

IX

Computer Networks, Proportionality, and Military Operations

James H. Doyle, Jr.

A Computer Network Attack (CNA) has been defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computer networks themselves.¹ Whether CNA operations are employed in offense or countered in defense, there are complex issues of proportionality, just as there are in conventional or kinetic attack situations. This chapter explores some of the proportionality judgments an operational military commander must make. But first, it is useful to consider the capabilities, limitations, and vulnerabilities of the computers and computer networks that are revolutionizing high-tech military forces.

Operational Proliferation

During the war in Kosovo and Yugoslavia, targets for NATO aircraft were developed and reviewed by a computerized network that linked, in real time, commanders, planners, intelligence officers, and data specialists on both sides of the Atlantic.² Simultaneously, Tomahawk cruise missiles launched from surface ships and submarines were planned and directed using computer programs. Inside an aircraft, tank, or the lifelines of a warship, there are computer chips at the heart of every weapons system. For example, to track Chinese M-9 missiles fired

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.

into the Taiwan Straits in 1996, USS BUNKER HILL (CG-52) loaded a theater ballistic missile surveillance and tracking program into the Aegis weapon system.³ Computer watchstations acquire, process, display, and disseminate data from sensors simultaneously. In air defense, the new Cooperative Engagement Capability (CEC) uses a network of microprocessors and a data distribution system to share unfiltered radar measurements for composite tracking by dispersed aircraft, ships, and ground batteries.⁴ Electronic, acoustic, infrared, and optical systems have many lines of computer code. Satellites and unmanned aerial vehicles, carrying sensors, communication, and data transfer links, are controlled by computer programs. National satellite imagery, when netted, enables precise geo-positioning for accurate targeting of standoff weapons, as well as mission planning, battle assessment, and intelligence support.⁵ Precision guided munitions depend on sophisticated computer programs for processing weapon engagement data, such as those embedded in the Low Altitude Navigation and Infrared-for-Night (LANTIRN) and the Joint Surveillance Target Attack Radar (JSTARS) systems. Commercial off-the-shelf (COTS) technology is being exploited so that redesigns and updates in military computers can keep pace with the rapid commercial development in home and business computers.

Webbing and Netting

The computing power in transistors mounted on microprocessors has increased dramatically for combat systems in individual aircraft, ships, and battlefield units. However, it is in the *netting* and *webbing* of computers associated with command and control, surveillance, targeting, and gathering intelligence that is adding a new dimension to warfare.⁶ In a computer web, commanders at all levels can simultaneously view the same battlespace. The synergism of several networks, such as the Joint Planning Network, Joint Data Network, and Joint Composite Tracking Network, enhance defense against ballistic and cruise missiles. In both offense and defense, decision-making is speeded up. Innovative tactics and “self-synchronization” at the warrior level are facilitated. Coordination and rapid maneuver among widely dispersed units are enhanced. There is a greater opportunity to get inside an adversary’s observe, orient, decide, act (OODA) loop. Secure video teleconferencing, data base connectivity, direct downlink, and broadcast/receive capabilities provide access to intelligence, logistic, and essential support data, including weather, mapping, terrain, and oceanographic predictions.⁷ The correlation and fusion of data from sensors in satellites, aircraft, ships, and battlefield units enable sensor-to-shooter connectivity and precision targeting. A soldier or Marine equipped with a Situational

Awareness Beacon with Reply (SABER) has access to thousands of friendly force positions every hour, which greatly minimizes fratricide in battle.⁸ The emerging global infrastructure of communication networks, computers, data bases, and consumer electronics provides the National Command Authorities and military commanders with new opportunities to gather intelligence and, most importantly, to get indications and warning of a crisis or threat of attack.

Capabilities, Limitations, and Vulnerabilities

But with all the high-tech capabilities and potential, computers and their networks are only tools of warfare. Humans must make judgments, often based on insufficient or ambiguous data. Identification and discrimination regarding military targets and civilian casualties are difficult issues and cannot be resolved entirely by computer networks. In Kosovo, for example, restrictions on minimum altitudes and the types of authorized targets made it difficult for NATO forces to destroy an enemy who had no requirement to shoot, move, or expose himself.⁹ Then there is the reality that computer networks are not always available or fully operable. Hard drives jam, memories fail, adapters burn out, cables sever, and servers saturate.¹⁰ Difficult challenges of configuration control, standard computer language, reliability, and interoperability abound.¹¹ The Office of Management and Budget places the number of Defense Department computer systems at 8,145, of which 2,096 are deemed critical to military operations.¹² Furthermore, it is not easy to move “zeros” and “ones” where needed when bandwidth is constrained. There is also the ever-present problem of recruiting and retaining trained personnel to operate and maintain the sophisticated computer networks. In addition, data is not information. It is raw material that needs to be processed to obtain ground truth and avoid saturation. Since all data when displayed looks equally valid, computer-aided tools and filters are required to assign confidence levels to the accuracy of the information.¹³

For high-tech military forces, the capabilities of computers and their networks far outweigh the limitations. But technical issues need to be vigorously addressed. Systems must be designed with greater robustness, redundancy, and the ability to degrade gracefully.¹⁴ Security systems (firewalls, shielding, intrusion detection devices, personnel checks, motion sensors, encryption, anti-virus software, and training) are required. But firewalls and intrusion detection devices can be bypassed, and all software is inherently flawed.¹⁵ It must be recognized that command and control, communications, intelligence, surveillance, and reconnaissance systems have become much more vulnerable in information warfare.¹⁶ This is especially true in communication systems, which rely on a

combination of military and civilian satellite networks and transponders. War games, modeling and simulation, and actual incidents reveal a number of methods to attack computer networks. These include physical disruption of hardware and software, insertion of a virus, worm, or logic bomb into a computer program, flooding networks with false data, buffer overflows, malformed data, and e-mail attachments, as well as unsophisticated jamming.¹⁷ Intelligence gathering satellites, military communication networks, sensor downlinks, and precision targeting could be disrupted or defeated. But low-tech military forces, while less dependent on computer networks, may, in some cases, be just as vulnerable to CNA. Command and control may be a single path network without redundancy and fall-back alternatives. Satellite communications may be completely unprotected. In addition to the vulnerabilities of information systems, computer network technology employed offensively has the potential of producing devastating effects on both military support (fuel, spare parts, transportation, mobilization, and medical supplies) and the civilian infrastructure (air traffic control, electrical generation, water distribution, hospital life support, emergency services, currency control, and, ominously, nuclear reactor operations). Thus, both high and low-tech military commanders and their national command authorities need to thoroughly analyze the legal and policy implications before resorting to CNA operations, either in offense or defense. Then, there are the unfriendly “hackers” and terrorist groups eager to exploit vulnerability asymmetries at whatever risk and at relatively low cost. Cyberspace is a highly competitive environment world-wide. The long term effectiveness of computer networks may be less about technology and more about the ability to organize and innovate.

CNA and Consequences

As indicated in the lead-off definition, a CNA can either be an attack on the information resident in computers and computer networks or a direct attack on the computers and their networks. Whether a CNA constitutes an “armed attack”¹⁸ depends not on the means and methods used, but on the resulting consequences.¹⁹ The means and methods of attack may be similar to other offensive information operations, such as psychological or electronic warfare, but the consequences may be severe injury, suffering, death, or destruction of property, and amount to or rise to the level of an armed attack. On the other hand, the consequences may be intrusive, annoying, or disruptive, but not an imminent threat to life or limb, or intended to cause direct damage or injury. In both offense and defense, US military commanders are guided by the Standing Rules of Engagement (SROE) for US military forces. The SROE bridge the transition

between *jus ad bellum* and *jus in bello* by implementing the inherent right of self-defense and providing guidance for the application of force to accomplish the mission.²⁰ They are based on national policy, operational requirements, and US domestic and international law, including the law of armed conflict. The elements of self-defense and mission accomplishment are necessity and proportionality, although the meanings in the self-defense context are much different than when applied under the law of armed conflict for mission accomplishment. The SROE make no distinction in the guidelines for self-defense and mission accomplishment between an attack with conventional weapons and a computer network attack. Thus, the same general criteria would apply, with supplemental measures for a specific operation that might well include guidance on CNA operations.

Self-Defense (*Jus ad Bellum*)

A military force on a post-Cold War mission (humanitarian, peacekeeping, crisis control) could well be confronted with a computer network attack. The attacker could be a malicious hacker, terrorist group, or foreign armed force. Under the US SROE, necessity requires that the military commander must first determine whether the CNA is in fact either a hostile act or a clear demonstration of hostile intent before he decides that it is necessary to respond. An armed attack, such as sinking a ship, firing on troops, invading territory, blockading ports, or mining harbors would in most circumstances be regarded as hostile acts. A physical or kinetic attack against the computer networks that are vital for command and control, surveillance, targeting, or early warning could well preclude or impede the mission and thus also be considered a hostile act. On the other hand, a cyberspace intrusion into these same computer networks may or may not be a hostile act, although a disruption of the satellite network that provides indications of an ICBM launch might, per se, be a hostile act since active defenses are not yet available, and in any event, cueing information is so crucial.

Although the CNA may not rise to the level of a hostile act, the consequences may demonstrate hostile intent, that is, placing the military force in imminent danger. Hostile intent, however demonstrated, has always been a difficult judgment call. The determination is both objective and subjective, influenced by up-to-date intelligence on an adversary and his prior conduct. One military writer has described the concept as an “expression of the national right of anticipatory self-defense at the unit level.”²¹ Locking on an aircraft with fire control radar, approaching on an attack profile, massing tanks and troops on the border, or mobilizing the military and civilian infrastructure for war can all be evidence

of hostile intent. In cyberspace, there are a wide variety of methods of attack previously mentioned that could adversely affect a military commander's computer networks. However, the means of attack and the consequences may not be tangibly present—no “see and touch” evidence. Besides, since cyberspace attacks are inherently anonymous, covert, seamlessly interconnected, and travel across international boundaries via relay points, it is difficult to identify and trace the source, and establish attribution. Is the perpetrator military or civilian, State-sponsored, a rogue organization, or an individual acting on his own? Absent a conventional attack component, manipulation or intrusion by itself does not automatically indicate hostile intent. A CNA intrusion into the communications network could be just an intelligence probe for future operations. But a CNA to disrupt the air defense and targeting networks could be the critical step before launching an armed attack. There are many examples on both sides of the ledger, and critical questions to ponder. Do the consequences of a particular CNA place the military force in imminent danger? Is an adversary attempting to prepare the battlefield for an armed attack that is likely, imminent, or unavoidable? Is this the last opportunity for the military commander to counter the threat?²² If so, the ingredients are there for hostile intent and the necessity to act.

In a CNA situation, just as in a conventional attack, the response to counter the threat must be proportional, whether in anticipatory or actual self-defense. That is, under the US SROE, “the force used must be reasonable in intensity, duration, and magnitude, based on all the facts known to the commander at the time, to decisively counter the hostile act or hostile intent and to ensure the continued safety of US forces.”²³ In self-defense “proportionality points at a symmetry or approximation in ‘scale and effects’ between the unlawful force and the lawful counter-force. . . . A comparison must be made between the quantum of force and counter-force used, as well as the casualties and damage sustained.”²⁴ A military commander must decide what weapons, means of delivery, countermeasures, and tactics are the most appropriate for the situation. For example, the Doctrine for Joint Operations in operations other than war provides that “military force be applied prudently. . . . Restraints on weaponry, tactics, and levels of violence characterize the environment.”²⁵ The objective is to respond with just enough force to control the threat and protect the forces. The response need not be in kind or executed on the spot, if time permits due consideration. For example, in Operation EARNEST WILL (reflagging and protecting Kuwaiti tankers during the Iran-Iraq Tanker War), after the USS SAMUEL B. ROBERTS (FFG-58) hit an Iranian-laid mine, the appropriate and proportional response selected by the National Command Authorities was to attack Iranian oil platforms, attacking Iranian ships only if they fired on US ships.²⁶ On the other

hand, a theater ballistic missile fired at the military force or a facility under its protection requires action within minutes to acquire, track, and engage the missile. Also guiding a military commander in responding to an attack, CNA or conventional, will be a nation's policy objectives. US policy, as stated in the SROE, is to maintain a stable international environment and provide an effective and credible deterrent to armed attack. If deterrence fails, in addition to being proportional, the response should be designed to limit the scope and intensity of a conflict, discourage escalation, and achieve political and military objectives.²⁷ Finally, the use of force is normally the last resort. When time and circumstances permit, the potentially hostile force should be warned and given the opportunity to withdraw or cease threatening actions.²⁸

During the Naval War College symposium, "Computer Network Attack and International Law," the Proportionality Working Group discussed various approaches for developing a response to a CNA.²⁹ One such framework would be to analyze the attack in categories of consequences, such as a network attack with only network effects, a network attack with network and conventional effects, and a conventional attack with network and conventional effects. For each category evaluated, a military commander could consider various options for a proportional response: computer network only, both computer network and conventional, or conventional only. In reaching a judgment, a military commander, guided by the SROE, might pose a series of questions to be resolved for each option, matched against each category: Is there time for a warning to cease threatening actions and an opportunity for the adversary to withdraw? Does the CNA place the military force in imminent danger? Is the CNA the final stage in preparing the battlefield for an attack? Is this the last opportunity for a military commander to protect his force? Is the response contemplated reasonable in intensity, duration, and magnitude? Will the response effectively counter the threat and remove his force from danger? Is a computer network response or a conventional response the most appropriate, or a combination of both? If a computer network response, is there an ability to accurately assess the consequences? Does a computer network response involve a cross-border intrusion? Will the response assist in stabilizing the immediate crisis? Is the response designed to limit the scope and intensity of an impending conflict? Does it discourage escalation? Is the response consistent with maintaining a credible deterrent to further CNAs? What will be the effects, intended or unintended, on civilians, their property and infrastructure? Can these effects be distinguished from effects on military personnel, equipment, and infrastructure?

In the case of a CNA with only network effects, the consequences, although degrading a particular computer network, may not place the force in imminent

danger or be evidence of an impending attack. The appropriate response might be to shift to an alternate network, use computer countermeasures to expel the intruder, sanitize the system, and report to higher authority. This situation would be analogous to tolerating an aircraft tracking radar, but not a locked on fire control radar. Higher authority, with the requisite technical expertise and network connections, could trace the intrusion, identify the perpetrator, and take appropriate action, such as a complaint to the relay State, if the CNA appears to be State-sponsored. Or, if the intrusion is an intelligence probe, higher authority might choose to play the game and “grab the hacker,” feeding him false information covertly. If, however, the network effects disable the air and missile defense network and are judged as the overriding evidence of armed attack, the immediate response might be to launch a conventional attack against the most threatening military targets—tanks and troops, aircraft on runways, missile sites, command headquarters, and the like. Such a response would be timely and might discourage an adversary from attacking or, at least, indicate that there will be a high cost to proceeding. This would not rule out a follow-up computer network response against, for example, the adversary’s military command and control network, executed at the appropriate level by trained network experts. In either situation of a CNA with network effects only, the proportionality set-point to trigger a response in kind should be high since the intrusion may be ambiguous and non-threatening or the response would not be timely, effective, or within the capability of the operational commander to execute.

In a crisis situation, an adversary may choose to initiate a CNA that has both network and conventional effects, such as manipulating the air traffic control network of an aircraft carrier that causes collisions or near misses of aircraft in the approach and landing pattern. This attack would be less risky than attacking the carrier or its air wing. The overall effect is to raise the level of hostility and resolve some of the ambiguity in identifying the source. Obviously the situation cannot be tolerated. If overall intelligence plus the conventional effects can presumptively attribute the CNA to a particular adversary, the initial response might be a stern warning to cease the hazardous computer operations, in addition to shifting to an alternate control mode, attempting to expel the perpetrator, and sanitizing the system. If, despite the warning and opportunity to cease, the disruption continues, the military commander might respond with a conventional, precision attack against the most appropriate military target that would reinforce the warning with force. Such targets might be a facility for the production of nuclear, chemical, and biological weapons, ballistic missile launchers that are not yet mobile, or a new warship about to be launched. This would be analogous to the response when the USS SAMUEL B. ROBERTS

hit the Iranian mine which was laid arbitrarily to hazard both warships and merchant ships. That response was neither in kind nor executed immediately. If the computer specialists also have the capability to intrude and disrupt one of the adversary's vital military computer networks, this would also be an appropriate and timely response. All of these responses are intended to control the crisis, discourage escalation, and avoid collateral damage and incidental injury to civilians.

In the case of a physical attack against a computer network asset itself, such as destroying a satellite (communications, navigation, imagery) or damaging a command and control (C2) node, the conventional effects are tangible and serious. The source and location can probably be pinpointed. Destruction of a satellite without other evidence of hostile intent would not warrant an immediate physical or CNA response. But such an extraordinary act would have implications and effects world-wide, and would merit immediate attention at the highest levels of government, as well as the United Nations Security Council. If the destruction of the satellite or damage to the C2 facility is the prelude to armed attack, a robust and direct conventional response to blunt the attack would probably be the most effective. All military targets that are part of or supporting the attack would be fair game. The objective would be to protect the force, control the threat, discourage escalation, and, at the same time, avoid collateral damage and incidental injury to civilians. A parallel CNA response to degrade, manipulate, or destroy information resident in the adversary's C2 computer networks might effectively complement the conventional response. This response might target networks that support the armed attack, taking care to avoid unintended network effects that injure or kill civilians or damage their property. Here, the problem is sorting out the network effects that may be inextricably linked in the military and civilian infrastructure.

There are numerous examples of network and/or conventional consequences and responses to a CNA that can be analyzed in the categories postulated. The most appropriate and proportional response will depend on a careful consideration of the facts, context, and intelligence in each particular case, whatever method of determination is pursued.

Mission Accomplishment (*Jus in Bello*)

A military force involved in a crisis or action in self-defense that develops into a low intensity conflict or prolonged war could be authorized to conduct CNA operations, that is, attack the information resident in computers and computer networks, or attack the computers and their networks directly. In applying force to accomplish a mission, the SROE provides that US forces will be governed by

the law of armed conflict³⁰ and rules of engagement. Also, as mentioned previously, the elements of mission accomplishment are necessity and proportionality. Hostile acts and intent are presumed. Necessity means that attacks must be limited to military objectives,³¹ and that force has to be constrained to that required to accomplish the mission.³² Proportionality in mission accomplishment, however, unlike self-defense, is not a comparison and symmetry between the quantum of force and counterforce used.³³ The objective is to defeat the enemy as rapidly as possible. Disproportionate force may be, and often is, required. But in applying counterforce, the law of armed conflict requires that a military commander observe the principle of distinction between combatants and noncombatants,³⁴ precautions in attack,³⁵ and the law of targeting.³⁶ Although it is not unlawful to cause incidental injury to civilians, or collateral damage to civilian objects, incidental or collateral damage must not be excessive in the light of the military advantage anticipated by the attack.³⁷ In applying this proportionality balancing test, a military commander must take all reasonable precautions, based on information available at the time, to keep civilian casualties and damage consistent with mission accomplishment. He must also consider alternative methods of attack to reduce civilian casualties and damage. In addition to *jus in bello* prescriptions, a military commander will be guided by supplemental measures in the ROE that “define the limits or grants of authority for the use of force for mission accomplishment.”³⁸

The Proportionality Working Group³⁹ also explored approaches for analyzing CNA offensive operations. For example, the CNA might be a network attack against a network target, a network attack against a non-network target, or a conventional (kinetic) attack against a network target. These categories, while overlapping and arbitrary, are intended to assist in focusing on the effects and consequences of a CNA. For each option evaluated in terms of effects and consequences, a military commander, guided by the SROE and battle plan, might pose a series of questions to be resolved: Will the CNA capture important enemy intelligence? Does it assist in getting inside the enemy’s OODA loop? Can the CNA disrupt, control, or destroy the enemy’s computer networks for intelligence collection and targeting? Will it contribute to establishing information dominance, air and maritime superiority, and space control? Does the CNA provide the military commander with new options for favorably controlling the rhythm of the battle? Will it influence the enemy to terminate military action and alter policy? Does the CNA degrade an enemy’s supporting infrastructure? Is it essential in protecting own forces, equipment, and facilities? Overall, does the CNA contribute to the partial or complete submission of the enemy with the least expenditure of life, time, and resources? In coalition warfare, does it

preserve unity of effort and consensus in waging war? Does the CNA respect the inviolability of neutrals and their commerce? Is the CNA consistent with United Nations Security Council enforcement action, if any? Does the CNA involve cross-border intrusions? Is it compatible with diplomatic and political efforts to achieve a cease-fire, suspension of hostilities, armistice agreement, peace treaty, or other termination of the war? What are the effects of the CNA on protected persons (civilians; wounded, sick, and shipwrecked; medical personnel and chaplains; and prisoners of war)? What incidental injury to civilians or collateral damage is anticipated from the CNA, based on the best means to accurately assess the primary and secondary effects of a CNA? Can the military effects be distinguished from the civilian effects? Is the incidental injury or collateral damage likely to be excessive in the light of the military advantage anticipated? Will it cause unnecessary suffering or be indiscriminate in nature? Are there alternative means and methods of attack that will reduce civilian casualties and damage from that considered likely from the CNA? Will a decision to withhold *network attacks* against network or non-network targets influence an enemy to also refrain from similar network attacks, and can this restraint be relied upon? Finally, pertinent to each of the questions, does the network or non-network target by its nature, purpose, or use make an effective contribution to the enemy's military action, and thus constitute a lawful military objective of the CNA.

In the category of a network attack against a network target, the intention is to adversely affect the *information* resident in the enemy's computer network. Examples include introducing information or disinformation (not perfidious) into the computer network to influence or mislead behavior, intruding with a data device or technique to degrade the military C2 network, disrupting vital links in the integrated air defense (IAD) network, or manipulating the military communication network to confuse the timing of a maneuver or attack. In these and similar offensive computer operations, the ultimate consequences are neither intended nor anticipated to involve incidental injury or collateral damage. Psychologically, the civilian population may, as intended, be influenced, but the effects would not be physical. A computer intrusion into the enemy's intelligence network to capture vital information, or indications and warning, would be a necessary step in preparing the battlespace, and probably would not even fall within the definition of a CNA. In any event, a network attack on the information in a computer network that is tailored to produce limited physical consequences may prove to be an effective non-lethal tool of warfare against military objectives. An alternative conventional attack calculated to degrade the C2 and IAD networks, for example, could result in civilian casualties and damage.

However, in most cases, these effects would probably not be considered excessive in the light of the military advantage anticipated.

In the case of a network attack against a non-network target, the intention is to damage or destroy military objectives through the medium of a CNA operating on the information resident in the enemy's computer network. Examples would include disrupting the military air traffic control system to induce collisions or crashes, causing a military satellite to lose control and implode, disabling the electrical system in the enemy's C2 facility, and manipulating the computer network that manages vital military support. For these and other military targets, and assuming an ability to accurately assess the primary and secondary effects, CNA operations may prove to be an effective method of prosecuting the war at less risk to one's own forces. However, network attacks on the civilian infrastructure, even though it supports the enemy's military effort, raises difficult issues. It may not be possible to distinguish the military from the civilian effects because of the inextricable linkage between the two. Even if that is possible, the CNA may set off a chain of effects that cascades beyond the military and into civilian institutions. This could raise questions of whether the CNA was indiscriminate and not directed at a valid military objective. Furthermore, a cascading CNA might result in disastrous consequences on essential services for the civilian population (electrical power, water distribution, life support, nuclear power operations). Even assuming, for example, a CNA against an electrical power grid that supports the military effort, and is therefore a valid military objective, there must be no indiscriminate cascading effects, and under the proportionality and balancing test, any incidental injury and collateral damage must not be excessive in view of the military advantage anticipated. The point is not to rule out CNAs in this category, but to urge caution in their use in view of the uncertainty in predicting effects.

An attack against an enemy's computers and computer networks with missiles, bombs, or artillery shells is the traditional means of attack. A military commander must insure that the various computer network sites and facilities are valid military targets and that incidental injury and collateral damage are kept to a minimum. Damage or destruction of C2 war rooms and command posts, for example, would contribute significantly to defeating the enemy. Air defense sites, microwave stations, data relay facilities, and communication satellites can also be electronically jammed from aircraft, ground stations, and warships. Damage or destruction of a dual-use military and civilian satellite would raise serious issues for high-tech military forces that are becoming extraordinarily dependent on satellites for both military and commercial purposes. Should the commander refrain from attacking the satellite in the hope that the enemy will also exercise restraint? Is the dual-use satellite a valid military target when the bandwidth used

by the military is relatively minor? Disruption, damage, or destruction of computer network facilities that provide essential civilian services, as well as support the military effort, such as electrical power grids, may be unavoidable in prosecuting the war. But difficult proportionality judgments must be made even though there may not be the unpredictable cascading effects produced by a CNA. An assessment must be made that the civilian injury and damage will not be excessive in the light of the military advantage anticipated. Temporarily disabling the power grids by attacking with carbon chaff, for example, may reduce casualties and avoid more serious consequences, as well as influencing behavior. Attacking computers and computer networks serving primarily the civilian infrastructure, such as banking systems, stock exchanges, water management, and research centers, would be difficult to justify in terms of a military advantage and would probably result in excessive civilian injury and damage.

Just as in the *jus ad bellum* situation, there are many examples of actual or potential CNA offensive operations. While mission accomplishment proportionality takes on a different meaning from that in self-defense, the balancing test of military advantage versus excessive incidental injury and collateral damage must consider both the actual and cascading effects of a CNA, whatever method of analysis is used.

Observations

CNA operations as part of information warfare or network-centric warfare are in their infancy, with far-reaching implications for law, policy, and rules of engagement. The ability to predict and assess the damage from executing a CNA in offense or defense, similar to a precision strike weapon, is far from assured. CNAs may well prove to be invaluable in defeating the enemy and countering an attack, provided that trained and experienced computer network experts can accurately “hit” the target, control the effects, and avoid unintended cascading consequences. This assumes that CNA operations are authorized at the appropriate level. All this adds to the complexity of proportionality judgments. However, the basic rules in *jus ad bellum* and *jus in bello* still apply. An analysis of the targeting must be conducted for a CNA just as it is conducted for attacks using conventional weapons. On the defense side, the old adage of the best defense is a good offense may be turned on its head in the case of CNA operations. There is no question that a high-tech military force with significant network vulnerabilities must have a robust, passive protection against CNA. This requires increased awareness, training, technical support, hardware and software improvements, greater redundancy, and an ability to degrade gracefully in computer network

equipment and systems. It also means that military commanders must plan and train to “work-around” network attacks that disrupt, deny, or destroy critical information resident in their computers and computer networks. This is particularly important since rogue and terrorist groups without asymmetrical vulnerabilities can wage network war on the cheap with little regard for the risk.

Notes

1. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at GL-5 (1998) [hereinafter Joint Pub 3-13].

2. See Michael Ignatieff, *The Virtual Commander: How NATO Invented a New Kind of War*, THE NEW YORKER, Aug. 2, 1998, at 33.

3. See Gary W. Schnurrpusch, *Asian Crisis Spurs Navy TBMD*, NAVAL INSTITUTE PROCEEDINGS, Sept. 1999, at 46-49.

4. See *The Cooperative Engagement Capability*, 16:4 JOHNS HOPKINS APPLIED PHYSICS LABORATORY TECHNICAL DIGEST 377-396 (1995).

5. See Austin G. Boyd and David G. Simpson, *Satellite Communications: C4I Link into the 3rd Millennium*, 21:5 SURFACE WARFARE, Sept./Oct. 1996, at 11-16.

6. For a discussion of the present and future potential of computer networks in warfare, see Arthur K. Cebrowski and John Garstka, *Network-Centric Warfare: Its Origins and Future*, NAVAL INSTITUTE PROCEEDINGS, Jan. 1998, at 28-35; James J. Kuzmich and Christopher P. McNamara, *Land Attack from the Sea*, NAVAL INSTITUTE PROCEEDINGS, Aug. 1999, at 52-55; Andrew F. Krepinevich, *Calvary to Computer: The Pattern of Military Revolutions*, in STRATEGY AND FORCE PLANNING 582 (Naval War College Faculty eds., 1995); William K. Lescher, *Network-Centric: Is it Worth the Risk?*, NAVAL INSTITUTE PROCEEDINGS, July 1999, at 58-63; Arthur K. Cebrowski, *Network-Centric Warfare and C2 Implications*, NAVAL WAR COLLEGE REVIEW, Spring 1999, at 4-11.

7. See David G. Simpson, *Using Space for a Battlefield Advantage*, 21:5 SURFACE WARFARE, Sept./Oct., 1996, at 7-9.

8. See Austin Boyd, *Rapid Response Through Space: Reducing Battlefield Fratricide*, *id.* at 27-28. Similarly, the new Joint Expeditionary Digital Information System (JEDI) is a briefcase-size command and control system with an Iridium satellite handset. It contains a personal digital assistant and a Global Positioning System (GPS) receiver, and can interface with the Global Command and Control System, displaying GCCS-like tracks. See Rupert Pengelley, *JEDI Returns for JSOC'S Mini C2 System*, JANE'S INTERNATIONAL DEFENSE REVIEW, Oct. 1994, www.janes.com.

9. See Phillip C. Tissue, *21 Minutes to Belgrade*, NAVAL INSTITUTE PROCEEDINGS, Sept. 1999, at 38-40.

10. See Michael Keehn, *Is the Navy Heading for a Crash?*, NAVAL INSTITUTE PROCEEDINGS, July 1999, at 88-89.

11. See Letitia Austin, *Linking Acquisition to the Fleet*, 21:5 SURFACE WARFARE, Sept./Oct. 1996, at 8-9.

12. See *Pentagon Report: Pentagon Seeks to Boost Public Confidence in Y2K Readiness*, NATIONAL DEFENSE, Sept. 1999, at 10.

13. See Alan D. Zimm, *Human-Centric Warfare*, NAVAL INSTITUTE PROCEEDINGS, May 1999, at 28-31.

14. See Robert F. James, *The Guts Behind the Glory*, 21:5 SURFACE WARFARE, Sept./Oct. 1996, at 2-7.

15. See Perry G. Luzwick, *What's a Pound of Your Information Worth?: Constructs for Collaboration and Consistency*, 20:4 NATIONAL SECURITY LAW REPORT, AUG. 1999, at 1, 6.

16. See Joint Pub 3-13, *supra* note 1, at III-1-15; 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).

17. For a description of the effects of a "logic bomb," "worms," and a "sniffer," see Steve Lohr, *Ready, Aim, Zap*, NEW YORK TIMES, Sept. 30, 1996, at D-1. See also David Tubbs, *Exploits: How Hackers Hack*, 20:4 NATIONAL SECURITY LAW REPORT, Aug., 1999 at 14-16.

18. For a discussion of the macro issues in the international law of information warfare, see LAWRENCE GREENBERG, SEYMOUR GOODMAN, AND KEVIN SOO HOO, *INFORMATION WARFARE AND INTERNATIONAL LAW* (1998) and WALTER G. SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* (1999).

19. For an innovative framework to analyze a CNA in *jus ad bellum* situations, see Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885-937 (1999).

20. Joint Chiefs of Staff Standing Rules of Engagement (SROE), Chairman, Joint Chiefs of Staff Inst. 3121.01, Oct. 1, 1994 [hereinafter SROE] (The current version of the SROE was promulgated on Jan. 15, 2000, as CJCS Instruction 3121.01A.) For an excellent discussion of the US Rules of Engagement, see James C. Duncan, *The Commander's Role in Developing Rules of Engagement*, NAVAL WAR COLLEGE REVIEW, Summer 1999, at 76-89.

21. Duncan, *supra* note 20, at 82.

22. See Schmitt, *supra* note 19.

23. SROE, *supra* note 20, at A-5.

24. YORAM DINSTEIN, *WAR, AGGRESSION AND SELF-DEFENCE* 231 (3d ed. 2001).

25. Chairman Joint Chiefs of Staff, Joint Publication 3-0, *Doctrine for Joint Operations*, at V-3 (1995).

26. WILLIAM J. CROWE, *THE LINE OF FIRE* 187-211 (1993).

27. SROE, *supra* note 20, at A-2.

28. SROE, *supra* note 20, at A-6.

29. Symposium on Computer Network "Attack" and International Law, Naval War College, June 1999.

30. SROE, *supra* note 20, at A-2.

31. "Military objectives are limited to those objects which by their nature, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage." Additional Protocol I to the Geneva Conventions of Aug. 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, *reprinted in* Documents on the Laws of War 419 (Adam Roberts and Richard Guelff eds., 3rd ed. 2000).

32. The Commander's Handbook on the Law of Naval Operations, NWP 1-14M/MCWP 5-2.1/ COMDTPUB P5800.1, para 5.2 (1995) [hereinafter NWP 1-14M].

33. See DINSTEIN, *supra* note 24, at 231-235.

34. Protocol I, art. 51, *supra* note 31, at 448-49.

35. Protocol I, art. 57, *supra* note 31, at 452-453.

36. NWP 1-14M, *supra* note 32, at para 8.1.

37. NWP 1-14M, *supra* note 32, at para. 8.1.21. See also Protocol I, art. 57 2(a)(iii), *supra* note 31, at 453; SAN REMO HANDBOOK ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA (Louise Doswald-Beck ed., 1995), para. 46, at 16; and William Fenrick, *The Rule of Proportionality and Protocol I in Conventional War*, 98 MILITARY LAW REVIEW 91, 125 (1982).

38. Duncan, *supra* note 20, at 83.

39. See Symposium, *supra* note 29.