CHAPTER 22

International Law and Information Operations

Thomas C. Wingfield

FUTURE WARS will feature information operations with novel weapons, techniques, and targets. Such information operations and cyber attacks will raise unprecedented legal questions to discriminate the lawfully compliant from the negligent, reckless, or intentionally maleficent.

The multiple denial-of-service attacks carried out against Estonia in April and May 2007 provide a rich fact pattern to test the emerging law of information conflict. Three legal issues proved particularly problematic. First, it may be very difficult to determine what person, organization, or country is ultimately responsible for any given cyber intrusion. Computer forensics may quickly and reliably identify the last server used in a multiserver attack, but the first server, its operator, and owner may never be known. Second, it is difficult to measure, or even properly characterize, the damage done in a cyber attack. In Estonia, the immediate damage to specific systems was fairly limited and rarely rose above the level of inconvenience. The second-order effects, however—fear, loss of confidence in banking and communications systems, and a national awareness of vulnerability—could lead to even more enduring negative consequences than a limited military incursion. Third, Estonian, Russian, and American authorities demonstrated, by their comments, an uncertain grasp of the applicable rules of law, variously describing the Estonian attacks as criminal activity, covert operations, or military actions. Each of these would implicate different legal regimes and would demand widely divergent responses. Thus, there is a need for greater clarity and certainty with respect to the principles of law that apply in cyber conflict. That is the subject of this chapter.

A first distinction is between peacetime (*jus ad bellum*) standards regulating the resort to force and wartime (*jus in bello*) principles governing conduct in war. These two rule sets are quite different, and specific terms have different definitions under the peacetime and wartime regimes; deciding which of the two rule sets to apply is the first task of attorneys advising decisionmakers in nations under attack.

Jus ad Bellum: Standards Governing the Resort to Force

The first question in applying peacetime standards is to determine whether an information operation or cyber attack rises to the level of a "use of force" prohibited under international law. Ample precedent exists for answers where attacks involve kinetic means such as bombs and bullets, but the novelty of information operations, with its innovative digital weapons, modes of attack, and target lists, is more problematic.

Until recently, there were two broad schools of thought. The common sense approach postulated, quite reasonably, that the international legal regime was in place to keep operations short of war from escalating into full-blown wars, and to identify war-level activities as soon as possible so as to attach the appropriate legal protections to the participants. Under this premise, the simplest and most sensible approach to applying the kinetic legal regime to the digital battlefield was to disregard the means of attack and concentrate solely on the quantum of damage done. It should be immaterial whether a refinery was destroyed by a 2,000-pound bomb or by a line of malicious code in its pressure regulation subroutine; what did matter was the size of the hole left in the ground after the attack.

This quantitative approach had the benefit of simplicity, clarity, and logic, but it is inconsistent with the prevailing structure of international law, the United Nations (UN) Charter paradigm. Article 2, paragraph 4 of the UN Charter states, "All Members shall refrain in their international relations *from the threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[1]

Thus, a second approach followed the logic of the charter's framers to its literal conclusion: that anything other than an armed attack—something like the tanks-across-the-border threat the charter was written to address—was not prohibited by international law.[2] The quantity of force was less important than the quality of force: military coercion was discouraged, with a very low threshold for prohibited activity, while diplomatic, economic, or political coercion would not be discouraged by the UN Charter, because they amount to a peaceful alternative to war. This approach had the advantage of academic consistency and consonance with mainstream international legal thinking. Unfortunately, as a half-century-old legal theory, it failed to take into account the newly destructive capacities of what had once been mere messages and signals.

Michael Schmitt noted that "as the nature of a hostile act becomes less determinative of its consequences, current notions of 'lawful' coercive behavior by states, and the appropriate responses thereto, are likely to evolve accordingly."[3] Schmitt examined why the framers of the UN Charter chose to characterize each type of coercion as they did:

> In the current normative scheme the consequences of an act are often less important than its nature. For instance, a devastating economic embargo is not a "use of force" or an "armed attack" justifying forcible self-defense, even though the embargo may result in enormous suffering. On the other hand, a relatively minor, armed incursion across a border is both a use of force and an armed attack. This contrary result derives from the law's use of "acts" as cognitive shorthand for what really matters—consequences. Acts are more easily expressed (to "use force" versus to cause a certain quantum and quality of harm) and more easily discerned than an effects- based standard, based on the harm suffered. This cognitive shorthand does not work well in the age of information operations because information attacks, albeit potentially disastrous, may be physically imperceptible.[4]

Schmitt suggested, instead, applying a quantitative scale to seven factors that he specified in order to locate any given operation along a spectrum between prohibited and permitted. Schmitt thus translated the qualitative charter paradigm into its quantitative components, providing a useful framework for scholars and practitioners to organize analysis.

Schmitt's brief description of the importance or distinctiveness of each of the seven factors is fleshed out below with some additional questions that would satisfy the requirements of the factor. Three qualitative answers to each question range between relatively clear cases at each qualitative extreme, with a central area of uncertainty. Results for these seven factors are then averaged for an overall score to give an indication of an operation's qualitative status as a use of force under international law. Schmitt's work thus offers a structure for discussion of the Estonia case.

Severity

According to Schmitt, "Armed attacks threaten physical injury or destruction of property to a much greater extent than other forms of coercion. Physical well-being usually occupies the most basic level of the human hierarchy of need."[5] Results of attacks might be categorized by:

- people killed; severe property damage
- people injured; moderate property damage
- people unaffected; no discernible property damage.

In other words, one must ask: How many people were killed? How large an area was attacked (scope)? How much damage was done within this area (intensity)?

Immediacy

Schmitt writes, "The negative consequences of armed coercion, or threat there-of, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case."[6] One might assess immediacy as:

- seconds to minutes
- hours to days
- weeks to months.

In other words, what was the duration of the action? How soon were its effects felt? How long until its effects abate?

Directness

Schmitt's third criterion is directness: "The consequences of armed coercion are more directly tied to the *actus reus* [culpable act] than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty."[7] Results could range as follows:

- action sole cause of result
- action identifiable as one cause of result, and to an indefinite degree
- action played no identifiable role in result.

Another way to ask the question is: Was the action distinguishable from parallel or competing actions? Was the action the proximate cause of the effects?

Invasiveness

Schmitt next assesses the invasiveness of an attack:

> In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences,

the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability.[8]

Thus, one could categorize operations as:

- border physically crossed; action has point locus
- border electronically crossed; action occurs over diffuse area
- border not crossed; action has no identifiable locus in target country.

Did the action involve physically crossing the target country's borders? Was the locus of the action within the target country?

Measurability

A fifth standard is measurability:

While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force.[9]

Assessing measurability means putting operations into one of these categories:

- effects can be quantified immediately by traditional means (such as bomb damage assessment) with high degree of certainty
- effects can be estimated by rough order of magnitude with moderate certainty
- effects cannot be separated from those of other actions; overall certainty is low.

One might, therefore, ask how the effects of the action could be quantified, whether the effects of the action are distinct from the results of parallel or competing actions, and what the level of certainty was.

Presumptive Legitimacy

Next is the question of presumptive legitimacy:

In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion—again in the domestic and international sphere—are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).[10]

Presumptive legitimacy might be assessed as follows:

- action accomplished by means of kinetic attack
- action accomplished in cyberspace but manifested by a "smoking hole" in physical space
- action accomplished in cyberspace and effects not apparent in physical world.

Presumptive legitimacy thus depends on whether this type of action has achieved customary acceptance within the international community and whether the means are qualitatively similar to others presumed legitimate under international law.

Responsibility

Finally, Schmitt would examine the factor of responsibility:

> Armed coercion is the exclusive province of states; only they may generally engage in uses of force across borders, and in most cases only they have the ability to do so with any meaningful impact. By contrast, non- governmental entities are often capable of engaging in other forms of coercion (propaganda, boycotts, etc.). Therefore with armed coercion the likelihood of blurring the relative responsibility of the State, a traditional object of international prescription, and private entities, usually only the object of international administration, narrows. In sum, the consequences of armed coercion are more susceptible to being charged to the State actor than in the case of other forms of coercion.[11]

One may ask whether:

- responsibility for action is acknowledged by acting state; degree of involvement large
- target state government is aware of acting state's responsibility; public role unacknowledged; degree of involvement low
- action unattributable to acting state; degree of involvement low.

Is the action directly or indirectly attributable to the acting state? But for the acting state's sake, would the action have occurred?

Overall Analysis

Have enough of the qualities of a use of force been identified to characterize the information operation as a use of force that is prohibited under Article 2(4) of the UN Charter; as arguably a use of force or not; or as certainly not a use of force under Article 2(4)? These issues are illustrated by a recent case.

The Estonia Cyber Attack: A Prohibited "Use of Force" under International Law?

Under these criteria, did the cyber intrusions of April–May 2007 rise to the level of a use of force? Despite the widespread and continuing nature of the cyber attacks in Estonia, it appears that no one was killed or even wounded, nor was any tangible property destroyed, although a great deal of intangible property was lost. Assuming that economic value in euros

or dollars is a suitable means of comparing intangible and tangible property losses, the severity of the attack appears to be in the moderate range of Schmitt's severity scale.

The speed with which the attack developed, beginning precisely at the midnight separating May 8 (the date on which Western Europe and the United States celebrate the end of World War II in Europe) from May 9 (the date celebrated by Russia), shows high levels of immediacy for the onset of the attacks. It appears that only minutes, perhaps just seconds, passed between the initiation of the cyber attacks and their culmination against their targets. Furthermore, the attacks were intensified and moderated at least three times in response to Estonian reactions, demonstrating a very brief time lag between offensive tactical decisionmaking and the resulting effect on the targets. Immediacy, then, appears to be in the high range.

The directness of the attacks is difficult to characterize. In such denial- of-service attacks, anywhere from several hundred thousand to several million individually harmless requests for access combine to overwhelm a system. If the widely distributed botnets that enable such attacks are themselves controlled by a single actor, then it is appropriate to characterize that actor's initiation of the attack as the single cause.[12] The damage done to the targeted banks, newspapers, government offices, or public utilities is the direct effect of this cause. Since a relatively small number of actors affected a relatively small number of large, institutional systems, the directness of the attack would be considered moderate.

Invasiveness may be characterized as the physical crossing of a border, which in this case was low, or as the focusing of attacks inside the territory of a particular nation, which in this case was high. Although no identifiable forces violated Estonia's border, the exclusive locus of the attacks was in Estonia: its newspaper Web sites were defaced, its large banks were shut down, and its national emergency telephone system was interfered with for several hours. On balance, the invasiveness of the attack was moderate.

The measurability of the attacks was likewise difficult to evaluate. Although there were several large, clearly identifiable targets, and although many of these targets suffered quantifiable damage in revenue lost, there is a great uncertainty in quantifying the resulting loss of confidence in the integrity of commercial systems and the reliability of public infrastructures. As in terror attacks, the immediate target is of less value to the aggressor than the fear instilled in the wider population. Paradoxically, the confident, even defiant, response by the Estonian government, and the prompt support lent by the North Atlantic Treaty Organization and the European Union, may have left Estonia in a stronger technical, political, and moral position after the attacks than before. The challenge of measuring the damage done by cyber attacks is less a matter of determining the degree of damage than of deciding what to measure. Overall, then, the measurability of theses attacks was low.

The presumptive legitimacy of the Estonian attacks was low. While targets may have been selected with an eye toward reminding Estonia of Russia's vastly greater power, the attacks themselves were not of such size or complexity that they could only have been mounted by a nation-state. Investigators identified several botnets used in the attacks, and these were available for hire by any government, corporation, organized crime ring, political group, or even individual with adequate means to employ them. The wide availability of this means of attack, and the common nature of these means, results in a low presumptive legitimacy rating.

Finally, the element of responsibility is low. It may be that the Russian government participated in, or even directed, the attacks, but it did not claim responsibility for them. Such a claim is a prime discriminator between military and nonmilitary actions. The Russian government was either uninvolved or chose to hide its role in the attacks. In either case, an

immediate or emphatic claim of national responsibility was absent.

The overall picture, then, is one factor in the high range (immediacy), three factors in the moderate range (severity, directness, and invasiveness), and three factors in the low range (measurability, presumptive legitimacy, and responsibility). This suggests that the attacks were quantitatively damaging enough, or qualitatively "military" enough, to be properly characterized under international law as uses of force.

There are two caveats to this conclusion. First, this analysis was performed on the attacks of April–May 2007 and not on any larger campaign by Russia against Estonia. Enlarging the scope of the analysis could identify a strategic use of force that comprised multiple elements that were, individually, below that threshold. Second, such actions in cyberspace, regardless of their initiator, are clearly unlawful because of their end result—destruction of property (whether tangible or intangible) or blocking access to emergency services, to give only two examples, would be illegal based on Estonian, U.S., or Russian law, regardless of the instrumentality employed. They also are potentially threatening to international peace and security, and, to the extent committed or permitted by a state, they are a violation of the UN Charter. Although they do not rise to the level of a use of force, this does not render them permissible; it merely requires that the initial response be other than military. Whether that response takes the form of a lawsuit, an arrest, a diplomatic offensive, or a covert operation is the choice of the victim state.

Jus in Bello: International Law on the Conduct of War

The novelty of many information operations—their targets, means, even "shooters"—has led to a great deal of confusion about what kind of conduct is lawful under the rules of war. It took many centuries to develop the certainty applicable to kinetic operations; as weapons evolved, their effects became different in degree but not kind. Certain information operations still fit this paradigm: the kinetic "kill" of a radio transmitter or the destruction by a special operations team of a computer complex would involve no new intellectual challenges. However, civilian contractors emplacing and then triggering a trojan horse in another country's governmental mainframe computer would raise a host of new issues: the action's character as mere espionage or the first stage of a full-blown military action, the contractors' status as combatants or civilians accompanying the military or purely private actors, and the degree of attributability of the contractors' actions to the contracting government, to name just a few.

To the extent these actions are properly characterized as military operations, traditional principles of the law of armed conflict apply: belligerents must distinguish between combatants and noncombatants, must avoid targeting civilians and civilian property, and must take all reasonable precautions against injuring civilians or damaging their property in the course of striking military targets. The *Commander's Handbook on the Law of Naval Operations* captures this rule as three interrelated proscriptions: "1. The right of belligerents to adopt means of injuring the enemy is not unlimited. 2. It is prohibited to launch attacks against the civilian population as such. 3. Distinctions must be made between combatants and noncombatants, to the effect that noncombatants be spared as much as possible."[13] The authoritative articulation of this principle under international law is found in the Geneva Conventions: "In order to ensure respect for and protection of the civilian population and between civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[14]

In war, combatants and other military objectives are, under these rules, lawful targets. Combatants are defined as:

> those persons who have the right under international law to participate directly in armed conflict during hostilities . . . includ[ing] all members of the regularly organized armed forces of a party to a conflict . . . [as well as] irregular forces who are under responsible command and subject to military discipline, carry their arms openly, and otherwise distinguish themselves clearly from the civilian population.[15]

However, "medical personnel, chaplains, civil defense personnel, and members of the armed forces who have acquired civil defense status" are not counted as combatants.[16]

Military objectives that may lawfully be attacked include:

> Combatants and those objects which, by their nature, location, purpose, or use, effectively contribute to the enemy's warfighting or war sustaining capability and whose total or partial destruction, capture, or neutralization would constitute a definite military advantage to the attacker under the circumstances.[17]

Noncombatants and civilian objects are unlawful targets:

> The term noncombatants may, however, also embrace certain categories of persons who, although members of or accompanying the armed forces, enjoy special protected status, such as medical officers, corpsmen, chaplains, technical (i.e., contractor) representatives, and civilian war correspondents…The term is also applied to armed forces personnel who are unable to engage in combat because of wounds, sickness, shipwreck, or capture.[18]

Civilian objects that are not lawful targets include "all civilian property and activities other than those used to support or sustain the enemy's warfighting capability." Specifically, for example, it is unlawful to destroy "food, crops, livestock, drinking water, and *other objects indispensable to the survival of the civilian population*, for the specific purpose of denying the civilian population of their use."[19]

Weapons that cannot be used in such a way as to discriminate between lawful and unlawful targets are themselves unlawful, under the doctrine of indiscriminate effect.[20] As this prohibition is explained by the *Commander's Handbook on the Law of Naval Operations*, "any weapon may be set to an unlawful purpose when it is directed against noncombatants and other protected persons and property."[21]

Although the concept of indiscriminate effect and the distinction between the armed forces and the civilian populace are clear in theory, their application to real-world targeting issues can become hazy and complex. This is clearly true in the world of information operations, where "shooters" rarely "see" their targets, where interconnected, dual-use infrastructures support civilian customers and military users, and where unintentional secondary and tertiary effects can cause results unforeseeable, or at least unforeseen, by the attacker. Separating military targets from civilian sites presents a special problem in intelligence collection, legal analysis, and operational execution.

The increasing interconnectedness of information systems vital to a nation's critical

infrastructure, and the special reliance placed by developing countries on the dual use of such systems, renders discrimination far more complex in cyberspace than in physical space. There are two keys to following the prescriptions of international law. First, an attacker must gather finely sifted intelligence so that competent decisions can be made regarding which computers or, indeed, which programs within computers, are lawful targets.

Second, information weapons sufficiently precise to attack specifically selected cybernetic targets must be developed. While a nondiscriminating approach would remain perfectly lawful for an attack against a standalone system, a more discriminating attack would have to be mounted against a system of systems, if the attacker wishes to comply with international law and prevent unanticipated secondary and tertiary consequences far more destructive than the primary attack.

The concept of military necessity, more quantitative than qualitative, limits the force that may lawfully be used: "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 with a minimum expenditure of time, life, and physical resources may be applied."[22]

Excessive force beyond that required to accomplish a lawful mission is unlawful. In addition, infliction of unnecessary suffering is prohibited; this proscription was "first applied very narrowly, to poisons, burning agents, or bullets of a certain size, shape, or composition."[23] However, approaches to limiting unnecessary suffering have become more broadly categorical.[24]

Just as the principle of necessity prohibits the use of excess force against combatants, the complementary principal of proportionality limits the effects of an attack against noncombatants.[25] While the principle of discrimination prohibits attacks against civilians per se, "it is not unlawful to cause incidental injury to civilians, or collateral damage to civilian objects, during an attack upon a legitimate military target."[26] The principle of proportionality, however, prohibits those attacks that "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."[27] This prohibition is expressed as a balancing test between the anticipated "concrete and direct" military advantage on one hand, and the expected civilian losses on the other.[28] As the value of a potential target increases, so does the level of permissible collateral damage. A corollary of this principle, stated in article 57 of protocol I of the Geneva Protocols, is that "commanders must take all reasonable precautions, taking into account military and humanitarian considerations, to keep civilian casualties and damage to the minimum consistent with mission accomplishment and the security of the force."[29]

These decisions must be based on an "honest and reasonable estimate of the facts,"[30] available at the time the decision is made. The International Committee of the Red Cross (ICRC) explicates the standard as:

> [T]he identification of the objective, particularly when it is located at a great distance, should be carried out with great care. Admittedly, those who plan or decide upon such an attack will base their decision on information given them, and they cannot be expected to have personal knowledge of the objective to be attacked and of its exact nature. However, this does not detract from their responsibility, and in case of doubt, even if there is only a slight doubt, they must call for additional information and if need be give orders for further reconnaissance…The evaluation of the information

obtained must include a serious check of its accuracy.[31]

A commander must consider whether to adopt an alternative method of attack, if reasonably available, to reduce civilian casualties and damage.[32]

Schmitt cites the three ways in which proportionality is frequently violated: a lack of full knowledge as to what is being hit; the inability to surgically craft the amount of force being applied to the target; and the inability to ensure the weapon strikes precisely the right point.[33] The calibration of force has been almost completely refined with modern technology, and the ability to steer toward a selected target is scarcely less advanced. The lack of complete intelligence, however, has been and will remain a problem. From the al Amariyah bunker in Baghdad to the Chinese embassy in Belgrade, examples abound of high-technology weapons being guided with flawless precision to an inappropriate target.

These issues have even greater application in cyberspace, where it may be extremely difficult to distinguish the code in a computer that governs delivery of electrical power to an early warning radar (which may be a lawful target of a cyber attack) from the code that controls power to a hospital intensive care unit. The risk of unintended consequences complicates the targeting picture. In cyberspace, the principle of proportionality may call for a fidelity and granularity of intelligence collection and analysis beyond current demonstrated capabilities, and may also call for modeling and simulation of attacks to give the commander at least minimal assurances that the attack will hit the intended target and not produce unlawful collateral damage.

Ruses and Treachery

The traditions of chivalry have informed the development of the principles of discrimination, necessity, and proportionality, applying to such issues as the protections accorded noncombatants and the amount of damage that may be done in "just" pursuit of a military objective. The chivalric code remains most unchanged in the distinction between lawful ruses and unlawful or "treacherous" perfidy, and these distinctions are particularly applicable to understanding what information operations are lawful in war.

Schmitt describes the standard: treachery is "a breach of confidence by an assailant." However, he points out:

> [O]ne must be careful not to define treachery too broadly. Use of stealth or trickery, for instance, is not precluded, and will not render an otherwise lawful killing [unlawful]. . . . Treachery exists only when the victim possessed an affirmative reason to trust the assailant. . . . [Lawful] ruses are planned to mislead the enemy, for example, by causing him to become reckless or choose a particular course of action. By contrast, [unlawful] perfidy involves an act designed to convince the enemy that the actor is entitled to protected status under the law of war, with the intent of betraying that confidence. Treachery, as construed by early scholars, is thus broader than the concept of perfidy; nevertheless, the same basic criteria that are used to distinguish lawful ruses from unlawful ruses can be applied to determinations of treachery.[34]

The criteria for discriminating lawful ruses from unlawful perfidy are essential to understanding what types of information operations are lawful or unlawful. The modern military

effort involves attempts to limit the physical violence of war by affecting the analysis and options of the opposing commander, for example, by persuading an opponent that it is surrounded, or that the arrival of a superior force is imminent when it is not. These are practically a synonym for "ruses of war." Precisely what in the realm of information operations is permissible and what is not, given the almost unlimited technical capabilities on the horizon, may be the principal legal question of operational military lawyers in the next century.

These criteria arise out of the European chivalric system, which was based on a complex network of personal obligations, especially the trustworthiness of knights, but it was loyalty of a precisely defined form. "Where no prior agreement was involved . . . surprise and guile might be considered perfectly legitimate. Low cunning was not itself dishonorable; what brought shame was perjury of an oath promising to abstain from certain acts."[35] For example, when "a party of armed knights gained entrance to a walled town by declaring themselves allies and then proceeded to slaughter the defenders, chivalry evidently was not violated, no oath having been made to the burghers."[36]

This doctrine slowly evolved from the end of the Middle Ages to the beginning of the modern era. Balthazar Ayala, a 16th-century commentator, proposed that a general duty to avoid treachery existed, whether or not a specific understanding existed between aggressor and defender. The key for Ayala was a distinction between permissible "trickery," similar to our understanding ruses of war, and impermissible "frauds and snares."[37]

Alberico Gentili, in the early 17th century, extended the concept of treachery to include not just those who took advantage of a reasonably placed trust in safety, but also those who encouraged or commissioned violations of that trust.[38] His contemporary, Hugo Grotius, removed the presumption of legality for acts perpetrated by the "just" party in a conflict, eliminating an excuse for atrocious behavior by those claiming their cause of war was just.[39] Later commentators, such as Vattel and Lieber, would sharpen and refine this doctrine, but Grotius' analysis of the distinction between ruses of war and perfidy is virtually indistinguishable from the modern standard. That standard is codified in article 37 of protocol I of the Geneva Conventions:

> It is prohibited to kill, injure or capture an adversary by resort to perfidy. Acts inviting the confidence of an adversary to lead him to believe he is entitled to, or is obligated to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence, shall constitute perfidy.[40]

Stratagem is a term encompassing both ruses of war and perfidy; it is addressed by the three principal U.S. reference manuals on the operational aspects of the law of war.[41] The U.S. Army manual states that among permitted stratagems are "ruses of war and the employment of measures necessary for obtaining in- formation about the enemy and the country are considered permissible."[42] Goodfaith is required in all dealings with the enemy, except those that the enemy can reasonably foresee and against which it can reasonably defend.[43]

This suggests that a key question for information operations is the breadth of the measures against which the enemy is expected to protect himself. If the area is broadly drawn, defining one such area as to "protect all computer systems from all intrusion," then the enemy is on constructive notice against almost any conceivable computer network attack. If, however, one defines the duty to protect as applying to more narrowly defined systems or against more narrowly defined techniques, then this aspiration toward good faith may be violated.

For example, suppose a nation sought to conduct psychological operations, perhaps

including false statements alleging an enemy dictator's scandalous personal conduct, and, using a new technology, inserted this information into the Cable Network News data stream reaching every TV set in the enemy country.[44] If a broad definition of *psychological operations* is accepted, then any psychological operation would be one against which the enemy could be expected to defend itself. If a narrow definition is chosen, perhaps limited to known technologies, then the duty of good faith would be violated because the enemy would not be protecting his civilian television system from "attack." On the other hand, where such targets and techniques were widely discussed in the open press, one could argue that the enemy was on constructive notice to protect any system now susceptible to attack. This type of notice would satisfy the rule's requirement for good faith in these operations.

U.S. Army Field Manual 27–10, *The Law of Land Warfare*, addresses treachery and perfidy: "Ruses of war are legitimate so long as they do not involve treachery or perfidy on the part of the belligerent resorting to them. They are, however, forbidden if they contravene any generally accepted rule."[45] The paragraph closes with the reason behind the rule: "Treacherous or perfidious conduct in war is forbidden because it destroys the basis for a restoration of peace short of the complete annihilation of one belligerent by the other."[46] This explanation is consistent with the article 37 definition from protocol I of the Geneva Conventions, prohibiting killing, injuring, or capturing an adversary "by resort to perfidy."

The U.S. Army manual provides a long list of permissible ruses, including: "surprises, ambushes, feigning attacks, retreats, or flights, simulating quiet and inactivity, use of small forces to simulate large units, transmitting false or misleading radio or telephone messages, [and] deception of the enemy by bogus orders purporting to have been issued by the enemy commander."[47] The Navy and Air Force manuals have similar lists.[48] On the Air Force list, the most important for the law of information conflict is the "imitation of enemy signals," a category under which many information operations could be accurately placed. The Air Force manual explains that:

> no objection can be made to the use by friendly forces of the signals or codes of the adversary. The signals or codes used by enemy aircraft or by enemy ground installations in contact with their aircraft may properly be employed by friendly forces to deceive or mislead an adversary. However, misuse of distress signals or distinctive signals internationally recognized as reserved for the exclusive use of medical aircraft would be perfidious.[49]

Camouflage is sometimes lawful, including disguising a military objective as a civilian object. The important distinction, for the purposes of likenesses that may be appropriated for ruses of war, is between protected symbols, discussed below, and ordinary civilian objects. It can be unlawful to use identifying devices improperly.[50] The Army manual says that: "[I]t is especially forbidden to make improper use of a flag of truce, of the national flag, or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention."[51] These insignia are protected because they directly induce the reliance of the enemy, and endanger those who legitimately rely on such symbols for protection.[52] The Army manual prohibits misuse of flags of truce,[53] of Geneva Convention symbols, such as the emblem of the Red Cross,[54] and of national flags, insignia, and uniforms.[55] The rationale is to avoid dilution of the absolute nature of these symbols, reinforcing the legal protections they bestow and the legal obligations they exact. The use of these protected symbols in information

operations would be included in the general prohibition.

It has been argued that "analogy 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—where such a message might be permissible without perfidious labels."[56] However, this statement incorrectly equates two kinds of information attacks. Such a message purporting to be the ICRC is clearly perfidious, in that it delivers a weapon under the protection of the Red Cross symbol—an action analogous to delivering a car bomb in an ambulance. The second, however, is clearly lawful, in that Microsoft Corporation enjoys no protected status under international law: a message from Microsoft would be no different from a message from any other firm with which a belligerent is doing business, although it might violate national laws or treaties intended to limit spam, viruses, and the like. The analogy here would be a commando team emplacing a bomb in enemy headquarters while disguised in the coveralls of a local plumbing company.

Intelligence operations in wartime—whether information-gathering (espionage) or destruction of property (sabotage)—are governed by two legal principles. One defines who, under international law, is a spy:

> A spy is someone who, while in territory under enemy control or the zone of operations of a belligerent force, seeks to obtain information while operating under a false claim of noncombatant or friendly forces status with the intention of passing that information to an opposing belligerent.

The definition applies to "members of the armed forces who penetrate enemy-held territory in civilian attire or enemy uniform to collect intelligence," but "personnel conducting reconnaissance missions behind enemy lines while properly uniformed are not spies;" nor are "crewmembers of warships and military aircraft engaged in intelligence collection missions in enemy waters or airspace. . . . unless the ship or aircraft displays false civilian, neutral, or enemy markings."[57]

There is no clear consensus on the application of the term "zone of operations of a belligerent force" to cyberspace. Until clearly distinguishable norms arise, it is probably best to apply, as closely as possible, the standards of the physical world by analogy.

The second legal principle regulates treatment of a captured spy. Cyber "entries" into and "exits" from the enemy country were not contemplated in the formulation of this rule of law and do not appear to provide the basis for liability. However, not all information operations are mounted from outside enemy borders, and those that require physical entry to enemy territory, and that could be characterized as intelligence operations, will expose the operator to traditional liability.

In summary, whatever use is made of the enemy commander's information environment, the techniques employed must resemble or be analogous to the Army list of permissible ruses, or the Navy or Air Force equivalents. Although there are exceptions due to specific circumstances, the general rule is that military forces may masquerade as civilians or civilian objects until engaging in hostilities, but they may not use protected symbols (such as the Red Cross or the UN flag) in any way that would induce the enemy's detrimental reliance or dilute the effect of those symbols and the safety of those depending on their protection.

Conclusion

A review of the international law governing information operations leads to several provisional conclusions. First, it is imperative to actually identify the governing body of law. There are three overlapping legal regimes—law enforcement, intelligence collection, and military operations—that may apply to any given activity in cyberspace. Each of these legal regimes operates at multiple levels: in addition to international law (treaty and customary), there is the domestic law of the United States (Federal and state), that of the target nation, and that of any intermediate nation through which an operation is routed. This creates a Rubik's Cube of potential liability that must be solved at the threshold of any information operation.

Second, determining the military nature of an information operation is crucial to fashioning an appropriate response. Here, the seven factors of the Schmitt analysis (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) offer a principled means of determining if an intrusion rises to the level of a "use of force" or an "armed attack" under international law, or if it is merely a criminal act.

Third, if an information operation is sufficiently destructive to be considered an armed attack, then the response must be guided by the four customary principles of the law of armed conflict: discrimination, necessity, proportionality, and chivalry. These principles, while formulated for application in the kinetic world, apply equally well to the results of information operations. They provide clarity for combatants wishing to mount a robust defense without themselves becoming war criminals.

These conclusions are, in reality, merely points of departure for even more thorough analyses in the years ahead. As new weapons and tactics are developed, as new organizations are designed and created, and as an increasingly professional corps of information operators are recruited and trained, clarity on these legal issues will provide the greatest operating space and the largest number of options for military commanders and political decisionmakers in the future.

---

[1] "Charter of the United Nations," United Nations Web site, available at <www.un.org/aboutun/charter/>; emphasis added.
[2] Ibid., article 51. "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."
[3] Michael N. Schmitt, "Bellum Americanum: The U.S. View of Twenty-first Century War and Its Possible Implications for the Law of Armed Conflict," *Michigan Journal of International Law* 19 (1998), 1051.
[4] Ibid.
[5] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37 (1999), 887, at 914–915.
[6] Ibid.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] See the discussion of botnets in chapter 7 of this volume, "Information Security Issues in Cyberspace," and chapter 18, "Cyber Crime."
[13] Department of the Navy, NWP 1–14M, *The Commander's Handbook on the Law of Naval Operations* (Newport, RI: Naval War College, 1995), sec. 8.1 (hereafter *Commander's Handbook*). See also Department of the Army, Field Manual 27–10, *The Law of Land Warfare* (Washington, DC: Department of the Army, 1956); and Department of the Air Force, AFP 110–31, *International Law—The Conduct of Armed Conflict and Air Operations* (Washington, DC: Department of the Air Force, 1993), secs. 5–3, 11–2.
[14] "Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of

International Armed Conflicts," art. 48, December 12, 1977, 1125, in *Documents on the Laws of War*, ed. Adam Roberts and Richard Guelff (London: Oxford University Press, 1989); hereafter Geneva Protocol.

[15] *Commander's Handbook,* 109, at sec. 5.3

[16] Ibid. This distinction is critical to the laws distinguishing permissible "ruses" from impermissible treachery, discussed below.

[17] *Commander's Handbook*, sec. 8.1.1. It goes on to list lawful targets: Proper targets for naval attack include such military objectives as enemy warships and military aircraft, naval and military auxiliaries, naval and military bases ashore, warship construction and repair facilities, military depots and warehouses . . . lines of communication and other objects used to conduct or support military operations.
. . . Proper naval targets also include geographic targets, such as a mountain pass, and buildings and facilities that provide administrative and personnel support for military and naval operations such as barracks, communications and command and control facilities, headquarters buildings, mess halls, and training areas. Also lawful as "economic targets" would be "enemy lines of communication
. . . industrial installations producing war-fighting products, and power generation plants. Economic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability may also be attacked."

[18] Ibid., sec. 5.3.

[19] Ibid., sec. 8.1.2.

[20] Geneva Protocol I, arts. 51, para. 4(b), and 51, para. 5.

[21] *Commander's Handbook,* secs. 9.1–9.1.2. However, a "weapon is not indiscriminate simply because it may cause incidental or collateral civilian casualties, provided such casualties are not foreseeably excessive in light of the expected military advantage to be gained."

[22] Ibid., sec. 5.2. It quotes a seminal elaboration on this definition from *The Hostages Case (United States v. List et al.)*, 11 TWC 759, 1253–54 (1950): The destruction of property to be lawful must be imperatively demanded by the necessities of war. Destruction as an end in itself is a violation of international law. There must be some reasonable connection between the destruction of property and the overcoming of the enemy forces. It is lawful to destroy railways, lines of communication, or any other property that might be utilized by the enemy . . . [even] [p]rivate homes and churches . . . if necessary for military operations. It does not admit the wanton devastation of a district or the willful infliction of suffering upon its inhabitants for the sake of suffering alone.

[23] Schmitt, "Bellum Americanum," 1084.

[24] *Commander's Handbook,* sec. 9.1.2 (emphasis added): "Antipersonnel weapons are designed to kill or disable enemy combatants and are lawful notwithstanding the death, pain, and suffering they inflict. *Weapons that are designed to cause unnecessary suffering or superfluous injury are, however, prohibited* because the degree of pain or injury, or the certainty of death they produce is needlessly or clearly disproportionate to the military advantage to be gained by their use."

[25] See generally William J. Fenrick, "The Rule of Proportionality and Protocol I in Conventional Warfare," *Military Law Review* 98 (1982), 91; and Judith G. Gardam, "Proportionality and Force in International Law," *American Journal of International Law* 87 (1993), 391.

[26] *Commander's Handbook,* sec. 8.1.2.1.

[27] Geneva Protocol I, arts. 51, para. 5(b,) and 57, para. 2(a)(iii).

[28] Robert G. Hanseman, "The Realities and Legalities of Information Warfare," *Air Force Law Review* 42 (1997), 173, at 182: "The military advantage gained by attacking military structures is generally minuscule compared to the resulting loss of human life and culture, and thus runs afoul of proportionality. This is why attacking hospitals, schools, religious structures and other cultural institutions is banned [under the doctrine of discrimination], unless the enemy is taking advantage of the situation by hiding military assets there."

[29] Geneva Protocol I, arts. 51, para. 5(b), and 57, para. 2(a)(iii); quotation from *Commander's Handbook,* sec. 8.1.2.1.

[30] *Commander's Handbook,* sec. 8.1.2.1.

[31] The International Committee of the Red Cross (ICRC), Commentary on Protocol I, at 680–681.

[32] *Commander's Handbook,* sec. 8.1.2.1.

[33] Schmitt, "Bellum Americanum," 1080.

[34] Michael N. Schmitt, "State-Sponsored Assassination in International and Domestic Law," *Yale Journal of International Law* 17 (1992), 609, 617.

[35] Michael Prestwich, *Armies and Warfare in the Middle Ages: The English Experience* (New Haven, CT: Yale University Press, 1996), 128.

[36] Barbara Tuchman, *A Distant Mirror: The Calamitous 14th Century* (New York: Knopf, 1978), 64.

[37] Balthazar Ayala, *Three Books on the Law of War and the Duties Connected with War and on the Military*

Discipline, in *The Classics of International Law*, trans. J. Bate (Washington, DC: Carnegie 1933; reprint Buffalo, NY: Hein, 1995), 84–85. See also Schmitt, "State-Sponsored Assassination," 614.

[38] Alberico Gentili, "De Iure Belli Libre Tres," in *The Classics of International Law*, vol. 16, trans. John Rolfe (Washington, DC: Carnegie 1933), 168. See also Schmitt, "State-Sponsored Assassination," 615.

[39] Hugo Grotius, *The Law of War and Peace*, in *The Law of War: A Documentary History*, ed. Leon Friedman (New York: Random House, 1972), 39.

[40] Geneva Protocol I, arts. 51, para. 5(b), and 57, para. 2(a)(iii). Protocol I offers four examples of perfidious behavior: "1. feigning a desire to negotiate under a truce or surrender flag; 2. feigning incapacitation by wounds or sickness; 3. feigning civilian, noncombatant status; 4. feigning protected status by the use of signs, emblems or other uniforms of the United Nations, neutral states, or other states not party to the conflict." Schmitt expands as follows: "Offering a bounty, equivalent to a ransom, is treacherous. So, too, is launching an attack in civilian clothes, unless the enemy is not deceived by or does not rely upon the civilian clothing worn by the attacker." Schmitt, "State-Sponsored Assassination," 635–639. See also 1907 Hague Convention IV, Customs of War on Land, art. 23, para F.

[41] *The Law of Land Warfare*, 22–23; *Commander's Handbook*, secs. 12.1–12.10; *International Law—The Conduct of Armed Conflict and Air Operations*, 8–1 to 8–5. An excellent distillation of the rules is Ashley J. Roach, "Ruses and Perfidy: Deception during Armed Conflict," *University of Toledo Law Review* 23 (1992), 395. See also Mary T. Hall, "False Colors and Dummy Ships: The Use of Ruse in Naval Warfare," *Naval War College Review* 42, no. 3 (Summer 1989), 52–62.

[42] *The Law of Land Warfare*, 22.

[43] Ibid., 22: Absolute good faith with the enemy must be observed as a rule of conduct; but this does not prevent measures such as using spies and secret agents, encouraging defection or insurrection among the enemy civilian population, corrupting enemy civilians and soldiers by bribes, or inducing the enemy's soldiers to desert, surrender, or rebel. In general, a belligerent may resort to those measures for mystifying or misleading the enemy against which the enemy ought to take measures to protect himself.

[44] Such an operation would not be mounted by the United States, which scrupulously adheres to a policy of disseminating selected facets of the truth in its psychological operations. The United States would mount such an operation only if the allegations were grounded in fact.

[45] *The Law of Land Warfare*, 22: The line of demarcation between legitimate ruses and forbidden acts or perfidy is sometimes indistinct, but the following examples indicate the correct principles. It would be an improper practice to secure an advantage of the enemy by deliberate lying or misleading conduct which involves a breach of faith, or when there is a moral duty to speak the truth. For example, it is improper to feign surrender so as to secure an advantage over the opposing belligerent thereby. So similarly, to broadcast to the enemy that an armistice has been agreed upon when such is not the case would be treacherous. On the other hand, it is a perfectly proper ruse to summon a force to surrender on the ground that it is surrounded and thereby induce such surrender with a small force.

[46] Ibid.

[47] Ibid., 22–23. Also permitted are "use of the enemy's signals and passwords, pretending to communicate with troops or reinforcements which have no existence, deceptive supply movements, deliberate planting of false information . . . removing unit identifications from uniforms, use of signal deceptive measures, and psychological warfare activities."

[48] *Commander's Handbook*, arts. 51, para. 5(b), and 57, para. 2(a)(iii), similarly lists, as permitted, "camouflage, deceptive lighting . . . false intelligence information, electronic deceptions, and utilization of enemy codes, passwords, and countersigns" and "allowing false messages to fall into enemy hands."

[49] *International Law—The Conduct of Armed Conflict and Air Operations*, 8–2.

[50] *The Law of Land Warfare*, 23. See also *Commander's Handbook*, secs. 12.2–12.5. Although land and ground forces are prohibited from using neutral flags, insignia, or uniforms, naval forces are permitted more latitude before hostilities commence; they may "fly false colors and disguise its outward appearance in other ways. . . . However, it is unlawful for a warship to go into action without first showing her true colors. Use of neutral flags, insignia, or uniforms during an actual armed engagement at sea is, therefore, forbidden."

[51] *The Law of Land Warfare*, 23.

[52] *See Commander's Handbook*, secs. 12.6, 12.7. For the same reason, feigning distress in order to attack a rescuing enemy, and falsely claiming noncombatant status, are perfidious and punishable as war crimes. See also Michael Bothe, Karl Josef Partsch, and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts* (The Hague, Boston, London: Martinus Nijhoff Publishers, 1982), 207: "It would be a legitimate ruse to use the electronic transponder aboard a combatant aircraft to respond with the code used for identifying friendly aircraft (IFF), but it

would be perfidious to use for this purpose the electronic signal . . . for the exclusive use of medical aircraft . . . [or] distress signals established under the Radio Regulations of the International Telecommunication Union."

[53] *The Law of Land Warfare*, 23.

[54] Ibid. Paragraph 55 prohibits using personnel, vehicles, and facilities displaying these symbols "for cloaking acts of hostility."

[55] Ibid. Paragraph 54 states: "It is certainly forbidden to employ [another's flag, insignia, or uniform] during combat, but their use at other times is not forbidden."

[56] Mark R. Schulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1999), 939, 959.

[57] *Commander's Handbook*, sec.12.8.