Parachute bundle with Joint Precision Air Drop system, using GPS navigation, drops from C-130J Hercules to remote Forward Operating Base, November 27, 2011 (U.S. Air Force/Tyler Placie)

Surfing the Chaos

Warfighting in a Contested Cyberspace Environment

By William D. Bryant

On a crisp fall day in mid-October 1805, two fleets met to decide the fate of Europe at the Battle of Trafalgar.[1] The combined fleets of the French and Spanish navies were larger, with heavier and more powerful ships, and their commander, Admiral Villeneuve, had even correctly deduced the battle strategy of his opponent. Contrary to the accepted naval practice of lining up parallel so that respective admirals could maintain control, Admiral Lord Nelson divided his smaller force into two columns directed perpendicularly against the enemy fleet. This produced a chaotic but decisive battle. And even though Nelson was killed, his more aggressive and self-synchronizing forces defeated the French and Spanish fleet on a scale not matched until modern times.

What can a battle from the age of sail and wooden ships possibly teach us about modern warfare? In a cyber-contested environment and facing a competent foe, the side that embraces the chaos, confusion, and lack of control on the modern battlefield is more likely to emerge victorious, much like Nelson's force. To win

Colonel William D. Bryant, USAF, is the Deputy Chief Information Security Officer for the U.S. Air Force.

in the new cyber-contested battles of the future, a combatant must still command, but let go of control and surf the chaos.

Future Warfare

In the strategic community, conventional wisdom holds that capable nation-states will fight future wars not only in the traditional land, maritime, air, and space domains but also in cyberspace. Analysts also often argue that the United States will be at a disadvantage in this type of warfare because it has a higher reliance on cyberspace-enabled systems.[2] Combatants will fight future wars in all domains, but the United States is not naturally at a disadvantage when cyberspace conflict is included in warfare. While it is true that U.S. forces are heavily dependent on cyberspace, potential foes are every bit as dependent on their cyberspace-enabled systems, which in some cases are more modern and sophisticated than those used by U.S. forces. It is important to look at potential near-peer foes of the United States as they actually are, not how they were 30 years ago. Accordingly, it is key to understand that both sides will be dealing with a contested cyberspace domain full of deliberate misinformation and sabotaged systems. In this environment, victory will most likely go to the side best able to function effectively with high levels of fog and friction. In this type of setting, the United States and other nations with strong cultures of openness, innovation, and adaptability have some key advantages that will be hard to replicate in less free societies. A key element of any cyber-contested environment is the level of fog and friction experienced by the combatants.

Despite the hopes that some analysts once placed on improved information in warfare, fog and friction will greatly increase in a contested cyberspace environment. The concept of fog and friction refers to the uncertainty and cumulative small mishaps that make outcomes in warfare difficult to predict.[3] Theorists from the time of Sun Tzu have explored ways to decrease fog and friction through improved intelligence or better command and control.[4] Some theorists around the turn of the millennium thought that ubiquitous semi-autonomous and smart command and control systems would largely dissipate fog and friction.[5] That prediction turned out to be incorrect due to unexpected advances on the offensive side of cyberspace and the other domains, which made it far easier to penetrate operational battle networks. When some sensors and command and control systems give false information, fog and friction greatly increase as commanders stop trusting the information they receive and are hesitant to act on it.[6] This is deeply uncomfortable for command staffs who work hard to reduce fog and friction, so they can carefully orchestrate a plan that leads to a clear victory. However, the vision of a frictionless cybernetic war machine that flawlessly executes some grand design was illusory long before attackers in cyberspace could easily insert false information and take down command and control systems at will.[7] To make matters more complex, command and control systems are not the only cyber-enabled systems that will come under attack in a cyber-contested environment.

Warfighting in and through Cyberspace

Cyberspace attacks will affect warfighting in different ways depending on the type of system under attack. The different types of systems can be broken down into information technology (IT), operational technology (OT), and platforms.[8] Traditional IT systems include the Department of Defense (DOD) Non-Secure Internet Protocol Router and Secure Internet Protocol Router networks as well as IT-based weapons systems such as the Air Operations Center and numerous other personnel and logistics systems. Operational technology refers to computer-controlled physical processes such as industrial control systems or other types of control systems such as building automation or heating, venting, and air conditioning.[9] This category is a relatively new one in military circles but has achieved wide acceptance in the civilian world. The final category is platforms, which are self-contained cyber-physical systems. An F-18 fighter or Abrams tank falls into this category. If we open the panels and look inside an F-18, we will find a large number of boxes full of electronic components connected by wires. While these boxes are mostly running specialized software and are generally not using the Transmission Control Protocol/Internet Protocol, they still comprise a network and are part of the cyberspace domain.[10] Thus, these cyber-physical systems are hybrids with physical and cyberspace components that combine to make a coherent whole. Using these three categories, what will warfare that includes modern cyberspace forces look like?

IT systems are the most obvious and familiar targets of cyber attack in a conflict. Combatants should expect creative enemies to penetrate their IT systems and introduce some amount of false information. Adding even small amounts of false information can be extremely effective, as it makes adversaries question all their information.[11] What would it look like for a warfighter if 10 percent of the orders received through command and control systems were false and the enemy altered 5 percent of intelligence reports? Major effects on the ability of units to maneuver and function will occur at even low percentages, as a handful of false messages will call into question the validity of all other messages as well.[12] A young, aggressive infantry lieutenant may think the unit can "fix bayonets" and take the hill anyway, but where did the bayonets come from? Most logistical systems will be easy targets compared to command and control or intelligence systems, as they generally rely on the Internet backbone and unsecure communication links. It is worth mentioning again how completely dependent the U.S. military has become on complex cyber-enabled logistical systems to enable warfighting in all the physical domains. While we understand our reliance on IT, we do not yet clearly grasp our reliance on OT.

Adversary attacks can be devastating because operational technology is highly vulnerable, yet it provides the infrastructure that modern militaries

operate on. While once considered largely untouchable, OT systems have already come under attack numerous times. The heart of Stuxnet was an attack on programmable logic controllers, which are a subset of OT.[13] The Ukrainian power grid has also come under attack several times, which shows that attackers can use OT to put pressure directly on the civilian population, much like the early days of strategic bombing.[14] OT can be the "soft underbelly" of military operations. For example, an enemy that wanted to attack a command center could use a sophisticated social engineering attack with multiple vectors intended to jump across air gaps—or it could connect to the relatively unprotected building automation system and turn up the heat in the data center and cause computer hardware to fail. Much of OT is largely unprotected, since engineers connected it for convenience and efficiency with little thought of security or mission impact. There is increasing recognition of the importance of protecting OT, but securing it will be difficult—partially because key elements of OT are often outside military control. Major OT systems on which the military relies, such as civilian power grids, are normally defended (or not) based on business decisions instead of national security concerns. Attacks on OT can cripple a combatant by removing critical support infrastructure or by directly targeting weapons systems.

An adversary can directly attack platforms through cyberspace to hamstring military forces.[15] Platforms and weapons systems now exist in the physical and cyber worlds simultaneously and are thus significantly vulnerable to cyber attack. Some military planners have been slow to recognize the danger, since they think weapons systems such as airplanes and ships are isolated and secure from cyberspace threats because they are air gapped, or physically disconnected, from the Internet.[16] Engineers also often refer to these types of systems as *standalone*. However, warfighters routinely connect these systems to maintenance devices that are conduits to the wider cyberspace world, and they are thus vulnerable to attacks through those systems. In addition, any antenna with a processor behind it is a potential entry point for an adversary. Automobile hacking has shown both these avenues of attack to be feasible and practical.[17]

Responding to Cyber Attacks

All three types of systems—IT, OT, and platforms—will be under continuous attack from cyberspace in a contested cyberspace environment, but defenders have several ways to prepare for and fight successfully in this arena. One option is to focus exclusively on keeping the enemy out of important systems; joint forces will want to exclude enemies from their systems and networks as much as possible. However, recent history shows that using IT-based defenses alone is ineffective when under attack from less-capable adversaries than nation-states, so it is unlikely that this approach would work against more capable adversaries. The best solution to the problem of warfighting in a contested cyberspace environment is not a frontal assault on misinformation and uncertainty. The answer instead lies in an indirect approach that attacks the problem from a different angle and builds a force that can thrive and maneuver in a chaotic and uncertain environment.[18]

Authors who depict warfare in a contested cyberspace environment often seem to forget that the United States also has highly capable cyberspace forces that will presumably be attacking enemy IT, OT, and platform systems in accordance with appropriate authorities and the laws of war. The enemy will be dealing with all the same issues of compromised command and control, intelligence, infrastructure, and weapons systems. So if both high commands will be essentially blind, deaf, and dumb, will it come down to simple mass and who can throw the biggest battalions into the fray? On the contrary, victory will go to the side best able to observe, orient, decide, and act at the tactical edge in the absence of detailed instructions or a complete picture of the situation.[19] Building a joint force able to accomplish that will require significant changes in education, training, exercises, organizational structures, and planning.

Education

Education is a critical component of a force able to execute on the tactical edge because it provides a foundation of how to think and respond to any number of situations, whether the warfighter has encountered them before. Carl von Clausewitz himself was a major proponent of education and theory for young officers, not because education provided answers to tactical problems but because it helped to guide and stimulate development.[20] There is no need for more time spent on education in the career path of a U.S. military officer—the current sequence of professional schools is sufficient.

What our force needs instead is a greater emphasis on developing the types of agile and self-synchronizing individuals who can thrive at the tactical edge when an enemy successfully attacks our command and control systems. We need to adjust our curriculum to place greater emphasis on creative maneuver and find innovative ways to achieve commander's intent in a contested cyberspace environment where much of the equipment is not functioning correctly, many communications systems are unavailable, and the enemy has compromised some of the command and control links that appear to be functioning.

Training

In addition to knowing how to think, which comes from education, agile forces must learn specific skills to cope with a cyber-contested environment through improved training. To be effective, training must be realistic and focused on those skills needed in an environment where many systems will be under attack. For example, modern fighter aircraft are capable of updating their navigation systems using a number of methods, only some of which rely on the global positioning system (GPS), but operators rarely practice these capabilities because GPS is so much more accurate and easier to use. In a cyber-contested environment, a pilot's

Servicemember from 3rd Infantry Division (left), trainer, and Servicemember of division's 2nd Battalion, 69th Armor Regiment, 3rd Armored Brigade Combat Team, observe spectrum of frequencies used in Red Team exercise (U.S. Army/Aaron Knowles)

theoretical ability to update an aircraft's position using ground references is of little use if the pilot is not trained or proficient, and that proficiency will only come from focused training and repeated practice.

It is important to note that there are only a finite number of minutes in any given day to accomplish training, and every training event has an opportunity cost of a training event that the individual or team did not accomplish instead. Training for fighting in a cyber-contested environment means that forces will train less with everything working, and more with backup and degraded systems. This type of training regime will greatly increase the joint force's ability to fight in a cyber-contested environment, but it comes at the cost of proficiency and capability when the enemy does not contest the environment and all systems are working as intended. Commanders must strike the right balance based on expected mission sets and adversaries, but there is some minimum level of competency in both environments that all forces should reach. Today, few forces deliberately train for a cyber-contested environment at all, so more training will be needed for this type of warfare. Training is an important building block that provides needed skills, but that training will only truly take root when the force also exercises it on a large scale.

Exercises

Agile forces ready to execute on the tactical edge need to put all the education and training together in large-scale exercises so they are familiar with operating and self-synchronizing in chaotic environments. Smaller exercises are useful in a building block program, but, much like Red Flag, maximum learning will come from large-scale, complex exercises.[21] The rules of exercises should clearly reward innovation and agility, and referees should grade forces against not how closely they adhered to the plan, but how effective they were at executing the commander's intent when everything went wrong. It is critical that these exercises be difficult and full of surprises, much like the enemy. If friendly forces end up winning every exercise, the scenario is too easy. In exercises, adversary forces should routinely defeat friendly forces, which will force a higher level of learning than is generally accomplished when the exercise invariably has the joint force winning on the last day, no matter how badly friendly forces bungled things. Commanders should replace individuals who handle their forces poorly and who are not able to operate effectively in a contested environment before lives are lost in

F/A-18C Hornet, assigned to Sharpshooters of Marine Fighter Attack Training Squadron, flies over flight deck of aircraft carrier USS *George H.W. Bush* in Atlantic Ocean, January 24, 2013 (U.S. Navy/Kevin J. Steinberg)

combat. Once agile forces are developed, DOD must support them with appropriate organizational structures.

Organizational Support

DOD needs to couple an agile and resilient force with a strong organizational structure and incentives for maximum effectiveness. Personnel systems must reward agile and resilient behavior in promotions and increased responsibility if other young leaders are going to focus their own efforts in that direction. Too often, military personnel systems reward a particular behavior such as agility of thought, but what they actually reward is precisely following a set of rules and norms that are comfortable for the organization. Senior leaders will have to go beyond talking about the importance of agility or taking risk and failing, and start promoting those people who do so instead of those who follow the safer path.

As leaders are cultivated to be agile and innovative, DOD needs to provide them with an environment that enables success. The joint force will accomplish a large part of this requirement by setting the conditions through changing from directive to emergent planning, which is a different type of planning than the military typically does.[22] Today's planning focuses on detailed scenario-driven plans that lay out precise schedules and timelines not that different from the Schlieffen Plan of World War I. Commander's intent is part of the process, but it is only one step in a long series that produces documents running many thousands of pages no one reads, except a few experts reading about their small sliver of an operation. In a contested cyberspace environment, the detailed plans will be worse than useless and will do great harm if commanders attempt to follow them in a radically changed context from the planning assumptions. Planning is helpful even if the actual plans are not, as it forces staffs and maneuver forces to think through problems to grasp the commander's intent and general scheme of maneuver. These elements provide the key to success.

The joint force has made great strides in recent years to embrace mission-type orders, and DOD is now discussing the need to acknowledge and plan for commanders who are still in command but cannot directly control their forces due to a contested cyberspace environment.[23] This distributed command provides field commanders with the overall commander's intent to keep them focused in the right direction, and the structure that allows them to self-synchronize into the largest and most effective warfighting elements possible in given circumstances. Meanwhile, the theater-level commander, who has had direct control over units in the conflicts of the last few decades, will at best be able to provide broad guidance

updates while pushing resources and reinforcements to particular geographic areas and continuing to fight for as effective a command and control as can be achieved.[24]

Conclusion

These strategies will help set the conditions for victory on a modern cyber-contested battlefield. Fortunately for the United States, we have the raw material available to us to execute at the tactical edge. Our population is flush with potential young warfighters who want to be innovative and agile and are comfortable with a pace of change and maneuver that was quite challenging for earlier generations brought up in more controlled hierarchical structures. Many potential adversaries do not have the same raw material because their societies are still far more command driven and less agile than ours. This will provide an important edge that our potential adversaries cannot easily replicate.

The commander who, like Admiral Nelson, educates, trains, equips, and exercises his forces to execute on the tactical edge and provides clear commander's intent while eschewing direct control is much more likely to find victory than the one who insists on attempting to control forces directly in a carefully synchronized plan. Detailed control will be impossible in a cyber-contested environment facing a competent foe anyway, and attempting to achieve it will do great harm because forces will be unable to maneuver or self-synchronize in the absence of direction from headquarters. The U.S. military has access to a new generation of joint warriors who, through a combination of education, training, organizational changes, emergent planning, and new command structures, can defeat the Nation's enemies and achieve national objectives even when our operational battle networks are under attack and degraded. We must now prepare the force and teach our commanders to command in new ways, let go of control, and surf the chaos. **JFQ**

Notes

[1] The details on Trafalgar in this paragraph are found in John Keegan, *The Price of Admiralty: The Evolution of Naval Warfare* (New York: Penguin Books, 1988).

[2] For a modern fictional version of what a conflict might look like with cyberspace attacks, see P.W. Singer and August Cole, *Ghost Fleet: A Novel of the Next World War* (New York: First Mariner Books, 2016). While I do not take issue with any of the types of attacks they discuss, I do find the idea that an enemy could achieve that level of surprise when tens of thousands of people knew about the attack ahead of time rather incredible. Instead, I posit that cyber attacks would be flying in both directions and both sides would be dealing with them at the same time.

[3] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976).

[4] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1971).

[5] John Arquilla, "The Strategic Implications of Information Dominance," *Strategic Review* 22, no. 3 (1994), 25.

[6] A good example of this can be seen in the results of "Eligible Receiver" in Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016).

[7] Antoine Bousquet, *The Scientific Way of Warfare* (New York: Columbia University Press, 2009), 222.

[8] William Young at Air University developed this typology as part of his work on determining key cyberspace terrain.

[9] "Operational Technology (OT)," Gartner IT Glossary, available at <www.gartner.com/it-glossary/operational-technology-ot>.

[10] Many of the same principles and models such as the Open Systems Interconnection (OSI) seven-layer model still apply, but the protocols and standards are different. For a discussion of the OSI model, see Shon Harris, *All in One CISSP Exam Guide*, 6th ed. (New York: McGraw Hill, 2013), 517–520.

[11] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 50.

[12] Kaplan.

[13] For an in-depth analysis of Stuxnet, see Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York: Broadway Books, 2015).

[14] Robert M. Lee, Michael J. Assante, and Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* (Washington, DC: SANS Industrial Control Systems, 2016), 20.

[15] For some fictional examples of what might be possible, see Singer and Cole.

[16] Stuxnet provides a real-world example of a cyber weapon crossing an air gap and illustrates the connected nature of "supposedly closed system[s]." See Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 63. Also see Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy* 8, no. 2 (2012), 323–324.

[17] Stephen Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security Conference, August 10–12, 2011, 3–5.

[18] B.H. Liddell Hart, *Strategy*, 2nd ed. (New York: Penguin Books, 1967), 5.

[19] There are many excellent discussions of John Boyd's Observe, Orient, Decide, Act (OODA) loop. For further information, see David S. Fadok, "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Phillip S. Meilinger (Maxwell Air Force Base, AL: Air University Press, 1997), 366.

[20] Clausewitz, 141.

[21] Earl H. Tilford, Jr., *Crosswinds: The Air Force's Setup in Vietnam* (College Station: Texas A&M University Press, 1993), 201.

[22] Simon Reay Atkinson and James Moffat, *The Agile Organization: From Informal Networks to Complex Effects and Agility* (Washington, DC: Department of Defense Command and Control Research Program [CCRP], 2005), 130.

[23] Gilmary Michael Hostage III and Larry R. Broadwell, Jr., "Resilient Command and Control: The Need for Distributed Control," *Joint Force Quarterly* 68 (1st Quarter 2014), 39.

[24] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command . . . Control . . . in the Information Age* (Washington, DC: DOD CCRP, 2003), 5.