Owltonomous, autonomous surface vehicle from Florida Atlantic University, competes during Office of Naval Research–sponsored Maritime RobotX Challenge, Honolulu, Hawaii, December 14, 2018 (U.S. Navy/John F. Williams)

Tactical Maneuver in the Cyber Domain

Dominating the Enemy

By Jennifer Leigh Phillips

As the platoon clears the alley, Corporal Stokely turns the corner and receives sniper fire from an elevated position near a cluster of high-rise apartment buildings. There is already chaos in the street from an unidentified explosion, and Corporal Stokely can see there are people clustered in the windows on multiple levels of the building where the sniper fire is originating. After several moments of attempting unsuccessfully to neutralize the sniper, the unit is able to identify him. He is located in the corner apartment of the sixth floor of the building. The unit is not able to call in kinetic support due to the high potential for civilian casualties in the area. The Joint Terminal Attack Controller [JTAC] *makes a call for fire: "CYBER01, THIS IS L63, IMMEDIATE SUPPRESSION GRID 211432, BUILDING 2, FLOOR 6, SW CORNER, AUTHENTICATION IS TANGO UNIFORM OVER." The response is immediate: "THIS IS CYBER01, IMMEDIATE SUPPRESSION, GRID 211432 BUILDING 2, FLOOR 6, SW CORNER, OUT." A moment later, an image materializes on the JTAC's Cyber ROVER screen of a man holding a rifle, his back to the camera device. "L63, THIS IS CYBER 01, TARGET CONFIRMED, REQUEST CONFIRMATION FOR IMMEDIATE SUPPRESSION." "THIS IS L63, CONFIRMED." The television*

Major Jennifer Leigh Phillips, USAFR, Ph.D., is Individual Mobilization Augmentee to the Deputy Chief of the Intelligence, Surveillance, and Reconnaissance Division, 607 Air and Operations Center, U.S. Air Force. She is also an Assistant Professor of Education at the University of Southern California.

set near the sniper explodes, sending glass and shrapnel through the room. The explosion disrupts the sniper, allowing the team to move quickly through the street, continuing on to their destination.

Imagine the possibilities if tactical teams were able to plan a raid that integrated not only air and ground support but also on-call fires in the *cyber* domain. In terms of achieving economy of force, limiting costs, and reducing physical collateral damage, the opportunities are endless. To effectively compete in future war, the United States must master the ability to maneuver through and in the cyber domain to seize the initiative by destabilizing the enemy's cognitive decisionmaking capacities. Achieving operational and tactical maneuver success in the cyber domain requires advances in U.S. military doctrine, tactics, and training beyond current capacities.

The concept of tactical cyber maneuver arises from an appreciation that the Internet of Things (IoT) will become ubiquitous, pervading every aspect of our daily lives over the next 20 to 40 years. The IoT will penetrate both large urban areas and the expanse of rural, virtually connected regions of the world currently considered "unconnected."

The large physical footprint that has been an advantage to U.S. military operations in the past is quickly becoming a liability. Disruptive use of force within and manipulation of the cyber domain both in close and deep battle to create surprise and shock is achievable through tactical and operational cyber maneuver. Military actions will not likely be at a time or place of our choosing. U.S. military forces may find they can control strategic use of force in the cyber domain, but commercial, civilian, and systemic influences will demand that tactical military entities function offensively in this domain. These fielded forces will interact with the IoT in the conduct of their duties across the range of military operations.

When facing an enemy of technological parity such as Russia or China, the military actor is potentially at a disadvantage in the cognitive, physical, and/or virtual dimensions. As a result, conceptual thinking about the cyber domain must move away from an obsession with strategic-level decisions toward full integration of cyber into combined arms for tactical and operational maneuver as a necessary condition for achieving national and strategic objectives. Our national defense mechanisms must invest in appropriate tactical capabilities and practical education of its personnel to effectively maneuver in the cyber domain as part of a holistic multidomain approach.

The operational and tactical initiative is empowered by exploiting cyber maneuver to cripple the enemy's cognitive linkages. Time and space also present challenges for intelligence, command and control, and logistics. Today's linear, strategically reactive approach to the cyber domain cannot overcome the tactical and operational coordination requirements to enable maneuver. To achieve the desired effects across the physical, virtual, and cognitive dimensions where wars are fought and won, a renewed emphasis is needed on the intersectionality between the cyber domain and physical space to refine joint force doctrine; operational practice; and tactics, techniques, and procedures (TTPs). Overcoming the cognitive barriers to conceiving of this intersectionality will require a concerted effort to deliberately query and challenge biases in our own conception of the cyber domain through education, training, simulations, and exercise trials across the joint force. Three key attributes of the cyber domain compel the U.S. military to sharpen its integration of cyberspace in combined arms multidomain maneuver considerations: an interactively complex system; the intersection of the physical, cognitive, and virtual; and nonlinear, disproportionate strategic effects to be achieved by appropriately integrating tactical maneuver in the cyber domain as part of operational design through all phases of warfare.[1]

Operational Considerations for Tactical Maneuver in Cyberspace

Maneuver. Tactical maneuver elements must take advantage of virtual, physical, and cognitive connections between the cyber domain and other domains to achieve operational and tactical objectives through multidomain maneuver. The success of distributed operations in the future will rely on the ability to achieve rapid maneuver in the cyber domain as part of sequential or simultaneous integrated movement across other domains. We must move away from a static understanding of focusing on tools used to conduct offensive and defensive operations in the cyber domain toward a focus on dominating the enemy by seizing the initiative through combined arms multidomain maneuver that fully integrates manipulation of the cognitive, virtual, and physical dimensions of the cyber domain. According to Marine Corps Doctrine Publication 1, *Warfighting*:

Success depends not so much on the efficient performance of procedures and techniques, but on understanding the specific characteristics of the enemy system. Maneuver relies on speed and surprise for without either we cannot concentrate strength against enemy weakness. Tempo is itself a weapon—often the most important. Success by maneuver—unlike attrition—is often disproportionate to the effort made. However, for exactly the same reasons, maneuver incompetently applied carries with it a greater chance for catastrophic failure.[2]

At the battalion level and below, tactical forces must effectively induce shock and surprise in the enemy, and the cyber domain may be the most effective means of doing so in a given particular situation. U.S. forces are currently integrating robotics, unmanned aerial vehicles, artificial intelligence, and other capabilities. Combined arms maneuver already integrates the cyber domain throughout the military force, but a real understanding of the interaction—the hinges—between the cyber domain and other domains is limited to few specialists at this time. The entire force needs to be better educated regarding the interplay between the cyber domain and other domains to bring about a paradigm shift in current concepts of multidomain maneuver. Clearly,

Commander of 558th Flying Training Squadron, left, discusses training mission utilizing T-6 Flight Simulator with enlisted remotely piloted aircraft pilot student, Joint Base San Antonio, Texas, July 17, 2018 (U.S. Air Force/Bennie J. Davis III)

cyber is not a replacement for other forms of maneuver and fire, but it is part of a complete whole in terms of our approach to conducting operations.

Much of the technology exists today within commercial entities to support mapping, overlaying, and exploiting cyber environments. Adapting these technologies for operational and tactical military purposes will require a clear picture of maneuver in the cyber domain as both physically and temporally overlaid with human and physical terrain features of interest to military missions. The activities described to support maneuver will also apply to the fires considerations and will require extensive investment in doctrine and training to understand the logistical and intelligence requirements needed to support these actions. Specifically, logistical considerations will need to encompass the architectural support and configuration management requirements needed to integrate new and emerging technologies into a distributed network environment. However, the ideas and concepts related to maneuver within the cyber domain must precede investment in technology tools and materiel solutions.

Fires. With the proper authorities and command and control structure in place, calls for fire in the cyber domain may resemble those in other domains. Destroying or activating a virtual-physical connector to achieve lethal effects through cyber during a "troops in contact" by what could be called a close cyber support mission rather than a close air support may or may not have physical effects visible to the naked eye. Tactics will need to meld both electronic warfare and information operations with coordination procedures to establish the equivalent of a cyber "call for fire."[3]

Fire support could be provided either through a cyber element embedded within a Tactical Operations Center or through deep fires support provided through U.S. Cyber Command or the joint cyber center established at the joint force command (JFC). In the absence of secure and reliable communications to these reachback elements, the tactical unit of the future must also possess the ability to conduct its own organic fires support within the cyber domain to the greatest extent possible. The ability to engage in direct tactical cyber fire mission, originating from the team rather than a reachback element such as CYBER 01 described in the opening vignette of this article, would not alleviate responsibility

for those disaggregated elements supporting that team to monitor the effects of the tactical cyber direct fire in the virtual dimension as previously described.

Cyberspace coordination procedures and rules of engagement (ROEs) established in advance are designed to mitigate cyber effects from spilling over and creating unintended consequences outside of the immediate cyber domain environment in which tactical maneuver is taking place. The environment(s) identified as viable for cyber maneuver in advance of the mission may or may not coincide with the specific area of operations within which the tactical unit is maneuvering physically. Even in a no communications or degraded communications environment, the reachback cells previously identified can monitor for spillover effects outside of the cyber environment, ensuring the joint task force commander and/or component commander is aware of changes in the cyber domain environment.

Command and Control. As can be seen from considerations discussed regarding maneuver and fires, planners and operators will need to develop similar control mechanisms to Airspace Control Mechanisms. However, geographic boundaries will not be sufficient given that applications and the network architecture supporting the IoT are not always collocated in the same city, region, or country as the device or program that must be manipulated to support maneuver and fires missions. Command and control of operations that integrate tactical maneuver in the cyber domain is essential in mitigating unintended consequences.

Decisionmakers should examine opportunities to expand authorities to the tactical commander below the JTF level to conduct maneuver in the cyber domain for both offensive and defensive purposes. This expansion should include a careful analysis of the applicability of current ROEs and the Laws of Armed Conflict to examine applications of force in the cyber domain. Further investigation is warranted into how the military force can expand and logistically support passive and nontraditional mechanisms for monitoring, communication, and coordination in real time to support a more diverse approach in the future to command and control.

Just War Considerations. Gregory J. Rattray has posited an interesting idea related to force in the cyber domain that may be worth further consideration for its implications for military ROEs. He specifically puts forward the concept of microforce, wherein "the use of nonviolent digital attacks to achieve political objectives must be understood as part of a new form of warfare. . . . At issue here is the amount of energy unleashed by a given weapon at the time of attack."[4] Putting aside the discussion of whether digital attacks represent a new form of warfare, understanding actions in the cyber domain as a form of energy or violence is useful to applying the precepts of just war theory. Perhaps the current concept of kinetic versus nonkinetic force may need to be adapted to understanding force as the act of violence regardless of how discernable the effects of that force may be to the naked eye or sensor. As demonstrated in the opening vignette, rendering effects through tactical maneuver in the cyber domain has the potential to cause unintended collateral damage to noncombatants either directly or because of bleed over of tools intended for military purposes on civilian networks.

Assuming the perspective that the cyber domain should be treated as an environment just like the other domains helps to clarify the cyber domain considerations in relation to *jus in bello*. Jus in bello, as it applies to the United States military, concerns the moral and philosophical Western tradition of just war theory as well as the international agreements and treaties that comprise international humanitarian law.

Arising Opportunities

Integration of tactical maneuver in the cyber domain by fielded forces focuses on achieving one's objective through offensive maneuver. Rather than emphasizing the *threat* of the individual actor and potential disproportionate effects achieved by the lone wolf, we should seek to *learn* from the lone wolf to inform tactical maneuver in the cyber domain. These lessons may also inform the imperative for restraint in the conduct of tactical offensive operations in the cyber domain precisely because of the potential disproportionate consequences of interactions within this complex system.

Understanding the Cyber Domain as a Complex System. Military planning is an exercise in problem-solving. When presented with a military scenario or challenge, the planner must design an approach that will result in success based on effective and thorough framing of the problem. Future planners must frame the context of tactical action in all domains, including the interactive networks and configurations of the cyber domain. Traditional military planning assumes that by translating the commander's guidance and mission to objectives and tactical tasks, the planner is able to maneuver and conduct operations across all domains in a simultaneous or sequential approach. However, proper planning requires careful analysis of the multifaceted nature of the influences of these domains on human perceptions and the environmental conditions across these domains.

Integration of the cyber domain in tactical military planning appears to threaten the principle of simplicity. The overdramatization of the domain in current strategic literature and discourse has a tendency to cloud clear thinking on problem-solving in this domain. However, while the domain is an interactively complex system, effective techniques for developing an understanding of the multifaceted connections and layers of the cyberspace domain are available today. Through disciplined investigation of connections, or hinges, among the virtual, physical, and cognitive dimensions of the cyberspace domain, military planners can hope to achieve opportunities to achieve both simultaneity and depth through the cyber domain in concert with other tactical actions. Keeping a close eye on the greater operational and strategic objectives is essential in all planning; integration of the cyber domain in planning is no exception.

A key component of future success in achieving simplicity in tactical maneuver in the cyber domain will be to move beyond a reliance on materiel solutions and to focus first on ideas and concepts such as presented here to evolve a shared understanding of the cyber domain. While common operating pictures, computer network defense, and computer network attack (CNA) tools will be requirements to conduct tactical maneuver in the cyber domain, a common and comprehensive understanding of the complexity of this domain in military operation is required. Integrating doctrine, organization, training, materiel, leadership, personnel, facilities, and policy (DOTMLPF-P) considerations as part of a functional solutions analysis is essential as a follow-on consideration of this initial work. Today's joint force is compelled to focus on baselining common knowledge of the cyber domain as essential to equipping military planners and operators with the necessary background for both understanding the cyber environment and conducting successful tactical maneuver in this environment.

While Department of Defense Information Assurance training has become a standard tool for teaching Servicemembers how to protect their own activities within the cyber domain, there is no single-source mandatory training that attempts to shape a common vernacular or language for communication across the joint force regarding this domain. While Intermediate Developmental Education introduces officers to cyber domain concepts, this training is too little and too late to equip the tactical force for planning required at the junior officer and junior enlisted level. A concerted effort to peel away the "mystique" of the cyber domain leads directly to clarity in planning and orders writing.

Finally, design should also consider the integration of just war principles in relation to the cyber domain. Myriad policies, legal considerations, and ROEs procedures will continue to influence the utilization of certain tactics within the cyber domain. The 1988 release of the Morris worm by a Cornell University student, Robert Morris, is an example of the potential negative impact deriving from poor planning and risk mitigation. Morris's intent in releasing the worm was to tally the size of the Internet at the time. However, the randomization measure Morris installed in the worm to ensure it would be able to succeed in penetrating systems resulted in a level of replication that effectively crashed every computer system it entered. As discussed, the utilization of TTPs and control mechanisms must include risk mitigation protocols to help to limit unintended consequences. Specifically, disruption of a particular WiFi or WiMax network in a village or town in order to prevent citizens from tipping local authorities to the location of a maneuver element could also have the unintended consequence of disrupting medical alert systems, home monitoring equipment for hospice patients, or other life-sustaining activities among the civilian population. As civil defense and civilian cyber infrastructures become more reliant on common architecture backbones, tool and TTP development must focus on discriminators and identification protocols for devices and networks in order to limit unintended collateral damage to the greatest extent possible.

Overcoming the perception that analyzing and problem-solving within the cyber domain is too complex without extensive and specific subject matter expertise undermines the military principle of unity of command. Problem-solving by the military planning team necessarily involves both diagnosing the problem as well as explaining the challenge clearly and concisely to senior leaders. Additionally, senior leaders must be well versed in the risks, assumptions, and opportunities the cyber domain presents. Finally, commanders must have confidence in the risks that the force is assuming in delegating freedom of action to the tactical level. The cyber domain proves to be no exception, but the commander who does not understand the domain will prove to be inherently more risk adverse.

Exploiting the Intersection of the Physical, Cognitive, and Virtual Through the Cyber Domain. Future planning requires that planners visualize the cognitive, physical, and virtual properties of the cyber domain as co-existing and interacting simultaneously with the physical domains of land, sea, air, and space. Effectively framing the problem in military operations will include mapping the hinges previously discussed between the cyber and other domains, identifying opportunities to exploit those bridges, and providing for deliberate mechanisms to take advantage of those bridges for either offensive or defensive purposes.

The case of the Stuxnet worm's ability to cause physical damage to the uranium gas centrifuge tubes at the Natanz nuclear facility in Iran is the clearest example of exploiting a hinge between the virtual and physical through the cyber domain.[5] Like the Morris worm, Stuxnet had a singular purpose, but designers scoped Stuxnet to specifications that attempted to limit effects only to those centrifuge tubes used at Natanz. Effective problem-framing and careful identification of the connection between the virtual and physical dimensions were required to identify the desired means for limiting the expansion of Iranian enrichment programs. This problem-framing effort allowed designers to achieve the desired effect in the physical dimension through manipulation in the virtual. Additionally, the worm initially went undetected by the Iranian government, and when the mechanical (physical) difficulties began to emerge, the initial assumption was that there was a physical defect or malfunction afoot. Stuxnet thus achieved both a physical and cognitive effect through virtual action in the cyber domain.

While the Stuxnet worm attack was authorized based on a strategic priority, the planning, worm development, and execution required tactical focus, including extensive cyber espionage by a skilled cadre of experts. In conducting the problem-framing to determine how to disable the Natanz enrichment efforts, planners necessarily envisioned a path across the virtual hinge in the cyber domain to achieve a physical effect. In this respect, the cognitive interplay with the cyber domain is present in both the attacker and victim of this attack. In particular, Stuxnet

Army Rapid Capabilities Office and Project Manager for Electronic Warfare & Cyber teamed with 173rd Airborne Brigade, 2nd Cavalry Regiment, and other receiving units while participating in Joint Warfighting Assessment 18, Grafenwoehr, Germany, April 2018 (U.S. Army)

informs the proper approach to tactical maneuver in the cyber domain from the perspective of economy of force and mass.

The Israelis achieved economy of force in the case of the Stuxnet worm through extensive intelligence preparation of the battlespace across all domains. This example also highlights the hinge between the technical and human considerations of the cyber domain. While the cybernetic problem of identifying the appropriate hinge is essentially one of scientific method, the intended geopolitical effect and following consequences fit in the larger scheme of "wicked" problems.[6] The decision to exploit an opportunity in the cyber domain became a selected option to resolve the Israeli problem precisely because it conformed to a range of "action-prospects" available to the decisionmakers.[7]

A team properly equipped with a "map" of identified hinge opportunities could maintain the offensive during tactical maneuvers while limiting unintended civilian collateral damage with further refinement of military doctrine, training, and tactics. Even in the least connected countries today, the widespread use of cellular and WiFi technologies (and in the absence of such technology-integrating networks the use of devices able to connect through peer-to-peer connections such as Bluetooth) creates opportunities to seize the initiative and exploit tactical advantages. Where it may be unacceptable to use a high-tonnage air-dropped munition on an apartment building where a combatant is firing from on a team, it may be possible to see passively into the room where the shooter is firing from through connected devices such as televisions and phones. If the team is able to pinpoint the exact source of the hostile fire, utilizing a hinge to initiate a physical effect by short-circuiting the electricity, overheating a phone battery to create a low-yield explosion, or turning on the television as a distraction all become possibilities. The objective of neutralizing the enemy is achieved.

Tactical maneuver in the cyber domain is only possible if embraced as a viable component of combined arms multidomain maneuver. U.S. military current force posture and technology certainly does not permit this scenario to come to fruition today, but a reorientation in doctrine and policy would allow for the full realization of DOTMLPF-P solutions to meet these requirements.

Nonlinear, Disproportionate Strategic Effects Achieved at the Tactical Level. Joint Publication 3-0, *Joint Operations*, states, "Commanders conduct [cyber operations] to retain freedom of maneuver in cyberspace, accomplish the JFC's objectives, deny freedom of action to enemies, and enable other

operational activities."[8] However, the majority of military discourse remains focused on strategic cyber or simply focusing effects in the cyber domain based on cyber-centric considerations rather than based on a true multidomain maneuver approach. While leadership and strategy to task metrics dominate discussions of leadership, training, planning, and kinetic operations in warfare, a consistent trend concerning the cyber domain is to compartmentalize its application because of the alleged "uniqueness" of the domain. But all tactical tasks performed on the battlefield should trace back to strategic aims. Tactical and operational cyber maneuver provide the potential to achieve nonlinear, disproportionate strategic effects for military forces.

To understand this vision of tactical cyber maneuver, the phrase *nonlinear, disproportionate strategic effects* should be taken in the proper context of problem-solving. The military planner seeks to solve problems, possessed of both scientific and human factors. The purpose of warfare is to crush the enemy's will, denying him the desire or ability to continue to fight. Human will is both expressed and influenced through the cyber domain. While policymakers cannot ignore the importance of strategic control of this medium, targeting the will of the individual is essentially a matter of tactical maneuver—exploiting his weaknesses while making our own weakness appear as strength. To do so effectively requires a shift in our conceptualization of the cyber domain. Russia's ability to conduct tactical maneuver in the cyber domain during the 2008 Georgia crisis provides valuable insight into the utility of applying multidomain maneuver principles that integrate the cyber domain for future military operations.

Though it has been asserted that Russian targeting of Georgian cyber infrastructure as part of its overland maneuver was not conducted at the tactical level, the value of seizing the initiative and achieving economy of force through preparatory cyberspace fires in this operation is clear. The CNA conducted on a wide scale against Georgian civilian and governmental cyber infrastructure, though not formally tied to the Russian government, achieved clear military objectives. The CNA prevented accurate estimations of the strength and direction of Russian overland movements, preventing communication and queuing among observers, military elements, and senior policy experts. The cyber domain attack was able to prevent an effective initial response to Russian aggression due to ambiguities and a lack of information. Additionally, the attack took advantage of pro-Russian sentiments of a portion of the civilian population, lending confusion to the true nature, intent, and extent of the Russian invasion. As the campaign moved forward, the extent, duration, and scope of Russian maneuver in the cyber domain would change to meet the military needs of the Russian planners.

Rather than focusing on the actions undertaken in the cyber domain, be they denial, deception, espionage, attack, or maneuver, the cyber domain must first be visualized as an organic environment. Humans both influence and are influenced by the cyber domain, much the same as they are on the land, sea, air, and space. Individuals pass through the cyber domain in the same way they walk on the land or sail across the sea. In a future world, the cyber domain is ubiquitous, connecting humans, devices, and even multilayered networks both passively and actively to one another.

Maneuver in the cyber domain is not a new concept given that we as individuals interact with and manipulate the physical, virtual, and cognitive dimensions of the cyber domain on a daily basis. Tactical maneuver in the cyber domain as part of a combined arms multidomain approach to military operations is a concept that must be further explored and elucidated in military doctrine and tactics. Effective education of the force regarding the cyber domain is essential to grooming future planners, operators, and leaders who are able to grapple with this domain. The future force must be able to visualize the operational and tactical hinges between the cyber domain and other domains as they conduct problem-framing and design campaigns to achieve strategic military and national objectives. A common understanding of the cyber domain as ubiquitous in civilian and military life is the first step for military forces to be prepared for this eventual future. **JFQ**

Notes

[1] The term *phase* specifically refers to the phases of an operational plan as articulated in Joint Publication 3-0, *Joint Operations* (Washington, DC: The Joint Staff, January 17, 2017), V-6.

[2] Marine Corps Doctrine Publication 1, *Warfighting* (Washington, DC: Headquarters Department of the Marine Corps, June 20, 1997), 38.

[3] Per Field Manual 6-30, *Tactics, Techniques, and Procedures for Observed Fire* (Washington, DC: Headquarters Department of the Army, July 16, 1991), calls for fire consist of six elements sent in three separate transmissions. While additional elements or subelements may need to be adopted for real-time cyber support in a close combat situation, the practical coordination mechanisms would remain the same.

[4] Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001), 20.

[5] For a detailed case study on the Stuxnet worm, see Chris Morton, "Stuxnet, Flame, and Duqu: The Olympic Games," in *A Fierce Domain: Conflict in Cyberspace, 1986–2012*, ed. Jason Healey (Washington, DC: Cyber Conflict Studies Association, 2013), 212–231.

[6] Horst W.J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4, no. 2 (1973), 155–169.

[7] Ibid.

[8] JP 3-0, III-9.