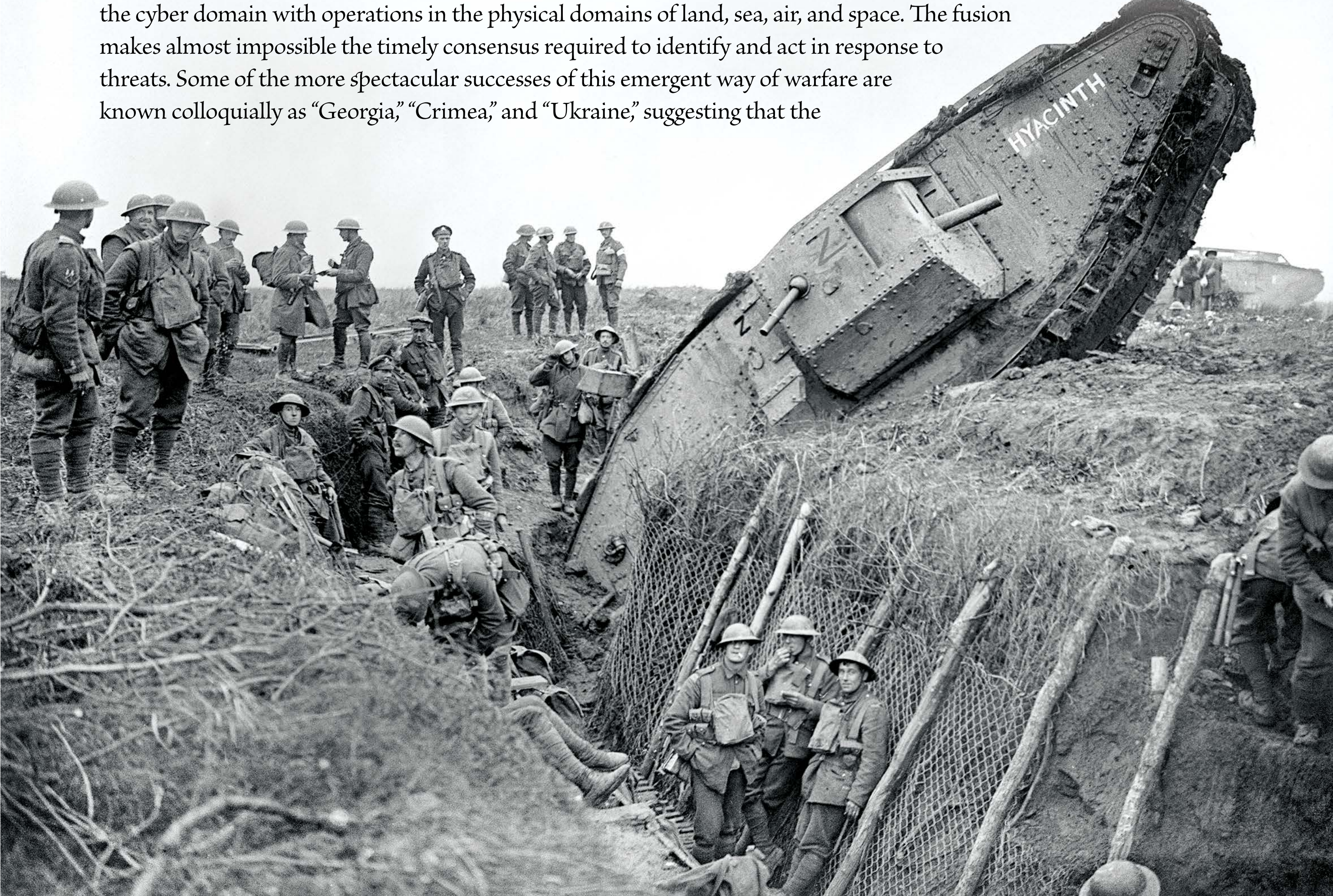
From Cambrai to Cyberspace

How the U.S. Military Can Achieve Convergence between the Cyber and Physical Domains

Maj. Anthony M. Formica, U.S. Army

The United States has run out of time for developing approaches to compete in the cyber domain, and it must use the assets and forces currently available to prevent future strategic setbacks. The United States' most likely geopolitical adversaries have developed operational concepts that fuse operations in the cyber domain with operations in the physical domains of land, sea, air, and space. The fusion makes almost impossible the timely consensus required to identify and act in response to threats. Some of the more spectacular successes of this emergent way of warfare are known colloquially as "Georgia," "Crimea," and "Ukraine," suggesting that the



convergence predicted by the Army's operating concept already happened roughly a decade ago. The Army and joint force cooperatively need to develop both an immediate solution and a new doctrinal framework while remaining clear-eyed about the challenges that convergence poses to U.S. elements of national power, its ethical and legal approaches to warfighting, and its conception of the profession of arms.

"An Urgent Warning"

Gen. Sir Richard Shirreff's 2016 novel *War with Russia: An Urgent Warning from Senior Military Command* contains a fictional description of Moscow initiating a war with Latvia. Long before conventional Russian military forces cross the narrow border separating their country from Latvian territory, Russian bots and trolls stage an elaborate social engineering effort that exposes the ethnic Russian population of Riga to "a constant stream of Russian TV broadcasts and social media highlighting the discrimination, the lack of employment opportunities, and the [Latvian] laws against speaking Russian."[1] Russian special operatives foment mass protests in the Latvian capital and stage the assassinations of young ethnic Russians during the ensuing unrest; Russian media immediately spins the murders as the work of deranged Latvian nationalists. The Russian president announces after twenty-four hours have elapsed that he has a responsibility to protect the lives of all Russians everywhere, and so deploys the Russian armed forces to this end. Meanwhile, the North Atlantic Treaty Organization (NATO), of which Latvia is a member, has not yet agreed on whether there is an actual threat to Latvian sovereignty unfolding in real time. Latvia is effectively annexed without the movement of a single NATO plane, ship, or soldier.

Shirreff retired from the British army in 2014; his last duty position was serving as the deputy supreme allied commander, Europe, the third-highest military position within NATO. His experience watching the events that metastasized into the Russian annexation of Crimea clearly informed his account of a future war between the Russian Federation and the NATO Alliance. His fictitious Latvian scenario is a close play-by-play approximation of the way the Russians prepared the battlefield in February 2014, when Russian cyber warriors relentlessly promoted the idea of "Ukraine as a neo-Nazi state," and where irregular Russian forces, private military companies, and nonuniformed militia organizations fanned the flames of social disorder.[2] Shortly thereafter, Crimea voted itself into the Russian Federation, albeit illegally.[3] Again, the United States and its NATO allies wrung their hands, held numerous meetings, and issued many statements—but none acted nor achieved the minimum consensus necessary to direct action to forestall Russia's victory.[4]

Both the fictitious and real accounts of the emergent Russian way of warfare highlight the role of cyber-enabled information operations and irregular forces working at the operational level to generate strategic success. Critically, both accounts depict these forces as operating in tandem to produce complementary and reinforcing effects. Western audiences tend to pay attention to visible effects, such as the lost territory, the changed flags over government offices, and the "little green men" carrying guns in riotous streets. Doing so at the expense of the invisible effects that precede these more dramatic images is a mistake and compromises the United States' ability to effectively engage in today's great-power competition. Yesterday's Crimea and Georgia are tomorrow's Suwalki and Latvia: they will happen just below the threshold of conventional conflict, and the first effects that will shape and enable them to be annexed will play out on the digital terrain of the information environment. These effects will capitalize on the way the cyber domain has fundamentally redefined U.S. strategic notions of time and space; they will be designed to disrupt the cognition and coordinated action of Western leaders just long enough to allow U.S. adversaries to secure their objectives.

The Army operating concept anticipates the merging of the capabilities and assets of the physical and digital domains with the term "convergence."[5] The concept's title gives away the aspirational nature of convergence. *The U.S. Army in Multi-Domain Operations 2028* envisions events that are seven years

Previous page: A Mark IV tank of H Battalion, "Hyacinth," ditched in a German trench while supporting 1st Battalion, Leicestershire Regiment, 20 November 1917 near Ribecourt, France, during the Battle of Cambrai. This battle demonstrated the potential of armored warfare and caused the German Wehrmacht to change the way it fought to enable mutually supportive infantry, armor, and artillery. Similarly, U.S. forces must determine how physical and digital soldiers can be mutually supportive at the operational and tactical levels of war. (Photo by Lt. John Warwick Brooke; courtesy of the Imperial War Museum, © IWM Q 6432) away. Unfortunately, America's adversaries achieved convergence yesterday. Fighting U.S. adversaries on the physical battlefield in 2021, 2028, or 2035 will hinge on a U.S. ability to find our adversaries in the terrain of cyberspace *today*. There is no time to develop a five-year plan in Brussels or reinvent the wheel through constructing yet another combatant command. For the United States to fight and win in a contemporary operating environment, it needs to integrate the many disparate but extant pieces of its intelligence collection and kinetic strike elements of national power *now*. It needs to construct task organizations and report channels that can rapidly detect enemy movement in cyberspace, rapidly direct real-world forces to respond to those threats, and mutually support the convergence of digital and physical capabilities.

From Cambrai to Cyberspace

There is not a senior captain or junior major in the Army who has not had the vocabulary of novelty and modernity stamped on his or her soul while learning how to comprehend his or her profession. Modern warfare, these officers are assured, is a complex, dynamic, and uncertain affair; information is imperfect, technology is constantly evolving, and translating political ends into tactical means is more difficult than ever. The cyber domain tends to feature prominently in this cognitive framework, representing as it does for many officers an abstract, intangible realm that is always present yet never seen. This invisible omnipresence partners with other technological trends such as artificial intelligence, automated weapon systems, and big data analysis to reinforce the common perception that the future is beyond any one individual's understanding, likely to move too fast to be kept up with, and dangerous on a scale never before seen in the history of the arms profession.

The infantrymen of World War I would contest this set of assumptions. The advent of cyber-enabled warfare is in many respects a reincarnation of the advent of armored warfare in the Great War over a century ago. Then, as now, a new tool transformed the way that tacticians perceived both space and time: tanks moved too fast and too far for conventional notions of the battlespace to remain relevant. Before the Battle of Cambrai, the front was the place where two armies met; it was generally limited in scope to the range of artillery, and time was counted in days. After Cambrai, the front was feasibly any location within one hundred kilometers of a moving tank platoon, and time had to be gauged in hours.

The tank was the classic "new thing" that tends to inspire revolutions in military affairs.[6] It disrupted every prior notion about the profession of arms' physical and temporal parameters. Some armies adapted well to this new reality, weaving tactical experiences and experiments into a coherent doctrine for armored warfare; others did not. Cambrai was a victory for the British mechanized community and stood as a seminal proof of concept for armored warfare, yet the British did not interpret it as such during the interwar period. The German army learned a different lesson from its Cambrai experience and dedicated its interwar mechanized experiments to integrating infantry and artillery into a supporting role for tank columns.[7]

The difference between the British and the German approach to armor was stark: the latter appreciated that a new modality of conflict had been created because of a tool, while the former persisted in believing that the old rules and doctrinal structures still applied. The British approach to the dilemma posed by the tank was to essentially ask how the new thing added to old, preferred British ways of fighting. In contrast, the Germans asked how their old, preferred way of fighting must change because of the new thing. Analogies are by nature imperfect things, and so it would be a mistake to view the tank as a perfect analog to cyber capabilities. Real-world forces cannot "extend" the operational reach of cyber forces in the same way that Wehrmacht infantry and artillery extended the operational reach of Panzer columns.

Maj. Anthony M. Formica, U.S. Army, holds a BS from the United States Military Academy and an MA from Yale University's Jackson Institute for Global Affairs, which he obtained through the Downing Scholars Program. Formica deployed in support of Operation Enduring Freedom with 1st Stryker Brigade Combat Team, 25th Infantry Division, and in support of Operation Atlantic Resolve-North as a company commander with the 173rd Infantry Brigade Combat Team (Airborne), where his company reinforced NATO's deterrent efforts in Lithuania. He has also served as an observer-controller at the Joint Readiness Training Center and currently serves in the 82nd Airborne Division.

That does not imply, however, that America's physical and digital soldiers cannot be mutually supportive of the operational and tactical levels of war—as America's current adversaries have resoundingly and repeatedly showed it over the past decade.

Fait Accompli

Russia's actions in both the real case of Crimea and the fictitious Latvian one that opened this article are examples of what the U.S. Army describes as fait accompli attacks: offensive operations that are "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 U.S. would entail unacceptable cost and risk."[8] Fait accompli attacks consist of both covert and overt military activities in the physical world employed in conjunction with information operations designed to "create ambiguity to prevent or delay political recognition, decision, and reaction."[9] The United States' most likely nation-state adversaries understand that the best way to defeat America's rapid-response OODA (observe, orient, decide, act) loop is to disrupt the first step of that sequence and make the consensus required to observe a threat impossible.[10]

While most of America's geopolitical rivals have recognized cyber-enabled information warfare as an indispensable tool for offsetting the United States' preponderance of conventional military superiority, Russia's application of these technologies and techniques tends to receive the most public attention from Western analysts; part of this is due to recent events, such as election interference efforts around the world orchestrated by Moscow, and part of it stems from Russia's legacy of Soviet-era active measures.[11] Ukraine provides an illuminating example of Russian cyber-enabled information operations at work, with blackouts of the Ukrainian power grid complementing social engineering, targeted disinformation campaigns, and agents of influence mobilizing internal opposition and fake elections.[12] These subversive activities played out predominantly in the cyber domain, both in the form of software-hardware attacks and in the form of cyber-enabled information operations designed to make reality unintelligible. By the time the United States and its Western allies had acknowledged the scope and scale of the threat, Russian proxy forces had been augmented by several thousand pieces of heavy equipment, including T-90 tanks, long-range artillery, air defense, and electronic warfare devices.[13]

There are clear differences between the Russian approach to and the American template for the convergence of cyber-enabled information warfare and physical, real-world effects. The Crimean as well as the Ukrainian cases cannot be cleanly cleaved into antebellum and postbellum time frames, at least not by an intellectually honest observer. The more accurate framework is suggested in America's own *National Security Strategy*, which observes that America's rivals have "become skilled at operating below the threshold of military conflict … with hostile actions cloaked in deniability."[14] Cyberspace operations were prominent, if not preeminent, before the tanks and nonuniformed soldiers entered the scenario, and continued to play an information-centric role afterwards, not only by setting conditions for the employment of conventional forces but also by complementing their efforts by weaving a web of muddled facts and plausible deniability.

Meanwhile, U.S. joint doctrine explicitly states that information operations occur only during times of military operations.[15] U.S. doctrine construes the information environment as existing between cognitive, informational, and physical dimensions, and states that cyberspace is included within the information environment.[16] The separate joint publication describing cyber operations does so in broad terms of offense, defense, and network security, but like information operations, it construes the augmentation of military forces with cyber capabilities as something that only occurs during wartime, "normally authorized by a military order."[17] American cyber planning straddles antebellum and postbellum and reflects a collective belief that the cyber domain supports intelligence collection before the onset of war and augments the air, land, sea, and space domains afterward. The proof of this belief is the Title 10- and Title 50-derived need to keep the National Security Agency and U.S. Cyber Command organizationally separate yet headed by the same individual.[18]

Fait accompli attacks as practiced by Russia succeed in part because they do not bifurcate the roles of cyber operations before and after the formal onset of hostilities. The entire point is to avoid the formal onset of hostilities by fomenting uncertainty in an adversary's cognition of events and maneuvering within the resultant window of opportunity. Intelligence collection, information operations, and physical attacks on hardware and software occur at all points in both time and space in the operating environment, simultaneously enabling and complementing the activities of conventional and unconventional troop formations. Another significant reason fait accompli attacks work is because America's own approach to the cyber domain is so stringently bifurcated and optimized for a particularly narrow conception of conflict by which nations exist in a state of either peace or of war.

Pfc. Dylan Taylor (*left*), a cyberspace operations specialist, Staff Sgt. Isaac Ware, a noncommissioned officer in charge of an expeditionary cyberspace electromagnetic activities crews, and Capt. Richard Shmel (*right*), a cyberspace operations officer, participate in a 915th Cyber Warfare Battalion field training exercise 9 October 2020 at Muscatatuck Urban Training Center in Butlerville, Indiana. (Photo by Steven Stover)

Cambrai Catches Up with Cyberspace

We have already seen the costs stemming from this gap in our cyber thinking: they are called South Ossetia, Crimea, and the Donbas. We do not call these incidents strategic defeats only because we use a distinctly twentieth-century schema and a nineteenth-century vocabulary to frame our understanding of twenty-first-century conflict. The joint force is diligently manning a modern equivalent of the trenches, expecting a coming battle that conforms to previous notions of how conflict works; it has not sunk in yet that the tanks have long since rumbled by and are threatening Paris. The United States does not see a conflict happening because it is not observing the battlefield, and it is not observing the battlefield because it has not classified it as a battlefield. By the time the United States recognizes that a threat actually exists and communicates that across all stakeholders within its government and those of its allies, several days have gone by and its adversary has established a foothold.

The Russians are following in the tread marks left by the Germans. They have taken the cyber domain—a "new thing"—that fundamentally transforms how space and time operate during war, and adapted their entire conception of conflict because of it. America, in

Air Force Master Sgt. Robert Kocsis (*right*) confers with an Estonian soldier 25 April 2018 during Locked Shields 2018 in Tallinn, Estonia. NATO's annual Locked Shields exercise is the largest and most complex live-fire cyber defense exercise in the world. (Photo courtesy of the NATO Cooperative Cyber Defence Centre of Excellence)

contrast, is asking how the cyber domain can augment its historical conception of warfare. This is not the fault of any particular group of officers, nor is it the result of deliberate ignorance. The simple fact is that the cyber domain is hard to understand and exceptionally diffuse in its potential military applications. There is a powerful temptation to simplify the problem set by either focusing only on the concrete and quantifiable (e.g., hardware, software, physical infrastructure, coder hiring policies) or entrusting the Nation's cybersecurity to private companies (e.g., Raytheon, Microsoft, and, until recently, Amazon).[19]

However, this does not change the fact that Ukraine and Crimea are not aberrations; they are the future of conflict. Actors like Russian President Vladimir Putin will continue to turn to the cyber domain as their first theater of operations so long as America's absence from the battlefield slows down its cognition of events. So long as the United States and its allies continue to focus on the men with guns and the tanks moving toward Kyiv and not on the host of hostile actions that precede them, it will remain significantly behind its enemies in its ability to shape and respond to events. Moreover, the United States does not have the time to develop a cyber plan for the year 202x in conjunction with, for example, NATO. Even though convergence has frequently happened on NATO's doorstep, it also happened nearly ten years ago. Construing the nexus of the cyber domain and battlefield effects as a future problem to be dealt with through procurement or technological innovation ignores what U.S. enemies have been practicing as a reality for the better part of a decade. The current situation demands that the United States use what it currently has both to establish a credible deterrent against future fait accompli attacks and to help it and its allies make the cognitive transition to the new age of warfare.

Toward a Solution: A Few Good NATO Force Integration Units

The tank was not developed for global deployment in all environments and all terrains; the United States' response to the modern incarnation of cyber-information-physical domain convergence should not be either. Its first step should be triaging its cyber vulnerabilities. The United States must be prepared to tailor regionally focused cyber responses with forces and assets it already has on hand. To that end, I recommend that the United States focus first on where there is most obviously a threat: Europe's borders with the Russian Federation, particularly the Baltic states of Lithuania, Latvia, and Estonia.[20] The United States should look to stand up tailored force packages (TFPs) specifically designed to detect convergence between cyberspace and the real world, and to respond in kind with real-world forces when situations demand.

> The Russians are following in the tread marks left by the Germans. They have taken the cyber domain—a 'new thing'—that fundamentally transforms how space and time operate during war, and adapted their entire conception of conflict because of it.

The template the United States should use in building such TFPs should be substantially informed from the 1986 creation of U.S. Special Operations Command, particularly in emphasizing the placement of the optimal combination of people, resources, and decision-making authorities in an organization.[21] Instead of serving as their own detached line of effort, the cyber components of TFPs would be but one feature of a joint endeavor to focus the elements of national power on a discrete and enduring problem. TFPs would have to be able to not only identify threats as they manifest in the cyber domain but also be able to rapidly respond to those threats with the authority, precision, and speed the modern battlefield requires. Any cyber-physical TFP in the Baltics must have the functional form of a seamless link between sensing, deciding, and shooting nodes.

NATO force integration units (NFIUs) are ideally suited to serve as the chassis for this concept. NFIUs exist in each Baltic capital and were initially designed to foster collaboration between the armed forces of their host nations and the NATO Very High Readiness Joint Task Force in times of crisis; they specifically provide broad planning support to allow the rapid deployment of NATO forces to the eastern members of the alliance.[22] The United States could surge the right combination of people, resources, and authorities to the NFIUs to create a parallel convergence early-warning fusion cell. Convergence fusion cells should not only onboard TFPs from the Department of Defense and the National Security Agency but also have the ability to combine personnel and data streams from the local Central Intelligence Agency station, Federal Bureau of Investigation liaison at the U.S. embassy, and law enforcement personnel from both the host country and regional enabler countries.[23] The primary mission of convergence fusion cells would be to combine intelligence from cyberspace and the information environment with developing events in the physical world to detect a fait accompli attack in its infancy and to have the ability to respond quickly enough to prevent the attack from being carried out.

Convergence fusion cells would require flattened reporting channels and clear authorities to rapidly translate observation of a threat into orientation of national assets on it. In drawing again from the example of U.S. Special Operations Command's creation, there needs to be an assistant secretary-level individual who is the primary recipient of convergence fusion cell data streams and who in turn has the authority to direct action based on that data.[24] Simultaneously, this individual needs to have both immediate and peer access to other critical decision-makers in the National Security Council to enable consensus, whole-of-government planning, and synchronization of government lines of effort. Simply because the Trump administration rescinded Presidential Policy Directive 20 does not make it advisable to pull off operations in the cyber domain in isolation.[25] The Russian model of warfare requires that the United States prepare to not only shut down troll farms and hacker units in cyberspace but to also be ready to move real-world troops, aircraft, and ships to preempt a fait accompli attack. Diplomacy has a prime and instrumental role in making this possible.

The status of forces agreements (SOFA) under which the U.S. military operates in a host of countries worldwide require an upgrade for the digital age.[26] The American military has numerous units that it maintains on a high alert status for immediate contingency deployment, and some of these units have developed operational concepts for deploying to support an ally during times of crisis. The scale and scope of the military operations these forces can conduct on host nation soil may be governed by the SOFA that exists between the U.S. government and the host nation. The United States' ability to no-notice deploy 10th Special Forces Group teams to hunt for and destroy Russian tanks entering Lithuanian territory as part of a fait accompli, versus sending a company from the 173rd Airborne Brigade Combat Team to help defend Vilnius, hinges on a shared understanding of risks, indicators, and required actions between the two governments. If the NFIU-based convergence fusion cells help both governments find the enemy preparing to deploy in the cyber domain, SOFAs allow them to preemptively design the force packages that can be expeditiously deployed against the enemy's follow-on forces in the physical world. While undoubtedly arduous and problematic, this level of engagement and serious thinking about emergent threats is what is required in the age of convergence. Any lag time between America's sensors, decision-makers, and shooters only entices its adversaries to lick their chops.

Challenges, Risks, and Requirements

New task organizations as represented by the convergence fusion cells, flattened reporting and decision channels, and a diplomatic framework to enable real-world shooters to rapidly respond to cyber-world sensor observations all suggest an approach to the age of convergence that can be implemented using what the U.S. government and military already have at their disposal. That is not the same thing as saying this transformation will be without risks or difficulties. The first and most obvious difficulty will be integrating all of the elements of American statecraft within the instrument of power represented by the convergence fusion cells.

Suppose that a convergence fusion cell detects the warning signs of election meddling emanating from the Russian Internet Research Agency (IRA) that indicate a deliberate attempt to foment societal division within Estonia, and that at the same time, the Russian armed forces conduct a snap military drill in the Western Military District surrounding Saint Petersburg. The U.S. government decides to focus its efforts on degrading the IRA's ability to conduct cyber-enabled information warfare, principally through a combination of U.S. Cyber Command-directed offensive strikes against the IRA's digital architecture, financial asset seizures orchestrated by the Department of Treasury against Russian oligarchs, and Department of Justice indictments against prominent Russian military and political leaders. The question remains whether this is a military, economic, or law enforcement response. The answer in the age of convergence is "yes," implying that the U.S. government will need to think about how its elements of statecraft relate to each other in a world where functional specializations merge and separate continuously in the digital and physical worlds. The convergence fusion cells can be given clear authorities, manning and equipment, and reporting channels, but these measures will not be sufficient to orient the entire American state apparatus on the patterns of thinking, collaborating, and decision-making that convergence portends.

The age of convergence also requires that the United States seriously rethink its legal approach to armed conflict. It is not novel to observe that cyberwarfare challenges conventional notions of distinction, proportionality, military necessity, honor, and humanity. Many nations' cyberwarriors are nonuniformed civilian contractors; can they be targeted for kinetic strikes under the current Law of Armed Conflict perceptions of distinction if they are deliberately fueling social unrest in an allied country?[27] Shutting down the servers that run the electric plant powering an enemy's antiaircraft radar might reduce the need to fire a Tomahawk missile at that facility, but it might also accidentally kill everyone in the intensive care unit attached to the same power grid. America's current Law of Armed Conflict framework does not provide a clean answer to the implicit questions of military necessity and humanity attending the decision to launch this notional cyberattack. Convergence has not created these issues, but it has brought them into sharp relief. Again, authorities, personnel, and equipment can only go so far in clarifying the targets convergence fusion cells can identify and the rules of engagement that flow from target designations. True domination of the cyber-physical domains' convergence requires clear ethical precepts and legal standards for the employment of armed force.

In addition to setting our own house in order organizationally and legally, American policymakers face the problems and risks associated with integrating the convergence fusion cell concept with the rest of NATO. The NFIU-based convergence fusion cells will require NATO augmentation to avoid becoming either a de facto or de jure bilateral American security agreement with individual Baltic nations. The NATO Very High Readiness Joint Task Force will need to be incorporated into any plans requiring the rapid response of real-world forces to events unfolding in the cyber domain; the dearth of a military equivalent to the Schengen Zone is only more problematic for European security in light of convergence's reality. There are myriad actions that must be undertaken to make the convergence fusion cell concept a viable, long-term solution to an enduring security dilemma, but that should not distract from the fact that immediate action is required and that the United States is uniquely postured to provide the expertise, capabilities, and leadership to start the process.

A poster outside Downing Street, London, in 2014 asking the British government to take action against Vladimir Putin for the Russian invasion of Ukraine. During the invasion, Russian cyber warriors relentlessly promoted the idea of "Ukraine as a neo-Nazi state," while irregular Russian forces, private military companies, and nonuniformed militia organizations fanned the flames of social disorder. (Photo by Mim Friday, Alamy)

Finally, there is also a risk of seeing a flash without experiencing a bang. The convergence fusion cells might perceive a threat forming; the United States might deploy its highly prized and expensive special operations forces in response to that threat, only to never see the threat manifest in the physical world. This risk underscores why it is important not to deploy cyber reconnaissance capabilities in isolation but rather to have them operating in conjunction with the full arsenals of the United States, NFIU host nations, NATO, and regional partners. Intelligence works best when it is multisourced. Additionally, U.S. leaders must be comfortable with what success looks like for the convergence fusion cells; it looks like SOF, or the 82nd Airborne Division, or fighter squadrons from Aviano Air Base that deploy but never actually fire a shot. One reliable sign of a successful deterrence effort is the absence of conflict.

Conclusion: Converging on Combat Leaders

These recommendations are intended to confront modern conflict with the assets on hand because expediency requires it. They are bridging actions only and do not obviate the need for force management responses to novelty and modernity. Convergence—the continual merging of the effects of the digital and physical worlds—requires new mentalities as much if not more than it requires new equipment, and so requires America's military leaders to ponder several foundational questions. The

United States needs to grapple with what foreign internal defense looks like in an age of cyber-enabled information warfare. It needs to consider whether the competencies and skills that America looks for in creating its most innovative, agile, and responsive forces are in need of revision. The cyber domain cannot and must not be the sole purview of computer coders and programmers any more than Army supply discipline should be the sole purview of supply room noncommissioned officers.

This raises the question of how the United States should train and educate its military's combat leaders, its paratroopers and submariners, its artillerymen and bombers, so that they can conceptualize the cyber realm. Combat leaders must grasp how the "always present but never seen" domain influences the physical employment of their forces; doing this is the only way for them to design innovative ways of fusing information, cyber capabilities, and physical assets into new modalities of warfighting, and for them to responsibly manage the joint force that will be required in 2028, 2035, and beyond. In this sense, the Army's conception of multi-domain operations is very much a modern analog of AirLand Battle; it is a response to material realities that cannot be wished away and an opportunity to redesign America's approach to both warfighting and the warfighter. The United States can only take advantage of this opportunity if it trains tomorrow's tactical commanders to "see" the battlespace, even when it exists in part or in whole in a digital environment.

Most officers have heard a variation of the idea, popular in military history courses, that armies that lose current wars spent too much time preparing for the last war they fought. The age of convergence has, thankfully, given the U.S. military repeated and loud warnings that it is here for the foreseeable future. America's defense leaders need to understand that however they prefer to construe current geopolitics and national strategic planning—such as large-scale combat operations, near-peer competition, great-power competition, and the like—Americans are all living under the new realities of time and space that convergence has wrought. The decisions the United States makes now regarding its current and future conceptions of conflict will determine whether it goes the way of the British or the Germans, if Suwalki goes the way of Crimea, or whether America has met the conditions to break out of its *while* loop.[28] ■

The author would like to thank Professor Nathaniel Raymond of Yale's Jackson Institute for Global Affairs for proofreading this article and helping to sharpen the recommendations regarding the employment of convergence fusion cells. Raymond's insight on previous examples of interagency/multinational collaboration, particularly in Macedonia, were indispensable; similarly, Raymond helped me think through the long-term implications that the age of convergence has for the way America thinks about its force structure and force requirements beyond the immediate needs of the present and for the ways it challenges long-standing American notions of the ethics and legal structures by which wars should be fought.

Notes

[1] Richard Shirreff, *War with Russia: An Urgent Warning from Senior Military Command* (New York: Quercus, 2016); *Merriam-Webster*, s.v. "bot," accessed 9 November 2020, https://www.merriam-webster.com/dictionary/bot. A bot is a computer program that performs automatic repetitive tasks, especially one designed to perform a malicious action; *Merriam-Webster*, s.v. "troll," accessed 9 November 2020, https://www.merriam-webster.com/dictionary/troll. A troll is a person who intentionally antagonizes others online by posting inflammatory, irrelevant, or offensive comments or other disruptive content.

[2] Sergey Sukhankin, *Unleashing the PMCs and Irregulars in Ukraine: Crimea and Donbas* (Washington, DC: The Jamestown Foundation, September 2019), 6–10, accessed 20 October 2020, https://jamestown.org/program/unleashing-the-pmcs-and-irregulars-in-ukraine-crimea-and-donbas/.

[3] Steven Pifer, "Five Years after Crimea's Illegal Annexation, the Issue is No Closer to Resolution," *Order from Chaos* (blog), The Brookings Institution, 18 March 2019, accessed 20 October 2020, https://www.brookings.edu/blog/order-from-chaos/2019/03/18/five-years-after-crimeas-illegal-annexation-the-issue-is-no-closer-to-resolution/.

[4] Kurt Volker, "Where's NATO's Strong Response to Russia's Invasion of Crimea?," *Foreign Policy* (website), 18 March 2014, accessed 20 October 2020, https://foreignpolicy.com/2014/03/18/wheres-natos-strong-response-to-russias-invasion-of-crimea/.

[5] U.S. Army Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 20.

[6] MacGregor Knox and Williamson Murray, *The Dynamics of Military Revolution, 1300-2050* (New York: Cambridge University Press, 2001), 12. I am applying the Knox-Murray definition of *revolution in military affairs*, which describes a series of events that "military organizations embark on … by devising new ways of destroying their opponents. To do so, they must come to grips with fundamental changes in the social, political, and military landscapes … *Revolutions in military affairs require the assembly of a complex mix of tactical, organizational, doctrinal, and technological innovations in order to implement a new conceptual approach to warfare or to a specialized sub-branch of warfare* [emphasis added]."

[7] Williamson Murray, "Armored Warfare: The British, French, and German Experiences," in *Military Innovation in the Interwar Period*, ed.

Williamson Murray and Allan R. Millet (New York: Cambridge University Press, 1996), 40.

8. Ibid., 11.

9. Ibid.

10. The OODA (observe, orient, decide, act) loop is an iterative cycle first postulated by retired Air Force Col. John Boyd, by which individuals and organizations observe a threat, orient on the threat, decide on how to respond to the threat, and act against the threat.

11. *Soviet Active Measures: Hearings Before the House Permanent Select Committee on Intelligence*, 97th Cong. (1982), 2; Michael V. Hayden, Heather A. Conley, and Seth G. Jones, interview by John J. Hamre, 11 June 2018, transcript, "Russian Active Measures: Past, Present, and Future," CSIS-TCU Schieffer Series, Center for Strategic and International Studies, Washington, DC, accessed 20 October 2020, https://www.csis.org/analysis/russian-active-measures-past-present-and-future; TP 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, 5–6. The term "active measures" was coined during the Cold War to describe Soviet influence operations, which blended covert actions with information operations and Soviet diplomatic ventures.

12. Phillip A. Karber, "Russia's 'New Generation Warfare,'" National Geospatial-Intelligence Agency, 4 June 2015, accessed 20 October 2020, https://www.nga.mil/MediaRoom/News/Pages/Russia%27s-%27New-Generation-Warfare%27.aspx (site discontinued).

13. Ibid.

14. The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 3, accessed 20 October 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

15. Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: U.S. Government Printing Office, 27 November 2012, Incorporating Change 1, 20 November 2014), GL-3. The full definition of information operations is "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO."

16. Ibid., I-2.

17. JP 3-12, *Cyberspace Operations* (Washington, DC: U.S. Government Publishing Office, 8 June 2018), II-1–II-2.

18. Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (2011): 101.

19. Naomi Nix and Bloomberg, "Why Amazon's Suit Over the $10 Billion Cloud Contract It Lost to Microsoft Will Be So Hard to Win," *Fortune* (website), 22 November 2019, accessed 20 October 2020, https://fortune.com/2019/11/22/amazon-microsoft-jedi-cloud-trump-lawsuit/.

20. Office of the Secretary of Defense, "Summary of the 2018 National Defense Strategy of the United States of America" (Washington, DC: Department of Defense, 2018), 1–2; TP 525-3-1, *The Army in Multi-Domain Operations 2028*, 7. The decision to explicitly focus on the Baltics and implicitly on Russia is in step with current U.S. defense thinking and joint concepts, which acknowledge China as the long-term geopolitical rival to the United States but identify Russia as the current "pacing threat for technical and tactical purposes."

21. Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law No. 99-433, 100 Stat. 1017 § 212(a)(2) (1986).

22. "NATO Force Integration Units (NFIU)," Supreme Headquarters Allied Powers Europe, accessed 3 May 2020, https://shape.nato.int/operations/nato-force-integration-units; "NATO Force Integration Units," NATO, last updated September 2015, accessed 20 October 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_09/20150901_150901-factsheet-nfiu_en.pdf.

23. Saska Cvetkovska et al., "The Secret Players Behind Macedonia's Fake News Sites," Organized Crime and Corruption Reporting Project, 18 July 2018, accessed 20 October 2020, https://www.occrp.org/en/spooksandspin/the-secret-players-behind-macedonias-fake-news-sites. Macedonia stands out as an example of a regional enabler country; it has partnered with the United States and several Western European nations to "probe possible links between Russians [and] U.S. citizens." Not all countries will have equal experience in identifying, tracking, and shutting down the various manifestations of convergence activities, which implies that those with more experience should take on a greater leadership role.

24. Charles Nemfakos et al., *The Perfect Storm: The Goldwater-Nichols Act and Its Effect on Navy Acquisition* (Santa Monica, CA: RAND Corporation, 2010), 8. The Goldwater-Nichols Act of 1986 that created the U.S. Special Operations Command also created the Office of the Assistant Secretary of Defense-Special Operations and Low-Intensity Conflict. This office and the individual who headed it were intended to prevent future recurrences of Operation Eagle Claw, the abortive special operations attempt to rescue American hostages from the U.S. embassy in Iran; specifically, they were supposed to work to ameliorate the identified shortcomings of "muddled and multiple chains of command, poor interservice planning and coordination … [and] the inability of one service to communicate to another."

25. Eric Geller, "Trump Scraps Obama Rules on Cyberattacks, Giving Military Freer Hand," Politico, 16 August 2018, accessed 20 October 2020, https://www.politico.com/story/2018/08/16/trump-cybersecurity-cyberattack-hacking-military-742095. Presidential Policy Directive 20 (PPD-20) was an Obama administration policy that only allowed military cyber operations to proceed after lengthy and multiple high-level discussions between various government agencies. While intended to have the effect of synchronizing U.S. policy, many defense planners perceived PPD-20 as significantly delaying the responsiveness of America's cyber forces.

26. Desiree Dillehay, "Status of Forces Agreement: What is it and Who is Eligible," Army.mil, 18 September 2019, accessed 20 October 2020, https://www.army.mil/article/227245/status_of_forces_agreement_what_is_it_and_who_is_eligible. A Status of Forces Agreement "provides the basis for the legal status of military, U.S. civilian employees and dependents who are stationed on orders in NATO partner countries."

27. *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013), 10, accessed 20 October 2020, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-083.pdf; Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volume I of II* (Washington, DC: U.S. Department of Justice, 2019), 14–27. Publicly available reporting suggests, for example, that both the Chinese People Liberation Army's Unit 61398—the military organization suspected to have been behind some of China's most extravagant episodes of cyberespionage—and the Russian Internet Research Agency are significantly staffed, supported, and funded by civilian contractors.

28. Bill Lubanovic, *Introducing Python: Modern Computing in Simple Packages*, 2nd ed. (Sebastopol, CA: O'Reilly Media, 2020), 87–89. Loops are frequently used in computer programming languages to execute a set of operations repeatedly and endlessly, until or unless specific criteria are met. After the criteria are met, the loop is broken, and the rest of the code can run forward.