THE LEGAL STATUS AND RESPONSIBILITIES OF PRIVATE INTERNET USERS UNDER THE LAW OF ARMED CONFLICT: A PRIMER FOR THE UNWARY ON THE SHAPE OF LAW TO COME

MICHAEL H. HOFFMAN*

> When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. The United States reserves the right to respond in an appropriate manner. The United States will be prepared for such contingencies.[1]

INTRODUCTION

The terms cyber-crime and cyber-terrorism have gained currency over the past decade. Most forms of Internet misconduct tend to be categorized as cyber-crime. Manipulations involving cyberspace that might have lethal consequences (e.g. hacking into the control system for a dam to unleash a flood) and large denial of service attacks are characterized as cyber-terrorism. Nevertheless, there are times when hostile use of the Internet by state actors might not inherently constitute criminal behavior. Even when consequences could prove life threatening, these acts might not be deemed to constitute terrorism. These would be situations where the Internet has been turned into a virtual battlefield, thus regulated by the law of armed conflict and breaches of law punishable as war crimes.

Assumptions offered here are qualified in that they look at future scenarios, but they are all realistic. If these assumptions are correct, then avid private users of the Internet (meaning those who are using the Internet in a personal rather than governmental capacity) need to be aware that their online activities may have consequences, legal and otherwise, that go far beyond anything they may have imagined. Efforts to provide virtual

---

* Michael H. Hoffman is an attorney with nearly twenty-years of private, public, civil, and military experience as a practitioner in the law of armed conflict. He has written extensively on legal aspects of terrorism, peacekeeping and peace enforcement, humanitarian assistance, and armed conflict. He can be reached via e-mail at michhof@comcast.net.

1. White House, National Security Strategy to Secure Cyberspace (2003), *available at* www.whitehouse.gov/pcipb [hereinafter National Security Strategy].

solidarity with a foreign nation, or with a far away cause that has captured their sympathy may, in the end, lead to capture and detention as a prisoner of war or worse. Likewise, cyber-conduct that private Internet users may regard as a patriotic gesture in support of their nation could, conceivably, transform them into combatants and possibly lawful targets for a military response.

In addition to hazards that might be waiting for Internet users when they wander into virtual war zones, there may be other risks as well. Some states, under the guise of countering cyber-terrorism or cyber-warfare, might be tempted to abuse and misappropriate the law of armed conflict in an effort to suppress free expression and exchange of ideas. This Essay reviews the basics of the law of armed conflict and then considers its applicability in cyber-space, with particular reference to private citizens who use the Internet in a manner that might ensnare them in warfare and its legal consequences.

This Essay is speculative in the sense that the law of armed conflict has not yet been extended to cover warfare waged over the World Wide Web. Therefore, potential risks posed for private-citizen users of the Internet are based on an extrapolation from existing principles of the law of armed conflict. It is, however, a modest extrapolation. Private-citizen Internet users who want to protect themselves in the cyber-realm will be well served to assume that the line of thinking presented in this Essay reflects the shape of law to come.

THE FAMILIAR LEGAL FRAMEWORK FOR INTERNET HAZARDS

Most Internet users think in terms of cyber-crime when they consider wrongdoing that takes place using the World Wide Web. United States legislation illustrates the legal parameters for that framework. Broadly stated, the Computer Fraud and Abuse Act[2] prohibits use of computers, without authorization, to obtain official information protected against unauthorized disclosure; to obtain information from financial institutions in furtherance of a fraudulent scheme; to transmit a program, code or command that damages a computer; to gain unauthorized access to a computer with damage resulting; to traffick in passwords with intent to defraud.

Internet users who employ computer technology for such ends will, increasingly, find themselves at risk for arrest and prosecution around the world. Such crimes will continue to be addressed through law enforcement channels and the judicial process. Consider, for example, this recent policy formulation announced by the U.S. government:

---

2. 18 U.S.C. § 1030(a)(1)-(7) (2003).

> The Nation will seek to prevent, deter, and significantly reduce cyber attacks by ensuring the identification of actual or attempted perpetrators followed by an appropriate government response. In the case of cyber crime this would include swift apprehension, and appropriately severe punishment.[3]

But not every form of potential jeopardy attaches through domestic criminal codes or civil liability for damages resulting from such misconduct.[4]

Internet users motivated by idealism (or their notions of idealism) or patriotism, could be inspired to use the Internet for purposes that extend beyond the realm of lawful exchange of ideas, beyond the scope of criminal law, and into a realm sometimes known as the law of war. It has already come close to happening.

THE LAW OF ARMED CONFLICT—A QUICK SURVEY

The body of international law that concerns us here is identified by more than one name. Traditionally, the law that regulated means and methods of warfare and established constraints on the behavior of combatants was called the "law of war." In the twentieth century, it also came to be known as the "law of armed conflict." Both of these terms are favored by armed forces. This law is also sometimes known as "international humanitarian law." There is some dispute as to whether international humanitarian law and the law of armed conflict cover precisely the same ground. In modern treaty law and state practice, the term "armed conflict" is preferred to "war" because it more broadly describes an actual state of armed hostilities, as opposed to the legal state of affairs known as war, which requires a formal declaration.

The law of armed conflict applies in full during interstate armed conflict. The treaty-based provisions for intrastate armed conflict are more limited in scope. Article Three Common to the Geneva Conventions of 1949,[5] sometimes known as a mini-Geneva Convention, includes broad principles of humanitarian protection for non-international armed conflict including prohibitions on murder, mutilation, cruel treatment and torture, taking of hostages, humiliating treatment, punishment without due process, requirement of humane treatment for those who are wounded, sick, or detained, and a provision that an impartial humanitarian body such as the

---

3. National Security Strategy, *supra*, note 2, at 28.

4. *Id.*

5. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, art. 3, 75 U.N.T.S. 31 [hereinafter Geneva I].

International Committee of the Red Cross (ICRC) may offer its services.[6] Though international armed conflict is our main focus, a few additional observations will first be made about the law of internal armed conflict.

Protocol II Additional to the Geneva Conventions of 1977[7] expands the legal protections that apply during internal armed conflicts. The law continues to develop, with some contending that many of the rules for international armed conflict now apply to internal armed conflict as well. A trend to apply new treaty-based rules to internal as well as international armed conflict can also be discerned.[8]

That such debate and development continues demonstrates that the law of armed conflict is an evolving body of law. New treaty-based restrictions on weaponry continue to develop (e.g. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-personnel Mines and on their Destruction of 1997). Influential interpretation of the law has been handed down by the International Criminal Tribunal for Yugoslavia and International Criminal Tribunal for Rwanda. New standards to regulate the conduct of hostilities may be emerging from the Rome Statute for the International Criminal Court. Some principles of international humanitarian law are already long established in treaty law, such as those that address the status and protection of medical workers, prisoners of war, civilians who are detained for security purposes or in occupied zones, and wounded and sick combatants.

The full provisions of the law of armed conflict apply during interstate (between nations) armed conflict. They are found in many sources, including most notably the Geneva Conventions of 1949 and Additional Protocol I of 1977.[9] These treaties ensure that during interstate conflict, wounded, sick and shipwrecked members of the armed forces will receive medical care without regard to the party for which they fought. They provide that military captives will receive humane treatment, benefit from visits by representatives from a

---

6. Common article 3 is sometimes referred to as a mini-Geneva Convention, as its provisions capture the spirit of rules that apply more fully during international armed conflict.

7. Protocol Additional 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 [hereinafter Protocol II].

8. *See, e.g.*, Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-traps and Other Devices as (Amended Protocol II), Oct. 13, 1995, 35 I.L.M. 1206 (1996).

9. *See* Geneva I, *supra* note 5. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S. 85 [hereinafter Geneva II]; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter Geneva III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter Geneva IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

neutral nation (protecting power) or humanitarian organization (the ICRC plays a crucial role in implementing this facet of international humanitarian law) and exchange messages with their families on a regular basis. In addition, military captives are to be repatriated at the close of active hostilities. Likewise, civilians caught in a war zone are entitled to humanitarian assistance (again by the ICRC) and, when detained for security purposes, to protective visits by the ICRC or a protecting power and to services like those provided for prisoners of war.

Targeting, an issue gaining in interest around the world, is a frequent subject of debate. Increasingly, it is a field that is also the subject of legal scrutiny. The law of targeting is not hard and fast because it can be difficult to target with absolute certainty in the fog of war. However, targeting law continues to develop and requires careful consideration. Broadly stated, civilian infrastructure not employed to support the war effort is protected from targeting. Such infrastructure, and more broadly the protection of the civilian population, is the principle focus in the debate on targeting.[10]

It remains an open question whether and how international humanitarian law or the law of armed conflict applies in cyberspace.

VISITING THE VIRTUAL WAR ZONE

Those fortunate enough never to have been in a war zone may assume that such areas resemble the Western Front during World War I; a ravaged moonscape bristling with heavily armed fortifications. In point of fact, many war zones look nothing of the sort. Sometimes the unwary may wander through quiet residential areas or down scenic country roads without realizing that they are approaching or crossing the front-line of a battlefield. Internet users run the same risk.

The law of armed conflict applies in war zones. To date, it is not established that cyberspace legally qualifies as a war zone. Cyberspace does not occupy a discernible geographic location, and the electronic attacks that impact combatants may be launched from or through networks in potentially neutral states where the authorities have no knowledge of the attack. Likewise, the attack could take place using platforms that have no obvious connection with traditional weaponry.[11] The net result is that there is no

10. *See* Rome Statute of the International Criminal Court, U.N. Doc. A/CONF.183/9 (1998). For a study of the law of armed conflict as found in the Rome Statute, see LEILA NADYA SADAT, THE INTERNATIONAL CRIMINAL COURT AND THE TRANSFORMATION OF INTERNATIONAL LAW: JUSTICE FOR THE NEW MILLENNIUM 129-71 (2002).

11. *See* Ruth G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, 76 INT'L L. STUD. 219, 227 (2000); COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt et al.

treaty that points to cyberspace as a place where the law of armed conflict applies.

However, the law of armed conflict is built upon customary law. It only became rooted in treaty law in the nineteenth and early twentieth centuries. Even where there are no established treaty rules, the principles of the law of armed conflict nonetheless apply during interstate armed conflict.[12] Rules of armed conflict have developed through state practice as well as through treaties. Total reliance on familiar, statutory-centered sources for new rules is not sufficient because such rules may emerge even in the absence of treaties.

States may decide, before long, to apply familiar treaty-based rules of war by analogy to guide the use of cyberspace as a tool for war.[13] Private-citizen users of the Internet should not assume that the law of armed conflict will not apply in cyber-war. Though interpretation of the law of armed conflict may differ among nations, modern state practice demonstrates that its rules will apply, in some form, even during international confrontations where governments are reluctant to acknowledge that warfare is actually underway.[14]

Private citizen users of the Internet should assume that the law of armed conflict will develop to encompass belligerent acts committed on-line. While other war zones may require a substantial journey before one reaches the front lines, cyber-war zones can be entered without leaving a work station or place of residence located thousands of miles from the scene of traditional hostilities. It would be wise to consider the implications.

---

eds., 2002).

12. This principle is enunciated in the famous Martens clause found in the Hague Conventions on land warfare of 1899 and 1907.

> Until 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 the dictates of the public conscience.

Convention (IV) Respecting the Laws and Customs of War on Land, October 18, 1907, 1 Bevans (631) Convention (II) with Respect to the Land and Customs of War on Land, July 29, 1899, 1 BEVANS 247.

13. For a careful analysis of the applicability of the law of armed conflict to computer network attacks launched by states see Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, 846 INT'L REV. RED CROSS 365 (2002).

14. *See generally* Michael H. Hoffman, *Peace-Enforcement Actions and Humanitarian Law: Emerging Rules of "Interventional Armed Conflict"*, 82 INT'L REV. RED CROSS 193-203 (2000).

IDENTIFYING CYBER-SPACE COMBATANTS

Private citizens have already taken to cyberspace to lend their support, to one side or another, during international confrontations. In 2001, there were numerous private cyber-attacks launched between China and the United States during tensions following the collision between a U.S. surveillance flight and a Chinese fighter that subsequently resulted in an emergency landing by the U.S. crew.[15] The Arab-Israeli confrontation has also led to conflict on the Internet, with supporters on each side attacking Web sites.[16] In another instance, cyber-attacks were launched against diplomatic missions by an individual supporting or sympathizing with of an insurgent group during an internal armed conflict.[17]

These events involving defacement of Web sites and spamming did not cross the yet to be defined legal threshold for cyber-warfare. However, an attack that disabled industrial sites, endangered public safety, or interfered with military operations might well establish that threshold. Those responsible for such attacks could discover that they have become combatants and, for that reason, a quick survey of the law of combatant status needs to be considered.

During interstate conflict, members of a state's armed forces qualify as combatants under international humanitarian law. Likewise, members of militias and organized resistance movements commanded by a person responsible for subordinates, who openly carry their arms, are readily identifiable by a fixed sign (identifier), and are subject to the laws and customs of war qualify as combatants.[18] The status of insurgents during an internal armed conflict is problematic. They can be punished for taking up arms against the state provided that they receive the full protection of the law, but there is also the possibility of amnesty at the end of the conflict (and thus some implicit recognition as lawful combatants) if they conduct themselves in a manner that would encourage the authorities to grant leniency.[19]

---

15. *Chinese Hackers Carry Through on Threats to Attack U.S. Web Sites* (Apr. 30, 2001), *available at* http://www.foxnews.com/story/0,2933,18657,00.html; *It's an All-out Cyber War as U.S. Hackers Fight Back at China* (May 1, 2001), *available at* http://www.foxnews.com/story/0,2933,19337,00.html.

16. Mideast Fighting Spills onto the Internet (Nov. 2, 2000), *available at* http://www.cnn.com/2000/TECH/computing/11/02/mideast.webwar.

17. *Second Incident of Cyber-Terrorism in Sri Lanka*, *at* http://www.lankaweb.com/news/items01/210501-2.html (last visited June 12, 2003).

18. *See* Geneva Convention I, art. 13; Geneva Convention II, art. 13; Geneva Convention III, art. 4.

19. *See* Protocol II, art. 6(5).

As described earlier, those who qualify as combatants during interstate armed conflict enjoy a substantial measure of protection when they fall into the hands of an enemy. Though they can be held for the duration of active hostilities, unless severe health problems suggest an earlier release, they are not prisoners in the sense of being criminals. They can be detained, but not punished for having served their country in wartime. Members of armed forces as described in the Geneva Conventions would qualify for full protection. The fact that they are utilizing new technologies for military purposes would not deprive them of their lawful combatant status.

There are certain categories of combatants whose actions are in fact prohibited by the laws and customs of war. Thus, participation in such activities deprives them of prisoner of war status and renders them susceptible to punishment for their activities if convicted "by an impartial and regularly constituted court respecting the generally recognized principles of regular judicial procedure. . . ."[20] Spies and saboteurs represent categories of individuals who do not qualify for full protection under the law of armed conflict and may face punishment for their activities.[21] Guerilla warfare was traditionally prohibited and punishable under the law of war, through an attempt has been made to define parameters for lawful guerrilla warfare in Protocol I to the Geneva Conventions. This change has not been universally accepted and some states, including the United States, have not ratified Protocol I.

Where might private Internet users fall within this existing legal structure? There is only one situation in which private citizens can spontaneously take up arms on their own initiative during an international armed conflict and attain the status of lawful combatants, and that is where:

> Inhabitants of a non-occupied territory, who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war.[22]

In any other circumstance, individuals who want to take up arms as lawful combatants must join a military unit that comes within the categories described in the Geneva Conventions (or Protocol I in cases where its

---

20. *See* Protocol I, art. 75(4).

21. *See* Geneva Convention IV, art. 5. *See also* Protocol I, art. 46.

22. *See* Geneva Convention I, *supra* note 5, art. 13; Geneva Convention II, art. 13; Geneva Convention III, art. 4.

provisions on guerrilla warfare have been accepted, via ratification, by the parties to the conflict).

Such spontaneous organization is sometimes known as a *levee' en masse*. Perhaps there will be situations where Internet users may organize themselves in an analogous manner to repel cyber-attacks on their country. However, if we extend the laws and customs of war by analogy to cover such cases, it will only apply to defensive measures. Cyber-attacks on the infrastructure or military capacities of another nation would go beyond the permissible operational scope of citizen participation in a *levee' en masse*.

To the extent that the existing framework of the law of armed conflict gives us some guidance on likely future trends, it seems that this will be the only context in which private Internet users would ever be able to stake a claim to lawful combatant status. Even that scenario for development of the law is speculative and, we might say, optimistic. As a general rule, private Internet users who decide to launch cyber-war attacks will, at best, find themselves classified as unlawful combatants.[23] Identification as a combatant, lawful or otherwise, brings with it practical issues and consequences.

IMPLICATIONS OF IDENTIFICATION AS A COMBATANT

Most private Internet users are aware that activities prohibited by the Computer Fraud and Abuse Act expose them to criminal investigation, prosecution, and penal sanction. However, if they engage in cyber-activities that states determine to constitute hostile military actions, there will be other, less familiar consequences to consider. The threshold between conventional computer crime and cyber-activities constituting hostile acts under the law of armed conflict will be difficult to determine. Sabotaging a server might be a "conventional" crime (to the extent computer crime has become conventional). At some still legally undefined point, an assault on computer networks, or infrastructure that depends on computer networks, will be considered to have morphed into a military assault. Private Internet users probe for that threshold at their own risk, with the potential for penalty under criminal law in some cases, under the law of armed conflict in others, and under both if their acts are deemed to constitute war crimes.

---

23. "Unlawful combatants" is terminology found in *Ex Parte Quirin*, 317 U.S. 1, 31 (1942) and not a term of art recognized in international humanitarian law. However, it is one of a variety of terms that have been used in efforts to describe, in legal terms, actors who engage in armed conflict without the legal authority and protection that is accorded to lawful combatants and are, therefore, susceptible to be tried and punished for their activities. Other terms and descriptions that have been used for the same purpose include irregular combatants, belligerent disqualification, and marauding.

If captured in circumstances where it is determined that Internet activities qualify the individual as a combatant under the law of armed conflict (a scenario unlikely to occur when the user is acting as a private citizen), that private Internet belligerent might be held as a prisoner of war. As such, the actor would enjoy no right to counsel, nor access to courts to challenge detention. The user would be entitled to protective visits as a prisoner of war, as described previously, but could be held until the cessation of active hostilities.

If a user's captor should determine that private Internet warfare qualifies as a form of unlawful belligerency, they may then find themselves placed on trial for that offense. Whether deemed a lawful or unlawful belligerent or combatant, the private Internet user would also face the additional prospect of trial for war crimes if their targeting, or the damage engaging cyber-attacks, constitutes a war crime. For example, a computer virus launched to disrupt hospital services may be considered analogous to a conventional weapons attack against the same site that would be unlawful under the established law of armed conflict.

Ultimately, combatants engaging in cyber-warfare, lawful or otherwise, might find themselves a target for the use of lethal force. This is unlikely where a belligerent state can prevail on another nation to shut down activities taking place in neutral territory. In those circumstances, private Internet users could well find themselves facing prosecution by their own government for violation of domestic neutrality legislation as well as other criminal offenses.[24] However, cyber-attacks launched from a location that cannot be reached through diplomatic or law enforcement channels might eventually be deemed to constitute a military threat susceptible to traditional military operations.

Likewise, private Internet users who get involved in cyber-attacks on the computer infrastructure of their own country may be considered insurgents involved in non-international armed conflict if such assaults support a group engaging in hostilities against the state. Depending on how state practice evolves, particularly damaging cyber-attacks may come to be recognized as a form of armed rebellion even where there are no conventional hostilities underway. Depending on the domestic law of the country concerned, Internet users may, in addition to criminal charges familiar in a peacetime context, face the prospect of trial for insurrection and war crimes.

---

24. *See, e.g.*, 18 U.S.C. § 960 (2003). This legislation has a venerable lineage dating back to 1794. It may or may not be sufficiently current to address private cyber-attacks by U.S. citizens or others residing in the United States, but it gives a sense of domestic law related risks run by private Internet users if they try to intervene in conflicts where their own country remains neutral.

The message here is that it will be best to stay away from cyber-war zones (regardless of how such zones come to be conceptualized) and refrain from any Internet activities that might be characterized as a new form of armed belligerency. However, there are times when Internet users need to remain vigilant so that emerging notions of cyber-war do not impinge on the free exchange of ideas and peaceful use of the Web.

IF STATES ABUSE THE LAW OF ARMED CONFLICT TO SUPPRESS INTERNET COMMUNICATIONS

Information and comment sent by way of the Internet will, in exceptional circumstances, cross a line from peaceful exchange of ideas to acts arguably military in character. Propaganda efforts, sometimes also known as psychological operations, are a form of warfare designed to destabilize and undermine enemy efforts and morale. Members of armed forces engaged in psychological operations are combatants. Private Internet users who decide to spread false information or rumors in order to undermine military or related national security efforts run the risk of drifting into combatant status if their activities should be found to qualify as psychological operations.

However, such uses of the Internet will be miniscule in comparison with peacetime use for dialogue, information sharing, and commerce. Freedom of expression has been enshrined in the developing law of human rights for over two hundred years.[25] In the twentieth century, this right expanded beyond domestic, constitutional sources and found its way into international law as well.[26]

Private Internet users who understand the importance of the World Wide Web as an instrument of freedom will not want to see it used in a manner that undermines this vital purpose. At the same time, private Internet users and human rights practitioners will need to remain vigilant against attempts to suppress freedom of expression by states that may misuse the law of armed conflict to claim that exchanges of ideas and information, via the Web, somehow constitute acts of belligerency.

---

25. *See* Fr. Const. of 1791, Title I; CONSTITUTIONS THAT MADE HISTORY 86 (Albert P. Blaustein & Jay A. Sigler eds., 1988); *see also* U.S. CONST. amend. 1 (1791).

26. *See, e.g.*, Universal Declaration of Human Rights art. 19 U.N. Doc. A/810 (1948).

CONCLUSION

The World Wide Web has obviously spurred a communications revolution. In shrinking the world, it is also gradually opening a portal for easy access to war zones and remote participation in hostilities. Virtual visits to war zones and incidents of hostile use of the Internet will likely be followed, if not accompanied by evolving standards in the law of armed conflict that turn some private Internet users into combatants with all the legal and security consequences that follow. Private users of the World Wide Web are well advised to avoid becoming test cases on application of the law of armed conflict to the Internet. They should, instead, contribute their efforts, talents, and energy to peaceful development of this vital new medium.