Jam. Bomb. Hack? New U.S. Cyber Capabilities and the Suppression of Enemy Air Defenses

Apr 07, 2014 GSSR Cyber Security , Military & Defense , The Forum 0

Photo by Naval Air Systems Command

By Shane Quinlan |

U.S. plans to bring cyber capabilities into the cockpit with systems like the Next Generation Jammer (NGJ) represent expanded options for military planners, but the question many are still left with is: what can these new cyber capabilities do? And perhaps more important, what can they not do? While many of these airborne cyber capabilities are classified, there are clear indicators that the U.S. military wants to use cyber for the Suppression of Enemy Air Defenses (SEAD), protecting aircraft threatened by increasingly high-tech anti-air defenses.

The Israeli Air Force (IAF) may have already shown how this could work. In 2007, a small flight of IAF fighter aircraft entered Syrian airspace undetected, dropped 17-tons of munitions on a military facility that reportedly housed fissile nuclear materials, and escaped unscathed.[1] The IAF strike, titled Operation Orchard, quickly led to rumors that the IAF was able to execute this strike despite the existence of Syria's formidable air defense network – the same defenses that worried US policymakers in 2011 – by using a U.S.-developed cyber capability.[2] Aviation Week's David Fulghum suggested the IAF made use of "a technology like the U.S.-developed 'Suter' airborne network attack system." Suter, though highly classified and officially unacknowledged, is thought to be a combination of airborne electronic warfare and computer network hacking that accesses the communications between the networked sensors and weapon systems that compose an Integrated Air Defense System (IADS).[3] Suter penetrates the information flows between networked systems and allows its user to both see the communications of enemy systems and insert false information.[4]

The US Navy's NGJ system and EA-18G Growler airborne platform – long overdue replacements for America's aging arsenal of EA-6B tactical electronic warfare aircraft and the AN/ALQ-99 jammer – are expressly intended to combine traditional SEAD capabilities with the sort of "electronic warfare-delivered computer network attack" witnessed in Operation Orchard.[5] The NGJ, in concert with its jamming and electronic intelligence capabilities, would act as a delivery mechanism for electronic information designed to suppress enemy air defenses. This Suter-esque cyber attack capability would complement the enhanced EW

capabilities and kinetic weapon systems of the EA-18G and NGJ, ideally giving U.S military planners a choice between and among three SEAD options: jamming, bombing, and hacking.

The reality of that decision is radically more complicated, and the addition of a third cyber capability to SEAD requires a careful examination of its uses and effects, particularly its costs and limitations. Cyber attacks are innately unique and discrete; they are only capable of being used against particular systems, programs, or networks and exist as compilations of computed logic-based code and programs designed to access specific computer networks and the information within them.[6] There is no universally-applicable cyber weapon; each is tailored to the composition of the particular program, system, platform, or network it is targeted against. While systems like the NGJ act as universal delivery platforms, each attack must be carefully constructed in advance.

Due to the unique composition of opponents' IADS, cyber attacks on these information communications are not best thought of as individual weapons but rather as complex military and intelligence operations designed to deceive opponents' networks into accepting false information. This deception allows a window of opportunity wherein electronic or physical actions can be hidden (i.e. a flight of aircraft slipping unnoticed past an IADS). These Computer Network Attack (CNA) operations require significant investments in time, money, and technology before their actual use (including training, equipping, and maintaining CNA developers as well as the operational costs of network reconnaissance, exploit discovery, and delivery mechanism determination).[7] Despite the costs of CNA development, these operations are easily thwarted if an opponent updates or denies access to their software, hardware, tactics, or procedures – which countries regularly do – requiring a continual effort to stay abreast of an opponent's advances in targeted systems. Advances in computational capacity and an expanded cyber workforce could reduce the costs of CNA development, but in the near future, CNA will be an expensive military tool that should not be used sparingly.

The notion that CNA could be another weapon to suppress an enemy IADS alongside jammers and bombs bears little relation to the relative costs and limitations of CNA. Instead of weapons, a better analogy for CNA's use in SEAD may be traditional battlefield deception operations designed "to mislead or confuse the enemy decisionmaker by distorting, concealing, or falsifying indicators of friendly intentions, capabilities, or dispositions."[8] Thinking about CNA as a deception operation better communicates the requirements, costs, and precarious nature of its employment. Like deception operations, any CNA can ultimately fail if an opponent discovers and accounts for its employment; discovery is nearly unavoidable after a CNA has been used, often making CNA a one-off option. By changing communication protocols, compartmentalizing components of a network, buying new equipment, actively denying access, or developing simple software patches, an opponent can negate the particular effectiveness of unique CNA components.

Turning again to the utility of CNA in airborne SEAD, it is important to note that SEAD actually consists of two different missions – pre-planned SEAD and Reactive SEAD (RSEAD).[9] RSEAD is a response to individual unplanned threats or opportunities, not a coordinated assault on an integrated series of targets. In recent conflicts that posed serious threats to U.S. airpower – principally Operation Allied Force in 1999 and Operation Unified Protector in 2008 – the United States faced capable opponents able adapt their IADS to effectively counter U.S. technology-centric pre-planned SEAD.[10] They blended civilian communication infrastructure and proprietary military technologies to build hybrid communication networks, developed "shoot-and-scoot" high-mobility tactics, made extensive use of decoys and camouflage, and reduced their use of radar and information communication technologies to increase survivability.[11] In these contexts, where RSEAD dominates threat response, CNA is an inappropriate tool because of its costs, limitations, and one-off usability.

As the United States moves to operationalize the cyber evolution of SEAD with the NGJ, military planners must remain continually aware of the limitations of cyber capabilities within each context and carefully weigh the costs and benefits of CNA in SEAD. Developing the ability to use CNA in SEAD requires advanced planning and serious consideration of resources allocation. Cyber SEAD capabilities will not replace jammers or kinetic attacks in all contexts, but they can offer uniquely effective options in particular circumstances. Just because new technologies like the NGJ give military planners the ability to conduct cyber operations does not mean their use is always warranted, cost-effective, or useful.

Shane Quinlan is an MA candidate in the Security Studies Program at Georgetown University. He is also the GSSR Associate Editor for National Security, SSP Programming Fellow, and the Director of the nascent Georgetown Cyber Policy Working Group.

---

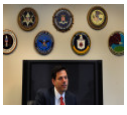
[1] David Markovsky, "The Silent Strike", The New Yorker, September 17, 2012. Available at http://www.newyorker.com/reporting/2012/09/17/120917fa_fact_makovsky.
Galrahn, "Electronic War in IAF Strike in Syria", Information Dissemination, October 16, 2007. Available at http://www.informationdissemination.net/2007/10/electronic-war-in-iaf-strike-in-syria.html.
[2] Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System," Wired, October 4, 2007. Available at http://www.wired.com/dangerroom/2007/10/how-israel-spoo/.
John Reed, "What Do We Know About Syria's Air Defenses?", DefenseTech, June 28, 2012.Available at http://defensetech.org/2012/06/28/what-do-we-know-about-syrias-air-defenses/.
David Axe, "New Navy Jammer Could Invade Networks, Nuke Sites", Wired, January, 21 2011. Available at http://www.wired.com/dangerroom/2011/01/jammer-could-invade-nets/.
[3] Weinberger, "How Israel Spoofed…"
Ward Carrol, "A Closer look at Israel's Syria Raid", DefenseTech, October 8, 2007. Available at http://defensetech.org/2007/10/08/a-closer-look-at-israels-syria-raid/.
John Leyden, "Israel suspected of hacking Syrian air defences", The Register, October 4, 2007. Available at

John Leyden, "Israel suspected of 'hacking' Syrian air defences", The Register, October 4, 2007. Available at http://www.theregister.co.uk/2007/10/04/radar_hack_raid/.
David Fulghum, Michael Dornheim, and William Scott, "Black Surprises", Aviation Week & Space Technology 162.7 (2005): 68.
[4] Leyden, "Israel suspected…"
Fulghum, Dornheim, and Scott, "Black Surprises."
[5] Spencer Ackerman, "In Combat Debut, Navy Jammer Targets Libyan Tanks," Wired, March 21, 2011. Available at http://www.wired.com/dangerroom/2011/03/in-combat-debut-navy-jammer-targets-libyan-tanks/.
James Sanborn, "Veteran Marine pilots: Don't retire the EA-6B Prowler yet", Marine Corps times, July 22, 2013. Available at www.marinecorpstimes.com/article/20130722/NEWS04/307220038/Veteran-Marine-pilots-Don-t-retire-EA-6B-Prowler-yet.
Axe, "New Navy Jammer…"
David Fulghum, "Cyberwar Spawns New Combat Aircraft", Aviation Week, September 27, 2007. Available at http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3a66251c2a-f208-4b98-befa-cf1e41f31794.
U.S. Government Accountability Office, Report to the Committee on Armed Services, House of Representatives, "Electronic Warfare: DOD Actions Needed to Strengthen Management and Oversight," (GAO-12-479) Washington: Government Accountability Office (2012): 27-28.
[6] Jason Andress and Steve Winterfield, Cyber Warfare: Techniques, Tactics, and Tools for Security Practicitioners (Waltham: Syngress, 2011), 119.
[7] Fred Cohen, "Simulating Cyber Attacks, Defenses, and Consequences", Fred Cohen & Associates, March 1999. Available at http://all.net/journal/ntb/simulate/simulate.html.
Eric Hutchins, Michael Cloppert, Rohan Amin, Ph.D., "Intelligence-Driven Computer Network Defense Informaed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, 2009. Available at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.
[8] Department of the Army, "Battlefield Deception (Field Manual No 90-2) Washington," Department of Defense, October 3, 1988. Available at http://library.enlisted.info/field-manuals/series-1/FM90_2/CH1.PDF.
[9] Maj. James Stewart, "JTTP for Joint Suppression of Enemy Defenses (J-SEAD) (Joint Publication 3-014)," Joint Chiefs of Staff, July 25, 1995. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/a401117.pdf.
[10] Major Jeff Kasselbaum, USAF, "The Art of SEAD: Lessons from Libya", Defense Technical Information Center, December 2011. Available at http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/student_readings/1C4_The_Art_of_SEAD-Lessons_from_Libya.pdf.
[11] Ibid.
Martin Andrew, "Revisiting the Lessons of Operation Allied Force", Air Power Australia Analysis, March 29, 2013. Available at http://www.ausairpower.net/APA-2009-04.html#mozTocId368006.

« Inspired by Inspire: Al-Qaeda Central's Latest Foray into Western Recruitment

Why the ISIS-al-Qaeda Conflict Isn't All Good News »

Related articles

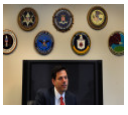

Demythologizing the Foreign Fighter
Oct 29, 2016 0


Protecting the Financial Sector from…
Oct 28, 2016 0


Professor Spotlight Series: An…
Oct 26, 2016 0


Russia's Disinformation War
Oct 25, 2016 0

More in this category


Demythologizing the Foreign Fighter
Oct 29, 2016 0


Protecting the Financial Sector from…
Oct 28, 2016 0


Professor Spotlight Series: An…
Oct 26, 2016 0


Russia's Disinformation War
Oct 25, 2016 0

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Archives

Select Month

Find Out More:

Africa | Americas | Asia | Cyber Security | Energy Security | Europe | Intelligence | International Security | In The News | Latin America | Lit Reviews | Middle East | Military & Defense | Nuclear and Unconventional Weapons | Special Issues | Terrorism | The Forum | The Review | US National Security

Follow us on Twitter

GUSecurityReview
@gssreview

Demythologizing the Foreign Fighter georgetownsecuritystudiesreview.org/2016/10/29/dem…

29 Oct

GUSecurityReview
@gssreview

Protecting the Financial Sector from Cyber Attacks: Why G7 Guidelines Need to go Further

DISCLAIMER

The views expressed in Georgetown Security Studies Review (GSSR) do not necessarily represent those of the editors or staff of GSSR, the Edmund A. Walsh School of Foreign Service, or Georgetown University. The editorial board of GSSR and our affiliated peer reviewers strive to verify the accuracy of all factual information contained in GSSR. However, the staffs of GSSR, the Edmund A. Walsh School of Foreign Service, and Georgetown University make no warranties or representations regarding the completeness or accuracy of information contained in GSSR, and assume no legal liability or responsibility for the content of any work contained therein.