Defense Communications: APL's Contributions Through the Decades

Robert A. Nichols

ABSTRACT

Defense communication systems have long played a critical role in the effectiveness of military operations, and their importance has only grown. In parallel, commercial communications continue to change rapidly as a result of massive investments in new capabilities. In recent years, the Johns Hopkins University Applied Physics Laboratory (APL) has made enduring contributions to capabilities for defense communications missions, leveraging commercial investments to provide unique solutions to the government. APL's involvement in improving communications capabilities spans nearly five decades and includes many transformational contributions to defense communications technologies. This article describes a number of those technologies and how APL has been critical to their development.

DEFENSE COMMUNICATIONS OVERVIEW

Communication systems have always been essential for military operations, from rudimentary semaphore signaling systems to the advent of wireless communications for military operations in World War I to today's global connectivity of fiber optic and satellite communications networks. The military's dependence on communications has increased significantly over the years, and today's military operations are critically dependent on information flow, as evidenced by terms like *network-centric warfare*. The military has an insatiable appetite for communications capabilities on many platforms; whether it is high-definition video, secure video teleconferences, or highly distributed sensor systems, there appears to be no end in sight to the needs for communications capabilities in warfare.

The information environment in which the military must operate has a parallel in the commercial sphere, where communications technology has changed the world over the last century, particularly over the last decade. Two domains, cellular technology and the Internet, have inextricably linked people and places around the globe and enabled profound changes in information access for billions of people worldwide. The unparalleled growth has resulted in a telecommunications industry with revenues over $2 trillion.[1] The explosion of technology is clearly evident to Johns Hopkins University Applied Physics Laboratory (APL) military sponsors, who often question how to leverage the massive commercial investment. Can commercial technology simply be repackaged and used in other environments? Can commercial technology be tailored for other uses?

To answer these questions, it is important to note the differences between the operational environment for conventional commercial communications and that

for military communications. First and primary is the multifaceted requirement for security in the military environment. Commercial communication systems are not typically designed with security features that are resilient to an adversary's actions directed against the systems. For example, commercial developers have increased emphasis on maintaining the confidentiality of user data, but not on the system's ability to operate against military jamming technology. A second significant difference is that commercial communications developers have access to infrastructure that is not available in military settings. Defense missions are inherently global, and many locations lack infrastructure or have insecure infrastructure. Third, the assurance of timely and accurate data delivery in many military applications, such as commanding a weapon, must be at a level far beyond the quality of service provided by most commercial systems, for which the requirements are less stringent.

APL's contributions to improved communications capabilities over the past five decades have focused on reconciling differences between commercial and military communications environments. APL has been exploring how to use the significant new capabilities of commercial communications to improve military communications while working to understand and address the additional capabilities required for military use. These efforts highlight APL's classic roles in strong technical systems engineering for development of new large-scale systems, technical evaluation of system performance, and prototyping solutions. This article is not comprehensive but highlights key activities that have been a hallmark of APL's work at pivotal points in the Lab's history.

EARLY CONTRIBUTIONS TO NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS

One of APL's first major contributions to defense communications was in the area of nuclear command, control, and communications (NC3), a harbinger of the specially tailored communications work that APL would conduct. With the numerous confrontations in the 1960s Cold War, the United States recognized NC3 as fundamental to the criticality of nuclear weapons in

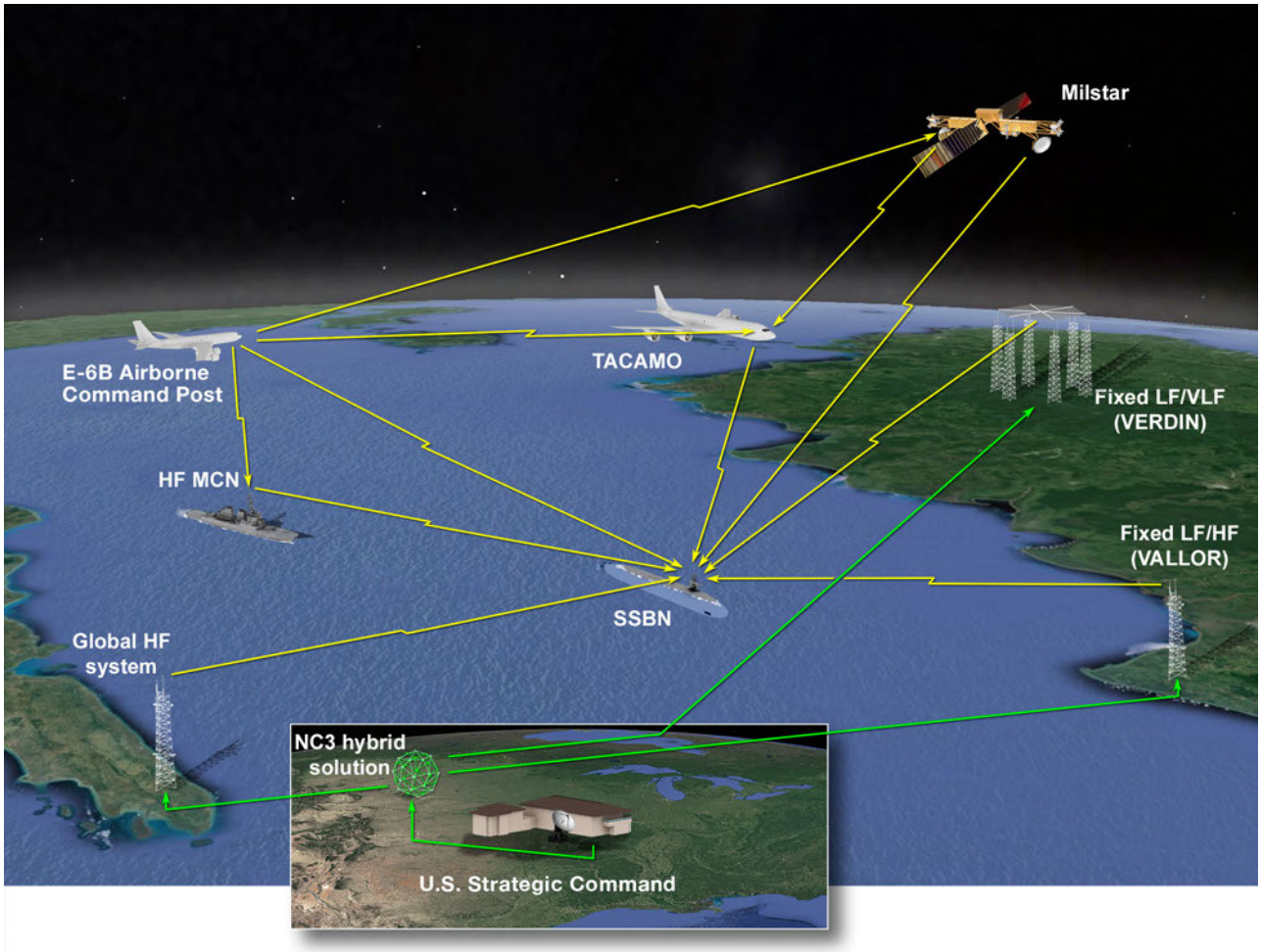

Figure 1. Diversity of NC3 communication links.

the overarching U.S. strategy. In 1970, the chief of naval operations required a method for continually evaluating the effectiveness of these systems. This directive began an effort that would span decades, with APL making a critical contribution to the nation.

Several unique aspects of the assessment have marked the path of APL's contribution. Clearly, the stakes cannot be higher for the performance of an NC3 system. The nuclear triad includes diverse weapon platforms, and the underlying communications are similarly diverse, including both low-band direct-path systems at very low frequency (VLF) and satellite communication (SATCOM) systems at extremely high frequency (EHF) bands, as illustrated in Fig. 1. The system performance metrics are highly scrutinized, the assessment must be comprehensive, and the diversity of systems must be correlated in the evaluation.

Unlike today's modern telecommunications infrastructure, which allows seamless communications through heterogeneous paths and network monitoring points, the NC3 architecture required significant operator involvement. Because of the level of operator involvement, one of APL's first tasks was to work with operators to assess numerous human performance issues, in addition to evaluating technical aspects of the system. The continuing assessment gradually moved from requiring operator involvement (e.g., manual logging) to sophisticated automation and instrumentation that provided reliable results more efficiently. A complement of radio frequency (RF) monitoring equipment supplied the details of the background context for the case studies.

Early on, the APL team recognized that it needed a comprehensive and detailed modeling and simulation campaign to understand the performance of the system in environments that could not be realized, such as propagation through atmospheric scintillation enhanced by nuclear effects, jamming, or the specific noise effects (e.g., lightning strikes on the VLF links). The team created physics-based models to provide performance estimates that could complement the real-world data gathering. These data provide the operators an understanding of the predicted performance in light of the ultimate metric, which is the success rate and timeliness of Emergency Action Messages as they traverse multiple links in the architecture. The assessments enabled marked quantitative improvements in performance. There is no commercial analog for such a system either in terms of applications or, at that time, the diversity of paths over which those messages would flow.

Despite dramatic geopolitical changes over the course of APL's work in NC3, the nation's need to ensure the effectiveness of the communications with its nuclear assets has endured. While the physics of the situation has not changed, the threats and nature of operations have been folded into APL's ongoing partnership with the system operators and stakeholders.

PIVOTING TO DEFENSE COMMUNICATIONS SECURITY

This strong portfolio led to further work in the tactical arena with assessments of vulnerabilities for the Navy in the 1980s. This was a key time for APL's work in defense communications, coinciding with the Laboratory's initial development of the Cooperative Engagement Capability (CEC), with its robust and tailored communication system, the Data Distribution System.[2] The work at APL first focused on finding vulnerabilities in tactical military links but then progressed to commercial links, a pivotal point in the Lab's history. DoD recognized that commercial systems must be used in some operational missions and that understanding their inherent vulnerabilities was important. This understanding was twofold: it helped planners select among a set of system options and also helped them potentially modify tactics, techniques, and procedures to operate within a particular system. As an example, it may be possible to configure a radio to lower-data-rate modes that naturally possess more link margin. These classified studies examined not only the links between users but also the control infrastructure supporting communications activities. A system could be rendered inoperable through access, human or otherwise, in a control facility without having to affect any of the signals traversing the network.

With APL's increasing staff and growing capabilities in vulnerability assessments, its long-standing role in SATCOM vulnerability assessments began in the late 1980s. While DoD uses a range of commercial SATCOM systems to support some operations (e.g., logistics), a set of specifically developed systems support the needed mission-critical functions. These systems operate in ultra high frequency (UHF), super high frequency (SHF), and EHF frequency bands and are characterized by different capabilities.[3] EHF SATCOM was originally developed through the Milstar program, which evolved to become the Advanced EHF system (protected MILSATCOM) and is the most robust of the MILSATCOM systems. The key performance discriminator of EHF SATCOM is the anti-jam (AJ) and low probability of intercept (LPI) performance. While Milstar was originally designed for NC3, it was modified to support tactical forces based on U.S. experiences in the Middle East in the early 1990s. APL was called on to determine whether the Navy SATCOM systems met those security requirements.

While specifications on LPI and AJ are easy to document, the ability to verify them is complex. RF propagation is highly varied in all bands and particularly difficult to assess in the millimeter-wave bands where EHF SATCOM operates, as there are fewer empirical models available for this band than for the more commonly used bands. At these frequency bands, antenna patterns are particularly jagged, and those gain differences have a significant impact on

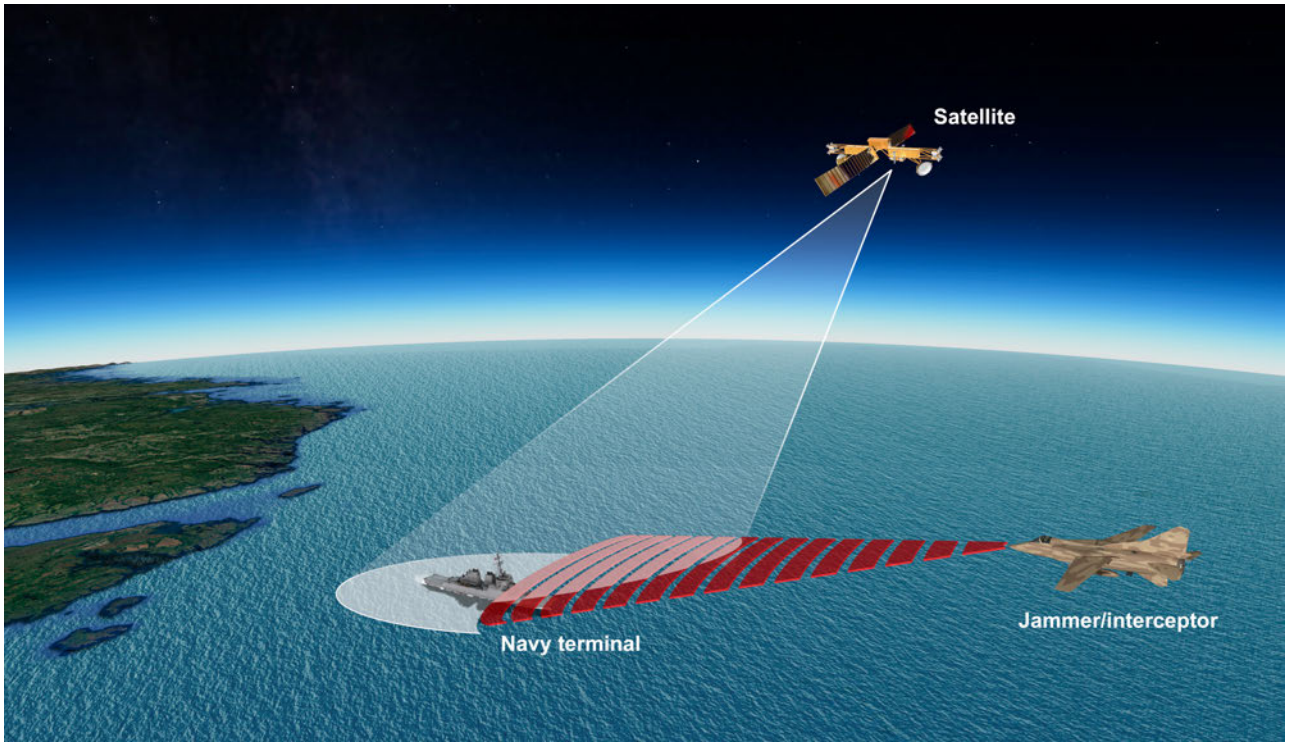

Figure 2. SATCOM security assessments.

intercept and jamming. The potential geometries of both blue forces and the threat are numerous and have a significant impact on performance, as illustrated in Fig. 2. Finally, the EHF SATCOM waveform is highly complex with many modes of operation and signal processing features.

APL has been the Navy's go-to organization to make these assessments over the generations of EHF SATCOM and has provided the acquisition and operational communities with ground truth on their terminal performance. Initial work was primarily empirical and involved APL staff at locations like the fjords of Norway and Vieques Island in Puerto Rico to achieve the required geometries. Other tests used airborne-mounted threat capabilities, although these tests were expensive to conduct. More affordable approaches were sought, and APL developed modeling and simulation tools to assess AJ and LPI, validating these models with carefully selected "spot check" empirical collections and analysis. Given this extensive verification and validation, the Navy approved the modeling and simulation tools as the methods used to perform the operational evaluation of the terminals, a remarkable step in test and evaluation and a credit to APL's technical rigor. In addition to serving in an acquisition role for the SATCOM security work, APL has recommended tactics, techniques, and procedures to members of the operational community, helping them to understand the best ways to use this highly capable system.

APL'S LEADERSHIP IN SATCOM DEVELOPMENT

APL's knowledge of space systems and work on DoD vulnerability assessments led to its expanded role in the definition of new SATCOM systems. The most significant contribution in this area was APL's work on the UHF portion of MILSATCOM. UHF provides mobile capabilities for military users and has been in operation since the late 1970s. A satellite reaches the end of its life when station keeping cannot be achieved because of fuel limitations and the decreasing reliability of components, so new generations of SATCOM systems must be developed. As the UHF constellation called UHF Follow-On (UFO) reached these limitations, APL played a central role in establishing a new system through several phases of design studies and technical leadership in an analysis of alternatives. Dozens of new approaches were considered, including two developed under APL independent research and development investments.[4,5] APL provided the key technical analyses in areas such as capacity, which involves link analysis, geographic coverage, AJ performance, and many other aspects of the system. The new system, called the Mobile User Objective System and launched in 2012, was based on a cellular model, providing another example of how APL leveraged commercial technology. Not only has the Lab set the direction for UHF SATCOM, but it has also been heavily involved in major architecture and system designs for other pillars of the wideband and protected MILSATCOM systems.

SATCOM systems are typically decomposed into three main components: the spacecraft and payloads, the user communication equipment known as terminals, and the control infrastructure. The control infrastructure involves not only "flying" the spacecraft but also managing the resources on the communications payload. Many of the early SATCOM systems were transponders, also known as bent pipes, where communications traffic is essentially uplinked from ground terminals to the payload and then transmitted back down to Earth on a different frequency. As SATCOM became more dynamic in U.S. military operations in the 1980s and was often oversubscribed, there was an increased need for SATCOM planning, management, and control capabilities. While some tools were available, the ability for operators to effectively plan resources was hampered by disparate computer control systems or manually intensive processes. With many companies playing a role, the government needed an organization that could provide unbiased counsel and a way forward.

Given APL's deep expertise in SATCOM, the government, through the Army, looked to APL for the near- and long-term objective architecture and approach for wideband military SATCOM, the primary backbone for secure global high-bandwidth communications needs. This effort included the construction of a facility devoted to SATCOM control (see Fig. 3). One component of the near-term architecture was an integrated capability for SATCOM control. The government called on APL to develop the Defense Satellite Communications System Integrated Management System,[6] which brought together industry's capabilities in an operator-centric environment. This prototype is currently hosted in operating centers around the world to provide support to the operational community and bridge the gap in capability. It has now been transitioned to contractor post-production software support. APL not only had a significant impact on wideband control, but it also developed and deployed hosted payload control capabilities for the Navy to bridge a gap in EHF SATCOM capabilities for the Fleet. APL had become recognized in the community as a center of excellence for SATCOM control systems.

APL's role has included not only integration of industry tools but also capabilities that provide more affordable and resilient operations. SATCOM ground operations centers around the world provide positive control of the spacecraft and payload resources but at significant cost. Given the concerns regarding affordability, APL developed a system to remotely control and monitor wideband SATCOM payloads. The Remote Monitoring and Control Equipment enables a globally connected set of operations centers and remote sites to perform the functions of global SATCOM operations. This capability provides resilience, with one site able to control resources associated with another, layering security into the architecture.

APL also stepped in to solve some other challenges with the aging SATCOM constellation. As the wideband SATCOM spacecraft reach the ends of their lives

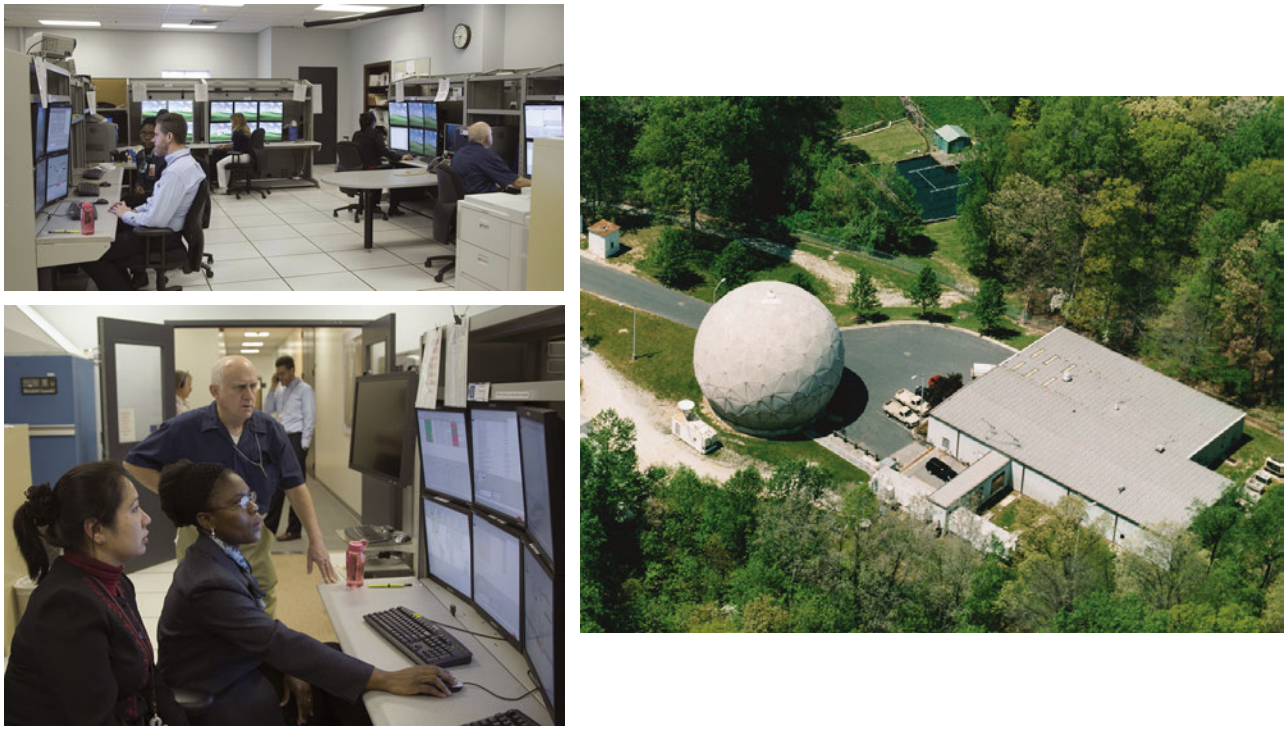

Figure 3. APL's SATCOM control facility.

and fuel is expended, the orbital inclination increases since the orbit cannot be maintained. In the mid-2000s, the wideband SATCOM system reached a point at which telemetry to support control systems was affected by Doppler shifts due to the inclination. APL performed the analysis to correlate the effects noticed by the operators (which were manually compensated) and to understand the detailed limitations of the control system receivers. APL devised a hardware/software solution that enabled continued control of these assets and introduced it into operations through industry development, effectively adding years to the useful life span of these expensive and mission-critical DoD assets.

Ultimately, SATCOM systems are one critical component in a heterogeneous global network with users distributed across multiple environments. With the advent of the Global Information Grid in 2002, DoD sought a more cohesive IP networking architecture, which meant that SATCOM/terrestrial connectivity was an important interface to design and engineer. The DoD Teleports would be the gateway between SATCOM and terrestrial fiber optic communications. APL led the study that determined the communications capabilities and optimal locations for these DoD Teleports given a set of options from legacy gateway facilities (Fig. 4). This study required APL's independence given that the armed services managed gateways with significant infrastructure and the selection required quantitative selection criteria based on metrics agreed on by all the stakeholders. Not only did APL complete this study, but it was also actively engaged in standing up the capability over the critical first years of implementation.[7]

U.S. MILSATCOM does not exist in isolation, and while new systems are born, international bodies govern the parameters for operation of these systems. The International Telecommunications Union governs orbital positions and associated frequency bands. Some of the implications are straightforward in that DoD can operate satellites in only certain positions and bands. However, more complex regulatory issues have arisen, requiring APL to deeply analyze problems and engage with the international community.[8] The Army is developing mobile SATCOM systems to enable higher-tempo operations, and these systems use small parabolic dishes on the mobile platforms. The issue is that with a mobile platform on rough terrain, the energy from that dish will be received by adjacent satellites. APL recognized that this would occur during a relatively small fraction

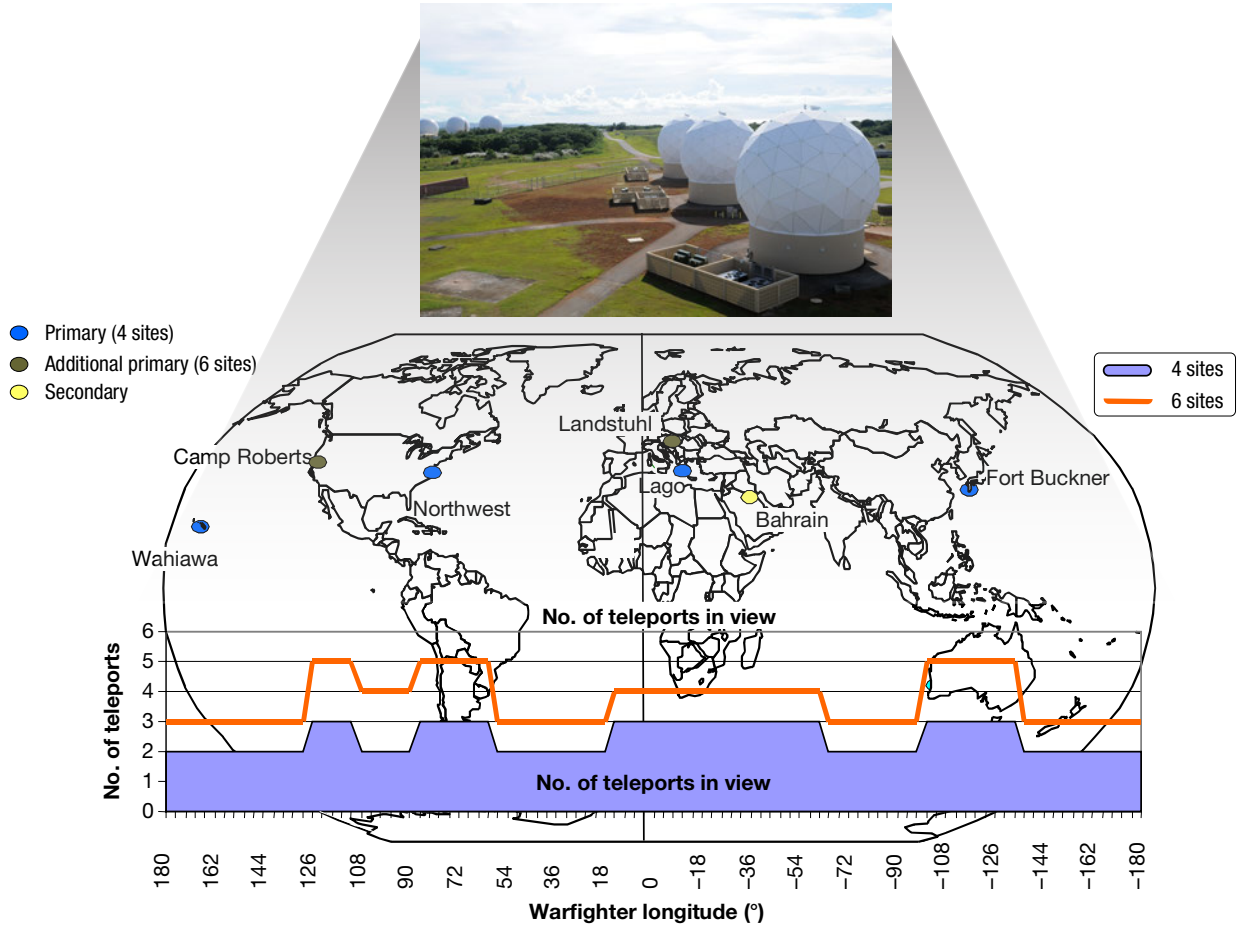

Figure 4. Analysis results on optimality of DoD Teleport locations.

of time, but the international standards were written as static and deterministic. APL began a multiyear process to bring the international community a fundamentally new approach, based on a statistical characterization, for this issue of adjacent satellite interference. This approach has been a linchpin in enabling the Army to proceed with its mobile SATCOM capabilities to ultimately support enhanced operations.

APL'S ADVANCED TECHNOLOGY CONTRIBUTIONS

In the domain of defense communications, APL has filled technical systems engineering roles but has also contributed to advanced technology exploration and development. Selecting a focus has been critical given that telecommunication companies are heavily investing in research and development. APL has simultaneously helped DoD harvest commercial technology, tailoring it to specific missions, while remaining on the forefront of new breakthroughs.

One such area is spectrum operations. Similar to the regulatory issues of SATCOM, spectrum is a commodity governed by international and national bodies and is a resource that DoD must use in parallel with commercial systems. The availability of spectrum is directly related to a system's performance, such as its data rate or link robustness. When DoD operates in countries around the world, spectrum usage must be approved, and this process is lengthy and uncertain. Due to increased wireless usage in the global markets, spectrum has become a precious commodity. In some cases, spectrum is auctioned to commercial wireless providers, leaving DoD with less spectrum despite increasing demands. The Defense Advanced Research Projects Agency (DARPA) set out to fundamentally change the approach to spectrum allocation, which is a century-old process of static allocations. The DARPA neXt Generation, or XG, program sought to use dynamic spectrum access (DSA) to add far more agility to DoD spectrum operations. As illustrated in Fig. 5, DSA's goal was to enable a capability that could sense spectrum and dynamically use "white space" in space/time/frequency.

APL was the test and evaluation arm for DARPA, tasked to provide ground truth of the performers' DSA approaches. The test and evaluation of DSA is complex, requiring simultaneous and highly synchronized spectral measurements at multiple locations because DSA depends on available spectrum at both the transmit and receive sites. Although APL was not a performer, its test and evaluation role required advanced technology and led to a patent[9] on the implementation of a simultaneous and controllable spectral observation system. APL is similarly engaged with the DARPA RadioMap project, which is focused on creating a spectral "terrain map" for users to understand and more efficiently allocate resources for both communications and other RF capabilities. APL recently began working with the Defense Spectrum Organization on broad strategies for employment of advanced technologies for the warfighter. Spectrum is the foundational resource for communications, and APL's contributions are enabling much greater efficiencies and opportunities.

APL has been at the forefront of a slowly emerging technology, software-defined radios (SDRs). The concept was proposed in the late 1980s/early 1990s[10] when processor speeds allowed radio functionality to be performed in software rather than discrete hardware electronics. This change resulted in several benefits, such as the ability to change waveforms and protocols more

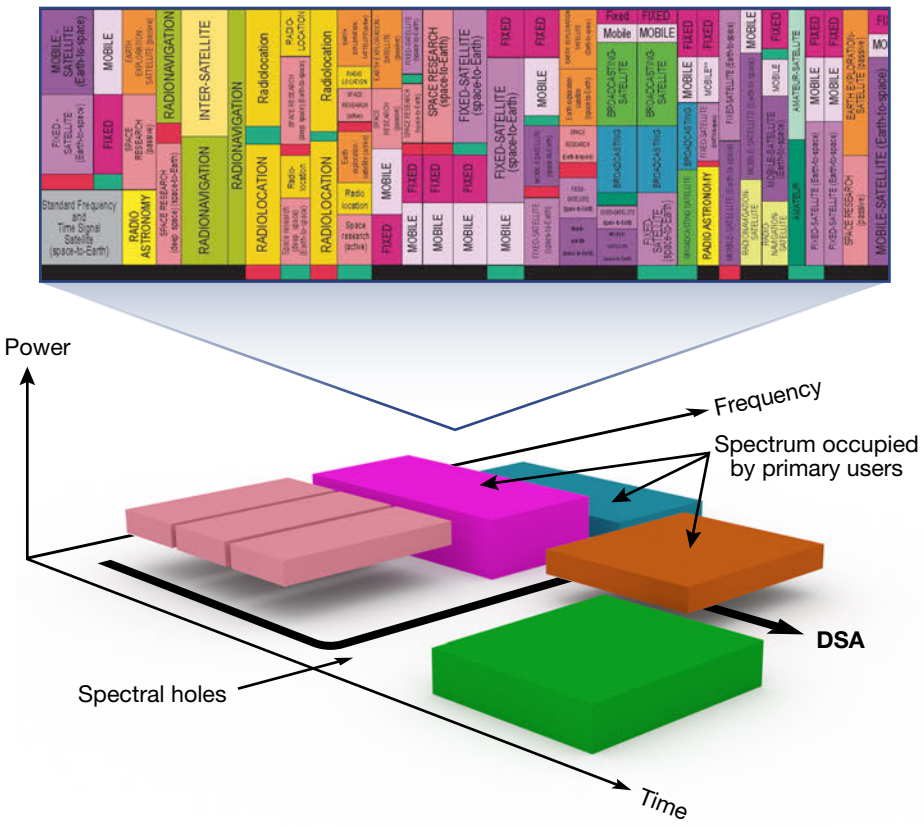

Figure 5. DSA and management.

easily. This concept has been evolving for two decades, and APL has been involved in several key studies and capability developments to determine the appropriate roles and approaches for SDRs. When the field was born, APL devoted independent research and development efforts to prototyping to understand how these SDRs would be used. It found that some of the major tenets of SDRs were not straightforward to implement. While the focus was on software and its portability across platforms, the hardware layers were still intertwined with those desired objectives.[11]

These early experiments facilitated APL's involvement with some of the key DoD programs related to SDR. The Joint Tactical Radio System (JTRS) program was an early adopter of the SDR concept, and APL participated in two prominent activities related to this program. At that time, JTRS operated from 2 MHz to 2 GHz, and a formal DoD analysis of alternatives sought to determine whether this approach should be adopted for radios above 2 GHz. Radios operating at higher frequencies typically operate at higher data rates, therefore requiring significant processing loads, or at lower rates but with processing-heavy waveforms. Through this analysis of alternatives, APL recommended a framework that differed from the approach JTRS was pursuing at the time. APL's role continued with a technology readiness assessment decomposing the JTRS to so-called critical technology elements and assessing their technology readiness levels. The technology readiness assessment was designed to create a consensus understanding of the state of the program. These research and assessment roles, hallmarks of APL's contributions in this technology space, helped shape the future of defense communications.

In recent years, a more refined view of SDRs and their role has emerged to include not only general-purpose processors but also field-programmable gate arrays and digital signal processors. The role of each is defined by the context and the capabilities required, with consideration of technical performance but also associated development issues like software portability. APL's SDR contributions have expanded to include numerous DoD programs for multiple sponsors and domains, such as wireless cyber operations and space exploration.[12] The concepts of SDR focus on the lower layers of the Open Systems Interconnection stack, but technologies like software-defined networking are taking these flexibility concepts and moving them up to the networking layers. This is an overall trend toward virtualization of functionality, which is likely to continue to expand, taking advantage of the horsepower of commodity hardware. This virtualization could extend beyond communications to all the RF capabilities of a platform.[13] But as in other areas discussed, the gains must be examined with respect to security. What happens to the attack space when introducing virtualization?

CONNECTING INDUSTRY AND GOVERNMENT DEFENSE

DoD and other critical government users at all levels want to be able to use improved commercial communications capabilities. These users often must switch from the modern smart devices they use in their daily lives to rudimentary and large-form-factor devices when operating in military or other government settings. Compared to the devices they use in their everyday lives, these less-capable devices and operational procedures make it more difficult for users to conduct their work. Users routinely ask why they cannot use commercial devices while conducting their missions. A tremendous potential performance advantage could be gained[14] by using commercial wireless devices; however, the limitations relating to security or availability of infrastructure restrict their use.

APL has been a major contributor to a sea change in this area over recent years. Security for classified communications has been the domain of specialized

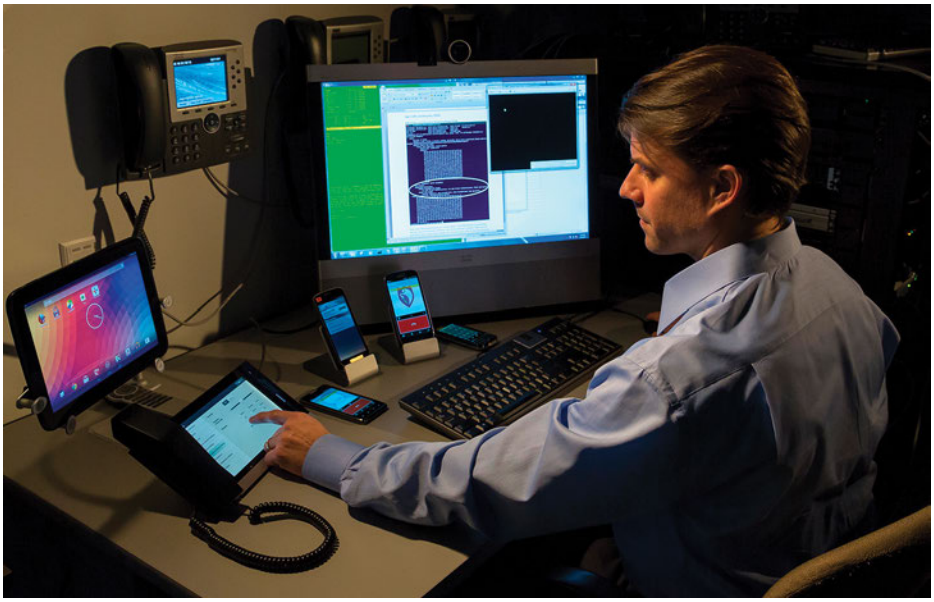

Figure 6. Commercial Solutions for Classified (CSfC) laboratory experimentation.

government-specified and -approved technologies. Government off-the-shelf capabilities have not been able to keep up with the rapid development of commercial technologies, which have incorporated increasingly stronger encryption technologies in recent years. The Information Assurance Directorate at the National Security Agency (NSA), working with APL as a principal contributor, has developed a completely new concept for information assurance solutions where government off-the-shelf technology is not the only option. DoD's chief information officer asked APL to spearhead an effort to enable senior national leaders, who in particular want to use commercial communications technology like cell phones for critical missions, to use the latest commercial devices. The use of the modern commercial devices is enabled through the NSA Commercial Solutions for Classified (CSfC) program. This program offers guidance and implementation templates for secure mobile access, communications via multiple types of networks, and secure data at rest in capability packages that can be adopted by different users.[15] APL laid foundations for ongoing efforts with a prototyping facility called the Secure Communications Assessment Network (SeCAN) Laboratory (Fig. 6). SeCAN maintains multiple CSfC test and evaluation systems to support experimentation, including the Sharktank system,[16] the Defense Mobile Classified Capability Evaluation Network, and KingsLanding, a leading-edge implementation of CSfC-based mobility that provides a platform for ongoing technical contributions to the overall architecture and approach for secure mobile communications. The CSfC methodology operates on a number of design tenets to achieve security, such as diversity in implementation of cryptographic algorithms (e.g., asymmetric encryption for authentication), layered encryption, and isolation from the carrier network. As in any engineering field, moving from concept to reality can be a major leap, and the SeCAN Lab is now the central venue to allow the government to ensure managed security of solution approaches for commercial products. Additionally, the SeCAN Lab offers users the opportunity to immerse themselves in the technology so that they can incorporate their operational views into development of the capability. In some sense, this capability for senior leaders has come full circle from APL's initial involvement in NC3 to a modern analog of global operations using advanced communications technology while continuing to rely on techniques, like diversity, to provide secure solutions.

SUMMARY AND FUTURE DIRECTIONS

The need for defense communications is as significant as ever, and the ability to leverage the tremendous commercial investments in communications technology can fuel new developments. APL will continue to serve in its classic role of bridging commercial and defense applications, working the individual technology components along with the large-scale systems engineering. APL not only helps DoD with advanced capabilities but also enables affordable approaches to challenges facing the nation. Being aware of and selectively involved in commercial technology is essential to bringing innovative solutions like CSfC, which represents a dramatic change in leveraging contemporary devices and systems.

APL will continue to focus on areas of the most criticality for the nation. Global communication solutions through SATCOM will remain a key area for APL. The threats against space-based communications are concerning,[17] and APL will be helping the government determine future directions. The issues related to spectrum availability continue to be a major challenge, and APL, as an objective partner to DoD, will help assess the myriad options from technology to policy. Adding optical communications to these advanced RF approaches to complement capabilities and further expand capacity appears likely at some point.[18] The virtualization of everything from IT systems to RF capabilities appears destined through the now foundational SDRs, the early years of software-defined networking, and commercial cellular control capabilities like network function virtualization. APL has helped sort through the hype and has led DoD to a refined use of SDRs, and it will be involved in these grander virtualized approaches as well.

Security of defense communications has been at the forefront of APL's decades of involvement in this discipline. From our earliest contributions in NC3 and tactical systems, security has been the key performance consideration in concepts, designs, and deployments. There is no bigger issue in the transition of commercial technology to defense environments. The security threats have only become more potent with the widespread access to advanced technology enabled by the global marketplace. The low-end threat is formidable; risk cannot be eliminated and must be managed. There is an operational disadvantage to not communicating or communicating with austere capabilities. Complex trade-offs must be understood and managed when deciding how to communicate operational information. With APL's ties to the government's operational, acquisition, and technology bases, the Lab will continue to help find solutions for important national issues.

REFERENCES

[1] *The 2015 Telecommunications Industry Review: An Anthology of Market Facts and Forecasts*, The Insight Research Corporation, Durango, CO (2015).

[2] Anonymous, "The Cooperative Engagement Capability," *Johns Hopkins APL Tech. Dig.* **16**(4), 377–396 (1995).

[3] Fritz, D. A., Doshi, B. T., Oak, A. C., Jones, S. D., Burbank, J. L., et al., "Military Satellite Communications: Space-Based Communications for the Global Information Grid," *Johns Hopkins APL Tech. Dig.* **27**(1), 32–40 (2006).

[4]Russo, A. A., "Multi-Beam GEO Satellite Concept for the Mobile User Objective System," in *Proc. 1999 IEEE Military Communications Conf. (MILCOM 1999)*, Atlantic City, NJ, pp. 1125–1130 (1999).
[5]Lee, S. C., Nichols, R. A., Yuan, R. L., Blackert, W. J., and Blair, M. P., "A LEO Satellite Concept for the Advanced Narrowband System," in *Proc. 1999 IEEE Military Communications Conf. (MILCOM 1999)*, Atlantic City, NJ, pp. 1136–1140 (1999).
[6]Hostetter, M. E., Noll, M. H., Molinaro, E. G., Fields, W. G., and Hanke, P. A., "A Decade of Large-Scale Software Systems Integration and Prototype Development for Army Wideband SATCOM," *Johns Hopkins APL Tech. Dig.* **25**(4), 316–325 (2004).
[7]Leonard, W., Pitts, C. Jr., and Chimento, P., "Designing a Net-Centric DoD Teleport," in *Proc. 2004 IEEE Military Communications Conf. (MILCOM 2004)*, Monterey, CA, pp. 1689–1693 (2004).
[8]Cuevas, E. G., and Weerackody, V., "Technical Characteristics and Regulatory Challenges of Communications Satellite Earth Stations on Moving Platforms," *Johns Hopkins APL Tech. Dig.* **33**(1), 37–51 (2015).
[9]Jones, S., Merheb, N., Abrahamson, J., Shuford, R., and Tomko, A., "Signal Observation System," U.S. Patent 7317765, filed 24 Nov 2003, issued 8 Jan 2008.
[10]Mitola, J., "Software Radios: Survey, Critical Evaluation and Future Directions," in *Proc. IEEE National Telesystems Conf.*, Washington, DC, pp. 13-13–13-23 (1992).
[11]Jordan, M. A., "Turbo Code Codec Implementation and Performance in a Software Radio," in *Proc. 1999 IEEE Military Communications Conf. (MILCOM 1999)*, Atlantic City, NJ, pp. 525–529 (1999).
[12]Crown, M., Haskins, C., Wallis, R., and Royster, D., "Demonstrating TRL-6 on the JHU/APL Frontier Radio for the Radiation Belt Storm Probe Mission," in *Proc. IEEE Aerospace Conf.*, Big Sky, MT, pp. 1–8 (2011).
[13]Debatty, T., "Software Defined RADAR: A State of the Art," in *Proc. 2nd International Workshop on Cognitive Information Processing*, Elba Island, Italy, pp. 253–257 (2010).
[14]Andrusenko, J., Burbank, J. L., and Ouyang, F., "Future Trends in Commercial Wireless Communications and Why They Matter to the Military," *Johns Hopkins APL Tech. Dig.* **33**(1), 6–15 (2015).
[15]Commercial Solutions for Classified Program (CSfC)," https://www.nsa.gov/resources/everyone/csfc/ (last modified 2 June 2016).
[16]Murphy, B., Akinpelu, A., DeSimone, T., and Forte, J., "Sharktank: The SeCAN Lab 'Tip of the Spear' for Commercial Solutions for Classified Mobility Systems," in *Proc. 2013 IEEE Military Communications Conf. (MILCOM 2013)*, San Diego, CA, pp. 1377–1382 (2013).
[17]Speech by Deputy Secretary of Defense Robert Work, Speech to Satellite Industries Association, March 2016, https://www.defense.gov/News/Speeches/Speech-View/Article/696289/satellite-industries-association.
[18]Young, D. W., Hurt, H. H., Sluz, J. E., and Juarez, J. C., "Development and Demonstration of Laser Communications Systems," *Johns Hopkins APL Tech. Dig.* **33**(2), 122–138 (2015).

Robert A. Nichols, Asymmetric Operations Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Rob Nichols is the chief scientist of the Cyber Operations Branch in APL's Asymmetric Operations Sector. He has been working in the area of communication and cyber systems since joining APL in 1992, initially in satellite communications and then in numerous other areas in wireless communications and cyber operations. He holds a B.S. and an M.S.E. in electrical engineering from Johns Hopkins University. His e-mail address is robert.nichols@jhuapl.edu.