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

XIX

International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement

Brian T. O'Donnell and James C. Kraska

This chapter offers a framework for military commanders and policy makers to begin constructing rules of engagement (ROE) for computer network attack (CNA) during armed conflict, military operations other than war, and other overt and covert national security activities. Focused on the operational commander rather than the academic, it introduces the legal and policy considerations surrounding the drafting of ROE for CNA, and discusses the unique legal issues that arise from CNA within the law of armed conflict. Such considerations are important for military commanders, their operators, planners, and lawyers in designing and employing CNA because they serve to facilitate and provide guidance that operationalizes the concept of computer network attack—removing it from the realm of speculation and placing it as a tool in the hands of military commanders. Moreover, since legal and ROE decisions impact the development of tactics and doctrine, and the acquisition and force structure processes, the discussion is relevant to force providers and trainers, as well as fleet commanders.

Emerging Technologies and War

Over the last decade, information technologies, including computer and communications systems, have brought about a sea change in the global economy. Technology has grown from just 6% of the US economy at the beginning of the 1990s, to over 20% today.[1] What was once a narrow "technology" sector within the whole economy has emerged as the "New Economy," comprised of that third or fourth of the economy that serves as the source of rapid innovation and engine of economic growth.[2] Entire subsectors of the New Economy have emerged, and whole new industries have grown virtually overnight: photonics, micro-electrical mechanical (MEMs) devices, wireless systems and specialty communications semiconductors, and, of course, the Internet, which has become omnipresent throughout the economy. The New Economy has transformed industry data management and storage, manufacturing, accounting, and inventory management. Many of the same technologies have even more dramatically recast military communications, command and control, targeting, logistics and weapons.[3] These technological changes are transforming thinking about military force structure and doctrine, and have opened up computer network attack as a viable instrument of military power.

Military technology displayed by coalition forces during the Gulf War in 1991, particularly those technologies that were used by the United States military, ignited broad interest among strategists and policymakers worldwide in how to best develop or channel the emerging "revolution in military affairs" (RMA).[4] RMA, which encompasses technologies that "gather, process and fuse information on a large geographical area in real time, all the time,"[5] has driven the creation of new military capabilities and doctrine based on advanced concepts and emerging technologies. It grew from Cold War planning in the West that sought to apply technology as a force multiplier to counter numerically superior Soviet forces in Europe.[6] After the Cold War, RMA began to be seen as a way to ensure Western superiority, or at least preserve military advantage, in a broad variety of post-Cold War conflicts that might be encountered within the context of a resource-constrained defense budget environment. Computer network attack is one of the latest and most advanced manifestations of RMA. With the growth of computer networks and integrated systems, computers have assumed a central role in enabling both offensive and defensive military operations. Despite widespread recognition that the technologies that enable computer network attack are already a reality, the specific legal and policy considerations that will control their employment have received scant attention. This is not surprising, since the

development of concrete legal analysis tends to lag the advancement in technology, particularly in the application of international law to new methods of warfare.[7] It is equally important to recall that history is replete with examples in which superior military technology was squandered, and advantage was surrendered, because the army employing the new weapon had an inattentive or feckless approach to developing corresponding doctrine and tactics for its employment.[8] In the modern era, the development of appropriate ROE for CNA, along with operational doctrine, tactics, and force structure, will determine whether CNA is an effective weapon.

In the mid-1990s, the initial US focus on computers and military conflict resided almost exclusively in defending perceived weaknesses and vulnerabilities in critical national information infrastructure—especially electronic banking, communications, and industrial energy grids. This focus, which emerged within the Department of Defense (DoD) as "Information Warfare—Defense" (IWD) was replicated by other governmental agencies, who also became concerned after 1995 about the vulnerability of their networks, coinciding with the widespread use of the Internet.[9] All of these efforts migrated under the umbrella term, "Computer Network Defense" (CND), which has served to concentrate interagency resources and attention toward protecting and defending critical computer and information networks from sabotage by individual hackers, terrorist groups, and unfriendly governments.[10] Planning for CND was accelerated with the advent of Presidential Decision Directive 63 (PDD-63) in May 1998, which ordered federal agencies, in concert with the private sector and state and local authorities, to create defenses against attacks on critical infrastructures from network assaults from all State and non-State actors that potentially threaten American "national and economic security."[11] The DoD responded by standing up the Joint Task Force Computer Network Defense (JTF-CND), which was renamed Joint Task Force Computer Network Operations (JTF-CNO).[12] The JTF is assigned to Commander-in-Chief, United States Space Command, but has representatives from each military service and many government agencies.[13] The CND movement has made great progress in identifying information infrastructure vulnerabilities, and organizing and resourcing defensive interagency plans to address them. Initial panic at perceived gaping holes in critical information infrastructure has recently given way to a more measured and sober, and more confident, vulnerability assessment. Now that the concern over CND has stabilized, US planners, particularly in the military, have begun to more seriously consider the potential advantages to be gained in military operations by offensive attack against an adversary's information infrastructure.

Computer Network Attack

Computer network attack has emerged as one of the more promising tools available to a military commander for mission accomplishment and self-defense. It encompasses activities designed to ". . . disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[14] While the legality of information warfare generally, or CNA in particular, is very fact-dependent and open to considerable debate, it has received at least some attention among international law scholars. Some scholars maintain that a CNA constitutes a use of force, whereas other scholars maintain that CNA is much more akin to adverse nonforceable influence.[15] This debate is healthy and serves to shape the international law in the area.

Despite the importance of CNA, military and civilian commanders have been unable to adequately explain it, or to achieve a consensus in designing CNA ROE. Moreover, military staff judge advocates, civilian lawyers within the national security and intelligence establishment, and academics are grappling with how to best articulate the legal and policy underpinnings for computer network attack decisions.

While theories and approaches that emerge from academia are useful to national decision-makers contending with these issues, they may be of limited value to operational commanders, including those at the Navy fleet and battle group levels. For the operational commanders, the legal and policy research surrounding CNA often raises more questions than it answers. This results in leaving those commanders who might integrate CNA into real-world operations confused and frustrated. Rather than offering a theoretical legal model for CNA, this chapter accepts the premise that CNA is quickly becoming a reality. There is a broad range of capabilities to attack computer networks that are in various stages of development, testing, and training, both in the United States and abroad. There is evidence that they are already being employed in actual operations by a growing number of nations. Furthermore, as these capabilities become better understood and easier to use, it is likely that the approval authority to employ them will gravitate downward in the chain of command to task force commanders. Eventually, proven methods of CNA could be authorized to individual units and platforms. This chapter presents a question of first impression by examining the development of operational CNA ROE for military operations, and it offers a practical approach to drafting CNA ROE. This pressing issue of exactly how a commander begins to approach the legal aspects of developing and applying CNA in the real world is on the cusp of wide discussions. There is a tremendous legal and policy gap—between rapidly advancing CNA

technical capabilities emerging from the laboratories—and the legal architecture to support them. The advancement of ROE for computer network attack, which has not kept pace with these developments, should begin to fill this gap. Determining the ROE process, considerations for creating the parameters of CNA engagement, and some guidelines for inclusion in operational orders are especially important for operational commanders executing real world missions. The commander should be able to understand which computer network and related military instruments may be used, under what conditions they may be employed, and to which missions they may be applied. This prevents a commander from either employing means or methods that lie beyond the scope of his or her authority, and ensures that the he or she does not unnecessarily limit the application of CNA because of confusion over the rules governing its use. There is a need to discipline and govern the process of development of ROE for CNA. The National Command Authorities (NCA) have a central stake in overseeing the process to ensure that the emerging CNA rules of engagement comply with international law and domestic legislation, as well as remain in concert with national military policy and national diplomatic and political goals.

For this chapter, we assume that some level of CNA is lawful within the context of international law, but the more practical question—indeed for commanders, the greater question—is how best to develop rules of engagement for an actual operation. The objective is to begin to fill in the vacuum pertaining to the control, application, and employment of CNA at the warfighting level.[16] Does the existing process for developing ROE adequately accommodate CNA? What can guide commanders, their warfighters, and operational judge advocates in developing rules for computer network attack? Is this an area best left to policymakers inside the beltway or is there a role for crafting rules for CNA at the operational level—forward deployed, at sea, or in the field? This chapter considers the historical basis for ROE, identifies the factors that fold into ROE development for computer network attack, explores the considerations that might limit or empower a commander, and suggests an architecture for designing computer network attack ROE that may be employed throughout the conflict spectrum. By providing a "navigational chart" to many of these issues, the goal is to begin to demystify the process for commanders and decisionmakers alike.

Historical ROE Development[17]

Modern ROE have their roots in the naval and maritime tradition. With the advent of oar and sail, effective central control of a military asset by the

sending government was lost once a ship got underway from port. It was incumbent upon the commanding officer to conduct the mission pursuant to the general guidance of the government. Virtually alone until the ship reached the next friendly port, or until the ship encountered another friendly vessel that could deliver news or orders, the commanding officer operated within broad parameters or rules issued by the leadership. The Continental Navy's first exposure to rules governing operations occurred on January 5, 1776, when Commodore Esek Hopkins received written orders to engage British raiders that included a broad discretionary clause of authority:

> Notwithstanding these particular Orders, which 'tis hoped you will be able to execute, if bad Winds or Stormy Weather, or any other unforeseen accident or disaster disable you so to do You are then to follow such Courses as your best Judgment shall Suggest to you as most useful to the American Cause and to distress the Enemy by all means in your power.[18]

Although modern technology has tremendously improved communication to underway vessels, naval vessels now routinely travel far from port, and transit much faster—sometimes even underwater—without access to detailed and real time guidance from a fleet commander or government leader. Prior to World War II, there was little need for a policy on use of force aside from occasional ships on diplomatic missions.[19] Following World War II regulations governing the use of force, now known as rules of engagement, were promulgated in the 1948 United States Navy Regulations with Article 0614, "Use of Force Against a Friendly State."[20] In 1962 the first in a series of ROE were issued that applied Navy-wide. Written to address the unique challenges and special concerns arising from surface, undersea, and aviation operations throughout the maritime environment, these ROE were subsequently updated in 1970 and 1981.[21] Even in the updated version, however, they still only applied to US naval forces.

In 1986, the United States issued generalized JCS Peacetime ROE that, for the first time, included guidance for air and land forces.[22] Two years later, following the experiences of the USS STARK (FFG-31) and USS VINCENNES (CG-49) in May 1987 and July 1988 respectively, the Peacetime ROE were again updated and revised. In 1994, a major revision was accomplished, and the ROE that applied to all US forces were promulgated by the Chairman of the Joint Chiefs of Staff as the Standing Rules of Engagement for US Forces (SROE)[23] Aside from the obvious title change that removed the "peacetime" reference, the 1994 document not only streamlined the ROE drafting and approval process, but also contained significant revisions, including a more

uniform approach. Separate ROE issued by the combatant Commanders-in-Chief (CINCs)[24] augment the SROE, and are referenced as "theater-specific" ROE.[25] This marked a break from past practice, in which each CINC had a theater-wide top-to-bottom set of rules. Also, the 1994 SROE clarified a commander's inherent right and obligation of self-defense, and articulated a bright-line distinction between self-defense and the use of force for mission accomplishment. For self-defense, the SROE are firmly grounded in responding to a hostile act or responding to a demonstration of hostile intent. One of the more significant changes was the declassification of the basic self-defense SROE provisions. This enhanced training and application throughout US forces and enabled better coordination between allies and coalition partners.

The most recent iteration of the SROE was released on January 15, 2000.[26] This latest version further refines and clarifies the concepts contained in earlier editions. It is comprised mainly of thirteen enclosures, including a separate enclosure for Information Operations. Unlike the 2000 revision, the 1994 edition contained little substantive mention of CNA, sticking mostly to definitional terms and basic concept statements. Under the SROE, use of CNA may be authorized to a commander under the umbrella of the mission ROE provisions and the international law of armed conflict (LOAC), subject to any additional supplemental authorizations or restrictions received from higher authority.[27]

Even though commanders of forces tasked to accomplish an operation or mission might be authorized CNA as a means of warfare, that does not mean they will decide to use it. Historically, personnel in the fleet or field did not question the ROE they were provided. Often, ROE were not well-understood within theater, or at the tactical level. Moreover, there was a sense that the ROE dictated from above could not be changed and were to be applied without question.[28] This was demonstrated during the 1981 Gulf of Sidra freedom of navigation operation off the coast of Libya. Prior to the operation, orders issued to the Navy F-14s restrained those forces from responding to indications of hostile intent even though the ROE in effect at the time authorized self-defense in response to hostile intent.[29] Another instance occurred during the bombing of the Marine Battalion Landing Team (BLT) Headquarters building in Beirut, Lebanon, in 1983, when a local commander's interpretation of the ROE led to orders for "sentries to keep their magazines in their ammunition pouches as a precaution against an accidental or over-eager discharge of a weapon that might kill or wound one of the thousands of Lebanese civilians who visited the airport daily."[30]

Innovation, Military Doctrine, and ROE

Limitations on the use of CNA may also fall victim to unnecessary restraint due to several factors. First, the complex and typically highly classified nature of CNA tools may not inspire confidence in commanders. They may be hesitant to rely upon bare promises that certain CNA tools can accomplish a mission, such as taking down an air defense site, when proven alternatives, such as air strikes or cruise missiles, are available. Commanders likely will have had training and experience with kinetic methods, but may not understand or appreciate CNA. During the 2000 Global War Game at the Naval War College, this dynamic was repeated by commanders who tended to move away from more speculative instruments toward those which were more familiar. This tendency toward traditional and proven methods of warfare has been demonstrated in war games of other services as well. Nevertheless, the war games also showed that US commanders were becoming more willing to adopt innovative methods to accomplish the mission, even when the methods lack historical record.

The military services are beginning to realize that to gain acceptance as a viable weapon system, the secretive nature of the tools must be reduced to a more accessible classified level so that commanders and their staffs and subordinate commands can familiarize themselves with the systems. Consider the development of the machine gun more than one hundred years ago. An American, Richard J. Gatling, patented and demonstrated a reliable, multi-barreled repeating gun in 1862, but the Belgian-invented and French-developed mitrailleuse was the first combat-tested machine gun.[31] On the eve of the Franco-Prussian war, the 11 mm mitrailleuse, recognized by the French army as a technical breakthrough in firepower, was kept in such tight secrecy in peacetime that very few French officers could discuss or develop doctrine or tactics for its use on the battlefield.[32] The weapon, which came as a complete surprise to the Germans, had the potential to swing victory to the French. Instead, advantage was lost because the French were caught up in marveling at the technical aspects of development without devising correspondingly effective doctrine and tactics for the weapon.[33] Similarly, although the Germans, British, and French were developing and fielding battle tanks during 1915-1916, they were ineffectively and wastefully employed on the battlefield. It was not until a coherent doctrine for their employment was developed—most notably by the innovative British strategist Major J.F.C. Fuller—that the tank was accepted as a viable weapon rather than a curiosity. On November 20, 1917, a spearhead of 476 British tanks penetrated German lines during the Battle of Cambrai, demonstrating that the armored vehicles could achieve rapid and complete command

of dug-in defenses.[34] Inertia prevents change, and we cannot assume that military commanders in the present day are immune from this phenomenon. Just as in the examples cited above, bringing ROE for computer network attack from the general and theoretical to the specific and concrete will help commanders migrate to computer warfare.

The method by which CNA will accomplish its end result likewise needs to be explained to commanders, and commanders need to be able to engage in professional debate on the subject. The ROE relate to the underpinning international and domestic authority for using CNA, the scope of the commander's authority within the context of the national and theater commander's mission, and the conditions, if any, in which CNA is considered a lawful attack. One especially important consideration is the potential for collateral effects of CNA in view of the law of armed conflict. How might CNA affect third countries or neutral forces beyond the scope of the conflict? What might be the effect on civil societies, civilian populations, businesses, and related public and private infrastructure? What impact might CNA have on protected persons or locations, such as sick and wounded personnel near the battle area or sites representing religious or cultural heritage? What about the effect on prisoners of war (POWs) and other protected classes of personnel, such as medical or religious personnel? Any anticipated or probable primary or secondary civilian injury or damage must be reviewed to determine whether it is excessive or disproportionate to the military advantage to be gained. Commanders are coming to view these issues personally and with growing interest since they bear the ultimate responsibility for the consequences of an attack. The trend toward creating universal multilateral "war crimes" jurisdiction only serves to exacerbate many commanders' uneasiness toward command and personal liability.

The first step is for a commander to be able to understand the foreseeable consequences of a CNA attack, including damage or disruption to non-military systems. A review of the potential consequences within the ROE and LOAC framework is essential to forming a decision on the use of CNA. In particular, commanders must estimate the expected military benefit of CNA, and weigh that calculation against the collateral costs of attack. Ideally, the commander should be supported by an ROE cell that can present a menu of options. The cell should include representatives from the operations, intelligence and plans directorate, as well as a judge advocate. The cell should analyze ROE, targeting and politico-military issues associated with CNA, and deliver recommendations to the commander.

Commanders are rightly hesitant to employ unproven systems as one critical component of a coordinated attack because if the CNA component fails, then

the entire effort is imperiled. Inherent risk is already attendant to real world missions without the injection of an unproven, and possibly speculative system. Doubt as to legality and ROE would only serve to magnify these concerns. Compounding this problem may be the short life span of the attack due to rapid advance in technology and creative enemy adaptation. Even more so than conventional weapons systems, once the impact of a particular CNA has been experienced, adversaries can be expected to devise a tailored defense, thereby limiting future effectiveness.[35] Moreover, the comparatively low cost and global availability of computer systems and trained programmers enables terrorist groups or developing nations to enter the realm of information and computer warfare. All of these factors serve to keep CNA tools underutilized, thereby foregoing potential military benefit. Doing so deprives a commander of the opportunity to observe its effectiveness in training or on lesser targets prior to applying it to a major target. A successful laboratory demonstration is not likely to do much to dissuade this opinion. As legal analysis continues to lag technological breakthrough, we can expect that without great attention, the development of mission-specific ROE for ever newer computer network attack systems will be a challenge.

Understanding this background, proponents of the new technology are beginning to realize that not only must they be able to adequately explain and demonstrate CNA, but they must also ensure that the commander understands how it functions. Computer network warfare and information operations are upsetting the existing Westphalian paradigm of warfare upon which traditional ROE and law of war are based. The very nature of CNA is rapidly changing. For instance, some suggest that the architecture of CNA is migrating from the traditional model of "waves" of attack to a model based on a simultaneous "swarming" or overtaking of an opponent's system. "Swarming occurs when the dispersed nodes of a network of small . . . forces converge on a target from multiple directions. The overall aim is sustainable pulsing of a force or fire."[36] Once in motion, swarm networks must be able to coalesce rapidly and stealthily on a target, dissever and redisperse, and then immediately recombine for a new pulse. In other words, information-age attacks may come in swarms rather than the more traditional waves.[37] Such a paradigm shift could completely transform the way many elements of ROE are applied in computer network attack. The concepts of "hostile act" and "hostile intent," for example, best fit a linear "wave" model, in which State action is directed toward another State in waves along a timeline—often becoming more permissive or aggressive as time lapses. Crisis war games bear this out; often, military exercises begin with a "Road to War" prelude of rising political tensions that gradually escalate into military confrontation. Then, conflict

slowly accelerates from peacekeeping to peace enforcement. The multilateral US-Thailand-Singaporean series of unclassified COBRA GOLD 00 and 01 exercises were built from this model. Crafting suitable ROE for those scenarios exposed the lack of flexibility inherent in a linear focus.

Swarming attacks would pose, simultaneously, a confusing mixture of actions by a State or non-State actor against a State, with some actions perhaps tantamount to a "hostile act" or demonstration of "hostile intent." At the same time, other actions would fall below that threshold, confounding the development of ROE.

> The blurring of offense and defense reflects another feature of net-war: it tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. A government has difficulty assigning responsibility to a single agency—military, police, or intelligence—to respond.[38]

Of course, this generates confusion over developing a common understanding of rules of engagement as the DoD vies with international and multilateral organizations, international coalition partners, a host of other federal agencies, state and local law enforcement, and private business to develop ROE. Lines of authority will crisscross, and the "operational paradigms of politicians, officials, soldiers, police officers, and related actors get fuzzy and clash."[39] In particular, the military's ROE, which are developed for military operations, may conflict with other agencies' approaches, which are often based on law enforcement. These fundamental questions must be addressed before mission-specific legal analysis can be thoroughly conducted. The essential law of armed conflict and generalized military rules of engagement for CNA, however, can be developed as a point of departure for policy and planning. This will enable commanders to begin a dialogue within the defense establishment and with their counterparts outside the military, facilitating interagency cooperation and action.

The ROE Process

The SROE has added granularity to what many commanders had realized all along—that they are ultimately responsible for developing and applying ROE. This responsibility cannot be abrogated to the Staff Judge Advocate or other directorate. During crisis action planning, the Director of Operations (J3) is key to generating options and ranking the choices available to the commander. When

engaged in deliberate planning, the Director of Strategic Plans and Policy (J5) is the central player. These directorates are closely assisted by the judge advocate, who serves as a facilitator to ensure that the principles of international and domestic law are honored.[40] Toward this end, subject matter experts are critical to forming meaningful ROE. Generally, the Director of Intelligence (J2) and the Director of Command, Control, Communications and Computers (J6) are key advisors regarding CNA capabilities and limitations.

Toward a Results-Based Model

During the drafting process, a "results-based" approach to ROE should be given preference over broad grants of authority to engage in CNA. Results-based ROE tie CNA into a specific mission type, along with the expected, as well as the desired, political or military effect. Using an air defense unit as an example, CNA ROE might be written to authorize CNA to disable an air defense site for a specific period of time in order to accomplish one part of an overall mission. This could prove extremely useful when the alternative of kinetic attack might release dangerous forces, physical destruction of the site is not required, or physical destruction might cause excessive collateral damage or adverse political consequences. CNA, by contrast relies upon a data stream to execute an attack, such as sending an attacking code to an air defense system computer, causing the power supply to short out. This is in contrast to using the electromagnetic spectrum, such as an electromagnetic pulse, that relies upon kinetic energy to obtain a similar result.[41]

Many commanders are concerned about the delay required to obtain supplemental ROE approval, especially if the requested rules require NCA approval.[42] During joint and combined exercises in the Western Pacific, scenario events typically overtook requests for supplemental ROE, as superseding events made the supplemental request irrelevant by unfolding scenario events. The same dynamic occurs in the real world, and the introduction of computer network attack ROE can only decelerate the process. One method that might speed this process along has been to request supplemental rules early in a scenario, delegating authorization to approve the ROE to a level closer to the commander ultimately charged with its use. For example, a combatant regional CINC might be delegated authority in advance for actions that would normally require NCA approval. Additionally, the supplemental ROE might be authorized pending occurrence of a certain set of events or tripwires. This type of thinking was evident in discussions with Australian operators and attorneys during Exercise TANDEM THRUST 99.[43] In the Australian Defence Forces, this concept is called "dormant ROE," and it may

prove to be adaptable to CNA ROE. In "dormant ROE," a set of pre-authorized supplemental or mission-specific rules becomes effective upon some triggering event or receipt of a specialized code word. This method has the advantage of commanders being able to see in advance the level at which authorizations will be given depending upon how a particular mission develops, rather than waiting for change to occur during the mission. This avoids the commander having to address ROE that are suddenly inadequate, and ameliorates the need for additional rules in the midst of a crisis. It would also let the military personnel involved in the mission train for a change in ROE with the actual rules that would apply. Personnel familiar with US and Australian ROE will quickly point out that while the American ROE are permissive in nature and US commanders feel comfortable with broad grants of authority without the need to have specific grants of authority, the Australian rules are more restrictive. However, in dealing with CNA, US commanders should expect more restrictions. When a commander is granted authority to employ CNA, a limited authorization will most likely be the norm. This will be the case until such time as decision makers become more comfortable with this new method of warfare, and the ROE mature. One way to accomplish this, without actual use in a conflict, is to better integrate CNA into war games and exercises. In the last two years in particular, ROE addressing computer network attack and defense have begun to enter the exercise lexicon. Unfortunately, war games and exercises still rarely contain an ROE development phase where supplemental rules are discussed and developed. The concepts should be gravitating more quickly from the national or theater levels to the operational and battle group levels. It is even rarer for the CNA procedures and effects to be explained, or the rules for their employment to be debated in the fleet. The highly classified nature of CNA serves to exacerbate this problem.

Training and Gaming ROE

Over the last two decades, the rules of engagement have matured considerably. Captain J. Ashley Roach, USN (ret.) recognized the need for greater understanding of ROE and practice prior to conflict when he wrote nearly twenty years ago:

> There is a very real need for greater knowledge of rules of engagement on the part of strategy and policy personnel, tacticians and operators, and even by our civilian leaders. At present these rules are rarely, if ever, exercised and too few planners and commanders seek contingent approval for additional or relaxed rules.[44]

Since that time, judge advocates and commanders have made great progress in integrating ROE with operations. Due to the rapid advance in capabilities and the explosion of computer networks in civil and military infrastructures throughout the globe, computer network attack has emerged as one of the few areas that require more immediate attention. Typically, when any type of CNA is included in a war game or exercise, a judge advocate is given the task of crafting ROE for their use, usually without operator input or a full understanding of the mission it is supporting. The problem of lawyer-operator decoupling during the drafting of ROE is certainly not unique to computer network attack issues. Nonetheless, the process of an attorney crafting ROE without the input of other staff representatives—the intelligence and operations directorates in particular—may yield rules that do not serve the commander's complete package of political and military goals. In exercises, CNA events often are handled "notionally." That is to say the "Blue" or "Red" team will state its intention to use CNA for an event, applying pre-authorized ROE developed prior to the game, and they will be informed by the exercise control group that the effort either succeeded or failed. Even when a supplemental ROE request is sent up the chain-of-command to the NCA, there is usually no discussion of the actual method to be employed, making the event much more of a showcase assumption than an actual exercise. Moreover, neither the Blue or Red force, or even the control group, has an understanding of the mechanics of the CNA and how it will operate, particularly the potential collateral effects—expected or unexpected. Ideally, there will be a military attorney advising the exercise control group that can work with the control staff to determine legal effects of CNA. One part of this analysis that might benefit from more attention is whether CNA affects persons with protected or special status under international law.

"Train As We Type"

No matter what shape the ROE begin to take, if we do not train like we actually anticipate utilizing a CNA tool, commanders may not have confidence in its use. Moreover, decision makers will lack confidence in their authorization. Incrementally, progress on increased use of CNA in war games and experiments is unfolding, much like early use of the concept of responding in self-defense based upon a demonstration of hostile intent. Many might assume this concept has been around forever—but although it was adopted into early US ROE and expressed as an inherent right under individual and unit self-defense, this did not guarantee acceptance or use.[45] Discussing the August 19, 1981, shoot-down of two Libyan Su-22 fighters by US Navy F-14s, Captain Roach observed:

> It is a common misperception that under the peacetime ROE a commander must "take the first hit" and cannot act in self-defense until the opposing force has missiles away. That is not the law and is not required by our general peacetime ROE.[46]

Interestingly, the tools and technologies for initiating computer network attack are expanding at a rapid pace, unsettling the associated ROE and complicating the ability of attorneys and commanders alike to fashion widely accepted principles. On the other hand, through the process of incorporating CNA into realistic war games and experiments, the familiarity of future decision makers and commanders is increasing. Once CNA is an option available in time of crisis, deliberate planning during an armed conflict or other military operation will expand the panoply of available tools for use by the commander. This offers flexibility, asymmetric action, and potentially reduced casualties among both friendly forces and opponents alike. In turn, it promises to favorably mold the political outcome.

Disciplining CNA

The surest way to control the use of CNA is to keep its authorization at the NCA level. Doing so simplifies the decision making process for the commander in the field, but it does so at the expense of removing a flexible instrument from his or her inventory. This approach tends to move away from the traditional American position on ROE construction that empowers military commanders with all necessary authority to accomplish an assigned mission, so long as the ROE are not limited by higher authority.[47] The goal should be to exercise and prepare task force and group commanders to engage opposing forces with computer network attack, but to do so according to accepted criteria or rules. Thus, we need to migrate from an ad hoc approach to ROE for CNA to a more routine crisis action checklist appropriate for its employment. Any such checklist would have to be frequently updated to reflect advances in computer technology. Only by standardizing rules for initiating ROE will commanders become comfortable with exercising independent judgment on how, when, where, and against whom to employ CNA. This requires judge advocates to convince commanders, and perhaps innovative technical developers, that computer network attack is properly analyzed within the traditional ROE and LOAC paradigm with which our leadership has grown accustomed. Of course, questions remain—and the dispositive issue of whether a computer network attack constitutes a "use of force" (and if so, what kind of force)—looms large in the

background.[48] Still, it would be shortsighted to await the resolution of this and other politico-legal debates before the military begins to think about a legal model for computer network attack. With that in mind, the existing approach of rules of engagement, embedded within the law of armed conflict, has several advantages. The construct is familiar within the United States and abroad, and it is accepted as a global standard for ameliorating the effects of military operations. It is also flexible and adaptable, and reflects hundreds of years of developmental thinking, so it is a solid foundation on which to build. Most importantly, to the extent that the law of armed conflict has been respected and observed in times of conflict, it has alleviated suffering, limited destruction and spared civilian casualties.

Law of Armed Conflict

The basic framework for all discussions of the laws of armed conflict center around the four principles that evolved from customary international law and subsequently codified in the Hague and Geneva Conventions. These principles are: military necessity, distinction, proportionality, and chivalry. They frame all military activities in armed conflict, and thus must be understood by policy makers and war fighters alike. Military necessity is a cornerstone principle of military action. A commander may employ only that degree and kind of force, not otherwise prohibited by the law of armed conflict, required for the partial or complete submission of the enemy. A minimum expenditure of time, life, and physical resources may be applied.[49]

As reflected in Article 49 of Additional Protocol I to the 1949 Geneva Conventions, distinction ensures "respect for and protection of the civilian population and civilian objects . . . ."[50] Article 51 protects civilian populations, and 51(4) defines unlawfully indiscriminate attacks as: (a) those which are not directed at a specific military objective; (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by Protocol I. Consequently, military strikes must distinguish between lawful combatants and civilians.[51] It would be a violation of LOAC to use civilians or a protected place or property to shield combatants or a valid military objective. The presence of civilians within or near a legitimate military target does not make an attack unlawful.

In the fog of modern war, in which a State's entire society becomes vested in warfare, it is especially difficult to distinguish between lawful and unlawful targets:

> One related issue is the extent that commanders could order preemptive or responsive attacks against non-state targets. It's not just the military. The Chinese, for example, put a lot of emphasis on people's information warfare—encouraging individuals to use their own technology to annoy and attack others.[52]

As we enter the computer warfare age, nations will attempt to further exploit this difficulty.

Loss of life and damage to property incidental to attack must not be excessive in relation to the concrete and direct military advantage expected to be gained. This concept of proportionality defines "concrete and direct" military advantage as "the advantage anticipated from the specific military operation of which the attack is a part taken as a whole and not from isolated or particular parts of the operation."[53] Collateral damage and incidental injury have historically been the product of three factors: (1) a lack of full knowledge as to what is being hit; (2) the inability to surgically craft the amount of force being applied to the target; and (3) the inability to ensure that the weapon strikes precisely the right point.[54] On the digital battlefield, collateral damage could affect entire sectors of the economy and society.

Finally, the main tenets of chivalry center around the principles of treachery and perfidy. The 1977 Additional Protocol I bans ". . . acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence. . . ."[55]

Perfidy includes: 1) feigning of intent to negotiate or surrender, 2) feigning incapacitation, 3) feigning civilian, noncombatant status, and 4) feigning protected status by use of signs or uniforms of the UN or neutral states. Ruses, however, are not prohibited in an armed conflict.[56] Legitimate ruses include camouflage, deceptive lighting, decoys, mock operations, simulated forces and use of enemy codes and passwords.[57] These long-standing principles of international law have direct bearing on possible future CNAs that might rely upon e-mail delivery. One author has advanced the premise that:

> While chivalry may seem archaic today, it retains some normative value. . . [by] analogy [it] strongly weighs against sending a logic bomb disguised as e-mail from the International Committee of the Red Cross (ICRC) or even from "Microsoft Software Support". . . . [S]uch a message might be permissible without perfidious labels. Using ICRC and Microsoft tags would constitute an illegitimate act of perfidy, much as would disguising any dangerous military intruder in the form of an innocuous invitee.[58]

With the principles of LOAC in mind, a commander must also possess additional information prior to requesting permission for, or directing, a CNA. As a practical matter, the commander must know the target—is it a network, link, facility or person? He or she must also understand the effect—both military and cascading or collateral—the CNA will cause.

What is the Target?

Determining the target, and evaluating its lawfulness, will continue to be a focus of rules of engagement, and attacks against information systems are no exception. Whether the target is purely military or civilian, or nominally civilian but intertwined with military purposes or uses (dual-use) is central to this analysis. In the computer network attack realm, achieving "Supervisory Control and Data Acquisition" (SCADA) over a target is often the objective. SCADA is the computer control of a power system, railroad or sewer system, or fresh water system. Over the last twenty years, the US military has relied more on targeting dual-use infrastructure systems. As this infrastructure becomes modernized and networked in most nations throughout the world, reaching system SCADA on a variety of lucrative targets is quickly becoming a milestone in any military operation.[59] At least one proponent has argued that the targeting of electric power distribution and civilian bridges is a violation of Additional Protocol I.[60] The Basic Rule of Article 48 states, "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives." Article 51 (4) states, "Indiscriminate attacks are prohibited."[61] Article 51 (2) states: "The civilian population as such as well as individual civilians shall not be the object of attacks. Acts or threats of violence, the primary purpose of which is to spread terror among the civilian population, are prohibited."[62]

Cascading Effects

Other than the desired military impact, what other probable and possible effects—cascading effects—can the CNA cause? Once such effects are assessed, the principle of proportionality must be examined. This would require an analysis of whether civilian systems will be affected. Is any damage excessive in light of the definite military advantage anticipated? What is the threshold of allowable civilian damage? Are there alternative means available to accomplish the mission?

Getting these answers is the toughest part of the process. Intelligence might be lacking, collateral effects may not be clearly understood, and the infrastructure being attacked may not be fully comprehended. Uncertainty is the order. In some ways, a CNA could be considered like a kinetic, indirect fire weapon. Firing a weapon into an area, even during combat, without proper intelligence, observation, and identification of valid targets is generally unlawful.[63] In much the same way, launching a CNA without sufficient understanding of the system being attacked would be improper. Add to that the fact that the weapon itself, in this case a CNA tool, and its effects on a given target system and other linked collateral systems may be poorly understood. That is not to say that the CNA tool will not have been reviewed prior to being placed in inventory—for the United States and many other nations, it is a prerequisite that a weapons review be accomplished prior to it being authorized for use.[64] However, unlike a hand grenade, CNA might have different effects depending upon the system it is launched against. Additionally, as technology changes, CNA might not have the same effect originally anticipated. Also of concern, due to the complex nature of computer programming and principles, is how the commander in the field will ever hope to reach the same level of understanding as computer and policy experts. Can he rely upon another's judgment when he is the one "pulling the trigger" by pressing the keyboard? Will this satisfy his requirements under international law? What is the minimum level of knowledge the commander must possess? Must the commander—

- understand what the targeted system does and how it operates?
- understand how and what CNA will do to the targeted system?
- be in a position, either through intelligence or direct observation, to judge the effects of the attack?
- determine what other systems share or are linked to the target system and how those other systems operate and what they control?
- determine what impact the CNA tool will have on the non-targeted shared or linked system?

Blurring Lines: CNA ROE for Self-Defense

Up to this point we have concentrated mainly on CNA ROE for mission accomplishment. However, a brief discussion of the use of CNA in self-defense is worthy of examination.

The 2000 SROE position on actions for self-defense seems to be clear: "These rules do not limit a commander's inherent authority and obligation to use all necessary means available and to take all appropriate actions in self-defense of the commander's unit and other US forces in the vicinity."[65]

It follows, then, that if CNA has been placed into the available inventory of weapons, it would be available for actions in self-defense, subject only to authorization by higher authority. Does the novelty of the weapon or the periodic comparison of CNA to a weapon of mass destruction (WMD)[66] alter the conditions precedent for the exercise of self-defense, namely necessity and proportionality?[67] If the CNA use conforms to the four LOAC principles, then characterizing CNA as a WMD is a dubious analogy. Although CNA is, at least for the present, a novelty, it does not require creation of an entirely new ROE. The unfamiliarity with CNA, the secrecy with which it is treated, and, perhaps most importantly, the misperceptions it may cause, could increase provocation and escalation. The SROE already stretches to accommodate these considerations.[68] However, taking CNA off the table for self-defense may be restricting an otherwise valid option for self-defense. If specifically tailored, CNA has the potential to remove or counter a hostile act or hostile intent threat in a "human-friendly" fashion. Unlike a kinetic weapon, CNA can disable systems without injuring civilians.

Concluding Comment

This chapter focuses on the process of developing rules of engagement for CNA within the greater context of the international law of armed conflict. It does not address the general lawfulness of CNA in international law, except as it bears on use of force, targeting, and the ROE process. That question is largely academic, often lying outside the immediate needs of the operational commander and forward-deployed judge advocate. Moreover, much of the analysis to date, tends toward the theoretical and thus is of greater interest and utility to scholars than operational commanders.

By offering some practical principles for developing ROE, we hope to begin closing the gulf between theoretical discussions of CNA and its operational application by theater and task force commanders. The ROE process includes developing the rules within the context of the law, doctrine, and force structure, as well as the boundaries of the mission. During the developmental process, and throughout the application of CNA across the conflict spectrum, the commander should be personally involved. ROE drive CNA and have a dispositive effect on the political and military landscape.

Notes

1. As measured by the technology sector of the Wilshire 5000, often referred to as the Total Stock Market Index, which is the largest index market in the world and provides a broad measure of trends in stock prices across the whole of the market. The Wilshire 5000 consists of approximately 7,000 US-based stocks traded on the New York Stock Exchange, American Stock Exchange and NASDAQ. *See* www.wilshire.com.

2. *See generally*, GEORGE GILDER, MICROCOSM: THE QUANTUM REVOLUTION IN ECONOMICS AND TECHNOLOGY (1990).

3. *See* John Arquilla and David Ronfeldt, *Cyberwar is Coming!*, 12 Comparative Strategy No. 2, 141–165 (1993).

4. Nicholas Lemann, *Dreaming About War: Someone in the Pentagon is Staging a Defense Revolution—and It's Not the Generals*, NEW YORKER, July 16, 2001, at 32. For recent debates on the revolution in military affairs, see Project on Defense Alternatives, RMA Debate, www.comw.org/pda/.

5. William A. Owens, *The American Revolution in Military Affairs*, JOINT FORCE QUARTERLY, Winter 1995–96, at 37.

6. For example, the deep strike concept of "Follow-on Forces Attack" (FOFA) was intended to design forces that would interdict Soviet mechanized and armored forces along the entire path of their attack into Western Europe—beginning at their starting point positioned at barracks and depots in Eastern Europe and the Soviet Union, throughout the entire course of their transit westward to the front in Western Europe. *See* F.W. VON MELLENTHIN ET AL., NATO UNDER ATTACK 12 (1984). The technologies and doctrine that grew from FOFA were applied with stunning results during the Gulf War, and are best illustrated by the tremendous devastation of Iraqi forces fleeing northward from Kuwait along the "highway of death."

7. Sean P. Kanuck, *Information Warfare: New Challenges for Public International Law*, 37 HARVARD INTERNATIONAL LAW JOURNAL 272 (Winter 1996).

8. *See* GEORGE M. CHINN, THE MACHINE GUN: HISTORY, EVOLUTION AND DEVELOPMENT OF MANUAL, AUTOMATIC, AND AIRBORNE REPEATING 65–68 (1951).

9. GARY F. WHEATLEY AND RICHARD E. HAYES, INFORMATION WARFARE AND DETERRENCE, 17–22 and 29–30, December 1996. *See also* Office of the Undersecretary of Defense for Acquisition & Technology, Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D), November 1996.

10. Report of the President's Commission on Critical Infrastructure Protection: Critical Foundations Protecting America's Infrastructures (Oct. 1997).

11. Alan D. Campen, Intelligence is The Long Pole in the Information Operations Tent, Mar. 30, 2000, www.infowar.com.

12. MG James D. Bryan, USA, Commander JTF-CNO, USCINCSPACE, Statement Before the House Armed Services Committee May 17, 2001, www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17bryan.html. *See also* Hon. Linton Wells II, Assistant Secretary of Defense for Command, Control, Communications and Intelligence (Acting) and DoD Chief Information Officer, Hearing on Information Assurance, Statement Before the House Armed Services Committee May 17, 2001, www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-17wells.html.

13. *Id.*

14. Chairman of the Joint Chiefs of Staff, Joint Pub. 3-13, Joint Doctrine for Information Operations, GL-5 (1998), www.dtic.mil/doctrine/jel/operations.htm.

15. *See* Richard W. Aldrich, *The International Legal Implications of Information Warfare*, Institute for National Security Analysis Occasional Paper 9, US Air Force Academy, April 1996, at ix and 6–7; M.E. Bowman, *Is International Law Ready for the Information Age?* 19 FORDHAM

INTERNATIONAL LAW JOURNAL 1935 (1996); Kanuck *supra* note 8, which were among the first to address the issue. *See also* LAWRENCE T. GREENBERG ET AL., OLD LAW FOR A NEW WORLD? THE APPLICABILITY OF INTERNATIONAL LAW TO INFORMATION WARFARE (1997), which was republished by the Institute for International Studies, Stanford University, and revised in 1998 by the Institute for National Strategic Studies, National Defense University under the title INFORMATION WARFARE AND INTERNATIONAL LAW. Analysis from current or former judge advocates include Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF INTERNATIONAL LAW 885 (1999); Roger D. Scott, *Legal Aspects of Information Warfare: Military Disruption of Telecommunications*, 45 NAVAL LAW REVIEW 57 (1998); and W. GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999). Within the Pentagon, the most authoritative address of the issue is a White Paper from Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The paper is appended to this volume as the Appendix.

16. The warfighting or operational level is defined as that intermediate level of military operations between the national or strategic and the individual or small unit tactical level, and includes, in the US Navy, the numbered fleet, carrier battle groups, amphibious groups and squadrons, and in the USMC, the malleable Marine Air-Ground Task Force (MAGTF). *See* Edward N. Luttwak, *The Operational Level of War*, INTERNATIONAL SECURITY, Winter 1980–1981, at 61–79.

17. Discussions with Jack Grunawalt, Professor (Emeritus), Naval War College, in Newport, RI (May 2001); Brian O'Donnell, Rules of Engagement (Oct. 1999–Jun. 2001) (unpublished Naval War College course material on file with authors).

18. JOSEPH BOUCHARD, THE USE OF NAVAL FORCES IN CRISIS 638 (1990).

19. *Id.* at 250.

20. US Navy Regulations, 1948, art. 0614:

> The use of force by United States naval personnel against a friendly foreign state, or against anyone within the territories thereof, is illegal. The right of self-preservation, however, is a right which belongs to states as well as to individuals, and in the case of states it includes the protection of the state, its honor, and its possessions and the lives and property of its citizens against violence, actual or impending, whereby the state or its citizens may suffer irreparable injury. In no case shall force be exercised in time of peace otherwise than as an application of the right of self-preservation as above defined. It must only be used as a last resort, and then only to the extent which is absolutely necessary to accomplish the end required. It can never be exercised with a view to inflict punishment for acts already committed.

21. Peacetime Rules of Engagement for US Seaborne Forces (1981).

22. Peacetime Rules of Engagement for US Forces (1986).

23. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, Standing Rules of Engagement for US Forces (1994).

24. Joint Chiefs of Staff, Joint Pub. 0-2, Unified Action Armed Forces (1995), www.dtic.mil/doctrine/jel/capstone.htm.

25. USCINCPAC, USCINCEUR, and USCINCCENT have all supplemented CJCS SROE with theater-specific ROE.

26. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01A, Standing Rules of Engagement for US Forces (2000) [hereinafter SROE]. The basic instruction is unclassified, but contains substantive topical classified enclosures.

27. For a discussion of SROE, see R. J. Grunawalt, *The JCS Standing Rules of Engagement: A Judge Advocate's Primer*, 42 AIR FORCE LAW REVIEW 245 (1997).

28. *Supra* note 17.

29. *Id. See also* A.R.Thomas, Joint Tactical Command and Control Course on Rules of Engagement (Feb. 25, 2000)(unpublished, on file with authors). The Task Group Commander is attributed as telling the pilots not to worry about the definition of hostile intent since that was the Admiral's job. The pilots were directed to just relay all Libyan aircraft information, such as armaments, maneuvering, speed, etc., back to the Admiral who would decide if the aircraft were hostile. Interestingly, Professor Grunawalt discussed this with commander years after the operation and he indicated that it was not his intent to limit the pilots' right of self-defense. The authority to respond to hostile intent is founded upon the theory of anticipatory self-defense under international law. For a historical discussion of anticipatory self-defense see G. K. Walker, *Anticipatory Collective Self-Defense in the Charter Era: What the Treaties Have Said*, 31 CORNELL INTERNATIONAL LAW JOURNAL 321 (1998). See also YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE (3d ed. 2001) for a discerning distinction between "anticipatory" self-defense, which he indicates is not permitted, and "interceptive" self-defense which is permissible under Article 51 of the UN Charter.

30. Bradd C. Hayes, Naval Rules of Engagement: Management Tools for Crisis (RAND, CA), July 1989, at 14 *citing* DAVID C. MARTINE AND JOHN WALCOTT, BEST LAID PLANS: THE INSIDE STORY OF AMERICA'S WAR AGAINST TERRORISM 121 (1988).

31. JOHN ELLIS, SOCIAL HISTORY OF THE MACHINE GUN 16–20. (1975).

32. F.W. VON MELLENTHIN ET AL., NATO UNDER ATTACK 12–13 (1984).

33. *Id.*

34. ERIC MORRIS ET AL., WEAPONS & WARFARE OF THE TWENTIETH CENTURY, 131–132 (1975).

35. *See* MARTIN VAN CREVELD, TECHNOLOGY AND WAR: FROM 2000 B.C. TO THE PRESENT (1991); JOHN KEEGAN, THE FACE OF BATTLE (1976).

36. John Arquilla et al., *Networks, Netwar, and Information-Age Terrorism, reprinted in* IAN O. LESSER ET AL., COUNTERING THE NEW TERRORISM 54 (1999).

37. *Id.*

38. *Id.*

39. *Id.* at 55.

40. SROE, *supra* note 26, at L-1.

41. Joint Chiefs of Staff, Joint Pub. 1-02, DoD Dictionary of Military and Associated Terms, 88 (2001), www.dtic.mil/doctrine/jel/ref.htm.

42. During the authors' experiences with several USCINCPAC bi-lateral exercises with US Pacific Command Partner Nations in the Western Pacific from 1999-2001, communications difficulties and the rapid pace of the exercises made it more difficult to obtain rapid approval of supplemental ROE requests.

43. Exercise TANDEM THRUST is a biennial Australian-US exercise held in the Pacific and uses a common set of classified ROE called the Combined Rules of Engagement (CROE) for Australian and US forces (on file with authors).

44. J. Ashley Roach, *Rules of Engagement*, NAVAL WAR COLLEGE REVIEW 46, Jan.–Feb. 1983. *See also* F. M. Lorenz, *Rules of Engagement in Somalia: Were They Effective?*, 42 NAVAL LAW REVIEW 62 (1995).

45. Roach, *supra* note 44, at 49. The central question by US Navy commanders was, "Do I have to take the first hit?" This question was definitively answered in the negative by Captain Roach in his article, nonetheless, it took more than a decade for commanders to fully internalize this rule.

46. *Id., citing to* T. Wood Parker, *Thinking Offensively*, US NAVAL INSTITUTE PROCEEDINGS, Apr. 1981, at 29 (footnote omitted). *See also* George Bunn, *International Law and the Use of Force in Peacetime: Do U.S. Ships Have to Take the Fist Hit?*, NAVAL WAR COLLEGE REVIEW 69–80, May–Jun. 1986. Also of note is that some eight years earlier authority to respond to a threat of force

was articulated in US Navy Regulations, art. 0915 (1973) which reads: "The right of self-defense may arise in order to counter either the use of force or an immediate threat of the use of force."

47. SROE, *supra* note 26, at J-1.

48. *See generally*, Schmitt, *supra* note 15.

49. The Hague Convention of 1907, Article 22, protects human life by stating "The right of belligerents to adopt means of injuring the enemy is not unlimited." Convention (IV) Respecting the Laws and Customs of War on Land, Hague, Oct. 18, 1907 *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 84 (Dietrich Schindler & Jiri Toman eds., 3d ed. 1988)[hereinafter Hague IV]. Article 23(g) does the same for property by stating "[it is especially forbidden] to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."

50. Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, opened for signature Dec. 12, 1977, art. 48., 1125 U.N.T.S. 3 (1979) [hereinafter Protocol I]. "Although the U.S. military takes the position that an attacker should accept some responsibility to minimize collateral civilian casualties," the United States has not ratified Protocol I because it shifts the burden to segregate civilians from military objectives to the attacker from its traditional situation where the defender carried this obligation. Danielle L. Infeld, *Note, Precision-guided Munitions Demonstrated Their Pinpoint Accuracy in Desert Storm; but Is a Country Obligated to Use Precision Technology to Minimize Collateral Civilian Injury and Damage?*, 26 GEORGE WASHINGTON JOURNAL OF INTERNATIONAL LAW AND ECONOMICS 109, 123 (1992).

51. Protocol (I), *supra* note 50, art. 51.

52. Charles Bickers, *Combat on the Web*, Far Eastern Economic Review, 16 August 2001, www.feer.com/2001/0108_16/p030innov.html.

53. MICHAEL BOTHE *ET AL.*, NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, 311 (1982).

54. Michael N. Schmitt, *Bellum Americanum: The U.S. View of Twenty-first Century War and its Possible Implications for the Law of Armed Conflict*, 19 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1051 (1998).

55. Protocol I, *supra* note 50, art. 37. *See also* US Navy, The Commander's Handbook on the Law of Naval Operations, Naval Warfare Publication (NWP 1-14M/MCWP 5-2.1/COMDTPUB 5800.7) chap. 12 (1995) [hereinafter Commander's Handbook].

56. Protocol I, *supra* note 50, art. 37; Hague IV, *supra* note 49, art. 24.

57. *See* Commander's Handbook, *supra* note 53. See also ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 507–13 (A.R. Thomas and James C. Duncan eds. 1999) (Vol. 73, US Naval War College International Law Studies) [hereinafter ANNOTATED SUPPLEMENT] for a discussion of customary international law allowing naval forces to fly false colors to deceive an enemy into believing a vessel is a neutral or friendly prior to combat.

58. Mark R. Shulman, *NOTE: Discrimination In the Laws of Information Warfare*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 939, 959 (1999). But see THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 169 (2000) contending that a false message from Microsoft would be lawful in that Microsoft Corporation enjoys no protected status under international law.

59. Major General Bruce A. Wright, USA, Deputy Director for Information Operations, Joint Chiefs of Staff, speaking before the Defense Colloquium on Information Operations (Mar. 24, 1999), quoted in William Church, Information Operations Violates Protocol I, www.infowar.com.

60. *Id.* at 2. 159 States have ratified Protocol I, including a majority of the NATO countries, Yugoslavia, Russia, and China, but not the United States.

61. Protocol I, *supra* note 50, art. 51. Indiscriminate attacks are defined as those which are not directed at a specific military objective.

62. Wright, *supra* note 59, at 1, footnote 1.

63. *See generally*, ANNOTATED SUPPLEMENT *supra* note 57, at chapter 8, for a discussion of the law of targeting.

64. DoD Dir 5000.1, Defense Acquisition (2000). *See also* ANNOTATED SUPPLEMENT, *supra* note 55, at 437. The weapons review is a two-step process, the first review is prior to acquisition, the second review occurs prior to use.

65. SROE, *supra* note 26, at A-2.

66. Russian officials have announced that a CNA would be considered a WMD. *See* Byard Q. Clemmons and Gary D. Brown, *Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction*, 79 MILITARY REVIEW, Sept.–Oct. 1999, at 35–45, *citing* V.I. Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'" (Concept of Information Warfare), Speech given at the *Russian-US Conference on Evolving Post-Cold War National Security Issues* Moscow (Sept. 12–14, 1995).

67. SROE, *supra* note 26, at A-4. See also DINSTEIN, *supra* note 29, at 202, discussing the conditions precedent to the exercise of self-defense and noting the addition of immediacy as a third condition.

68. SROE, *supra* note 26, at A-6.