

Homeland Security's Cyber Component: A Survey of Legal Issues

¹James B. Michael, ²Thomas C. Wingfield and ³Steven E. Roberts

¹Department of Computer Science, Naval Postgraduate School, Monterey, California 93943-5118

²The Potomac Institute for Policy Studies, 901 North Stuart Street, Suite 200, Arlington, VA 22203

³Security Researcher and Author, 2801 NW 23 Boulevard, Gainesville, FL 32605

¹bmichael@nps.navy.mil, ²twingfield@potomac institute.org, ³amtap@yahoo.com

Abstract

In this panel we discuss the legal developments related to the cyber aspects of homeland security. Through analysis of statutes, Executive Orders, and case studies, we highlight the rapid development of a new body of law and its consequences for the government, the private sector, and the public at-large.

1. Introduction

Critical infrastructures are America's lifeblood: from power plants and water reservoirs to telecommunications systems and mass transit networks, America depends on the safe and efficient operation of its critical infrastructures. However, as ubiquitous examples of economic efficiency and sophistication, terrorist attacks against critical infrastructures are fast becoming a matter of when, not if.

Increasingly, critical infrastructures are automated and interlinked, relying on a cyber backbone that might be exploited by sophisticated cyber-terrorists. Indeed, open source reports, widely known and rarely disputed, suggest that terrorists have expressed interest in this form of asymmetrical warfare. AlQaida computers, seized by American forces during operations in Afghanistan, reveal AlQaida operatives visited web pages that offered information and instructions on Supervisory Control and Data Acquisition Systems (SCADA) and Digital Control Systems (DCS), which are used to control and manage critical infrastructure operations.

As the risk of attack in or through cyberspace has grown, the domain of legal issues surrounding this cyber aspect of homeland security has expanded. Liability, duty of care, use of force, and information sharing issues are now inseparable from any analysis of homeland security and cyberspace.

2. Legal Issues in Cyberspace

Consider the following survey of legal, homeland security cyberspace issues:

- The Gramm-Leach-Bliley Act imposes security requirements for the protection of consumer information within the financial indus-

try. The Health Insurance Portability and Accountability Act does the same for health-care.

- The *National Strategy to Secure Cyberspace* and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released by the Bush Administration in early 2003, give credibility to the position that critical infrastructure owners and operators may owe a "security duty of care" to customers and shareholders. Failure to provide reasonable security measures to mitigate terror vulnerabilities might breach that duty, and thus create a cause of action for damages under tort law.
- As narrow areas of regulation broaden to become the *de facto*, if not the *de jure*, standards for other vulnerable critical infrastructure sectors, general guidance, such as that already issued by the Administration, will be "operationalized" with more nuts-and-bolts implementing regulation. The executive departments charged with protecting various aspects of the nation's critical infrastructure will convert broad executive order-based mandates into federal regulations. Where this requires too great a leap, the appropriate Congressional committees will consider narrowly tailored legislation to further the scope of federal oversight. The USA PATRIOT Act, passed in October of 2001, provides a lesson in the speed with which newly-perceived threats may be addressed. It provides a complementary lesson on the limits within which Congress may operate, itself overseen by the courts and attentive interest groups.
- California Senate Bill 1386, which went into effect on July 1, 2003, requires companies to inform customers when their personal information is "reasonably believed" to have been compromised, typically at the hands of computer hackers. Companies that fail to disclose the security breach to affected consumers may

To appear in *Proc. Twenty-seventh Annual Int. Computer Software and Applications Conf.*, IEEE (Dallas, Tex., Nov. 2003).

be required to do so, and the putative victims may sue for damages. While many voters would agree that this is a good idea, and that it would provide a strong incentive for corporations to clean up their information-handling practices, there are problems with the approach. First, the standard of “reasonably believed” provides a good deal of flexibility—perhaps too much to a company looking for every bit of legal gray area in which to hide its misfeasance. Second, disclosure need not be made until the completion of the investigation into the putative info-loss. While this protects the integrity of the investigation, it also provides a safe harbor for corporations hoping to bury bad news. In the past, many investigations have stretched to months and even years, and this law provides an incentive to stretch them further still.

- “Use of Force” under international law is another crucial issue. While individuals, corporations, and government entities in the United States will obviously follow domestic law as it applies to law enforcement, intelligence collection, and even military activities within the US, it is far from clear, even to educated laymen, that Americans must also follow that portion of international law recognized by the United States. There are two key questions here: what constitutes a “use of force” or “armed aggression” under international law, and, if the country is at war, how does the traditional (kinetic) law of armed conflict apply to operations in cyberspace? The first of these questions may be resolved through the Schmitt Analysis, a method of reconciling and effects-based quantitative analysis of damage done with the means-based qualitative paradigm of international law as codified in the UN Charter. The second question involves taking a step back to first principles, and applying the doctrines of discrimination, necessity, proportionality, and chivalry to activities in cyberspace. These doctrines do not lie in the often-debated and easily-dismissed realm of legal theory or political posturing, but are the core doctrines accepted by the United States and the democracies of the civilized world as the minimum standards of conduct in any kind of international conflict. Correctly applying their requirements to the most coercive actions in cyberspace is literally a matter of life and death.
- In addition to creating the Department of Homeland Security, which represents the largest reorganization of the federal government in more than fifty years, the Homeland Security Act of 2002 also recast the Freedom of Information Act (FOIA). Under new FOIA provisions, critical infrastructure owners and operators may provide security related information to the Department without worry that such information may be subject to a FOIA disclosure. Information in the hands of critical infrastructure owners and operators sought by government, such as information related to threats, vulnerabilities, or security best practices, will now be shared more evenly and openly between the private sector and their government allies. However, such provisions have not come without debate. Critics allege that the FOIA exemption is too broad and provides a safe-haven for critical infrastructure owners and operators to conceal wrongdoing from regulators and the public.
- *Posse committatus* is another doctrine which is frequently misunderstood, even by some legal professionals. It does *not* prohibit the use of the military within the United States, but only the use of military as a law enforcement agency within the US. The use of the military to pursue non-US persons in the US was contemplated by the framers of the Constitution, and was not obviated in 1870’s with the codification of the doctrine of *posse committatus*. Therefore, correctly drawing the line between law enforcement and military activities in the US becomes even more important in the absence of a convenient bright-line rule forbidding all use of the military domestically.
- Safe Harbors, that provide a legal liability exemption for specific security practices, are increasing. Encryption, for instance, is a safe harbor “built-in” to California’s new information breach disclosure law.
- Data retention and data preservation pose many legal issues. For instance, there is little customary international law on data retention; we primarily rely on bilateral and multilateral agreements. In addition, there are different legal regimes in place for governing communication data and content. Moreover, use of communication data could be used for predictive purposes: do we need special controls to avoid becoming an Orwellian society?