AH-1Z Viper helicopter attached to Marine Medium Tiltrotor Squadron (VMM) 163 (Reinforced), 11th Marine Expeditionary Unit, takes off during strait transit aboard USS *Boxer*, Strait of Hormuz, August 12, 2019 (U.S. Marine Corps/Dalton S. Swanbeck)

The Tactical Defense Becomes Dominant Again

By T.X. Hammes

It has become widely accepted that the convergence of technological advances is leading to a revolution in military affairs or perhaps even a military revolution.[1] One of the unanswered questions concerning this shift is whether it will lead to continued dominance by the offense or a period of defensive dominance. Offense dominance means that battle requires much greater resources to defend than attack. Defense dominance reverses that balance. Investing in the wrong side of the competition is a rich nation's game that the United States may no longer be able to afford. Against peer competition at scale, misguided investment could lead to strategic defeat. In fact, the answer to this question should guide force development and posture and therefore must be a part of the national security discussion.

To examine this question, this article provides a couple of historical examples of the shift between offense and defense dominance at the tactical level. It then examines how the offense-defense balance is shifting in each of six warfighting (land, sea, air, space, cyber, and electromagnetic) domains. Next, it examines how interactions between the domains could further reinforce the defense and finally what the shift to defense dominance means for the Nation.

Dr. T.X. Hammes is a Distinguished Research Fellow in the Center for Strategic Research, Institute for National Strategic Studies, at the National Defense University.

The Shifting Balance in History

History records a constantly shifting balance between offense and defense, driven by a combination of social, economic, and political changes. Despite Americans' love for technology, it alone cannot drive major shifts. For instance, defense was dominant during much of the medieval period because of the cost and difficulty of reducing a castle. This was based not only on the technology of building a castle but also the political, social, and economic structures necessary to do so. Offense was not restored until a wide range of social, political, technological, and military changes necessary for the development of military establishments capable of rapidly reducing the castles occurred. While cannons provided a key technology, the society first had to develop the political, social, and economic systems to produce and sustain them.

A much later major shift of advantage to the defense was driven by the development of rifled muskets and the cannon, the mass production of these weapons, the tactical adaptation of field fortifications, mobilization of mass manpower, economies that could pay for them, and governments that could marshal those resources. The combination of these factors led to defense dominating the tactical battlefield from the late U.S. Civil War until near the end of World War I. Governments could field and arm forces that combined the tactics and technology, which meant any unit moving above ground could be quickly observed and taken under fire. The opposing armies were forced to go to ground in massive trench systems that could be held even against numerically superior attacking forces. Failure of military leaders to recognize these changes—despite the lessons of Crimea, the Boer War, and the Russo-Japanese war—led to repeated, bloody, futile attempts to cross World War I's "no-man's-lands."

It was not until the Germans applied new concepts and tactics to technology emerging from the second industrial revolution—first lightweight machine guns and mortars, then armor and aircraft—that movement was restored to the battlefield. The transition was not completed before the end of World War I. During the interwar period, political, social, and economic systems had to evolve in parallel to produce the skilled engineers and operators, the financial backbone, and the will to conduct the global mechanized warfare of World War II. Since then, the offense has generally dominated tactically in conventional conflicts.

Today, convergence of 21st-century technologies is dramatically changing the battlefield environment. Commercial satellite networks tied to artificial intelligence (AI) processing tools mean that we are approaching a period of constant surveillance of the planet with visual, infrared, and electromagnetic sensors, as well as synthetic aperture radar. At the same time, nations are developing AI-assisted command and control systems that will allow them to absorb, understand, and act promptly on the resulting intelligence. This will enable them to coordinate attacks across all domains, including long-range precision attacks and swarms of autonomous hunters, informed by many sources and sensors, that will seek out their prey.

These co-evolving concepts, tactics, and commercial and military technologies are once again creating a battlespace in which movement becomes extremely dangerous. If a unit moves, it will create a signal and can be attacked at much greater ranges than in the past. At the same time, cyber, space, and electromagnetic domains will provide both reinforcement for and increasingly powerful alternatives to kinetic attacks.

Whether this convergence leads to offense or defense dominance is a complex question. In fact, the sheer complexity of interaction among the six domains requires that we consider the impact on each domain before we try to understand the overall impact on the character of war. (I have assigned electromagnetic spectrum as a domain. Although it is not yet considered one in U.S. doctrine, both China and Russia are dedicating great resources to dominating this domain.) This article focuses on major power conflict. Conflicts between states and nonstate actors play out in fundamentally different ways than state conflicts, and this article does not attempt to address the impact of the interrelated societal and technological changes on those conflicts.

It is essential to understand the difference between offense domination and a temporary advantage gained by offensive action. Offense domination provides the aggressor a major advantage that can be pursued throughout the conflict. Thus, it is inherently escalatory because the side that attacks first is perceived to have a war-winning advantage. Attacking first has historically provided the advantage of selecting the time and place of the battle. But it has also often provided only a temporary advantage because the attack did not prove sustainable for several reasons. These can best be expressed by the attack reaching its culminating point before it attained its strategic goals. This has been particularly true when concepts, tactics, and technology combined to increase the inherent advantages of the defense.

It is essential to note that temporary advantage in one domain may also allow a much more powerful attack from another domain. An obvious example is a temporary advantage in the electromagnetic domain that neutralizes air defense, thus allowing a much more destructive attack from the air domain into other domains. It is also essential that leaders understand the balance between offense and defense. Failure to do so has often led leaders to start a war they are confident will be short, only to be bogged down in a long, brutal conflict. As noted by Cathal Nolan in *The Allure of Battle*, the confidence is too often an illusion based on false assumptions. The U.S. Civil War and World War I are examples of this hazard.

Land

The impact of the fourth industrial revolution on this oldest domain of war has already been dramatic. As noted, the balance between offense and defense in land combat has shifted through the ages. Since the last year of World War I, the offense has dominated conventional ground combat. (Irregular warfare has followed its own pattern.) However, emerging technologies are shifting the balance in conventional warfare back to the defense.

Since new systems allow units to remain passive and yet see the battlefield clearly, the defense will have a distinct advantage. Electro-optical and electronic warfare sensors can provide a great deal of information that, combined with external sensors such as satellites and drones, can allow the defenders to visualize the battlefield without revealing their own positions. The defenders will not have to emit signals until they choose to fire. And they will have the advantage of fighting from prepared positions. While most current systems must be manned to operate, autonomous and remote-control systems are being developed worldwide. As these systems mature, defenders can be located at a distance from their weapons and thus not be at risk even after firing. Recent events have shown ground forces will be subject to attack by the emerging families of swarming drones.[2] Inexpensive autonomous drones are flying now and can be mass produced using advanced manufacturing techniques. It is not unreasonable to expect a defender to be able to launch hundreds or even thousands of loitering munitions against each brigade-size attack.

In contrast, attackers will have to move if they intend to execute anything but strike missions against the defender. The very act of moving will create a signature. While attackers will retain the traditional advantage of selecting the time and place of attack, the advantage of physically massing either offensive or defensive forces is declining as weapons ranges increase dramatically. Mass can be achieved by assembling long-range fires rather than massing forces. This favors the defender since attackers may well be forced to pass through restrictive chokepoints, while defenders can disperse to the maximum effective range of their weapons. However, as the Azerbaijanis demonstrated against the Armenians, the offense can remain dominant if the attacker adopts modern concepts and weapons while the defender relies on 20th-century weapons and concepts.

Sea

Today, land-based antiship systems are dominating the surface of the sea out to ever increasing ranges. These land- and air-launched ballistic and cruise missile systems, vertical takeoff and landing drones, and attack aircraft cued by ubiquitous surveillance systems have the enormous advantage of hiding in the cluttered land environment. Their surface ship targets must operate in much more open environments. Land-based systems also have the advantage of both range and magazine depth. And if emerging laser and microwave systems prove effective, land-based forces will have an enormous advantage in power generation capacity. The adage, attributed to Admiral Horatio Nelson, "A ship's a fool to fight a fort," remains true—but now extends to ever greater ranges from shore.

Geography as well as oceanography can enhance the power of land-based systems. The sea has chokepoints that have been major factors in conflicts between major powers since the Peloponnesian War. Even today, control of straits such as Hormuz or Malacca can allow a power to determine what resources flow to an opponent. In these confined waters, land-based defenses can gain an even greater advantage by employing many less expensive, shorter range antiship systems and smart sea mines (essentially tethered torpedoes).

Extended range land- and air-launched cruise missiles mean many naval fights will include land-based participants. As Captain Wayne Hughes, USN, demonstrated in his work, the first fleet to conduct successful pulse attacks against an opposing fleet gains a major advantage. Land-based systems can provide more missiles at less cost for each pulse attack.[3] However, as fights move further from shore, the number of land-based systems that can range the fight decreases. At some point, the tactical advantage will shift back to the offense.

The subsurface fight will continue to favor offense in the deep ocean but the defense in the vicinity of chokepoints. Emerging technologies are making shallow water more transparent than ever. And fixed-sensor arrays can cover key passages between open seas. Rapid advances in autonomous submarine drones will thicken the sensor nets in restricted waters as well as enable swarms of weapons to be launched against infiltrating submarines. In short, emerging technologies are making waters both more transparent and more congested.

Mining of enemy ports may well be the most effective and viable offensive naval action simply because autonomous drones with small signatures will be able to penetrate enemy defenses to lay mines. Smart mines can be programmed to attack specific classes of ships, thus giving the miner an ability to select targets for best effect without having to maintain forces in the vicinity of the port.

Air

With missile weapons outranging most manned aircraft, winning in the air will really be about the ability to sustain the fight logistically. The current generation of manned aircraft needs major operating facilities. Even the F-35B requires significant, easily identified, and targetable maintenance facilities. Nor is the threat limited to in-theater airbases. The advent of containerized long-range cruise missiles and drones deployed on a wide variety of shipping means that bases almost anywhere in the world can be struck. Thus, a key question is whether the joint force can defend its base facilities against swarms of missiles and drones. The United States is betting heavily on directed energy—lasers and microwave (electromagnetic pulse [EMP])—weapons to defeat swarm attacks. While these systems still face numerous challenges, they have promise.

While directed energy weapons could protect air bases from drones and missiles, they also can certainly engage manned aircraft. When they are deployed, these weapons will provide significant advantage to the defense for two reasons. First, they require large power systems to operate. Attackers must bring those power systems with them and thus the power available is limited by the ability to lift it by land, sea, or air. In contrast, the defenders can either tap directly into the national power grid for virtually unlimited power or use as many generators as they need. Second, the defender has

Senior Airman with 55th Aircraft Maintenance Squadron disconnects external power cord from extensively modified RC-135V/W Rivet Joint, with onboard sensor suite allowing mission crew to detect, identify, and geolocate signals throughout electromagnetic spectrum, August 5, 2018, at Offutt Air Force Base, Nebraska (U.S. Air Force/Drew Nystrom)

the enormous advantage of blending into the cluttered ground environment. The actual systems are relatively small and can thus be camouflaged as air conditioning units on tops of buildings or small sheds in the countryside. Again, the attacker must move toward the defended area and thus will generate signals, while the defenders need not generate a signal until they choose to engage. As directed energy weapons become operational, they will increase the advantage the defense holds over the offense in the air domain.

Space

Conventional wisdom has stated for years that war in space will be offense dominated because antisatellite systems are cheaper than satellites. An attacker could quickly destroy an enemy's key satellites, and it would take months, if not years, to replace these large, very expensive assets. Given the heavy dependence of U.S. forces on space services, this is a truly alarming situation.

However, rapid developments in space launch and satellite miniaturization are changing that situation. The exponential increase in the number of satellites in orbit, the disaggregation of functions into many platforms, and the increasing ability to rapidly replace satellites in orbit mean that defense may now have the advantage. Disaggregating functions such as gathering intelligence and providing communications links mean that the attacker must engage many more targets to degrade space systems. In addition, vastly improved space awareness, the difficulty of acquiring these small targets, and their ability to maneuver to prevent interception increase the advantages accruing to the defense.

Part of successful defense will be restoring space functions damaged by an attack. In addition to the U.S. Space Force's Space Rapid Capabilities Office, private firms are developing high-altitude drones as potential replacements.[4]

However, a major vulnerability remains the PNT (positioning-navigating-timing) information provided by the GPS constellation. Timing has become central to the functioning of a wide range of critical civilian systems—banking, communications, retail sales, and uncounted other applications all rely on precision timing. Systematic attacks on the GPS network will cause massive disruption of the U.S. economy as well as society in general. The key question is whether these critical functions can be quickly replaced by other systems in the event of an attack. Fortunately, both civilian and governmental organizations are developing alternatives to the GPS functions. However, until the United States can quickly replace this critical function, offensive action can provide a window of

Soldiers with 1st Battalion, 1st Air Defense Artillery Regiment, rehearse battle drills with Patriot long-range, all-altitude, all-weather air defense system to enhance crew-drill proficiency during bilateral exercise Keen Sword/Orient Shield 21, at Misawa Air Base, October 28, 2020 (U.S. Army/Raquel Birk)

opportunity to an attacker. Yet, as noted, the benefits of such an attack are likely to be fleeting and will almost certainly trigger a reply in kind. In short, space will become an arena of ongoing conflict with the advantage to the defense.

Cyber

In 2019, then–Secretary of Defense Mark Esper noted that winning in cyberspace requires offense. This continued the theme established in 2012 when then–Secretary Leon Panetta warned of a "cyber Pearl Harbor."[5] Yet there is a growing pushback against the idea that cyber is inherently offense dominated.

In their 2018 book, Brandon Valeriano, Benjamin Jensen, and Ryan Maness noted that cyber-offensive operations consist of espionage, disruption (temporarily reducing the capacity of an opponent's system), and degradation (damaging of elements of the system).[6] But in contrast to the two secretaries, these authors do not see offense as dominant. Other scholars, including former cyber operators, agree with them. They see offense dominance as being overstated. The cost of "breaking into a particular network may be cheap after the tools and infrastructure are in place," but "building and maintaining the infrastructure for a program of sustained operations requires targeting, research, hardware engineering, software development, and training. This is not cheap."[7]

In short, we have well-informed experts with contradictory views on the value of cyber as an offensive weapon. This is consistent with the historical pattern of new technologies. Advocates did not really know the impact of emerging technologies until they were employed in open conflict. Thus, despite advocating defending persistently forward (which is essentially offensive), the U.S. Cyber Command Vision states, "Cyberspace is an active and contested operational space in which superiority is always at risk."[8]

So how should we evaluate cyber as a weapon? Clearly, cyber espionage/theft works. It has allowed China, Iran, North Korea, Russia, and numerous criminal organizations to steal personal information, intellectual property, and money on a scale not seen before.

Cyber disruption also has a record of limited success as indicated by repeated attacks from the Love Bug virus to NotPetya malware. A significant number of these attacks have disrupted the targeted systems for a period ranging from hours to weeks. NotPetya also caused significant damage to numerous organizations that were not the target of its attack but were simply collateral damage. These incidents indicate that cyber disruption attacks can assist an offense but are inherently difficult to coordinate with real-time attacks—and to date have not reliably produced the desired effects.

Destructive attacks have also had limited success, the most famous being the Stuxnet attack on the Iranian centrifuges

attributed to the United States and Israel. This attack reportedly damaged about 20 percent of the centrifuges, yet the International Atomic Energy Agency reported that Iranian production increased during the period—perhaps in response to the attack.[9] Increasing the uncertainty about the offense-defense balance in cyber, there have been other operations, such as SolarWinds/Holiday Bear, that have achieved widespread penetration of computer networks but whose objective remains unclear.[10]

There are two other major options, however, that have not been used to date in cyber attacks that require much deeper study—kinetic weapons and EMP. Kinetic attacks can damage the well-mapped networks of fiber optic cables, switches, downlink stations, and processing centers essential to an information network. The increasing availability of long-range, autonomous, precision weapons means cross-domain attacks from land, sea, and air platforms will be an integral part of counter-cyber operations. The potential to hit hundreds of key nodes either in theater or even in the United States is growing.

The fact that the Internet was initially designed to work even when under major attack will mitigate the impact of kinetic attacks, but the attacks will still cause significant disruptions. Fortunately, the Internet is a complex adaptive system and thus will show remarkable resilience when under attack. EMP attacks will be dealt with in the following section on electromagnetic domain.

Electromagnetic Spectrum

In January 2021, General John Hyten, Vice Chairman of the Joint Chiefs of Staff, stated, "We have to be able to effectively fight and win the electromagnetic spectrum fight right from the beginning—that is, electronic warfare in every domain."[11] Given the increasing reliance on communications networks, highlighted by the Pentagon's efforts to create the Joint All-Domain Command and Control system, the ability to use the electromagnetic spectrum or deny an opponent its use will be critical to success. Although it has not been officially designated a domain by the Pentagon, the electromagnetic spectrum requires the same level of thought and effort as the five named domains.

Once again, land-based defenders may well have an advantage in this domain; they can use fiber optic communications systems to avoid the electromagnetic domain. In addition, they have access to the national power grid to provide effectively unlimited power for jammers.

A potential gamechanger in the electromagnetic spectrum is an EMP weapon. These weapons represent a major threat from the tactical to the strategic levels. At the tactical level, the United States has demonstrated a drone that can create an EMP directed at specific targets. Since it is delivered by a drone, this type of attack is really a cross-domain attack but, like kinetic attacks, must be considered as part of any cyber offense-defense balance.

A defending unit can do more to harden its electronics against this kind of attack than an attacker can. However, EMP weapons can overturn the defender's advantage if the defender has not exploited the inherent advantage of the defense. We know these attacks can cause major damage to unprotected electronics, and even the most basic systems today have embedded electronics. The attacker has one major advantage: he can attempt to employ his EMP weapon before any of his own systems are within range of the pulse. Yet if they cannot prevent a response in kind, the attacker loses the advantage when a retaliatory strike hits his forces.

For both offense and defense, building resilient, redundant systems can reduce the damage done by tactical EMP weapons but will be costly and require massive retrofits for existing weapons. Of course, the miniaturization necessary for offensive systems will make them significantly more expensive.

At the strategic level, a nuclear-generated high-altitude EMP could seriously damage the national infrastructure for a period of months. The fact that this type of attack currently requires a nuclear device to be detonated over the target area means that it must be discussed as part of nuclear deterrence/warfare. At the same time, the cost of protecting civilian systems from large-scale EMP weapons will be extraordinarily high. Large-scale EMP weapons are truly weapons of mass destruction and thus should be treated as part of a nuclear deterrence program. Since all major powers can deploy large-scale EMP weapons, perhaps the best that can be hoped for is the stability inherent in mutually assured destruction.

A Caution

As always, perception is reality. Unfortunately, the perception that cyber and space are offense dominated is inherently escalatory. If political leaders believe they can achieve decisive dominance in these domains only by attacking first, crisis management becomes much more difficult. Therefore, it is critical to counter the idea that going first in cyber, space, or the electromagnetic spectrum provides unrecoverable advantages. This is not only necessary to prevent aggression but also to prevent escalation on the friendly side.

Interaction Between Domains

Understanding the relative strengths of the offense and defense in the various domains is essential to the joint warfighter. For instance, while degradation or destruction has proved to be a difficult challenge within the cyber domain, the use of precision weapons delivered from land, sea, air, or space can have a devastating effect on the cyber capabilities of an opponent. Unclassified sources provide maps of critical nodes and links (downlinks, fiber optics, and terrestrial switches) of many commercial networks that could allow massive attacks across the networks.[12]

The increasing range and number of autonomous precision-attack systems are steadily improving the ability of the land, sea, and air domains to conduct effective cross-domain attacks. Ground-based forces have the advantages of operating in complex terrain (whether rural or urban) and access to deep magazines and national power grids. The increasing ranges of ground force weapons will allow defenses to reach out much farther to target

Airman prepares spacer on intercontinental ballistic missile during Simulated Electronic Launch–Minuteman test, September 22, 2020, at launch facility near Great Falls, Montana (U.S. Air Force/Tristan Day)

land, sea, and air forces as well as critical infrastructure for space and cyber forces.

All-domain offensive operations are incredibly complex, not least because each domain operates on different execution timelines. Major land and naval operations take from weeks to years to execute. It can take weeks to position the forces for air operations, but they can be executed in hours with campaigns lasting days to weeks. Cyber, space, and electronic warfare operations can also take weeks to years to put forces in place but can measure execution in microseconds to days. Thus, coordinating the offensive operations of the separate domains is particularly challenging—yet cross-domain attacks may be the most effective. Space Development Agency Director Derek Tournear has stated that cyber is a greater threat to satellites than missiles.[13] Air forces have stated for years that the most effective way to defeat an air force is to destroy its bases and its aircraft on the ground. Today, ground-based forces can do this from beyond the range of most aircraft delivered weapons. Naval forces have historically been able to appear suddenly out of the vast expanses of the oceans but increasingly are being closely tracked by space assets. In short, cross-domain attacks will become more powerful but will be an order of magnitude more difficult than coordinating a defense.

What Does It Mean for the United States?

If the United States leads the shift to defense dominance in land, air, and sea domains while maintaining the ability to contest the space, cyber, and electromagnetic domains, it gains major strategic advantages. Perhaps the greatest advantage will lie in deterring aggression. MIT political scientist Stephen Van Evera argued that war is more likely to occur when the tactical offense dominates the battlefield because conquest is perceived to be easy. He listed 10 reasons leaders were more likely to take their nations to war under these conditions than during periods when the defense dominates tactically. During periods of defense dominance, then, aggression becomes less likely simply because the probability the attacker succeeds decreases greatly.[14] Fortunately, in the two current Great Power competitions, the United States is essentially on the tactical defensive. To achieve regional hegemony, both China and Russia will have to cross borders and seize territory; the United States and its allies only have to defend.

In Asia, China has worked hard to develop antiaccess/area-denial (A2/AD) capabilities for the region. Fortunately for the allies, A2/AD works both ways. As defense becomes dominant, the United States can cooperate with its allies and friends to take advantage of the fact that they are separated by water from China. They can create an A2/AD based on the First Island Chain. A family of smart and relatively inexpensive weapons on the First Island Chain can both deny China commercial use of the East and South China seas and prevent either China's navy or merchant ships from reaching the Pacific

Ocean. Already existing cruise missiles, drones, and smart sea mines can create a defense in depth. Japan, Australia, South Korea, and Singapore all have the capability to produce these systems. By applying advanced manufacturing techniques, they can produce them in large numbers. The United States can cooperate with them to co-produce these weapons and then train together to employ them in concert with existing land-, sea-, and air-based platforms. This strategy reinforces deterrence because it directly addresses three of China's strategists' greatest fears: being cut off from global trade (the Malacca Dilemma), the desire for certainty in military planning, and the impact of a long war on domestic stability.

While the tactical situation is dramatically different in Europe, the North Atlantic Treaty Organization (NATO) can also exploit the rising dominance of defense to deter and, if necessary, deny Russian incursions into Eastern Europe. The combination of inexpensive short-range drones, loitering munitions, cruise missiles, mines, and improvised explosive devices (which could easily include 50,000 pounds of explosives in a 20-foot container full of fertilizer) could immediately create responsive, thick belts for a defense in depth. This approach solves NATO's number one problem in defending Eastern Europe—the inability to deploy sufficient forces before Russia can mobilize its own forces for an invasion. While a Russian invasion is both highly unlikely and not in keeping with Russian doctrine, NATO planners have focused on the intractable problem of reinforcing Eastern European states.

Unfortunately, these plans are often conceived in terms of heavy armor units deploying from home stations to the battle front. The Alliance lacks the funding, the will, and the infrastructure to forward deploy the number of heavy armor units, aviation, and logistics support necessary to execute such a defense before the Russians can mobilize.[15] By adopting a defense that reinforces selected existing systems with small, smart, and numerous systems, NATO can create an affordable force that can mobilize faster than the current Russian forces.

Today, the United States faces flat (effectively decreasing after inflation) defense budgets as well the need to modernize its nuclear triad while facing major maintenance backlogs in its air and naval inventories. Fortunately, the rising dominance of defense provides an opportunity to shift from the previous generation of few but exquisite weapons systems such as the F-35 and *Gerald R. Ford*–class carriers to the new generation of smart, small, and much less expensive systems that take advantage of the shift to defense.[16] This approach meets America's need to support its allies and efficiently deter its enemies, even as its effective defense budget decreases. **JFQ**

Notes

[1] Military revolutions are rare and have a much greater impact than revolutions in military affairs. See MacGregor Knox and Williamson Murray, eds., *The Dynamics of Military Revolution, 1300–2050* (New York: Cambridge University Press, 2001).

[2] Shaan Shaikh and Wes Rumbaugh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies, December 8, 2020, available at <https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense>.

[3] Wayne Hughes and Robert Gurrier, *Fleet Tactics and Naval Operations*, 3rd ed. (Annapolis, MD: Naval Institute Press, 2018).

[4] See "Space Rapid Capabilities Office," n.d., available at <https://www.kirtland.af.mil/Units/Space-Rapid-Capabilities-Office/>.

[5] Elisabeth Bumiller and Thomas Shanker, "Panetta Warns of Possible 'Cyber-Pearl Harbor,'" *New York Times*, October 12, 2012.

[6] Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford, UK: Oxford University Press, 2018), 11–13.

[7] Charles Smythe, "Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance," *Yale Journal of International Affairs*, June 10, 2020, available at <https://www.yalejournal.org/publications/cult-of-the-cyber-offensive-misperceptions-of-the-cyber-offensedefense-balance>.

[8] *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command* (Fort George G. Meade, MD: U.S. Cyber Command, 2018), 6, available at <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>.

[9] John Glaser, "Cyberwar on Iran Won't Work. Here's Why," *CATO Institute*, August 21, 2017, available at <https://www.cato.org/commentary/cyberwar-iran-wont-work-heres-why>.

[10] "Examining the SolarWinds/Holiday Bear Hack: SIPA Experts Consider the Shifting Standards of Cyberespionage," Columbia University School of International and Public Affairs, available at <https://www.sipa.columbia.edu/news/examining-solarwindsholiday-bear-hack>.

[11] Theresa Hitchens, "'Spectrum Superiority' Key to All Domain Operations: Gen. Hyten," *Breaking Defense*, January 7, 2021, available at <https://breakingdefense.com/2021/01/spectrum-superiority-key-to-all-domain-operations-gen-hyten/>.

[12] Matthew Cole, "A Dissertation So Good It Might Be Classified," *Wired*, January 1, 2004, available at <https://www.wired.com/2004/01/a-dissertation-so-good-it-might-be-classified/>; "Finding Fiber in Your Area May Be Easier Than You Think," *GEOTEL*, available at <https://www.geo-tel.com/finding-fiber-in-your-area-may-be-easier-than-you-think/>.

[13] Sandra Erwin, "DOD Space Agency: Cyber Attacks, Not Missiles, Are the Most Worrisome Threat to Satellites," *Space News*, April 14, 2021, available at <https://spacenews.com/dod-space-agency-cyber-attacks-not-missiles-are-the-most-worrisome-threat-to-satellites/>.

[14] Stephen Van Evera, *Causes of War: Power and the Roots of Conflict* (Ithaca, NY: Cornell University Press, 1999).

[15] See Max Bergmann and Siena Cicarelli, "NATO's Financing Gap: Why NATO Should Create Its Own Bank," Center for American Progress, January 13, 2021, available at <https://www.americanprogress.org/issues/security/reports/2021/01/13/494605/natos-financing-gap/>; "WIN/Gallup International's Global Survey Shows Three in Five Willing to Fight for Their Country," Gallup International, May 7, 2015, available at <https://www.gallup-international.bg/en/33483/win-gallup-internationals-global-survey-shows-three-in-five-willing-to-fight-for-their-country/>; Kevin Blanchford, "Can NATO and the EU Really Defend the Baltic States Against Russia?" *The National Interest*, February 7, 2020, available at <https://nationalinterest.org/blog/buzz/can-nato-and-eu-really-defend-baltic-states-against-russia-121711>.

[16] See T.X. Hammes, *Technologies Converge and Power Diffuses: The Evolution of Small, Smart, and Cheap Weapons*, Policy Analysis No. 786 (Washington, DC: The Cato Institute, 2016), available at <https://www.cato.org/policy-analysis/technologies-converge-power-diffuses-evolution-small-smart-cheap-weapons>.