International Law Studies - Volume 76
Computer Network Attack and International Law
Michael N. Schmitt & Brian T. O'Donnell (Editors)

I

CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers

Arthur K. Cebrowski

IT 21 and Network-Centric Warfare

As President of the Naval War College, I am charged with examining advances in technology and asking the question: "what are the implications for the Navy and its activities in the next century?" Admiral Jay Johnson, former Chief of Naval Operations, has described the future as being shaped by three growing—and irreversible—trends: networking, greater globalization and economic interdependence, and technology assimilation. Critical to our understanding is a recognition that these trends operate synergistically. Using the Internet, intranets, and extranets, networking has rapidly become a powerful force for global organization, one that fosters an interdependency unprecedented in human history. The phenomenon is the result of extraordinary leaps in technological possibilities. Within the next twenty years, for instance, constellations of satellites will blanket the earth providing television, telephone, Internet access, and business opportunities to all but the furthest reaches of the world.

Complicating the difficulties of coherent planning and systems development in this environment of continual flux is the fact that technology is being assimilated at

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.

an ever-increasing rate. It took nearly three generations for electric power to become an everyday part of people's lives. It took radio and television about a generation and a half. The Internet will achieve that status within a single generation.

Obviously, these trends have enormous implications for the armed forces. We are now in the midst of a revolution in military affairs unlike any seen since the Napoleonic Age. In that period, the practice of maintaining small professional armies to fight wars was replaced by the mobilization of citizen armies composed of much of a nation's adult population. Henceforth, societies as a whole would, perhaps tragically, become intricately vested in warfare. The character of armed conflict had changed fundamentally.

Today we are witnessing an analogous change in the character of war and warfare—an information revolution that enables a shift from what we call platform-centric warfare to Network-Centric Warfare. Understanding of these new operations remains nascent; no great body of collated wisdom has emerged to explain how this revolution will alter national and international security dynamics. That is one of the challenges with which I charge readers, to identify and explore the operational and legal issues associated with the new way in which wars of the next millennium will be waged.

Perhaps most notably, Network-Centric Warfare enables a shift from attrition based warfare to a much faster and effects-based war fighting style, one characterized not only by operating inside an opponent's decision loop by speed of command, but by an ability to change the warfare context or ecosystem. At least in theory, the result may well be decisional paralysis.

How might this be achieved? The approach is premised on achieving three objectives:

(1) The force achieves information superiority in terms of accuracy, relevance, and timeliness, thereby having a dramatically better awareness or understanding of the battlespace.

(2) Forces acting with speed, precision, and the ability to reach out long distances with their weapons achieve the massing of effects versus the massing of the forces themselves.

(3) The results that follow are the rapid reduction of the enemy's options and the shock of rapid and closely coupled effects on his forces. This disrupts the enemy's strategy and, it is hoped, forecloses the options available to him.

Underlying this ability is an alteration in the dynamics of command and control. Traditionally, military commanders engaged in top-down direction to achieve the required level of forces and weapons at the point of contact with the enemy. However, top-down coordination inevitably results in delays and errors in force disposition. It is an unwieldy process that denies flexibility to subordinate commands. Combat power is needlessly reduced and opportunities present themselves to one's enemy. In contrast, bottom-up execution permits combat to move to a high-speed continuum in which the enemy is denied operational pause to regroup and redeploy.

The key to this possibility is the ability to provide information access to those force levels that most need it. In a sense, the middle-man is cut out. Allow me to offer one illustration.

Three years ago, the Navy launched an effort called Information Technology for the 21st Century, or "IT-21." It reflected the Navy's understanding that 21st Century combat power must come from warriors and platforms operating in a networked environment. What is required is linkage between systems that accurately provide the necessary levels of understanding of the battlespace (the sensors) and systems that link the ships and aircraft (the shooters). Therefore, overlying these two systems, or grids as they are referred to, must be high-performance information links—a complex and responsive information grid that empowers real-time C4ISR processes (command, control, communications, computers, intelligence, surveillance, and reconnaissance). Although the full integration of the three grids—sensor, engagement, and information—remains incomplete, and new technologies must be developed to optimize Network-Centric Warfare, this vision is clearly the future of United States war fighting.

Challenges

One indispensable need in building our Network-Centric Warfare capability is adequately defending the information grids that support our capabilities. We know all too well that our enemies recognize the vulnerabilities posed by our network dependent systems. Because information and the network will be valued, it will become a target. Therefore, a core strategic goal must be to design, build, and operate secure IT systems resistant to computer network exploitation (CNE) and computer network attack (CNA). Disruption or corruption of these systems could have devastating strategic effects. Think, for example, where we would be today if the Yugoslav intelligence agencies had through CNA caused Allied Forces to "inadvertently" bomb the Russian Embassy in Belgrade . . . or a hospital . . . or a school. Information assurance is the *sine qua non* of effective, reliable Network-Centric Warfare. Assurance need not be absolute . . . nothing is in war. But some aspects require higher levels of assurance.

A troubling reality we must deal with is that most military systems obtain and process information from civilian systems over which the Department of Defense has a lesser—or no—degree of control. These civilian systems are likely to be much more vulnerable to CNE and CNA than military systems because of public access, and may have fewer resources dedicated to their security. Along the same lines, our military infrastructure is dependent upon the domestic civilian infrastructure. Military supply, logistics, and routine communications systems rely extensively on the public telecommunications grid, the domestic electric grid, and domestic transportation systems. Each is itself dependent on potentially vulnerable computer networks.

The threats cannot be overestimated because the value cannot be overestimated. Some are new; others are merely new forms of existing threats. CNA is certain to be used in conjunction with traditional warfare by those who are otherwise unable to match the United States' military wherewithal. In particular, it is guaranteed to appeal to terrorists and rogue States. Further, we may expect to see computer network exploitation as a new form of an age-old threat—espionage.

In facing such threats, the United States and its allies should strive for, but should never presume, technological dominance. When people say CNE and CNA technologies are warfare on the cheap, I think of the National Security Agency budget. But formidable capabilities can be developed and obtained relatively inexpensively. The critical capital in this industry is brainpower and computing power. With only a fraction of the world's population, and given the widespread nature of computing power, it may become difficult for us to maintain our present advantage. Though defensive mechanisms will constantly improve, so too will the offensive abilities of potential adversaries. The environment will be hostile and dynamic. It may be impossible to determine who has the advantage at any time. In the conventional world of land forces, ships, planes, and submarines, US intelligence agencies have a fair ability to determine the enemy's order of battle; that luxury disappears in the world of cyberspace.

The face of war is truly changing. In particular, we in the United States face a different reality in the effort to shape international law than faced in the past. In the post-Cold War era, attacks on the territory of the United States by conventional forces have not been a great concern. On the North American continent, separated from potential adversaries by the Atlantic and Pacific oceans, we were relatively protected. With CNE and CNA, those large expanses of ocean only serve to provide a false sense of security. Today, the homeland threat is from any country, terrorist organization, or hacker behind a computer anywhere in the world.

During future crises, the United States must expect significant CNE and CNA activity against both our military *and civilian* infrastructures. Though our forward-deployed battle systems should be impenetrable, the support systems reaching back to and in the United States will be far less secure. This new reality, of the United States homeland as a viable target, will inevitably influence our approach to international law. The Department ofDefense's interest in the shaping of international law in the recent past has arguably been driven by the desire to further our offensive interest—our interests as a shooter rather than as a target. Today, with the homeland at risk, a new balance between our offensive and defensive interests must be achieved.

Many questions are presented by this new paradigm. Particular attention must be paid to the following:

- Does international law require us to wait until lives are lost or property destroyed before we may engage in acts of self-defense?
- What is the new context of rules of engagement? Proportional response? Precision? Perfidious act?
- How is targeting affected by the fact that military systems are networked to civilian IT systems controlling communications, energy, finance, and transportation?
- Are legal consequences of international law triggered upon the perpetrator gaining *access* to our IT systems, or do they depend upon the *effects* or tangible consequences of access?
- Are there differing perspectives on the desired direction in which the law should develop among US Government agencies and among different nations?

Framework of the Law

The Hague and Geneva Conventions, and other sources of international law, both *ad bellum* and *in bello*, provide guidance for future conflicts. Consider the critical principles that regulate the conduct of nations during armed conflict:

(1) Only military objectives may be attacked.

(2) It is prohibited to launch attacks against civilians.

(3) The loss of civilian life and damage to civilian objects must not be excessive in relation to the military advantage anticipated.

No reasonable person would disagree with these norms; but their application in cyberspace attacks will place stress on commanders, targeteers, and their lawyers. There will be considerable difficulty in identifying sources and locations of threats in cyberspace. Dual-use technology will render the ability to distinguish between a military and civilian target elusive. And determining second and third order effects from information attacks will be a complex task indeed.

Despite the difficulties in application, I am persuaded that we will be well served by applying the core principles of international law to information age warfare. We cannot, in our zest for tactical mission success, lose sight of our goals as a nation—to protect life and liberty, in our country and throughout the world. Adherence can be difficult, but our commitment to protecting the innocent, the noncombatant, reflects our national values. One commentator stated it with precision: "Adherence to the law reflects who we are as a nation, and separates the good guys from the bad guys." Therefore, the warfighters, IT professionals, and lawyers must all ask what steps need to be taken so the cyberwarriors of tomorrow can remain the good guys.

Finally, I would caution that we should not rush to place undue controls on information operations before we understand the implications of such control. The law of armed conflict developed over centuries as nations determined what restrictions on their war fighting capability they were willing to accept. Time and experience are the brick and mortar of international law. As our understanding of the technology increases, so too will the ability of nations to best determine the desired international norms. We must be cautious not to advocate new law regarding information warfare without understanding its moral, legal, and practical implications.