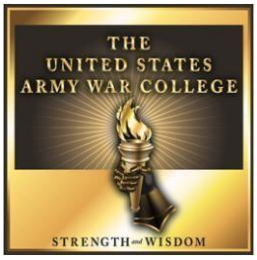
Strategy Research Project

Exquisite Vulnerability: Communications and Deterrence

by

Colonel Joel D. Babbitt
United States Army

Under the Direction of:
Colonel Douglas Orsi



United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Exquisite Vulnerability: Communications and Deterrence

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Joel D. Babbitt
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Douglas Orsi

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 5,493

14. ABSTRACT

For decades, the United States has stood alone as the world's sole superpower, leading to a lack of focus on emerging great power threats. As a result, the U.S. military has built exquisite communications systems that are not designed to withstand the dangers of a peer or near-peer conflict. However, with the reemergence of Russian aggression in the Ukraine and China's militarization of territorial claims in the South China Sea and their reluctant backing of North Korea, the remote possibility of a peer conflict is becoming ever more probable. This increasing possibility requires a readjustment in the U.S. deterrence posture. This is perhaps most apparent in U.S. military communication methods. To remain competitive, communication systems designed for operating in a low-intensity conflict must be retooled, and old paradigms of command and control and network design need to adapt to overcome the demonstrated exploitations of peer adversaries. This paper points out several of these exquisite vulnerabilities and suggests alternate paradigms for addressing them.

15. SUBJECT TERMS
Network, Satellite, Command Post, Radios, GPS, Navigation, Russia New Generation Warfare

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	28	

Exquisite Vulnerability: Communications and Deterrence

(5,493 words)

Abstract

For decades, the United States has stood alone as the world's sole superpower, leading to a lack of focus on emerging great power threats. As a result, the U.S. military has built exquisite communications systems that are not designed to withstand the dangers of a peer or near-peer conflict. However, with the reemergence of Russian aggression in the Ukraine and China's militarization of territorial claims in the South China Sea and their reluctant backing of North Korea, the remote possibility of a peer conflict is becoming ever more probable. This increasing possibility requires a readjustment in the U.S. deterrence posture. This is perhaps most apparent in U.S. military communication methods. To remain competitive, communication systems designed for operating in a low-intensity conflict must be retooled, and old paradigms of command and control and network design need to adapt to overcome the demonstrated exploitations of peer adversaries. This paper points out several of these exquisite vulnerabilities and suggests alternate paradigms for addressing them.

Exquisite Vulnerability: Communications and Deterrence

Deterrence means "persuading an opponent *not to initiate* a specific action because the perceived benefits do not justify the estimated costs and risks."[1] Deterrence is built by having the force structure, capabilities, training, and the political will to use them. Credibility in deterrence is always a measure of comparison. Does the enemy have superior or inferior capabilities to our own? Can our forces stand up to theirs? Does our side have any fatal flaws? Can the enemy inflict unacceptable losses on our forces, breaking our political will, or can we cause them unacceptable pain and break their political will first?[2]

For nearly three decades the U.S. military has been a force without peer. During this time, it has been a strategic assumption that Russia and China are not peer but *near*-peer competitors. However, while the U.S. Army significantly slowed its rate of modernization and cancelled almost all of its big-ticket modernization programs, near-peer competitor countries have not; instead, they have focused their development on exploiting U.S. vulnerabilities. The effect has been both a closing of the gap between U.S. Army capabilities and those of Russia and China in several categories, as well as a new generation of enemy doctrine and capabilities focused on exploiting U.S. vulnerabilities.

In recognition of the dangers adversaries' technological and doctrinal evolutions represent, General Mark Milley (Chief of Staff of the U.S. Army) and LTG Bruce Crawford (U.S. Army Deputy Chief of Staff G-6) have both stated that the network we have is not the network we need.[3] Indeed, the Army's communications infrastructure is the soft underbelly of the Army's ground deterrent.

This vulnerability has not only been noticed by senior army leaders, but is articulated in the objectives of the *Capstone Concept for Joint Operations* as well: "Improve Resilience along Electromagnetic Spectrum. Mitigate the effect of threats and hazards to personnel, equipment, and facilities from EMS exploitation, denial of access, and kinetic/ non-kinetic targeting of EMS dependent capabilities."[4] The purpose of this paper is to not only point out these vulnerabilities in the U.S. military's exquisite communications capabilities, but to propose real solutions.

Strategic Context

The adaptations in Russia New Generation Warfare doctrine are specifically tuned to the current posture of the U.S. Army after nearly two decades of counter-insurgency focus. To show how, it is useful to explain both for comparison.

Russia New Generation Warfare

Nowhere is the demonstrable potential for an upending of the status quo in ground combat dominance more apparent than in the case of Russia. The Russian military has developed a new doctrine called New Generation Warfare,[5] along with a supporting suite of capabilities from their recent modernization, showcasing it to devastating effect in the Ukraine conflict. The key aspect of this doctrine is to attack their adversaries asymmetrically and exploit perceived weaknesses, rather than attempting to develop and field better symmetric capabilities.

While much of Russia New Generation Warfare focuses on whole of government efforts (which include diplomatic, economic, and informational aspects in addition to military efforts) and fighting in the gray zone (conflicts short of recognized war), one key aspect is exploiting the dependence of potential western adversaries on high bandwidth satellite and terrestrial communications by using a combination of electronic warfare to

jam communications and control signals, drones to triangulate enemy vehicles and command posts, and extended-range artillery to engage quickly and from sanctuary.[6] This combination destroyed two Ukrainian mechanized infantry battalions in minutes and, should hostilities arise, will be used with similarly devastating effectiveness to defeat U.S. units unless changes are made to the tactical and operational communications systems on which the Army depends.[7]

Russia New Generation Warfare doctrine represents a direct challenge to the U.S. Army, calling into question the tactical effectiveness of current battalions, brigades, and divisions, and their ability to engage and defeat Russian forces. This raises the possibility of unacceptably high casualties and clearly affects U.S. tactical deterrent credibility, resulting in a weakening of the overall U.S. strategic deterrence.[8] In other words, potential adversaries have evolved to target the fundamental flaws of U.S. communications systems, putting the Army at risk of operational failure in future conflicts, giving potential adversaries the opportunity to shape strategic outcomes.

The U.S. Army Posture

After nearly two decades of low-intensity conflict and counterinsurgency operations, the U.S. Army finds itself tuned to the lower end of conflicts with command and control systems built to operate in permissive environments, equipped with only the remnants of legacy equipment tuned to high-intensity conflict. The Big 5 programs of the 1970s and ‘80s, namely the M1 Abrams Tank, M2 Bradley Infantry Fighting Vehicle, Apache Attack Helicopter, Blackhawk Utility Helicopter, and Patriot Missiles, fundamentally transformed land warfare in their day and are still the mainstay of U.S. high-intensity conflict capabilities—four decades later.[9] Communications technology, however, is evolving at such a rapid pace that capabilities from four decades ago are

seen as archaic. For example, AN/PRC-77 radios and maps where puck-drivers move unit markers on large maps for situational awareness were out of date before most of today's soldiers were born.

Such rapid developments in communications technology have resulted in communications systems that are fundamentally unsuitable for high-intensity conflict. In a world where the possibility of conflict with near-peer adversaries had begun to seem remote, anti-jam capabilities have been routinely ignored or put off until later software releases in most modems, thus leaving these most exquisite satellite systems vulnerable to not only enemy jamming events but to jamming due to friendly forces misconfiguring their own systems.[10] Meanwhile, anti-scintillation waveforms and electro-magnetic pulse hardening, critical for dealing with the obscuring fallout and the blast effects of nuclear events, are seen as a quaint legacy of the Cold War and completely unnecessary.[11] Perhaps President Obama expressed the mentality shift of the U.S. post-Cold War sole-superpower status best in the 2012 presidential debates: "The 80s called, they want their foreign policy back"[12] After that Russia invaded the Crimea, then the Donbass region of eastern Ukraine, and as of this writing the U.S. military is preparing for war with North Korea—who has a mutual defense treaty with a rapidly modernizing China that some are now calling a peer competitor.[13]

Russia and China both possess weapons that can easily reach U.S. strategic and operational facilities and assets.[14] At the tactical and perhaps operational levels in a near-peer conflict, the U.S. choice of operating out of static Forward Operating Bases and large, bloated command posts has to end.

Rethinking Network Paradigms

The networks that make up the communications backbone for U.S. strategic, operational, and tactical forces worldwide are numerous, disparate, and could easily fill volumes to describe. However, three sets of characteristics clearly shaped the Army's current networks: extension via satellite, robustness of services, and the expectation of constant connectivity. An honest look at the vulnerabilities inherent in these characteristics show that the paradigms and assumptions driving them must change.

The strategic level of communications is characterized by thousands of locations all in constant communications with each other over terrestrial means with satellite facilities providing backup, whereas the tactical level of communications is characterized by a relatively few locations communicating mostly transitory data over satellite or radio: headquarters move of "jump," intelligence teams move their exploitation mission from one target to another, etc. Data centers that host large service applications and huge amounts of persistent data reside at the strategic level, whereas historically tactical users have made do with a small amount of transitory data. Additionally, tactical networks and services must of necessity be disconnected from any larger or enterprise network for large periods of time.

In the past decade, attempting to blend the above attributes between strategic and tactical networks has had the effect of constraining maneuver and introducing vulnerabilities that were not very apparent from a counter-insurgency mindset. For instance, Warfighter Information Network-Tactical Increment 2 (WIN-T Inc 2) capabilities, designed to be mounted on tactical trucks and given to battalion and brigade key leaders, hosted a Windows Server Domain Controller—a large database that required some six hours to rebuild when it crashed.[15] Additionally, bringing up a

brigade's WIN-T Inc 2 network typically took several days, often upwards of two weeks.[16] These are common characteristics in a strategic network, but are completely out of place in a tactical network by artificially constraining maneuver commanders' flexibility and response times. Speed and maneuver are the coin of the realm in high intensity conflicts, and network paradigms must change to give maneuver commanders the edge over potential adversaries, rather than lagging behind them. Clearing the tactical networks of ill-fitting strategic capabilities and simplifying what is left is a good place to start.

Another fallacy of attempting to blend the strategic and tactical networks is unwisely applying cloud technologies. Senior leaders and senior civilian architects, all of whom live on high speed strategic networks that are constantly connected via fiber, have bought into the cloud services (putting all the servers in distant data centers) concept wholeheartedly. Both the Army G-6 and DOD CIO have made moving to a cloud architecture for their enterprise-level services a major focus.[17] The positive effects of this are that complex, expensive servers and the unique expertise to run them can be consolidated into large strategic data centers outside the battlespace. The drawbacks of it are that user data is now physically far away from the user. This rarely impacts the mission, until one puts user networks at the other end of low-speed satellite links, as is the universal case with maneuvering battalions and brigades. Suddenly, the data pipes start to look more like an hourglass, with huge amounts of data up in the cloud, a very small neck of satellite connectivity constraining access to it, and a large group of users at the bottom of the hourglass (see Figure 1). The cloud's true achilles heel, however, is that when that neck is strangled, so is the tactical unit that relies on it. It is not

reasonable to assume that, in a peer-to-peer conflict, tactical units will not experience communications disruptions, or that tactical units will not choose to turn off transmitters in order not to draw fire.

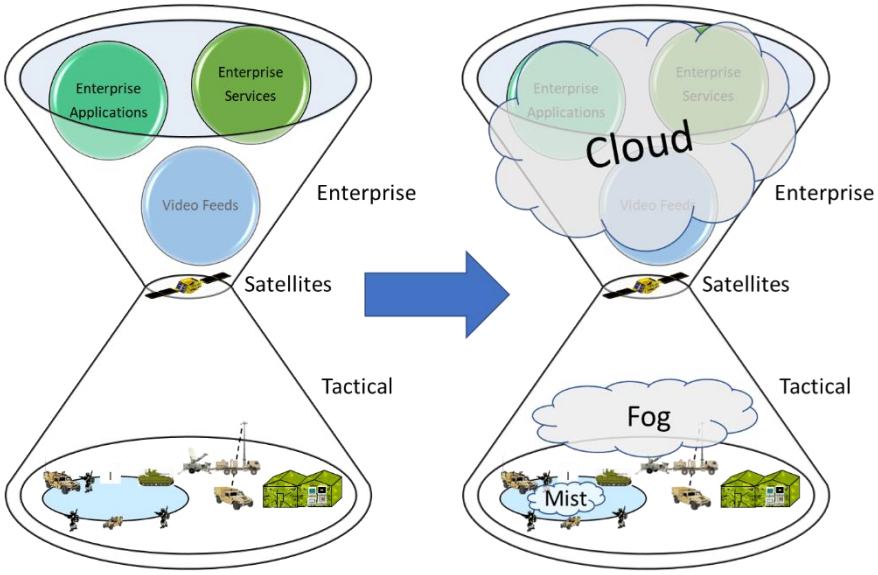


Figure 1. Solving the Hourglass Problem: Moving to Cloud/Fog/Mist Distribution[18]

A more useful paradigm for distributing services and their data is to think in terms of three tiers: cloud, fog, and mist.[19] Cloud services are up in the enterprise, fog services are enterprise-like services down at the tactical level (following the analogy that fog is a cloud that is on the ground), and mist services are the minimalist yet essential services that reside on an individual platform or in a small unit. Entire tactical formations in high-intensity conflicts with peer or near-peer adversaries will likely go days or weeks without access to the cloud, and so will have to rely on mist data and relatively close fog data an echelon, at most, above themselves. As such, rather than constantly driving toward more data and higher-bandwidth communications capabilities, the U.S. military should consider tailoring down the data required and simplifying the tactical-level of

communications by designing the synchronizing of enterprise-dependent services for extended periods of disconnectivity.

The third characteristic involves connectivity. At the strategic level of communications, people expect to be constantly connected. If a cell phone tower goes down, or a network glitch makes the internet temporarily unavailable, or if we cannot access Wi-Fi for whatever reason, we notice. There are a range of capabilities that do not depend on consistently transmitting, but are open to constant receipt of information. The voice channel on tactical radios is a good example of such capabilities: receiving voice traffic when others transmit, but only transmitting when pressing the handset button. However, for them to function as intended, most Communications, Command, and Control capabilities—including the current generation of tactical radios and smart phones—not only *can* be constantly connected, but *must* be constantly connected. For that matter, many users do not know how to keep their devices from transmitting. This has led to several security and privacy concerns similar to parents being able to track their children by their smartphones. Anyone with a rudimentary direction-finding capability can track tactical forces as well—in real time.[20]

Parents of bygone ages used simple control measures to track their teenagers, such as “Be home by dinner,” or “Come in when the streetlights come on.” Military commanders used similar control measures in the past with subordinate commanders. However, the advent of constant connectivity between echelons has led to a requirement to be constantly in contact, one of the key tenets of mission command.[21] This constant state of connectivity has led to a generation of leaders who expect to be tethered to their higher commander at all times, asking permission to employ weapons,

seeking permission for dealing with out-of-the-norm situations, and such. If units are going to have to maintain communications blackout or radio listening silence, in order to avoid targeting on the battlefields of the future, this new cultural norm must be consciously reversed.

If the U.S. Army is going to avoid the fate of several Ukrainian formations in any future near-peer conflict, tactical formations must learn to live in a disconnected state or use only local low-powered communications for significant amounts of time—only transmitting with mid- to long-range communications devices when on the move or when preparing to move.

Solutions by Aspect

Contemporary military networks are built on a number of underlying paradigms. Following is a fusion analysis of the weaknesses inherent in how the U.S. military has built its current communications systems, the future trends that will demand adaptation, and proposed characteristics that the U.S. military should build toward in order to meet these challenges for the coming decades of great power competition.

Hardening and Dispersing Satellites

The U.S. military currently relies on large, extremely expensive communications satellites, such as the Wideband Global Satellite (WGS) Communications and Advanced Extremely High-Frequency satellite constellations and their still-existent predecessors, as well as a host of civilian communications satellites, all of which sit in a geostationary orbit, which makes them very easy to locate and track.[22] These satellites have several vulnerabilities and disadvantages. Specifically, they are excessively expensive, vulnerable to attack, vulnerable to jamming, and take weeks to maneuver.[23] The United States must change its space capabilities paradigm by transitioning to

dispersed constellations of persistent nanosats and microsats (suitcase-sized satellites), taking a page from missile defense on anti-jam capabilities and finding terrestrial solutions either as primary or secondary capabilities to reduce dependence on satellites.[24]

With launch costs, each new WGS satellite costs approximately $1 billion, including launch and control software costs.[25] However, China clearly demonstrated to the world that they have anti-satellite missiles when they destroyed one of their own satellites in 2007, and they have a diverse and active anti-satellite program, as does Russia.[26] China's swarms of anti-ship missiles with their 2,500 mile range threaten U.S. sea dominance inside what they call the second-island chain and challenge the usefulness of aircraft carriers and most exquisite U.S. naval capabilities in a China-U.S. war.[27] Similarly, China's anti-satellite missiles and emerging anti-satellite capabilities also clearly show that the United States cannot count on a permissive space domain to host such exquisite and vulnerable targets as the current constellations of communications satellites.

Many more countries have jamming capabilities that can and will render U.S. and allied communications satellites unusable for extensive periods of time in any potential conflict. Chinese and Russian-made jamming equipment is prevalent enough, but making a local Global Positioning System (GPS) jammer does not take much more than a trip to any country's equivalent of Radio Shack and Home Depot.[28] Jamming GPS in a few kilometer radius is a trivial task. While the U.S. GPS satellite constellation is notoriously easy to jam locally, periodic and select jamming of communications satellite uplinks is not much more difficult.[29]

These vulnerabilities demand adaptation to mitigate the risks they pose. Conducting operations in a satellite-denied environment has already been added to the training environment at the National Training Center.[30] In order to provide a material adaptation to help warfighters overcome the challenges of a lack of satellite coverage, a number of things should be considered.

First, for the GPS challenge, in addition to the current M-Code (next generation encryption) efforts, inertial navigation must be much more widely implemented.[31] Additionally, there are automated navigation capabilities that leverage the stars to provide exact location, such as the Precision Pointing System on the WGS satellite constellation or existing and emerging celestial navigation ship systems.[32] Such a system works both at night and during the day. Defense Advanced Research Projects Agency is currently investigating alternative methods, leveraging microwave pulses such as those used by the U.S. Atomic Clock infrastructure, polar alignment, and other alternative methods.[33] The U.S. military needs to begin the maturation, miniaturization, and integration of other navigational technologies.

Second, for communication satellites, anti-jamming must be taken seriously. Being able to get all of a 256 kilobit per second highly-resilient link in a jamming environment is much better than getting none of a 1 megabit per second uncontested link. Dynamic Forward Error Correction and Dynamic Modulation technologies have become the mainstay of almost all modems in use tactically as of this writing.[34] It is time to build on that resilient foundation and adopt robust Cold-War strength anti-jam capabilities, such as those implemented by the Missile Defense Agency's standard modem, which is in the process of being miniaturized for tactical use.[35]

Third, for all satellites it is time to change the paradigm from constellations of a few large, monolithic, exquisitely expensive satellites to swarm-like constellations of small, disposable satellites. Networks of microsats and nanosats are an emerging technology, which have proven in the communications realm that they can collectively provide the same capabilities as today's satellites.[36] With a loiter time of a year or more and a price tag less than a hundredth of that of a conventional satellite—including launch costs—the U.S. military no longer needs to plan a fifteen or twenty-year lifespan for its satellites. It is much cheaper to simply launch a network of nanosats annually and make constant improvements with each succeeding generation.[37]

Additionally, small satellites sit in low-earth or medium-earth orbit as opposed to the highly contentious geo-stationary earth orbit. This almost eliminates the half-second of latency associated with today's communications satellites and accommodates terminals that operate on much lower power, reducing their electromagnetic signature and thereby making the terminal signatures harder for an adversary to detect and triangulate. Additionally, satellites in low-earth orbit and medium-earth orbit do not sit stationary in the sky, which makes them much more difficult to target for jamming while allowing the new generation of terminals with auto-tracking to leverage. Finally, being the size of bread boxes and trash cans, each individual nanosat in a globe-covering nanosat coverage network is both impractical to fire an expensive anti-satellite missile at and much more difficult to hit. Nanosats change the Satellite vs Anti-Satellite Missile economics.[38]

The U.S. Department of Defense is in different stages of the Analyses of Alternatives for both the Protected Satellite Follow-On and the Wideband Satellite

Follow-On constellations of satellites, which are meant to begin replacing today's military communications satellites by 2030.[39] To date, small satellites have not been seriously considered. The only non-standard discussions seem to have been evolutionary, not revolutionary, talking about the merits of the DoD building large satellites or simply purchasing hosted payloads on commercial satellites. Better to force the small satellite discussion now than in five or ten years when it is obvious that the DoD did not take the overall more robust, more protected, less expensive path, after the outbreak of hostilities with a near-peer competitor with anti-satellite capability and decides to use it. Indeed, if current trends continue, war in space may well be likely within years.[40]

Changing the Command Post Paradigm

The Chief of Staff of the Army, General Milley, laid out his vision of the future battlefield in an October 2016 speech: "There will no clear front line, no secure supply lines, no big bases like Bagram or Camp Victory with chow halls, air conditioning, and showers. With enemy drones and sensors constantly on the hunt for targets, there won't even be time for four hours' unbroken sleep."[41]

The Army must rethink how it commands and controls its forces at the battalion, brigade, and even division level. At the Army's semi-annual Network Integration Exercises at Fort Bliss, Texas, the time required to jump a battalion headquarters was approximately twelve hours. For a brigade headquarters, it was far longer. Just setting up a brigade tactical operations center (TOC) would commence before dawn and typically be completed around midnight.[42] At the National Training Center, the author heard reports from his field service representatives that brigade commanders decided to

“just take the casualties” rather than jump their brigade TOC when the observer-controller comes in with an artillery simulator.[43]

The sheer size and complexity of a modern command center has the unintended effect of limiting tactical forces’ ability to maneuver. How did this happen? The answer lies in understanding two dynamics. First, the Army has been engaged in a low-intensity conflict which has not routinely required maneuvering command posts for sixteen years. Just as people need to get up and move in order to keep trim, so do organizations and command posts. Second, this same set of low-intensity conflicts, matched with America’s native spirit of innovation, has led to a proliferation of capabilities that all seem to have found themselves in the command post: multiple computer networks of every classification, tactical drones and their video feeds, stacks of computer servers, miles of ethernet cables and hard flooring to protect it, and massive, inflatable tents to house it all. Two decades gone are the days of the expandovan, and the G-3 sergeants major seem to have lost the fight against command post bloat.

In order to address a problem, it helps to understand the problem and how it came to be. In the author’s talks with a former G-6 of the 82nd Airborne Division, the drivers behind some of the changes in the Army’s tactical command infrastructure became obvious. Though a more thorough study, rather than a back-of-the-napkin discussion, would likely yield more exact figures, the following story illustrates the trend.

In the 1990s the 82nd Airborne had a Division Main Command Post (DMAIN) of approximately 125 people, run by a Deputy Commanding General and a Division Tactical Command Post (DTAC) of approximately 25 people where the Commanding General (CG) was located. The G-6 (communications officer), then a lieutenant, was the

senior signal officer in the DTAC. Twenty years later in 2015, the G-6, now a lieutenant colonel, was again the senior signal officer in the DTAC, only the DTAC had grown to approximately 125 people. Because it had grown so large and lacked mobility, the CG had created an Assault Command Post (Assault CP) where he was located, which was approximately 25 people in size. Simultaneously, the DMAIN had grown from 125 to approximately 400 people.[44] Because the DMAIN was so unwieldy, a much more robust Home Station Mission Command Center was proposed and funded, the concept being to leave the DMAIN back at home station at the other end of a satellite link from the DTAC, which would serve as the DMAIN-Forward, with the Assault CP supporting the commander.[45]

The end state of all these moves will be to have the same size and roles of command post organizations as in the 90s, only with an essentially new organization of 400 people back at home station supporting the division via satellite link, as illustrated in this chart:

Table 1. 82nd Airborne Division Command Post Growth[46]

	DMAIN	**DTAC**	**ACP**
90's Div CPs	125	25	N/A
2015 Div CPs	400	125	25

In future conflicts, due to the driving necessity to maneuver or be defeated and the immobility of today's command posts or the tenuous links that connect them, divisions face the very real possibility of outrunning some of their command posts

(especially the home station portion), leaving them out of the fight and unable to support for large portions of the battle.

The disparity between General Milley's vision of a tactical army that can move every two to four hours, which echoes the survival recommendations from the Russia New Generation Warfare analysis, and the day-plus long process of jumping TOC today could not be more stark.[47] If the U.S. Army is going to be able to fight and win against the Russian Army or other near-peer adversary or collection of adversaries employing such tactics, a complete paradigm shift in how to conduct mission command must occur.

The Chairman of the Joint Chiefs of Staff has summed up the required changes as follows:

> Improve the Joint Force's ability to operate in contested and degraded information environments… This requires improving the force's ability to mitigate risk to its information systems through investment in advanced technologies. It also requires that the force improve its ability to operate with less information by developing alternative operating methods for degraded information environments and developing agile, adaptable leaders.[48]

Such fundamentally difficult problems suggest that a fundamentally different solution must be applied: to reduce or eliminate these vulnerabilities, the Army must transform its idea of how a command post should look. Applying the attributes of dispersion, mobility, ubiquity, and resiliency suggests a command cluster rather than a command post.

Dispersion and Mobility: Russian artillery may have a 4 to 1 advantage over U.S. and allied artillery, but it is still centrally commanded and controlled.[49] That centralization of command and control limits the number of targets that can be engaged simultaneously. Therefore, dividing a unit's leadership among a number of mobile and

dispersed nodes provides a set of medium to low-value targets rather than the current centralized command posts, which provide one high-value decapitation target. Army leaders must think outside the tent. Leveraging the model of today's Silicon Valley and sales professionals with mobile offices, it is not difficult to imagine a command cluster, rather than a command post, where a battalion commander and his staff each sit in their individual vehicles leveraging a low-footprint, mounted computing and communications capability, such as a next-generation Joint Battle Command-Platform or Mounted Family of Computer Systems connected via a line-of-sight spread-spectrum capability, to do ninety percent of their planning and administrative functions—and coming together for a face-to-face only rarely.[50] When in line of sight of each other, voice, video, and full data would be the tools of choice. When spread out and relying on small-drone or other relays to link the group together, these services could be scaled back to text or chat, with voice and file sharing when possible.

Ubiquity: Wherever there are communications on today's battlefield, there will be electromagnetic emissions. Relying on a lighter communications capability and putting it on every platform provides saturation. Such ubiquity will obviously advertise a unit's location, but ubiquitous fielding to every platform will also hide the more important targets among a myriad of indistinguishable targets—and security through obscurity can be one aspect of force protection. If the current command post gives way to dispersed staff functions leveraging the same communications suites as the logistics and maneuver vehicles, the enemy could be faced with an overwhelming number of indistinguishable targets.

Resiliency: Current hub-spoke satellite communications technologies are highly vulnerable to disruption via jamming of the satellite uplink. However, other technologies could and should be leveraged to build communications resiliency into tactical formations. Ultimately, multiple links between higher and lower echelons of command are the best method of ensuring resilient communications.

Large tropospheric scatter capabilities exist in the U.S. Army's Expeditionary Signal Battalions. It is not much of a technological leap to build and field much smaller, highly-mobile tropospheric scatter capabilities.[51] The acceptance of such a capability is only possible if the Army reduces the extremely high data rates required by current requirements documents and accepts that the primary links between higher-echelon and lower-echelon command clusters of necessity switch modes of connectivity or not be connected for periods of time.

Directional line of sight capabilities exist for a fraction of the exorbitant costs of WIN-T Increment 2's line of sight antennas, even today within the WIN-T program's labs as well as within the microwave and free-space optics commercial market. Relaying such communications via small, relatively cheap flying or ground relay drones is clearly in the realm of the possible already.

Perhaps the greatest step that can be taken for command post resiliency is training and allowing current and future maneuver leaders to operate independently of their higher headquarters within established control measures, as in generations past. In other words, the Army needs to exercise Mission Command, not Command and Control. This will help formations adapt to the periodic and partial connectivity that will

be the expected norm as the electromagnetic spectrum, space, and cyberspace domains become contested.

Tactical Vehicles and Platforms

The U.S. tactical advantage is in a state of hypercompetition.[52] Missile vs anti-missile systems, exploitation of the electromagnetic spectrum, the introduction of autonomous tactical platforms, and numerous other areas of competition have or are threatening to erode U.S. military dominance at the tactical level. Adversaries' ability to target and destroy U.S. combat vehicles and formations at longer ranges and with precision must force communications systems to adapt to the threat by taking several pages from past, now-unexercised practices of communications security.

Radio Listening Silence and Chirping: Vehicle commanders in a high-end, force-on-force fight against a near-peer adversary need to follow the procedures of generations past: pop up on the net, get what they need, then drop off again and move immediately or while communicating. Paired with spread spectrum transmissions (spreading the signal below the noise floor) and passive listening for connectivity requests, such burst transmissions have both a low probability of detection and they significantly reduce the windows where friendly troops can be found and targeted by an enemy exploiting their electronic signature.[53] As past generations learned when being hunted, carefully managing communications is key to not giving away position.

Resiliency: In order to help build resiliency into a unit's network, mobile ad-hoc networking or mesh networking can and should be adopted by tailoring the profiles for its use based on how permissive an environment is.[54] Mesh networking has the added benefit of being a native platform for peer-to-peer communications, easily enabling

Position Location Information and Friendly Force Identification at close ranges, as well as texting, file sharing, and more, generally enabling greater team interaction.[55]

In order to overcome the growing overdependence on satellite infrastructure, High Frequency (HF) radios (a cousin of the ham radio) can be readopted as a secondary means of beyond line of sight communications. HF radios were shelved by the U.S. Army in the 1990s and early in the wars of this century due to their low data rates and the sporadic over-the-horizon connectivity they provide. However, as they do not require satellites, HF radios are still in use worldwide by almost all countries' militaries (the United States being a glaring exception), including advanced allied partner nations.[56] Leveraging automation and other developments by NATO allies, HF can be improved and can become a viable voice and low-rate data (text, chat, file sharing) capability for Beyond Line of Sight (BLOS) communications without satellites.

Autonomy: A key aspect to survivability is the artificial intelligence required for unmanned vehicles to operate without a remote-control link back to a pilot and without having a lead vehicle to guide off of. Much as robotic supply convoy trucks follow a manned truck and predator drones return to base if their control link is severed, so all future unmanned capabilities will have to have the ability to operate without BLOS control, but with greater autonomy. If supply convoys are going to eventually operate completely unmanned and if unmanned helicopters or drones are going to be relied on to do casualty evacuation missions in a satellite-denied environment, then a high level of autonomous function and decision-making, enabled by autonomous waypoint navigation and independent decision-making, is going to have to be engineered into these platforms.

Conclusion

Since the end of World War II, the people of the United States of America have shown themselves to be the dominant world engine of innovation. The ongoing information revolution, powered primarily by U.S. inventions and companies, is a reconfirmation of the U.S. role of the world's lead innovator. The U.S. military has also proven to be a powerful force for innovation on the battlefield, as shown in the first Gulf War, the counter-insurgency victory in Iraq, in the nuclear and precision weapon offsets, and in hundreds of other examples.

These innovations have given pause to potential adversaries and changed their risk versus gain calculus, effectively deterring any actual challenge to the U.S. position of military dominance. However, adversaries and competitors have studied these successes and have built capabilities designed to leverage the U.S. communications' achilles heel. If the United States is to keep its battlefield advantage, then the United States must also adapt to deter.

Endnotes

[1] John F. Troxell, U*.S. Army War College Guide to National Security Policy & Strategy* (Carlisle Barracks, PA: U.S. Army War College, July 2004), 190.

[2] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, November 5, 2008), 2.

[3] Paul McLeary, "Army Looks to Replace $6 Billion Battlefield Network After Finding It Vulnerable," November 21, 2017, http://foreignpolicy.com/2017/11/21/army-looks-to-replace-6-billion-battlefield-network-after-finding-it-vulnerable/ (accessed 3 Feb 2018); Jared Serbu, "New Army CIO: Network We Have Is Not the Network We Need," August 2017, https://federalnewsradio.com/army/2017/08/new-army-cio-network-we-have-is-not-the-network-we-need/ (accessed 3 Feb 2018).

[4] U.S. Department of Defense, *Capstone Concept for Joint Operations*, Joint Force 2030 (CCJO), Draft Working Document, Predecisional (Washington, DC: U.S. Department of Defense, as of June 28, 2016), 12.

[5] Phillip Karber and Lt. Col. Joshua Thibeault, "Russia's New Generation Warfare," May 13, 2016, http://www.armymagazine.org/2016/05/13/russias-new-generation-warfare/ (accessed November 5, 2017).

[6] Ibid. See "High Casualties" section at end of report.

[7] Ibid.

[8] Troxell, *U.S. Army War College Guide to National Security Policy & Strategy,* 191.

[9] COL David C. Trybula, *"Big Five" Lessons for Today and Tomorrow* (Alexandria, VA: Institute for Defense Analyses, May 2012), http://www.benning.army.mil/Library/ content/ NS%20P-4889.pdf (accessed February 26, 2018).

[10] The modems the author managed at WIN-T only integrated anti-jam capabilities after over a decade in service. Additionally, in the author's experience of managing the Army's WGS transponder management program, almost every jamming incident experienced was from friendly forces or commercial entities misconfiguring their equipment.

[11] This observation came from the author's interactions with the requirements writers, higher echelon engineers, and satellite requirements developers. Also, to the best of the author's knowledge, only one modem that is still in production (the PAAWNS modem) has anti-scintillation (AS) capability.

[12] Jillian Rayfield, "Obama: The '80s Called, They Want Their Foreign Policy Back," October 23, 2012, https://www.salon.com/2012/10/23/obama_the_80s_called_they_want_their_foreign_policy_back/ (accessed February 3, 2018).

[13] Brian Everstine, "The Air Force's 'Forever War' Is Its Toughest Pill to Swallow," *Air Force Magazine*, February 1, 2018.

[14] Sydney J. Freedberg Jr., "Missile Defense vs. China, Russia: Decentralize, Disperse, & Hide," *Breaking Defense Online*, January 2018, https://breakingdefense.com/2018/01/missile-defense-vs-china-russia-decentralize-disperse-hide/ (accessed February 3, 2018).

[15] Commonly known problem within WIN-T. The author observed this first hand at a JROTC rotation in 2013. The author does not have awareness of improvements made after 2015 to this portion of the system.

[16] Based on the author's experience in the Warfighter Information Network-Tactical (WIN-T) Program Office.

[17] Jason Miller, "Army's Path to IT Modernization Buoyed by Private Cloud Pilot," December 2016, https://federalnewsradio.com/ask-the-cio/2016/12/armys-path-modernization-buoyed-private-cloud-pilot/ (accessed February 12, 2018); Terri Moon Cronk, "Defense Department to Move to Cloud Computing," December 21, 2017, https://www.defense.gov/News/Article/Article/1402556/defense-department-to-move-to-cloud-computing/ (accessed February 12, 2018).

[18] Author-generated figure.

[19] Michael J. Martin, “Cloud, Fog, and Now, Mist Computing,” December 24, 2015, https://www.linkedin.com/pulse/cloud-computing-fog-now-mist-martin-ma-mba-med-gdm-scpm-pmp (accessed February 12, 2018).

[20] Sydney J. Freedberg, “Jam The Russians: Army Electronic Warfare Kit Comes To Europe,” May 3, 2017, https://breakingdefense.com/2017/05/jam-the-russians-army-electronic-warfare-kit-comes-to-europe/ (accessed March 14, 2018).

[21] Headquarters, Department of the Army, *Mission Command*, ADP 6-0 (Washington, DC: Headquarters, Department of the Army, May 2012), ,https://usacac.army.mil/sites/default/files/misc/doctrine/CDG/adp6_0.html (accessed March 14, 2018).

[22] Australian Space Academy, “Locating Geosynchronous Satellites,” http://www.spaceacademy.net.au/watch/track/locgsat.htm (accessed March 14, 2018).

[23] Federation of American Scientists, *United States Space Systems: Vulnerabilities and Threats 2004* (Washington, DC: Federation of American Scientists, 2004), https://fas.org/pubs/_docs/10072004163734.pdf (accessed February 26, 2018).

[24] A good primer on microsats, as well as several relevant references, is located at https://en.wikipedia.org/wiki/Small_satellite (accessed February 28, 2018).

[25] Phillip Swarts, “Pentagon Ready to Launch First Upgraded WGS satellite,” November 30, 2016, http://spacenews.com/pentagon-ready-to-launch-first-upgraded-wgs-satellite/ (accessed February 12, 2018).

[26] Chinese Anti-Satellite [ASAT] Capabilities, https://www.globalsecurity.org/space/world/china/asat.htm (accessed February 12, 2012); Russia and Anti-Satellite Programs, https://www.globalsecurity.org/space/world/russia/asat.htm (accessed February 12, 2012).

[27] Harry J. Kazianis, “China's DF-26 Anti-Ship Ballistic Missile: What Does the Pentagon Really Think?” May 18, 2016, http://nationalinterest.org/blog/the-buzz/chinas-df-26-anti-ship-ballistic-missile-what-does-the-16260 (accessed February 12, 2018).

[28] GPS Signal Blocker ~ Ensure Your RIght To Privacy, https://www.youtube.com/watch?v=GavkPyhXGKU (accessed February 12, 2018).

[29] Robert K. Ackerman, “Space Vulnerabilities Threaten U.S. Edge in Battle,” June 2005, https://www.afcea.org/content/space-vulnerabilities-threaten-us-edge-battle (accessed March 14, 2018).

[30] Sean Kimmons, “'Space Kits' Help Soldiers Recognize Jamming on Comms Devices, Networks,” November 28, 2017, https://www.army.mil/article/197418/space_kits_help_soldiers_recognize_jamming_on_comms_devices_networks (accessed February 12, 2018).

[31] Capt Travis Mills, *M-Code Benefits and Availability*, (GPS.gov, April 29, 2015), https://www.gps.gov/multimedia/presentations/2015/04/partnership/mills.pdf (accessed March 14, 2018).

[32] "Options in the Stars: Automated Celestial Navigation Options for the Surface Navy," December 13, 2017, http://cimsec.org/options-stars-automated-celestial-navigation-options-surface-navy/34759 (accessed February 12, 2018).

[33] Jamie Lendino, "DARPA to Reinvent GPS Navigation Without the Use of Satellites," March 27, 2015, https://www.extremetech.com/extreme/202111-darpa-to-re-invent-gps-navigation-without-satellites (accessed February 3, 2018).

[34] While a simple Wikipedia search can reveal what FEC and Modulation are in the context of modems, the "Dynamic" part of that is the ability to change FEC rates or modulation schemes in reaction to weather, scintillation, or jamming. For example, if bad weather is generating errors in a signal, DFEC and DM would increase the FEC rate automatically and in real time to account for the errors and decrease the modulation rate to provide a less error-prone signal.

[35] Protective Anti-Jam/Anti-Scintillation Wideband Net-Centric (PAAWNS) Modem. Author's knowledge from experience in the Wideband Enterprise Satellite Systems (WESS) program office within Army PEO Enterprise Information Systems.

[36] A good primer on this subject, as well as several relevant references, is located at https://en.wikipedia.org/wiki/Small_satellite (accessed February 28, 2018).

[37] BBC, "The Disruptors; the New Space Race," http://www.bbc.com/news/resources/idt-sh/disruptors_the_new_space_race, (accessed February 12, 2018).

[38] The cost of anti-satellite missile programs are classified. However, the estimated cost to the U.S. of shooting down one malfunctioning satellite was $30-60M (http://www.cnn.com/2008/TECH/02/15/spy.satellite/). By comparison, the cost of putting up a constellation of tens of microsats or nanosats has fallen precipitously and is likely in the hundred million or so range (http://www.defenseone.com/technology/2018/01/cost-put-microsatellite-constellation-space-just-fell-through-floor/145405/), far less than the $400-$600M to shoot them down, if they could be hit.

[39] Based on author's involvement in the listed efforts.

[40] Colin Clark, "CSAF Predicts War In Space 'In A Matter Of Years'," https://breakingdefense.com/2018/02/csaf-predicts-war-in-space-in-a-matter-of-years/ (accessed February 28, 2018).

[41] Miserable, Disobedient & Victorious: Gen. Milley's Future U.S. Soldier, October 2016, https://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/ (accessed February 17, 2018).

[42] From the author's experience, as documented in the following article: Amy Walker, "Army to introduce new command post wireless capability," https://www.army.mil/article/149704/Army_to_introduce_new_command_post_wireless_capability/ (accessed February 28, 2018).

[43] From the author's 2015 discussion with his field service representatives.

[44] Personal discussions between the author and the 82nd Airborne Division G-6 in 2015.

[45] Lt Gen Robert S. Ferrell, "Enabling the Army Network for a Complex World," October 2, 2015, https://www.army.mil/article/156585/enabling_the_army_network_for_a_complex_world (accessed March 20, 2018).

[46] Based on the author's conversations with the 82nd Airborne Division's G-6 in 2015.

[47] Phillip Karber and Lt. Col. Joshua Thibeault, "Russia's New Generation Warfare," May 13, 2016, http://www.armymagazine.org/2016/05/13/russias-new-generation-warfare/ (accessed November 5, 2017).

[48] U.S. Department of Defense, *Capstone Concept for Joint Operations*, Joint Force 2030 (CCJO), Draft Working Document, Predecisional (Washington, DC: U.S. Department of Defense, as of June 28, 2016), 9.

[49] War on the Rocks, "Outnumbered, Outranged, and Outgunned: How Russia Defeats NATO," April 2016, https://warontherocks.com/2016/04/outnumbered-outranged-and-outgunned-how-russia-defeats-nato/ (accessed February 17, 2018).

[50] PEO C3T Website, http://peoc3t.army.mil/mc/jbcp.php (accessed February 17, 2018).

[51] PEO C3T Website, http://peoc3t.army.mil/wint/tropo.php (accessed March 20, 2018).

[52] Wikipedia, "Hypercompetition," https://en.wikipedia.org/wiki/Hypercompetition (accessed February 17, 2018).

[53] Wikipedia, "Spread Spectrum," https://en.wikipedia.org/wiki/Spread_spectrum (accessed March 20, 2018).

[54] Wikipedia, "Mobile Ad Hoc Network," https://en.wikipedia.org/wiki/Mobile_ad_hoc_network (accessed March 20, 2018).

[55] Based on author's experience with special operations.

[56] The author has had these conversations with British, Australian, and NATO communications counterparts over time. Additionally, a cursory search reveals many articles from individual militaries about their own HF radio infrastructure.