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

XII

Proportionality, Cyberwar, and the Law of War

Ruth G. Wedgwood

The advent of the computer has enormously increased the efficiency of modern economies, lending computational prowess to the organization of industrial production, inventory, communications, the integration of power grids, the control of financial transactions, and transportation routing. The decentralized architecture of the personal computer, and its Internet platform, have linked economic actors screen-to-screen, allowing direct communications and disintermediated transactions, bypassing a costly institutional structure of wholesale and retail agencies. The real-time communication of common written texts through e-mail and document formats has strengthened coordination within and between organizations, permitting consultative processes to work in staggered time. Cybernetic life has also brought new problems in public and private law, including data privacy, jurisdiction for regulating speech and the protection of intellectual property.

Challenges for the law in a cybernetic age will extend to the battlefield. Cybernetics have transformed war. In data-sharing, military planners were the first to engineer joint access to a common pool through the "DARPANET," fabled forerunner of the civilian sector's Internet. In air operations and even for ground forces, computer and sensor technology can eventually be used to construct a real-time picture of an integrated battlespace, to be shared among friendly forces.

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.

Computers, supporting sensors and global positioning satellites will enhance the precision of weaponry and maneuvers, supplementing human judgment with digital assessments. The accuracy of kinetic weapons will be improved by using optical matches of targets and trajectory, and reconciling the real coordinates of projectiles and aim points. (Even in the last ten years, the navigational capabilities of cruise missiles have been transformed.) Though budget constraints and procurement cycles may slow down the implementation of this virtual battlespace, the prospects are clear. A shared system of observation and control will support the adjustment of tactics, the dynamic targeting of the adversary's assets, the full integration of multiple weapons platforms, and safeguards against friendly fire. Advanced electronics and computing capabilities also hold the promise of confusing an adversary's command and control, disrupting his operating systems, and masking his view of the battlespace. The future of national missile defense also depends on the extraordinary computing capabilities that can handle massive data on launch speed, trajectory, and atmospheric perturbations.

Computer technology will also continue to support American military transportation, communications, and logistics—essential in mobilizing, deploying, and sustaining a combat force, so often the Achilles' heel of lesser military forces. The American military is a far-flung force, deployed around the globe, conducting exercises, patrols, and peace operations in numerous theatres at once. Access to common data and immediate communications can integrate a decentralized force structure.

But the luxury of a new technology also can create vulnerabilities, and enhancement can become dependency. The sophistication of American military operations may invite a new mode of asymmetric attack. Opposing forces whose own organization is far more primitive may attempt an electronic version of jiu-jitsu. The same technological doors that permit easy communication also allow unwanted foreign entry. The portals for adjustment of operations may permit deliberate disruption. Encryption of data and communications has grown in power, but code-breaking has also benefited from number-crunching bionics. Protecting sensitive information through compartmentalization is more difficult when access may be gained through trap doors and undetected keyholes. The quickly changing design of software and hardware, and the Pentagon's frequent reliance on commercially available products for "non-critical" operations, also means that information technologists may not fathom the vulnerability of the systems they employ. Rather like war-gaming, defensive understanding is often gained only after a simulated attack. The advantages of cybernetic organization for military campaigns must be weighed against the dangers of compromise and disruption.

Military law must also address the new architecture of cyberwar, including the ill fit of existing normative structures for electronic warfare. A primary challenge for military thinkers is what to do about civilian safety. Over the centuries, the operational harshness of warfare has been challenged by the ideals of proportionality and discrimination. These ideals of the profession of arms, implemented by military commanders and their legal advisors, ask for a critical distinction between civilian and military targets, and teach that military advantage always must be measured against civilian loss. Cybernetic conflict may pose new hazards to civilian safety, taxing our traditional notions of the division between the battlefield and civilian life. It is well to consider some of these problems in advance in order to construct the necessary safeguards.[1]

Discrimination among targets is a fundamental norm of military law, acknowledging that there is, ultimately, an important distinction to be made between civilian objects and military assets. The idea of discrimination is rooted in the belief that warfare should be effective, rather than punitive, and that wars can be won without deliberately harming civilians. The moral compromises of war do not extend to unnecessary cruelty. Noncombatants are considered innocent (even where, in their political lives, they may have favored a war) and enjoy a right to life protected even in warfare. Apart from the ethical claim, there is a practical reason to observe this scruple. The reciprocal practice of discrimination means that a soldier has greater assurance that his own family members will survive the conflict. A military operator also will see discrimination as the practical application of economy of force, saving one's firepower for targets that matter. The norm is further supported by a working hypothesis about war termination—armed conflicts may end earlier where defeated soldiers can reintegrate into a workable civilian society, in which there is something to return to. Renewal of the conflict may be more likely if civilian society is left destitute and a generation reared seeking revenge.

Proportionality extends the protection for civilians beyond the ban on deliberate targeting. Proportionality argues that dominant intention is not enough in choosing the objects of destruction in a war. Even with a military target directly in view, there must be some balancing between the advantage to the war effort from a target's destruction and the foreseeable "incidental" damage to civilians. The terms of trade in this moral exchange are not terribly clear, to be sure—the relative weighting of military gain and civilian harm is a complex judgment that involves both battlefield expertise and situational ethics. But at the limit, there is an admitted case in which an ephemeral military advantage could not outweigh enormous harm.

In the idealized account of the law of war, the operational code of *jus in bello* is equally binding on both sides no matter who was at fault in starting the conflict. In this view, the operational norms regulating how a war is fought do not vary according to the purpose of the war. The same tactics govern a virtuous or condemnable war. *Jus in bello* binds a combatant despite his status as invader or as a victim defending his homeland. The perceived value of this separation is that a third party or protecting power can monitor the observance of humanitarian law without venturing into the hotly disputed territory of *casus belli* and the merits of the underlying dispute. The international limits on the initiation of warfare, *jus ad bellum*, are placed in a separate normative framework. (The practical tolerance of political publics for this attempted distinction is another matter. Indeed, in the preparation for the Nuremberg trials, at least one prominent scholar argued that any use of force by the Axis, even against traditional military targets, should be considered a war crime, since each use of force aided the Nazi war of aggression.[2] The obverse conclusion, that any tactic was permissible to defeat Nazism, was not openly mooted, but may underlie some of our practical assessments.)

Protecting civilians is harder than it sounds on paper for a number of reasons. First, in modern warfare, the mobilization of national economies and war production makes industrial plants and infrastructure into a second battlefield. Economic assets are considered military targets for their support of the war effort. Critics have questioned the efficacy of particular air campaigns, but the legitimacy of weakening an adversary's industrial base and war production facilities is generally accepted. Unless an air campaign can be confined to night-time bombing, the targeting of war industries will endanger workers in the plants, even though they are technically noncombatants. Locating war industries in urban areas is also likely to endanger residential areas, unless precision bombing is used.

Second, the rural conflicts of the Cold War and decolonization also challenged the protection of civilians. The techniques of guerrilla warfare typically involve camouflaging insurgent forces among the civilian population as protection against more powerful adversaries. Distinctive military insignia or dress has been a long-standing requirement of legitimate warfare in order to distinguish civilians from combatants and the failure to identify forces traditionally deprived the disguised combatants of the protections of the law of war, including prisoner of war status. But the norm of self-identification was derided as a luxury in an era of wars against "colonial domination."[3] Undermining this rule of combatant identification poses obvious dangers to innocent civilians.[4] In civil war, terrorist tactics against civilians also have been deliberately used as a powerful advertisement that the established government cannot guarantee

protection. Governments, in turn, have used terror to persuade civilian populations to withhold support from insurgents.

The problem of target masquerade extends even to conventional warfare, since combatants are sometimes tempted to disguise military assets as civilian facilities. Secreting a weapons cache inside a school building serves to collapse the attempted distinction between civilian and military sites, and is an act of perfidy punishable as a war crime. Misuse of a civilian facility deprives the target of its protected status, but the damage remains because it makes combatants less inclined generally to respect the protection guaranteed to civilian sites.

The third source of heightened danger for civilians stemmed from nuclear confrontation in the Cold War, with its strategies of deterrence through mutually assured destructive capability, flexible response, and counterforce targeting. Even with the confinement of nuclear targeting to military objects such as missile silos, troop concentrations, and ports and airfields, the externalities of radiation, electromagnetic pulse, and a broad radius of immediate destruction meant that civilian populations would have been gravely endangered.

Since the end of the Cold War, the proliferation of ethnic conflicts has continued to pose grave hazards to civilians. In a war whose target is the civilian population itself, atrocious acts are often committed against noncombatants as one way of causing populations to flee. The war aim of creating a mono-ethnic territory is used to justify terror tactics in order to displace populations. Attacks on civilians are not incidental, but rest at the center of the conflict, serving the central war aim of purging minorities and ethnic rivals. Where advantage may be gained by the rapid consolidation of territory, the employment of terror against civilians is hard to contain.

Even with the most worthy war aims, the principled distinction between military and civilian targets may be under pressure (though it is still mandatory to avoid terror tactics). In a humanitarian intervention such as the 1999 Kosovo campaign, designed to stem the gross mistreatment of civilian populations, responsible leaders must seek to undermine the transgressing adversary's will to resist, using war as a mode of coercive diplomacy. Winning such a limited conflict is quite different from the unconditional surrender sought in the great land campaigns of the world wars. Striking mobile military vehicles, tanks, and artillery pieces in a mountainous terrain is exceedingly difficult, and (in a humanitarian intervention designed to thwart genocide) an expedited end to the conflict may be urgent. At least one high Yugoslav official has suggested that the Kosovo campaign was abandoned by Belgrade because Milosevic doubted the ultimate loyalty of the Yugoslav military. This disaffection was caused in part by the military's concern about how the steady destruction of Serbia's infrastructure would

affect the welfare of their own families. While there is widespread consensus that civilians must not be deliberately reduced to starvation or other life-threatening conditions, at least one analyst has suggested that the rule of discrimination should permit the disabling of facilities that sustain some conveniences of modern civilian life. The danger of a slippery slope is evident—the loss of water purification and sewage disposal, for example, could cause devastating disease and lies beyond the pale of easy ethical analysis. Yet the problems of stopping a war that seems remote to the controlling polity are also evident, and the limit of "mere inconvenience" does not abandon the broader norm of protecting civilian survival. The troubling question of how to persuade an adversary to desist has not been made easier as well by the last decade's record of ineffective employment of economic sanctions as an alternative instrument of coercion.

Another difficult challenge to the conceptual categories of civilian and military objects has been created, ironically, by the new precision of guided munitions. With navigation by global positioning and optical recognition, aim points and target impact may be as exact as the particular courtyard of a building in an urban area. Targeting has an exactitude, and therefore a transparency of intention, unknown to other wars. The targets sought in an air campaign are evident and public. The five-mile radius of uncertainty that surrounded the aerial delivery of munitions in the Second World War served to obscure the target aim, apart from internal knowledge of the campaign plans. But precision-guided munitions announce their destination, and pose the questions of target distinction masked in earlier wars.

Finally, there is the serious dilemma of dual-use targets. This is again a problem of distinction between military and civilian objects. It stems from the joint infrastructure of modern economies. Military and civilian facilities share a need for electricity, natural gas, and oil to sustain their basic services. Rarely is there a dedicated infrastructure exclusively serving military facilities. To disable the facilities that sustain a military adversary may unavoidably burden the local civilian populations. In the Kosovo and Iraqi air campaigns, allied forces needed to suppress anti-aircraft capability and ground radar guidance in order to allow safe allied entry into hostile airspace. Mobile facilities, camouflaged and positioned under the lee of a hill, are difficult to target even in clear weather. The only assurance of safe air space may lie in pulling the plug on anti-aircraft by disabling a power grid. The legitimacy of doing so depends on a judgment about proportionality. Vital civilian functions such as schools, old age homes, and hospitals may also depend on electrical power. The civilian harm from their temporary disability must be conscientiously weighed against the military advantage. The merger of military and civilian electrical infrastructure shows the difficulty of a

strict principle of distinction, and the quandaries of judgments on proportionality. Oil and gasoline supplies, too, present a dual-use dilemma. Loss of refining and storage facilities can severely limit an adversary's ability to field armored divisions for extended operations. Yet oil supplies may be necessary for the winter heating of civilian dwellings in urban areas. The ability of a regime to deprive its civilian population in favor of continued military capability makes the linkage even more painful. None of these real-world problems of ethics, law, and principle can be easily solved,[5] even while the law of armed conflict must maintain the ideals of discrimination and proportionality.

The legal texts that have accompanied these historical changes are worthy of note, as a preliminary matter. The Hague Rules of 1907 were modest in their scope, anticipating in the Martens Clause that a changing technology and the unsettled practice of States might make codification difficult.[6] The Hague Rules forbid pillage and attacks on undefended towns, and require sparing, "as far as possible," cultural and medical institutions. Arms "calculated to cause unnecessary suffering" were also banned. But some of the modern operational dilemmas lay beyond anticipation or consensus.

Operational targeting was incidentally addressed in the 1949 Geneva Conventions, through the establishment of protections for hospitals and neutralized zones for civilians who "perform no work of a military character," as well as the right of evacuation of children and aged persons from encircled areas.[7] But in the 1977 Geneva Protocols,[8] there was new attention both to a broader definition of proportionality and the nature of civilian targets. The effort was not altogether successful for Protocol I has been disputed in several of its features. The Protocol was signed but not ratified by the United States, and was excluded by the Security Council from the Statute of the International Criminal Tribunal for the former Yugoslavia as a direct source of law for the tribunal. Its formal definition of proportionality has been modified further in the Rome negotiations for a permanent international criminal court.

Article 51(b) of Protocol I deems an attack "indiscriminate" if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." The International Criminal Court (ICC) treaty limited the language, noting that military advantage is to be assessed in the context of an "overall" military campaign—allowing military commanders and operators to seek more distant, as well as immediate objectives.[9] A military advantage, for example, need not be "temporally or geographically related to the object of the attack."[10] In addition, the ICC treaty notes that the military commander breaches a criminal rule only where the

incidental loss of civilian life or injury to civilians is "clearly" excessive.[11] "Knowledge" is an essential element. The uncertainties of war are legendary, and the commander's assessment must be based on the information he has available at the time. Only where a commander, based on the information available to him at the time, "knew" the damage caused would be clearly excessive, is there a criminally culpable act.[12] This may include self-conscious knowledge of the breaching of a legal limit, as well as knowledge of the actual facts of the campaign. As noted by the committee of experts advising the prosecutor of the International Criminal Tribunal for the former Yugoslavia:

> It is much easier to formulate the principle of proportionality in general terms than it is to apply it to a particular set of circumstances because the comparison is often between unlike quantities and values. One cannot easily assess the value of innocent human lives as opposed to capturing a particular military objective.[13]

So, too, the text of the 1977 Protocol defining civilian objects was deemed incomplete by the Rome negotiators. Article 51(2) of Protocol I says, with apparent clarity, that the "civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited."[14] Article 52 prescribes that "civilian objects shall not be the object of attack or of reprisals," but notes, tautologically, that "[c]ivilian objects are all objects which are not military objectives as defined in paragraph 2."[15] The search for specificity is not greatly aided by the next bundle of negotiated language. Paragraph 2 of Article 52 notes broadly that "military objectives are limited to those objects which by their nature, location, 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."

The difficulties of definition were implicitly recognized in the Rome negotiations for the permanent international criminal court. The implementation of Article 51 noted the centrality of intention—requiring proof that a commander "intended" that civilians as such be "the object of the attack"—arguably requiring specific intent to cause such harm and knowledge of the legal status of the protected persons.

The Rome drafters also attempted to craft a criminal rule to implement Article 52, condemning attacks where the "object of the attack" was "civilian objects, that is, objects which are not military objectives."[16] But the difficulties of distinction in regard to dual-use assets is implicitly acknowledged elsewhere in Protocol I. In Article 54, starvation of civilians as a method of warfare is

prohibited, and it is equally prohibited to attack or destroy "objects indispensable to the survival of the civilian population" where the "specific purpose" is to deny them to the civilian population. But attack is concededly permitted where the asset is used in "direct support of military action," unless this would cause starvation or forced movement.

How do these principles apply to computer attacks and computer defense, in an age of cyberwarfare?

The requirement of discrimination between civilian and military objects presents a substantial challenge in cyberwarfare—complicated as well by the question of neutrality. If, in a defensive mode, the United States were the victim of an attack on vital computer systems, the temptation to respond in kind would be considerable. Yet the ultimate source of a computer attack can be acutely difficult to determine—a problem magnified by the deliberate use of "looping" or "weaving"—using another's server to disguise the origination of the attack. An attack is likely to be sent through an unrelated server in order to mask its authorship, and a response in kind may end up damaging or disabling the "looped" server. The intermediate servers may be largely dedicated to civilian functions, and may even be in a country other than the originator of the attack. Even where the retaliatory response successfully limits its impact to the ultimate point of origin, the counterattack may end up disabling civilian functions. The attacker can use a civilian platform for convenience or in order to mask State-sponsorship, even though the latter could qualify as perfidy.

In a world of real geography, it is simpler to frame a response to the problem of unauthorized use of platforms. A sovereign State is held responsible to police the misuse of its territory. An insurgent force cannot launch cross-border attacks with impunity, and one rationale for permitting a counterattack across the border is that the harboring State abandoned or was unable to discharge the duty to police its own soil. The same duty could be imposed on the proprietors of electronic space and governing civilian authorities. But the organization of cyberspace is in private hands, and has no single authoritative source of police. Misappropriation of a server can be accomplished quickly and secretly, and even if a server's vulnerability has been detected before, not every trespass on a server is worth preventing. Unless the involvement of a nation State is evident, say by advertising an available "free zone" for cyberpirates, a retaliatory response may be disputed.

In addition, it may be far harder to confine the effects of the counterattack than in a land-based response. Cyberspace counterattack is especially troublesome because the topography is unknown. The shape of cyberspace is truly *terra incognita*, including a server's network linkages to civilian structures. In a

conventional military campaign employing land forces or air attack against an adversary, the proximity of civilian structures and other protected objects can be mapped by surveillance aircraft, drones, or ground spotters. The information may be imperfect, and there may be no realistic way to avoid all incidental harm, but there is some relative idea of the likely consequences of an attack. A prepared target list or "bombing encyclopedia" is designed to permit estimates of probable civilian casualties. The method of approach to a target may be altered in some cases in order to minimize civilian harm should munitions go wide of the mark. But in cyberspace, there is often a rapidly changing architecture of linkage and control, and the attempt to intrude in order to map its geography may itself be detected and considered a hostile act. Nonetheless, one might be inclined to propose a defeasible duty of "benign" or "humanitarian" espionage—attempting to map cyberlinks in order to contain the consequences of a defensive counterattack. The technical feasibility of this is open to question, with the added difficulty that the very act of intrusion may be detected.

For any form of cyber counterattack, one necessary scruple may be to build firewalls into the very instrument of intrusion. Where it is not feasible to conduct benign mapping in advance, it may be conceivable to have the intrusion device map or filter as it goes, for example, by characterizing the content of files before it destroys them. This might help to distinguish between military and civilian objects linked to the same server. Another palliative may be to conceive of proportionality as a dynamic matter. Greater damage to civilian objects may be tolerated in order to eliminate a security threat, so long as the damage is reversible or, indeed, aid is given in its restoration.[17]

An additional problem in applying proportionality is the twilight between criminal acts and acts of war. In the midst of a major conflict fought by conventional means, any accompanying electronic attack will be regarded as a matter of utter gravity, justifying a strong response against the actor, even with ensuing collateral damage. But in a more ambiguous setting, for example, where a State actor is gathering information that would facilitate illicit entry and hostile operations, there is no predicate that provides a classical justification for the use of overwhelming force in response. To be sure, intrusions even by non-State actors, where they cause serious interference with vital operations or loss of life, would fit the ordinary understanding of terrorism. But Washington has chosen to emphasize the tools of criminal law in responding to most forms of terrorism, attempting to arrest and indict members of international networks, rather than treating them as combatants in an undeclared private war. Force is fully warranted to capture an international terrorist or thwart a planned attack, but criminal law creates a set of expectations that are often frustrating to an effectively

fought conflict. Criminal law withholds any justification of punitive force until after proof has been mustered in court and a verdict is rendered by an independent fact finder. Its proceedings are public, and the sources of evidence are often compromised during a trial by the public disclosure of the methods of surveillance. Proof beyond a reasonable doubt is an appropriate standard for protecting domestic liberty in a civil society. The extraordinary difficulty of detaining an individual offender is a worthy price to pay in order to preserve a libertarian political culture. But criminal law's demanding standards are founded on the assumption that civil society enjoys the underlying fidelity of the relevant actors. International politics and the security decisions of nation States must sometimes proceed on more ambiguous indicators.[18]

In addition, the invocation of criminal law creates the expectation that action taken abroad will defer to local State consent. Because criminal processes are public, any related government action abroad is likely to become known. Actions taken for intelligence purposes that do not enjoy the consent of the foreign territorial State may do especially grave damage to bilateral relations if they are broadcast. Thus, when invoked, the criminal law paradigm tends to dominate Washington's response to a situation, since all other modalities must be weighed in light of the cost of their public disclosure. (Sometimes it is the mere fact of publicity that will cause a foreign government to react strenuously to an international security measure out of a perceived affront to its public dignity or *amour propre.*)

Recent negotiations for a convention on cybercrime illustrate the point. Lengthy talks were conducted through the Council of Europe, with the participation of the United States, Canada, Japan, and Australia. The draft treaty requires each participating country to criminalize various forms of computer misuse, including deliberate denial of service through distributed network attacks, and to create real-time methods of preserving and gathering relevant proof.[19] This is especially important since tracing an attacker may be possible only while the attack is underway and the actor is still on line. One of the treaty's more controversial features would require Internet service providers to preserve information at the request of a State party. Nonetheless, a successful criminal inquiry will depend on the treaty cooperation of each country through which an attacker loops his communication. It will not take much sophistication for a cyber adversary to filter his messages through countries outside the treaty regime. Any direct response to the attack, through counterattack or disabling measure, may be resented by the treaty States in the loop as "derisive" of the treaty regime and discourage their later cooperation. Deference to the enforcement jurisdiction of local authorities is a premise of the treaty architecture, and

yet may be unworkable for intelligence operations and national security measures. Private hackers in Europe offered their services to Iraq during the Persian Gulf War, and, in a similar situation, the slow and deliberate processes of criminal law may not be adequate for infrastructure protection.

Even if there is a decision to treat State-sponsored cyber attacks as acts of war rather than crimes, it will remain difficult to identify these more serious incidents in a timely way. In biological warfare, it has recently been observed, it may be hard to distinguish the spread of natural pathogens from deliberate acts of contamination. The same difficulty can arise in distinguishing a prankster or technological sociopath from an international adversary. The difference is surely important in assessing whether the attack is likely to escalate as the diversionary prelude to other more deadly methods of warfare. The ambiguity of sponsorship that one saw in the surrogate conflicts of the Cold War is likely to plague cyber defense as well.

The dilemmas of civilian protection in cyber conflict are a circumstance to be lived with. Technology may solve some of the problems it has created. And the technological superiority of the United States in all modalities of conflict may mean that we can afford to accept some risk for the sake of maintaining a moral high ground. The best answer to the Solomonic cyber quandaries will require the continuing collaboration of technologists, warfighters, ethicists, and, lest we forget, experts in the law of war.

Notes

1. Thoughtful commentaries on the law of war and its relation to cyber conflict include Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); Mark Russell Shulman, Legal Constraints on Information Warfare, Occasional Paper No. 7, Center for Strategy and Technology, Air War College, Maxwell Air Force Base (March 1999); and Office of the General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (Nov. 1999). The latter paper is appended to this volume as the Appendix.

2. *See* SHELDON GLUECK, THE NUREMBERG TRIAL AND AGGRESSIVE WAR 105 (1946) ("Since the initiation and conduct of such a war of aggression is at least unlawful, all acts of warfare in pursuance thereof—whether they violate the laws and customs of war or do not do so—are illegal. They also become *criminal* in considering the effect of illegality upon the defense of 'justification' in criminal law.").

3. *See* Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 44(3), Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

4. The 1977 Protocols to the Geneva Conventions were criticized by some for the suggestion that guerrillas should only be required to distinguish themselves en route to an attack. *See* Colonel G.I.A.D. Draper, *The Status of Combatants and the Question of Guerrilla Warfare*, 1971 BRITISH

YEARBOOK OF INTERNATIONAL LAW 173, *reprinted in* REFLECTIONS ON LAW AND ARMED CONFLICTS: THE SELECTED WORKS ON THE LAWS OF WAR BY THE LATE PROFESSOR COLONEL G.I.A.D DRAPER, OBE (Michael Meyer and Hilaire McCoubrey eds., 1998).

5. It is worth recognizing that the law of war has both rules and principles—or, if you like, self-executing rules that require little interpretation, and others that are highly fact specific and context sensitive in their application. In a report of experts assessing the 1999 NATO bombing campaign in Yugoslavia, prepared for the prosecutor of the International Criminal Tribunal for the former Yugoslavia, it was noted that "[e]veryone will agree that a munitions factory is a military objective and an unoccupied church is a civilian object. When the definition is applied to dual-use objects which have some civilian uses and some actual or potential military use (communications systems, transportation systems, petrochemical complexes, manufacturing plants of some types), opinions may differ. The application of the definition [of civilian object] to particular objects may also differ depending on the scope and objectives of the conflict. Further, the scope and objectives of the conflict may change during the conflict." *See* Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, para. 37, www.un.org/icty/pressreal/nato061300. htm.

6. The Martens Clause noted that "[u]ntil a more complete code of the laws of war has been issued, the high contracting parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and from the dictates of public conscience." *See* Convention respecting the Laws and Customs of War on Land and Annex: Regulations respecting the Laws and Customs of War on Land, *in* PROCEEDINGS OF THE HAGUE PEACE CONFERENCES 620-631 (1920). This reunion of law and conscience may disturb positivists, but is not so dissimilar from the working sources of customary legal norms in other social contexts.

7. Convention Relative to the Protection of Civilian Persons in Time of War (Geneva IV), Aug.12, 1949, arts. 15, 18, and 19, 6 U.S.T. 3516, 75 U.N.T.S. 287 (entered into force Oct. 21, 1950; entered into force for the United States Feb. 2, 1956).

8. Protocol I, *supra* note 3, and Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 (entered into force Dec. 7, 1978).

9. Rome Statute of the International Criminal Court, art. 8(2)(b)(iv), U.N. Doc. A/CONF.183/9* (July 17, 1998) [hereinafter Rome Statute].

10. Report of the Preparatory Commission for the International Criminal Court, Finalized draft text of the Elements of Crimes, U.N. Doc. PCNICC/2000/1/Add.2 (Nov. 2, 2000), art. 8(2)(b)(iv), para. 2 and note 36.

11. Rome Statute, *supra* note 9, art. 8(2)(b)(iv).

12. Finalized draft text of the Elements of Crimes, *supra* note 10, art. 8(2)(b)(iv), para. 3 and note 37.

13. Final Report to the Prosecutor, *supra* note 5, para. 48.

14. This leaves open the question, however, whether diminishing civilian morale is a legitimate war aim.

15. Protocol I, *supra* note 3, art. 52.

16. *See* Rome Statute, *supra* note 9, art. 8(2)(b)(ii), and Elements of Crimes, *supra* note 10, art. 8(2)(b)(ii).

17. A "first strike" against an adversary's computer systems, as part of anticipatory self-defense, is another possibility that we may imagine. The disruption of a national computer network may disrupt an adversary's military communications, military mobilization, the processing of targeting information, and other vital military functions. But the attack may also present the same "dual server" problems discussed above. The same preventative measures of benign espionage and a

dynamic conception of proportionality (permitting greater damage with speedy restoration) may be called for.

18. War and peace entertain different standards for lethal force in enforcement measures. In civilian societies, the use of lethal force is generally limited to the prevention of immediate deadly harm, with a high threshold of knowledge. In a state of war, the threshold for using force is lower. The identification of combatants is made on the basis of information reasonably available in the situation. A foot soldier will rarely be expected to use the sparing rules of engagement of a civil policeman.

19. *See* Draft Convention on Cyber-Crime and Explanatory Memorandum Related Thereto, Council of Europe, European Committee on Crime Problems, Strasbourg, France, June 29, 2001, www.conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm and www.conventions.coe.int/Treaty/EN/projets/FinalCyberRapex.htm.