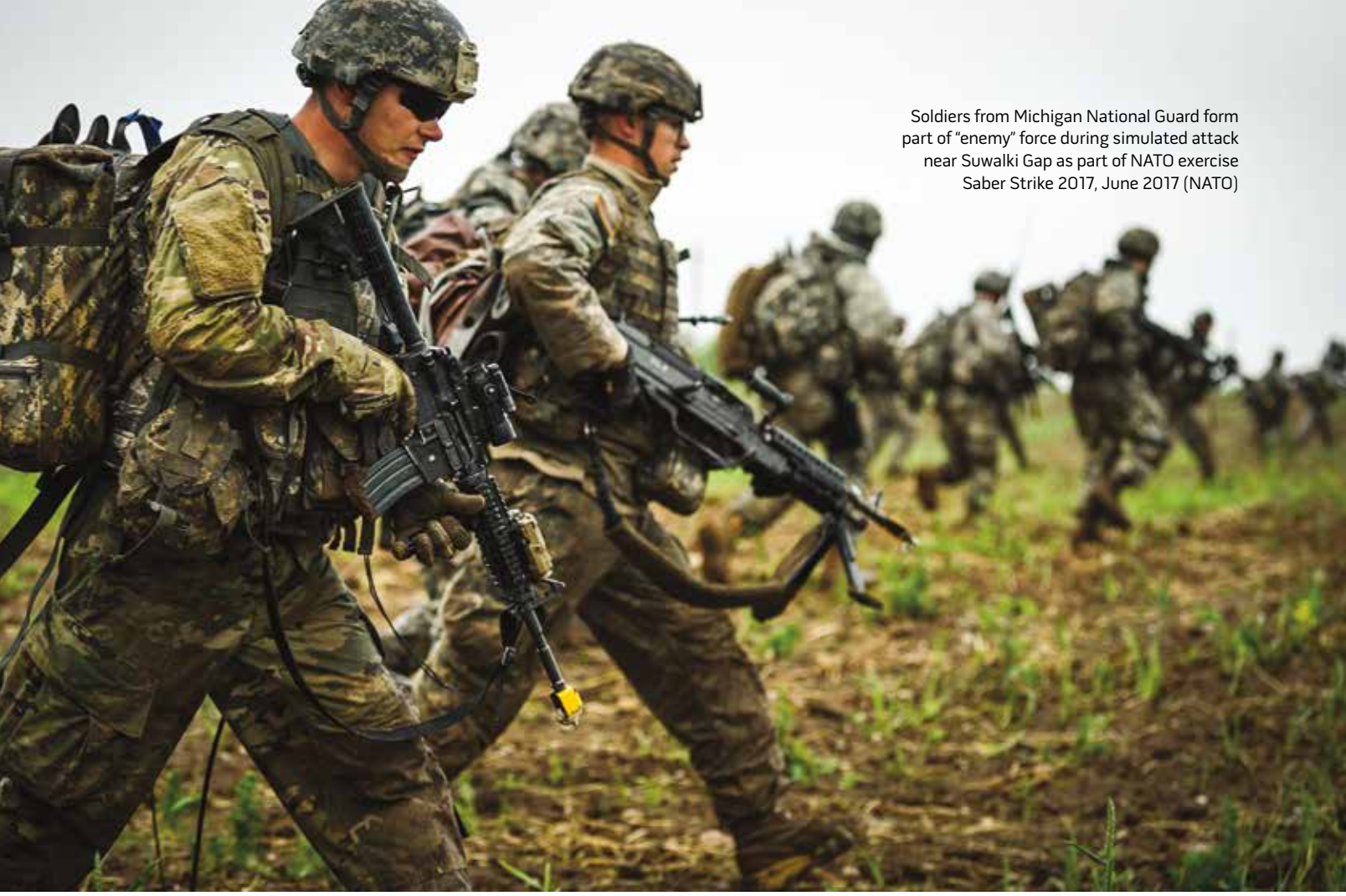


Soldiers from Michigan National Guard form part of "enemy" force during simulated attack near Suwalki Gap as part of NATO exercise Saber Strike 2017, June 2017 (NATO)

Electronic Warfare in the Suwalki Gap

Facing the Russian "Accompli Attack"

By Jan E. Kallberg, Stephen S. Hamilton, and Matthew G. Sherburne

The Joint Operating Environment 2035 predicts that for the foreseeable future, U.S. national interests will face challenges from both persistent disorders and states contesting international norms.[1] One of these outfalls could be "accompli" attacks from near-peer and peer states to exploit disorder, challenge international norms, and enjoy a quick advance with a limited resistance that cannot be realistically reversed. The rapid attack could establish territorial gains requiring a large-scale land war to liberate—with the imminent threat of an escalation to nuclear war—and the potentially massive cost in life, pain, and devastation to reverse the attacker's gains could be used to get negotiation leverage for the attacker in a final peace settlement. The attacker could also escalate the conflict once its territorial objectives are reached by declaring that a counteroffensive by the North Atlan-

Dr. Jan E. Kallberg is an Assistant Professor of Political Science in the Department of Social Sciences at the United States Military Academy at West Point and a Research Scientist in the Army Cyber Institute (ACI) at West Point. Colonel Stephen S. Hamilton, USA, Ph.D., is an Academy Professor at West Point and the Technical Director of ACI. Major Matthew G. Sherburne, USA, is Mission Team Lead, 156 Cyber Protection Team, at 1st Cyber Battalion, Cyber Protection Brigade, Fort Gordon, Georgia.

tic Treaty Organization (NATO) could face a tactical nuclear response, practically denying the Alliance the option to free the occupied territory with conventional military means.

In Eastern Europe, a rapid invasion in various scenarios could create a fait accompli attack that favors the Russians. Possible settings include the Baltic states, the Suwalki Gap to open a corridor to Kaliningrad, parts of eastern Poland, or the northern sector of Nordkapp and Svalbard as a perimeter defense of Murmansk. According to a U.S. Army publication, a "fait accompli attack is intended to achieve military and political objectives rapidly and then to quickly consolidate those gains so that any attempt to reverse the action by the [United States] would entail unacceptable cost and risk."[2]

The rapid accompli attack would likely be well planned because the attacker would have the time to prepare and identify targets and goals pivotal for reaching the desired endstate. Today's information-rich public environment and public access to infrastructure in the potential target area enable the covert planning of an accompli attack with a high level of granularity and certainty regarding the physical environment in the target area. In this planning, the attacker needs to validate assumptions of future outcomes of the engagement with the defending force, as these assumptions must be true for strategic success.

The first assumption is that the United States and NATO would not be the first to use nuclear arms. Kenneth Waltz writes, "Deterrence depends on what one can do, not on what one will do."[3] As long as the United States and the Alliance have nuclear capabilities, this assumption is a part of the equation for a potential attacker planning an accompli attack. Even if NATO has a declared posture not to be the first actor to use nuclear arms, it is irrelevant, as an actor could change its will and intent within a fraction of a second. It cannot ignore the presence of nuclear capabilities.

The second assumption is that the movement of larger U.S. and NATO forces to the theater will take more time than the Russian advancement. Depending on the scenario, the time for ground force formations to arrive from Western Europe and the continental United States could be several weeks after factoring in uncertainty for readiness, activation, and capacity.[4] Recent joint NATO and U.S. exercises such as Trident Juncture 2018 have shown the complexity and time expenditure of moving large formations across Europe. These movements are preplanned and in peacetime. In a conflict, the sea port of debarkation (SPOD) and aerial port of debarkation (APOD) can be assumed to be under attack from standoff weaponry and hypersonic missiles. Even if U.S. and British forces arrived in the Netherlands, Belgium, and Germany, eastern Poland is still 800 miles farther east, equal to the distance between Chicago and New York City. Also, there are three major river crossings: the Elbe, the Oder, and the Vistula. In a darker scenario, disruptions through cyber effects and infrastructure sabotage have occurred already, as units seek to leave home bases toward ports of embarkation.

The estimates for the arrival of major U.S. forces to the theater depend on variables that are hard to quantify with certainty, but we assess it to be several weeks. Partial air assets, smaller formations, and U.S. forces already in Europe will arrive sooner. The European NATO countries are likely not activating and mobilizing their main unit formations until the accompli attack is under way. The NATO fixed command and control facilities are likely targeted in the initial hours of the accompli attack by Russian ballistic, cruise, and hypersonic weapons. This will lead to increased confusion and disruption and will lay a foundation for Russian information dominance. These factors add to the concern over the length of time needed for friendly units to arrive in theater.

During the past year, U.S. lawmakers have raised concerns about the readiness and capacity of military sealift.[5] For an adversarial planner of an accompli attack, this time lapse until major forces arrive in the theater represents a window of opportunity. Even if Russia is strategically inferior to the United States and NATO, the rapid accompli attack expects to face resistance from only a fraction of U.S. and NATO forces during its short execution.

The third assumption is that the Russians can break up the joint forces and disallow multidomain operations limiting the fighting abilities of the present ground force. The fourth assumption is that the adversary's advantage in electronic warfare can neutralize U.S. and NATO forces' ability to communicate, leading to the adversary's information supremacy. Indirectly, if the fourth assumption is valid, the third assumption is then validated because the electronic attack on satellite communications and line-of-sight (LOS) tactical radio would deny joint operations and the utilization of air strikes and standoff weaponry. In a future peer conflict, a strategic surprise by the loss of ability to communicate due to electronic warfare is a tangible threat that could break up joint forces, disallow multidomain operations, and paralyze the defender; meanwhile, the adversary will advance with momentum and force.

Senior Army leadership presented the change in the strategic and tactical environment in an email to the force: "Many of the conditions we have grown accustomed to over the past eighteen years will not exist in future battles. Control of the air will be contested; Forward Operating Bases will not provide a safe haven; units will be continuously targeted by enemy fires; and communications and navigation systems will be intermittent at best."[6]

For a potential future conflict with capable near-peer adversaries such as Russia, it is notable that they have heavily invested in the ability to conduct electronic warfare (EW) throughout their force structure. During the Cold War, the Soviets advanced electronic warfare and used both active EW and passive means in the electromagnetic spectrum (such as direction finding and signals intelligence).[7] The Russians benefit from decades of uninterrupted prioritization and development of EW. Skills and techniques inherited from the Soviet Red Army are today the foundation for Russian ground force EW doctrine. The

Russian integration ranges from a company-size EW unit at the brigade level, a battalion-size EW unit in the Russian combined arms army, to an EW brigade in the military district.[8]

In the early days of a conflict in Eastern Europe when the primary U.S. and allied EW assets are still in Western Europe and the continental United States, the Russians would likely have a first-mover advantage and would be seeking information supremacy by denying and degrading the defending forces' communications. In a future peer conflict, a strategic surprise by the loss of the ability to communicate due to electronic warfare is a lethal threat. The Russians are not alone in upgrading their EW abilities. Several potential peer and near-peer adversaries are increasing their efforts to counter U.S. forces by denial of the radio spectrum through jamming and other EW efforts. Especially vulnerable are satellite communications (SATCOM), very high-frequency (VHF), and ultra high-frequency (UHF) line-of-sight communications, all of which U.S. forces depend on in the multidomain fight. The U.S. and NATO forces have had limited experience with EW against tactical communications since the end of the Cold War three decades ago and almost two decades of counterinsurgency operations. During these recent decades, U.S. and NATO forces have experienced undisrupted VHF, UHF, and SATCOM. These communication modes provide reliable high-bandwidth communications allowing streaming video and high-volume data transfers. Friendly forces cannot assume that there will be undisrupted communication and bandwidth in the future; the adversary will exploit and take advantage of a single point of failure found in the friendly force use of only LOS communication channels.

The Initial Conflict

Hostile electronic warfare elements deployed within theaters of operation threaten to degrade, disrupt, or deny VHF, UHF, and SATCOM. In this scenario, high-frequency (HF) radio is a viable backup mode of communication. HF radio systems have limited bandwidth that does not allow streaming video, massive data flows, and larger files to be shared. However, it has a capacity sufficient to transfer short messages and support command of the ongoing fight.

The focus in recent years has been on Russian hybrid warfare and special forces, but if there is a future peer-to-peer conflict with Russia, the main encounter will be with the core of the Russian army: the infantry and armor. The Russian army focuses on an offensive posture favoring an intensive and aggressive initial stance in the early stages of a conventional conflict.[9] The Russian army has inherited a legacy from the Soviet Union, where electronic warfare is an integrated part of maintaining speed in the offensive.[10] It enables forward-maneuver battalions to engage and create disruption for the enemy and an opportunity for exploitation.

Russian Doctrine and Inherited Soviet Offensive Tactics

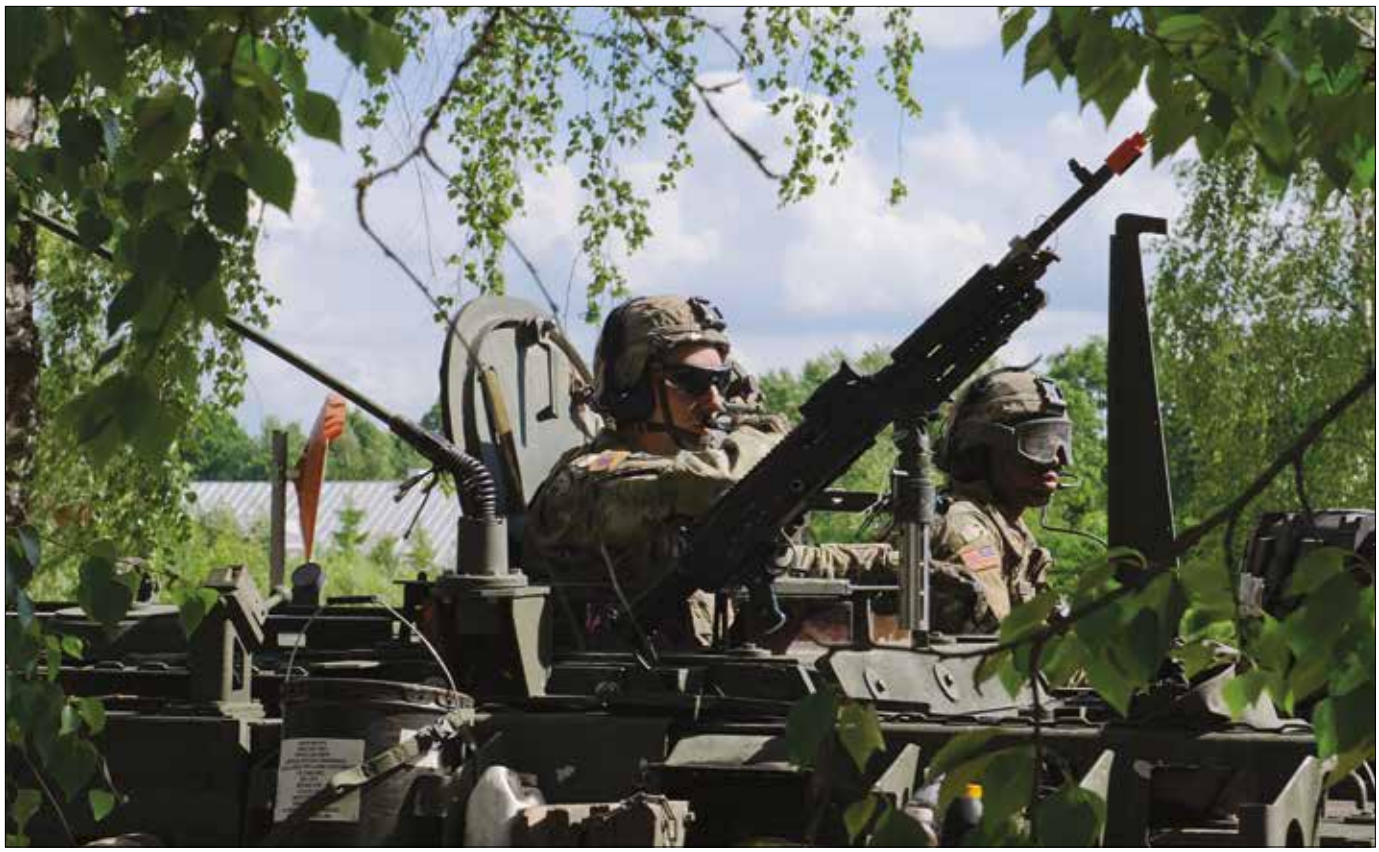
The Russian EW tradition goes deep. In the early days of the Soviet Union, the Communist leadership focused on hard science, equating science with progress. Science, in combination with ideology, would lead the way to the utopian society that the Communists envisioned. Once they took ownership of the means of production and the riches of Russia, science would enable a more prosperous and better life. Science was knowledge, and in the hands of the working class it became an alternative to religion. This also led to advances in math, physics, chemistry, and other natural sciences. As a result, the Soviets had advanced EW abilities in the early 1950s, and Russia has maintained the capability through the years.

Recently, Russia has executed hybrid warfare, specifically in the Donbas region of Ukraine. This action displayed a doctrine utilizing multiple attack vectors to seek information dominance. These different attacks are information operations to confuse, cyber attacks and electronic warfare to deny the adversary access to the spectrum, and direct kinetic strikes on the adversary information infrastructure.[11] At a strategic level, before a conflict takes place, the Defense Intelligence Agency (DIA) notes the Russian doctrine: "Russian propaganda strives to influence, confuse, and demoralize its intended audience, often containing a mixture of true and false information to seem plausible and fit into the preexisting worldview of the intended audience."[12] The doctrine seeks to create cleavages and exploit internal tension in targeted societies as well as to weaken societal cohesion and willingness to fight. The formal Russian phrase is *information confrontation*, which utilizes all means to gain an advantage over another state by using information as a vehicle, and this concept is both technical and psychological.[13]

The psychological goal is to influence adversary beliefs, perceptions, choices, preferences, and decisions, and serves as a psychological weapon, following the heritage of the Soviet propaganda apparatus. This information manipulation is often termed "perception management," which is focused on how the target perceives reality and its options instead of its perception of Russian abilities.[14]

The Russian doctrine seeks dominance as early as possible in a conflict, during the initial period of war.[15] When Russian strategic leaders assess that conflict is imminent (and in the accompli attack, they are the first to know), the initial stage is entered with the goal of reaching information dominance to support the speed and mobility of contemporary operations. The force is designed to be offensive and to seek dominance early in the conflict, creating early stage opportunities for exploitation by splitting NATO multinational and joint operations through denial-of-spectrum access. Information dominance becomes the nonnuclear way to break through U.S. and NATO defenses. Vladimir Slipchenko, the Russian general and influential military thinker, wrote that "superiority over an opponent was only possible after superiority in information, mobility, and rapidity of reaction were assured."[16]

Earlier, the Soviet offensive doctrine emphasized the use of tactical nuclear



Soldiers with Enhanced Forward Presence Battle Group Poland arrive in Rukla, Lithuania, after 2-day tactical road march across Eastern Europe, June 18, 2017, as part of exercise Saber Strike 17 (U.S. Army/Justin Geiger)

weapons to maintain momentum and thrust in the assault: "Nuclear strikes do not represent some kind of isolated act, but a component of combat. The operations of tanks and motorized rifle units are closely coordinated with them. Nuclear strikes and troop operations represent a uniform and inseparable process joined by a common concept."[17]

In the Soviet-Russian army from the 1960s and forward, the basic building block of the order of battle has been the motorized rifle regiment, and the dominant tactical stance is offensive.[18] A DIA publication titled *The Soviet Motorized Rifle Battalion* includes a short introduction to Soviet doctrine:

Soviets stress the decisive nature of the offensive and emphasize the meeting engagement more than any other type of offensive action. High rates of advance are anticipated from the actions of combined arms units operating in conjunction with airborne, airmobile, and special operations forces in the enemy rear area.[19]

The same publication describes combined arms:

The Soviets identify three types of combat action—the meeting engagement, the offense, and the defense. The offense is further subdivided into the attack and its exploitation, and pursuit is culminating in encirclement. The offensive is conducted by maximizing maneuver, firepower, and shock action.

The Russian doctrine favors rapid employment of nonlethal effects, such as electronic warfare, to paralyze and disrupt the enemy in the early hours of conflict.[20] The Russian army inherited the legacy of the Soviet Union and its integrated use of EW as a component of a greater campaign plan, enabling freedom of maneuver for combat forces. The backbone of Russian doctrine for maneuver warfare tactics has remained almost intact since the Cold War. The rear echelons are postured to to utilize either a single envelopment, to attack the defending enemy from the rear, or a double envelopment, to destroy the main enemy forces by unleashing the reserves. Ideally, a Russian motorized rifle regiment's advanced guard battalion makes contact with the enemy and quickly engages on a broader front, identifying weaknesses permitting the regiment's rear echelons to conduct flanking operations. These maneuvers, followed by another motorized regiment flanking, produces a double envelopment and destroys the defending forces.

The Russian formation is likely to seize and retain as much ground as possible before the enemy can react—producing either a decisive victory or a prolonged low-intensity conflict. Russian forces need an advantage that paralyzes NATO and U.S. troops. In World War II, the overwhelming massed artillery fire that fixed or destroyed the enemy paved the way for the advancement of forces. During the Cold War, tactical nuclear munitions were intended to paralyze and disperse the NATO defenses.

In the coming decade, it is highly plausible that the Russians could execute an already prepared preconflict EW blitz, seeking information dominance that degrades or denies VHF, UHF, and SATCOM. When these communication modes are degraded, having the ability to use HF communication will enhance the U.S. and NATO ability to communicate.

Reliance on LOS Communications

After two decades with uncontested spectrum, the Armed Forces are used to having available bandwidth, communications, and ability to switch between communication channels with limited interruption and excellent quality. Counterinsurgency operations have provided rear operational areas with a stable energy supply, the ability to set up satellite and radio links, and stable communication channels to higher commands, air assets, medical resources, and the logistics chain. Our potential near-peer adversaries are fully aware of our dependence on these communications channels and how their loss would impact the U.S. way of warfighting. Satellite communications are especially vulnerable for several reasons. First, the satellites transmit at lower power levels, making them easier to jam. Second, weather and space weather (solar flares) can negatively impact satellite communications. Third, the compact and fragile design of satellites themselves makes them subject to failure due to space debris or potentially an attack from an adversary's satellite. Finally, the satellites can be difficult to upgrade and could, over time, be vulnerable to cyber attacks.[21]

Former Deputy Secretary of Defense William J. Lynn III noted that

the willingness of states to interfere with satellites in orbit has serious implications for our national security. Space systems enable our modern way of war. They allow our warfighters to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity. Without them, many of our most important military advantages evaporate.[22]

Avoiding Strategic Surprise

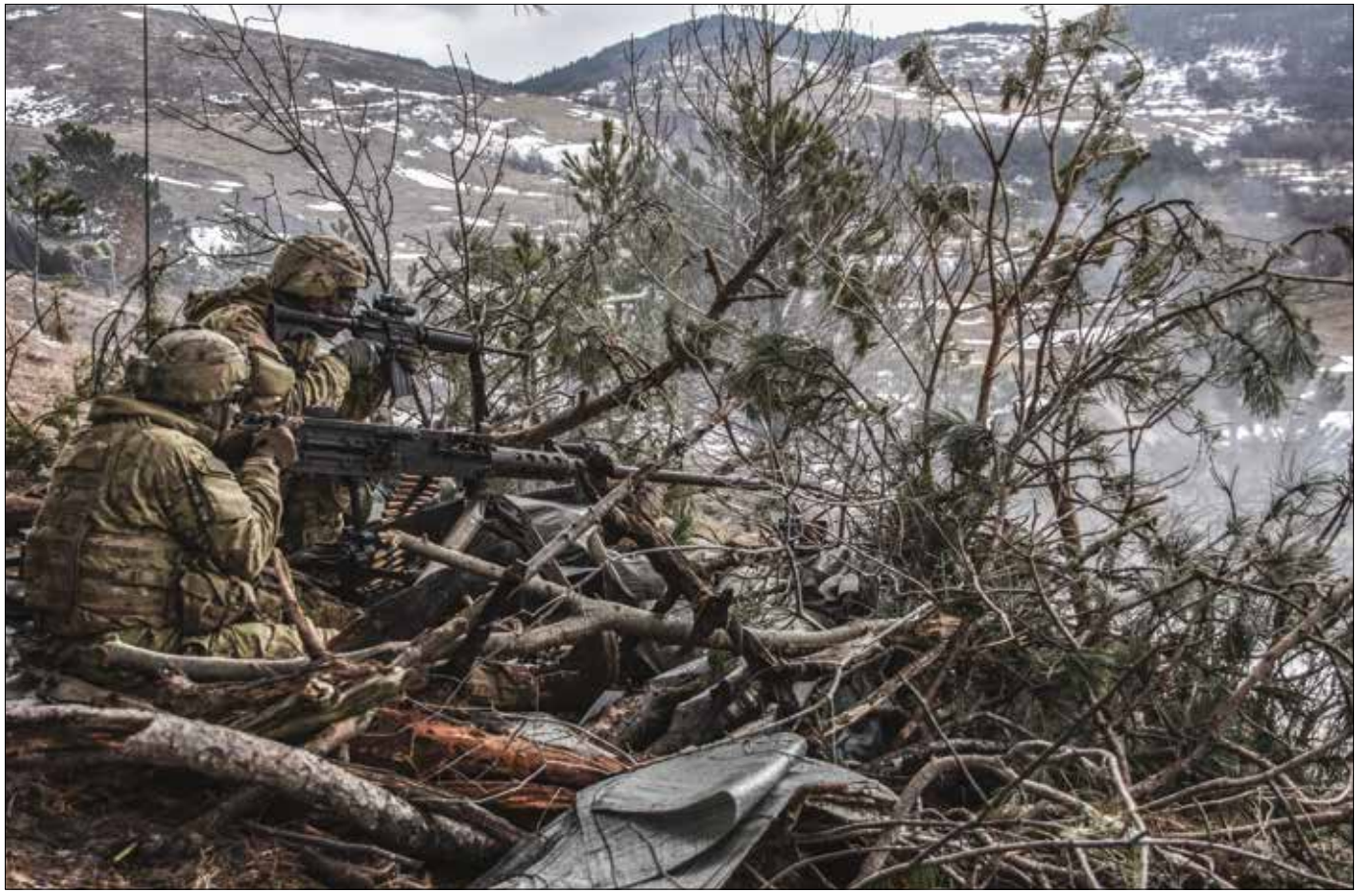
The Russian investment in EW capabilities is significant, and EW units are organic to any Russian formation from the brigade combat team and higher. This can provide a significant strategic advantage in the early stage of a conflict. The Russian formations can already engage cyber and electromagnetic effects in the initial period of war.

U.S. and allied ground forces could offset initial strategic inferiority with airpower, naval power, and global strike capabilities, but doing so depends on communication channels between ground forces and joint assets. The focus of the adversary's electronic warfare is to deny U.S. communications. One alternative is to retrograde and utilize HF communications, which was the communication channel of World War II and the Korean War. HF radio waves propagate by bouncing off the ionosphere, allowing for beyond-LOS communications. Due to the skywave propagation pattern, it is more difficult for the enemy to perform spectrum denial. Also, modern digital transmission modes allow for communications to occur at low power levels, complicating adversary detection.

The Army's ability to employ HF radio systems has atrophied significantly since the Cold War, as the United States transitioned to counterinsurgency operations. Meanwhile, the Air Force and Navy have maintained a fundamental ability. Alarmingly, as hostile near-peer adversaries reemerge, it is necessary to reestablish HF alternatives should VHF, UHF, or SATCOM come under attack and be lost as viable options for battlefield communications. HF communication has its inherent weaknesses and challenges, but they do not negate the fact that it can provide communications beyond the line of sight, which can serve as an alternative in critical junctures. By stepping back and being able to retrograde to HF as a resiliency measure, the United States is increasing communication redundancy. This also adds an asymmetric advantage when the adversary has to divert EW assets with a different set of requirements to address the HF ability, which requires more resources to disrupt and degrade. The HF propagation patterns would send signals to broader areas, which allows the adversary to hear the signal and direct countermeasures, but it also will enable parts of the propagation to pass through sufficiently to get communication established even in a highly saturated EW environment.

HF jamming equipment requires more energy and has a significant signature, which enables U.S. and NATO neutralizing attacks with standoff weaponry and anti-radiation missiles to be successful. The Russian armed forces utilize HF communications as well, and a broad and unrestricted HF jamming can degrade and disrupt their own communications. There is also a possibility that the HF transmission propagates in a way that cannot be heard by the adversary, providing an undisrupted communication. On the other hand, LOS communications have a more narrow propagation channel, which allows the EW attacker higher certainty that communications are denied or degraded.

All the branches have limited competency with HF radio systems; however, there is a strong case to train and ensure readiness for the utilization of HF communication. Even in electromagnetic spectrum (EMS)–denied environments, HF radios can provide stable, beyond-LOS communication, permitting the ability to initiate a prompt global strike. While HF radio equipment is also vulnerable to electronic attack, it can be difficult to target when configured to use near-vertical incident skywave (NVIS) signal propagation. This high-angle take-off propagation method provides the ability to refract signals off the ionosphere in an EMS-contested environment, establishing communications beyond the line of sight out to 400 miles. Due to the high-angle signal path, the ability to direction find and target an HF transmitter is more complicated than transmissions from VHF and UHF radios that transmit LOS ground waves. Also, Russian listening posts located outside of the 400-mile radius cannot intercept the communications. The recent digital modes utilizing 3G Automatic Link Establishment (ALE) technology allow for



Soldiers from 173rd Airborne Brigade prepare for Joint Warfighting Assessment 18 in Grafenwoehr, Germany, April 2018 (U.S. Army/John Hall)

digital communication at lower power levels than what was previously required for voice. This technology allows for tac chat messaging along with digital voice within a 3G ALE network. Using lower power is a crucial advantage when trying to prevent direction finding, and adding encryption to the digital signal helps prevent signal interception. These are low-cost opportunities for the United States to increase unit survivability and battlefield effectiveness by achieving a stealthier communication channel that potential adversaries will have difficulty locating.

The expense to attain an improved HF-readiness level is low compared to other Department of Defense initiatives, yet the return on investment is high. The equipment (Harris AN/PRC-150) has already been fielded to maneuver units. The next step is leaders prioritizing soldier training and employment of the equipment in tactical environments, linking to HF networks, and integrating the HF networks into the joint force.

After almost three decades of limited interest for ground force HF communications, there are knowledge gaps to fill to ensure the optimal tactics, techniques, and procedures. Science and technology have advanced during these decades; therefore, there are multiple opportunities to cost-effectively enhance and improve the HF communication ability, especially pushing targeting data through HF communications. The revival of HF communications as a resilience measure will posture the joint force in a state of higher readiness for future conflicts.

Recommendations

We propose five activities that would rapidly improve joint force and NATO ability to utilize HF as an alternative communication channel in the future fight.

First, each branch of the joint force must train on the equipment already fielded with the focus on establishing communication in an EW-saturated environment. The HF equipment is seldom properly used or connected in an HF network.[23] The equipment is in many cases assembled and tested to see if it transmits but is not integrated into the exercises as a fallback when other ways of communications fail. All branches of the Armed Forces have through the years acquired significant knowledge about how to use HF, but since the end of the Cold War, the understanding and experience are no longer shared on a large scale. An instrumental path to success in an HF training program is understanding HF antenna configurations. Since HF is a beyond-LOS communication channel, operators must understand how to optimize antenna arrangements depending on where they intend to propagate their signal. These skill sets are in many cases today almost nonexistent, even if the unit has fielded HF equipment and needs to be trained. This training can be supported by online training, applications that provide guidance for directions, antenna configuration, optimal transmission

Space and Missile Systems Center's Wideband Global SATCOM-10 encapsulated satellite, mated with Delta IV launch vehicle, stands ready for launch at Cape Canaveral Air Force Station, Florida, March 15, 2019 (Space and Missile Systems Center/Van Ha)

power, and advice on how to create ad hoc antennas. The ability to communicate using HF within the joint force and with NATO requires that each branch first and foremost can communicate within itself.

Second, a revised joint spectrum management effort within U.S. European Command and other unified combatant commands is necessary to ensure optimal usage of a limited spectrum. The HF range provides NVIS, which creates propagation patterns that cover 300 miles and would serve a theater. The increased HF range compared to tactical LOS communication requires predefined spectrum management.

Third, HF communication must be injected as a part of the operations in joint and multinational exercises. The East European NATO armies have upheld an HF capacity since the Cold War. In an accompli scenario, the ground forces that are engaged in the initial fight are Baltic, Polish, and East European forces. For these forces, HF is an integrated part of their communications, and the ability to fight as a unified NATO force is strengthened by a coherent ability to use HF communications. Joint and multinational exercises should include HF training and maintenance and the ability to relay messages, create simple HF networks, and transfer tactical and operational data through them. The HF networks' ability to transfer data is limited, but orders, directions, calls for fire, and updates can be text messages that parsimoniously use bandwidth.

Fourth, HF capacity, once seen as obsolete and replaced by VHF/UHF, has been removed to free up space and lower weight in several fixed-wing, helicopter, and vehicle assets. In some cases, versions of a particular platform can differ in the ability to communicate using HF where the older version has the HF ability as delivered from the factory in the 1990s while the updated version has had HF radios removed. This requires retrofitting HF ability back into the platform. Each branch of the Armed Forces needs to add, modify, and update the HF capacity, even if the equipment is fielded to fighting formations and the ability across the branches is fragmented and not uniform.

Fifth, in our view, the ability to connect the fight on the ground to joint and NATO strike abilities is pivotal to delay, disrupt, and destroy Russian progress in an accompli attack and slow down the advance until major NATO formations arrive. Joint Terminal Attack Controllers (JTACs) and their NATO equivalent, affected by adversarial electronic warfare, are of no operational value if they cannot communicate the targeting information. The rapid injection of JTAC ability across the theater, even in the territorial forces of our East European allies (such as the Polish Territorial Defence Force, which uses HF to communicate), brings the strike abilities of the joint force to NATO forces on the perimeter that risk being overrun by a rapid Russian advancement.

Mechanized infantry battalion 45 Painfbat, Regiment Infanterie Oranje Gelderland, Royal Netherlands army, during cold weather training as part of NATO's exercise Trident Juncture 2018, Norway, October 2018 (Courtesy NATO/The Netherlands/Hille Hillinga)

As General Mark Milley stated, "Units will be continuously targeted by enemy fires; and communications and navigation systems will be intermittent at best."[24] In a combat environment where communication systems will be intermittent, we have sought alternative solutions to ensure that the JTAC communication goes through even if SATCOM and VHT/UHF fails, where theater-wide HF NVIS was presented as an alternative route. If HF NVIS fails, the Military Auxiliary Radio System (MARS) could fill a new modern role where JTAC and other tactical information using other than NVIS frequencies propagates out of theater and is received by MARS, which relays the information to the appropriate receiver. The approach is nontraditional, but numerous MARS-enrolled radio amateurs comprise a highly knowledgeable asset in HF communication. Our fifth recommendation is to draw attention to the complexity and necessity to link JTACs to the joint force facing an accompli attack that rapidly unfolds.

Conclusion

U.S. and Alliance deterrence on the eastern NATO border has several components that depend on each other in the calibrated force posture against Russian aggression and attack. One identified concern is the Russian ability to quickly launch an accompli attack with limited or no early warning. An accompli surprise attack is a rapid move, with little preparation and forewarning, to establish a fait accompli and to radically strengthen the adversary's bargaining position.

If Russia launches a fait accompli attack in Eastern Europe, the arrival of sizeable U.S. and NATO forces in the theater is likely weeks away. If APOD, SPOD, and transportation infrastructure within Western Europe is under attack, the attacker has additional time, as these attacks will cause delays for the NATO forces. The risk is that it is enough time to establish a fait accompli territorial gain with limited resistance against the invading force.

A pivotal part in the Russian calculation is the ability to separate joint operations and disallow defending ground forces access to airpower and standoff weaponry. A key component in achieving separation of joint forces is electronic warfare and the disruption and denial of U.S. and NATO communications.

The U.S.-NATO ability to maintain communications that hinder a split of joint operations, even at less quality, bandwidth, and reliability, creates uncertainty for the potential attacker. Our NATO allies, especially the Eastern European countries, still maintain an HF communication infrastructure. With limited investments in time and personnel and using existing fielded equipment, U.S. forces can strengthen the communication and information resiliency against massive hostile EW activities. An enhanced U.S. ability to communicate by HF radio would strengthen the ability to conduct joint operations, as

communications could relay through NATO allies to the U.S. joint force.

The risk that a small and outnumbered U.S.-NATO ground force can sufficiently communicate through an EW-saturated environment to link up with the joint force represents a single point of failure for any Russian fait accompli attack planning. The U.S. ability to retrograde and use HF communications creates an uncertainty hard for any Russian war planner to quantify and grasp as a potential risk for operational failure of a fait accompli attack. HF radio communication is not a perfect alternative to SATCOM and VHF/UHF line-of-sight communications, but it is an option that is tangible, fielded, and can cost-effectively increase both abilities and regional deterrence. From a U.S. perspective, the fear is that it might not work. From a Russian perspective, the concern is that it might work. Uncertainty is by itself a deterrent. **JFQ**

Notes

[1] Department of Defense, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, 2016).

[2] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, December 6, 2018).

[3] Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review* 84, no. 3 (September 1990), 733.

[4] Mahyar A. Amouzegar, "Military Logistics," in *Routledge Handbook of Defence Studies*, ed. David J. Galbreath and John R. Deni (Abingdon-on-Thames, UK: Routledge, 2018), 113.

[5] Geoff Ziezulewicz,"Lawmakers Express Concerns over Navy's Aging Surge Sealift Fleet," *Navy Times*, March 9, 2018, available at <www.navytimes.com/news/your-navy/2018/03/09/lawmakers-express-concerns-over-navys-aging-surge-sealift-fleet/>.

[6] Daniel A. Dailey, Mark A. Milley, and Mark T. Esper, "Army Senior Leaders Send—Lessons from D-Day," *Army.mil*, June 6, 2019, available at <https://home.army.mil/stewart/index.php/about/news/army-senior-leaders-send-lessons-d-day>.

[7] *Threat Handbook: Battlefield Survival and Radioelectronic Combat* (Fort Monroe, VA: TRADOC, February 1983).

[8] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electro-Magnetic Spectrum* (Tallinn, Estonia: International Centre for Defence and Security, September 2017).

[9] Valeriy Gerasimov, "The World on the Verge of War" [Mir na granyakh voyny], *Military Industrial Courier* [Voyenno-promyshlennyy kuryer], March 15, 2017, available at <http://vpk-news.ru/articles/35591>; Aleksandr V. Rogovoy and Keir Giles, *A Russian View on Land Power*, The Letort Papers (Carlisle Barracks, PA: U.S. Army War College Press, April 2015).

[10] *Russian Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017).

[11] T.S. Allen and A.J. Moore, "Victory without Casualties: Russia's Information Operations," *Parameters* 48, no. 1 (Spring 2018), 59–71.

[12] *Russian Military Power*, 38.

[13] Olga Filatova and Radomir Bolgov, "Strategic Communication in the Context of Modern Information Confrontation: EU and NATO vs. Russia and ISIS," in *Proceedings of the 13th International Conference on Cyber Warfare and Security*, ed. Jim Q. Chen and John S. Hurley (Washington, DC: ACPIL, 2018), 208–219.

[14] Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters* 26, no. 4 (Winter 1996–1997), 81.

[15] Timothy L. Thomas, "Russian Forecasts of Future War," *Military Review* (May–June 2019).

[16] Ibid., 88.

[17] Andrei Alekseevich Sidorenko, *The Offensive (A Soviet View)* (Washington, DC: U.S. Government Printing Office, 1973).

[18] Frederick R. Wilson, *United States Perceptions of Soviet Tactics versus Contemporary Soviet Tactical Writings* (New York: U.S. Army Russian Institute, 1979).

[19] Robert M. Frasche, *The Soviet Motorized Rifle Battalion*, DDB-1100-197-78 (Washington, DC: Defense Intelligence Agency, 1978).

[20] V.I. Kuznetsov, Yu.Ye. Donskov, and A.S. Korobeynikov, "Electronic Warfare and Information Warfare: How They Compare," *Military Thought* 22, no. 1 (2013).

[21] Jan Kallberg, "Designer Satellite Collisions from Covert Cyber War," *Strategic Studies Quarterly* 6, no. 1 (2012), 124–136.

[22] William J. Lynn, III, "A Military Strategy for the New Space Environment," *The Washington Quarterly* 34, no. 3 (2011), 7–16.

[23] Robert L. Edmonson et al., "Tactical Employment Considerations of HF Radios in the Cavalry Squadron," *The Cyber Defense Review* 4, no. 1 (Spring 2019), 23–32, available at <www.jstor.org/stable/26623064>.

[24] Dailey, Milley, and Esper, "Army Senior Leaders Send—Lessons from D-Day."