scorpius-G employs Israeli-produced ELTA Active Electronically Scanned Array (AESA) radar technology, enabling early detection and countering of massive drone attacks, even in electromagnetically dense environments.

- The Scorpius-N, the sea-based version of the platform, is capable of creating an "electronic dome of protection" against threats to naval vessels like Iranian drones and is resistant to EW jamming and spoofing.

- In addition, the Scorpius-EJ version, a jammer which counteracts adversary EW surveillance campaigns along mission flight paths, such as the one China reportedly engaged in during Speaker of the House Pelosi's visit, could be utilized in U.S. military flights in the Indo-Pacific.

» An Israeli EW technology, the EnforceAir counter-drone platform, was used in September 2021 to neutralize a rogue drone in the vicinity of an outdoor Mass attended by Pope Francis in Slovakia.

- The Israeli technology firm D-Fend Solutions announced that, using EnforceAir, it had been able to remotely take control of the unidentified drone and return it to its original takeoff site.

- EnforceAir not only detected the presence of the previously undetected drone, potentially averting an attack on the Pope or the estimated 60,000 attendees, but also negated the need for a conventional jammer, which could have disrupted security operations.

• Recognizing its EW vulnerability gaps, the United States has already begun coordinating with allies and partners to enhance EW readiness against shared threats as part of the Department of Defense's Electromagnetic Spectrum Superiority Strategy.

» An ongoing multilateral effort to bolster EW readiness is NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), launched in April 2022 to boost cooperation in emerging technologies, including electromagnetic spectrum and directed energy research.

- DIANA's research in the EW sphere, which incorporates academic research and private sector investment, utilizes over 100 research and development centers across NATO alliance countries.

- On August 31, NATO announced three DIANA pilot programs to address energy needs, intelligence collection issues, and information sharing.

» Bahrain and Jordan host regional hubs as part of the U.S. Fifth Fleet's Task Force 59 (TF59), which employs small unmanned naval vessels that use EW in the Middle East's waterways for intelligence, surveillance, and reconnaissance (ISR) purposes.

- TF59's unmanned systems primarily use sensors to increase maritime domain awareness, though Fifth Fleet spokesman Timothy Hawkins noted in January that these systems could also be used as offensive EW assets.

- TF59's platforms, including unmanned surface vehicles like the MANTAS T-12, can support operations by jamming, spoofing, or otherwise interfering with Iranian unmanned explosive-laden boat attacks and, unlike manned ships, can easily avoid detection.

» The United States and United Kingdom have a strong EW partnership that includes joint drills at the Spadeadam Electronic Warfare Tactics Range in England, the only NATO facility in Europe that simulates EW real-world settings and involves joint interoperability between member states.

- Israeli pioneering in the EW domain presents opportunities for the United States to bridge its EW readiness gap, as both countries seek to further cultivate their EW capabilities against growing threats.
  - Congress is exploring passage of the United States–Israel Future of Warfare Act of 2023, which would establish a $50 million annual fund through 2028 for joint research into emerging technologies including EW.
  - In 2019, Congress authorized the U.S.–Israeli Counter Unmanned Aerial Systems program, which now also includes research into directed energy weapons, after the authorization was modified in the FY2023 NDAA. The modification extended the program through the end of 2026 and raised annual funding to $40 million.

What Should the United States Do Next?

- The United States should explore increasing funding for the U.S.-Israeli Counter Unmanned Aerial Systems program, extending the program past 2026, and expanding its scope to include electromagnetic spectrum research and countering naval or ground-based unmanned threats.
- The United States should explore possible avenues for Israeli collaboration with existing Department of Defense initiatives, including cooperation between:
  - The U.S. Joint Electromagnetic Spectrum Operations Center and the IDF's EW center that could be modeled on the successful U.S.-U.K. bilateral EW research relationship, and
  - The U.S. 350th Spectrum Warfare Wing and the Israeli Air Force's EW personnel and researchers on ways to address mutual threats through EW advances.
- The United States should explore ways to integrate Israel's EW advances into a broader architecture of EW readiness enhancement in the Middle East.
  - One option is the formation of a "Middle East DIANA" modeled on NATO's DIANA emerging technologies collaborative forum, which should involve other countries in the Middle East that have begun to bolster their EW capabilities, such as Saudi Arabia and the UAE, as well as any other willing participants.
  - Israel's Scorpius-N system, if deployed by the U.S. Fifth Fleet in its freedom of navigation operations or by regional partners, could protect commercial vessels against both conventional and unconventional threats from Iran.
  - As JINSA has previously recommended, the United States should look to integrate Israeli capabilities into TF59's operations.
    - Israeli advances could further enhance TF59's ISR capabilities. Israel's state-owned IAI revealed a prototype of an unmanned submarine in May, which would enhance TF59's ability to detect threats such as Iranian naval mines and other threats to global shipping.