An Overview of the Evolving Law Related to Computer Network Defense

by Richard Aldrich

IANewsletter (5), 2. Summer 2002, pp. 10-12.

The law related to Computer Network Defense (CND) is a complex web of statutes and court decisions. Unfortunately, that web consists of gaping holes, conflicting case law, overlapping statutes, and the recognition of distinctions which technology has long since made obsolete. This is not totally unexpected. The traditionally slow evolutionary process of legal change has had difficulty keeping up with the extremely fast pace of changes in technology and the paradigm-shifting developments in CND. Nevertheless, significant progress is being made and the following discussion sets out a basic conceptual framework for understanding the legal landscape in this area.

Currently the law recognizes four fairly distinct roles, or "lanes of the road," in the area of CND. First, and perhaps most important to CND, is the service provider role. Representative players of this role are the Defense Information Systems Agency (DISA), the service Computer Emergency Response Teams (CERTs), and each network's Designated Approval Authority (DAA) and system administrators. Attacks against a network are most likely to be identified first by these service providers. Fortunately, Congress created a service provider exception to the general prohibition against interceptions set out in the Federal Wiretap Act (for more information see 18 U.S.C. §2511(2)(a)(i)). For law enforcement or counterintelligence agents to intercept such communications would generally require, in the absence of an exception to the Wiretap Act, a Title III court order or a FISA (Foreign Intelligence Surveillance Act) court order, respectively. Obtaining court orders can be a trying and time-consuming operation, so the importance of the service provider exception in providing a first warning of attack cannot be overstated. Service providers may also be able to rely on the consent exception, where users are required to sign user agreements or click through consent banners. Pass-through consent banners may establish implied consent. The consent and service provider exceptions are two separate and distinct exceptions and should not be merged into one as some want to do.

The second major lane in the road is that of law enforcement. It is important to note that computer intrusions can initially look very similar, whether they are in fact an information warfare attack from a foreign power, the work of a foreign intelligence agency, a terrorist attack, a criminal act, or the work of a "script kiddie." [1] Understandably, the law provides for radically different permissible responses in each case. Presidential Decision Directive 63, DoD policy, and the vagaries of the law have indicated the most appropriate means of resolving the identity and intent of the intruder, beyond that permitted to service providers, is through the use of law enforcement agents. Representative players in this role are the Federal Bureau of Investigation (FBI), the U.S. Attorneys Offices, and the Defense Criminal Investigative Organizations (DCIOs) [i.e., Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Criminal Investigative Division (CID), Defense Criminal Investigative Service (DCIS)]. Some of these players have split personalities and can assume other roles as well, most commonly a counterintelligence role. This creates additional legal problems in the sharing of data even within such an agency. Some of those problems were resolved in the USA PATRIOT Act, which permitted increased sharing of information between law enforcement and intelligence entities. The overriding limitation to activities in the law enforcement area is the Fourth Amendment to the Constitution. Thus, law enforcement agents must generally obtain court authorization whenever their activities would contravene one's reasonable expectation of privacy. In fact, however, it is additional statutory layers of protection that Congress has added over the years that have caused the most difficulty. Up until the passage of the PATRIOT Act, law enforcement agents could not even attempt to identify a hacker, who had illegally penetrated a Government computer, without the hacker's consent or a court order. Some Government entities placed consent banners on their six or eight most commonly used ports in an attempt to obtain implied consent from trespassers. Unfortunately, since computers

generally have over 65,000 ports, hackers were inevitably able to penetrate a system through an unbannered port and thereby bind the hands of law enforcement. The PATRIOT Act recognized a new exception for intercepting the communications of "computer trespassers." [2] Thus, law enforcement agents may now generally rely on the consent exception, the computer trespasser exception, or court orders to obtain the information necessary to accomplish their investigations.

There remain many other legal hurdles for law enforcement to negotiate in computer intrusion investigations domestically, and the law becomes much more complicated once one goes beyond the U.S. "cyber shoreline." International law and foreign country law will oftentimes require the use of letters rogatory or other time consuming legal processes. The new Convention on Cybercrime attempts to facilitate international cooperation in the fight against cybercrime and makes some positive steps in that direction. Thirty-three countries, including the United States, signed it in December of last year, but only one country has ratified it so far.

The third major lane in the road is that of the intelligence community. Representative players in this role are the FBI, the Central Intelligence Agency (CIA), and the myriad of DoD intelligence components, including most notably the NSA and the Service intelligence components.
What many do not seem to realize is that the intelligence components are also limited in their activities by the Fourth Amendment (at least as to activities within the United States or against "United States persons," as that term is defined in Executive Order 12333). Frequently the basis for an investigation within this lane comes initially from information provided by a service provider or law enforcement agent, working within their respective lanes, though some positive intelligence agencies operate specifically to gain advance intelligence of proposed intrusions. Intelligence agents will generally rely on consent, the computer trespasser exception and FISA warrants to obtain the information necessary for their investigations.

The last lane is the one for the warfighter. This lane is the least defined under the law. Certainly the President, as Commander-in-Chief of the Armed Forces, wields significant potential authority under the Constitution. Nevertheless the exact contours of that authority are unclear. President Truman's attempt to seize the steel mills during the Korean War was rebuffed by Congress and the Supreme Court in Youngstown Sheet & Tube Company v. Sawyer, 343 U.S. 579 (1952). Nevertheless, the reliance by the Court on Congressional action aimed specifically at narrowing presidential authority in that specific instance means the opinion leaves as an open question the scope of presidential power in the absence of such. Again, however, domestic law is only part of the equation. In the warfighting arena, the impact of the U.N. Charter and international treaties is also significant. Articles 51 (defining the scope of self-defense), 2(4) (defining what is an unlawful use of force), and Chapter VII (setting out permissible activities of the Security Council) of the U.N. Charter all figure prominently in the debate over what is and is not permissible. Whether such provisions even apply to "information warfare" is itself an unsettled question, though most would hold it does. Most legal commentators would also agree that the set of international law collectively referred to as the law of armed conflict also applies to information warfare, though this is also unclear since most of this law far predates computers and so one must apply new interpretations to established terms.

It is important to recognize that some governmental organizations may have subordinate entities playing in each of the four lanes. As such, it would make no sense to ask whether the government or even, for example the U.S. Air Force, could legally perform certain activities. Rather, to answer the legal question, one must ask who within that organization is to perform the activity and in what role will that person be acting. Because the law is fairly discrete in its application of where an individual can perform roles in more than one lane, it is important to identify the role being performed at the time of the activity in question. Extreme caution should be exercised in any potential "hat switching" and should generally only be done after appropriate legal consultation. Indeed, because the law of CND is still rather complex, persons who work in this field are advised to seek the advice of their organization's legal staff whenever they are unclear as to what is and is not legally permitted. ■

References

1. The list is not disjunctive, as many of these categories may overlap. "Script kiddies" are inexperienced hackers who rely on pre-written attack scripts, available over the Internet, because of their own technical inabilities. Frequently they will not even understand how or why the script works.
2. 18 U.S.C. §2511(2)(i).

About the Author

Rick Aldrich

Mr. Aldrich is Senior Computer Network Operations Policy Analyst for IATAC. Previously, he served as the Deputy Staff Judge Advocate for the Air Force Office of Special Investigations, specializing in the cybercrime and information operations portfolios. He has been awarded several grants by the Institute for National Security Studies and has multiple publications related to the legal implications of information warfare. He has a B.S. in Computer Science from the U.S. Air Force Academy, a J.D. from UCLA, and an LL.M. in Intellectual Property Law from the University of Houston.