

## III

---

---

# Technology and Law: The Evolution of Digital Warfare

---

---

David Tubbs, Perry G. Luzwick, Walter Gary Sharp, Sr.

### Introduction

**T**echnology began shaping the conduct of war when the first warrior picked up a stone to increase his killing power during hand-to-hand combat.<sup>1</sup> Ever since, new technologies have increasingly affected the balance of power by:

- leveraging existing strategies or efforts of either the attacker or the defender;
- enabling new and unexpected strategic uses of existing weapons technology;
- providing new weapons of increased destructive force;
- neutralizing or mitigating the effects of enemy weaponry or strategy; and
- providing or denying the element of surprise.

Telecommunications and information-related technological advances, however, have perhaps been the most fundamental in shaping warfare. Telecommunications enables command and control by providing rapid, accurate, and secure communications among friendly forces. Without communications, the Strategic Air Command Commander-in-Chief, General Tommy Powers, once

observed, “all I would command is my desk, and that’s not a very lethal weapon.” Telecommunications has allowed the battlespace to grow from a grassy field to encompass outer space, the atmosphere, the earth’s surface, and under the seas. Table 1 demonstrates how telecommunications has reduced by several orders of magnitude the time needed for command and control.

<b>Circa</b>	<b>Methodology</b>	<b>Time</b>
1775	Message from Boston via horse and courier to a ship, which then sails to London and taken by horse and courier to the King – and return reply	Months
1850	Message from New York to San Francisco via telegraph and the Pony Express	Weeks
1925	Message from Washington, DC to Tokyo via high frequency radio	Days
2000	Message from Washington, DC to Tokyo	Seconds

Telecommunications today give fighting forces incredible capabilities to be proactive and adaptive, and to take meaningful response. Today’s warfighters expect and demand reliable, fast, interoperable, and protected communications. Telecommunications also enables the acquisition of information concerning the disposition, objectives, and vulnerabilities of the enemy to gain a strategic advantage, creating warfighting disciplines such as Communications Intelligence (COMINT), Electronic Warfare (EW), Electronics Intelligence (ELINT), Foreign Instrumentation Signals Intelligence (FISINT), Imagery Intelligence (IMINT), Open Source Intelligence (OSINT), and Signals Intelligence (SIGINT). High-speed communications cannot occur, however, without computers, and the pervasive use of computers in almost every device inextricably link telecommunications, computers, and the warfighting capability of any modern military force.

Information Operations (IO) and Information Warfare (IW) compose the modern construct that embodies and demonstrates the dependency of modern warfare on telecommunications and computers. Fundamentally, IO and IW include any activity that influences the production, modification, falsification, distribution, availability, or security of information relative to any aspect of the pursuit of war. These activities may be wide-ranging, even low technology, as long as they influence the gathering, analysis, distribution, or implementation of useful warfighting information. Sabotage, bombing of communications infrastructure, radio frequency jamming, High Energy Radio Frequency (HERF) weapons, and electromagnetic pulse generation are all examples of relevant, modern IW.

Offensive and defensive IW implications of new technologies must constantly be assessed by the professional warfighter. Specifically, computer networking technologies are becoming ever more integrated into modern commerce and communications; consequently, attacks on these computer networks must be integrated into offensive and defensive warfare strategies. Relevant IW computer technologies include the full networking spectrum—from small, hardened, independent Local Area Networks (LANs) and regionally distributed Wide Area Networks (WANs) to the use of the global, publicly-supported Internet.

### **Enter the Internet**

Although the impact of telecommunications on warfare has been dramatic, the invention of the Internet has been profound. Because of its pervasive integration into modern technology infrastructures, the Internet will very likely be used as either the primary or a collateral medium for any computer network attack. The commercial interests of developed nations, and even many unclassified military functions of these same nations, are now dependent on the availability and reliability of Internet communications. Exploitation, elimination, or compromise of this vulnerable asset will often be the primary component of a nation's IO campaign.

The Internet began in 1969 as the ARPANET.<sup>2</sup> Originally the ARPANET was simply an experiment in highly reliable information networking. The experiment connected the Department of Defense with military research companies and specified universities who had military research contracts.<sup>3</sup> High reliability was achieved through the development of a new set of technologies, collectively named "packet switching."

In 1990, the ARPANET shut down, and was replaced by the NSFNET.<sup>4</sup> At the same time, non-DoD related commercial enterprises started to recognize the value of such a pervasive, distributed communication medium and they began connecting their previously private computer networks to the Internet, supplying new paths for all transmissions. These commercial entities brought commercial employees, suppliers, and customers to the Internet for the first time. They also began making a profit selling Internet access to the public. As commercial connections and traffic burgeoned, the NFSNET backbone handled less and less of the total traffic volume. While the NSFNET is not completely gone, the process of replacing the government's Internet infrastructure with commercial equivalents is well under way.

The essential, high reliability concept of packet switching used by the ARPANET, NSFNET, and now the Internet, is the elimination of a central,

single-point-of-failure, control and switching center. Packet switching first divides an electronic communication into pieces, known as packets. A header then prefixes each packet with identifying data such as:

- the sender of the message;
- the intended recipient of the message;
- the subject of the communication (for e-mail);
- the date and time of the transmission; and
- the position of this packet in the series of packets for this message.

Each packet is then independently routed to a computer that forms part of the backbone of the Internet (an Internet node). Each Internet node passes packets on to any computer on the network that is “nearer” to the destination identified in the header information than the present location. Recognize, however, since Internet node routing considers existing network traffic loads, and the definition of “nearer” is an estimate of total travel time rather than physical distance, the node to which a packet is routed may be physically farther away from the destination. Packets often travel quite circuitous routes to their destination. In fact, the various packets of a message may travel very different routes to the destination and will almost certainly arrive at different times. The header information allows the packets to be reassembled in proper order at the destination computer.

### **Internet Vulnerabilities**

For many reasons, however, these commercial and governmental initiatives seldom considered security as a part of the infrastructure. The main reasons for not implementing greater security were capability, cost, and schedule. Security uses system resources and thus slows the system down or, worse from a user’s perspective, does not permit certain features. Security is costly in terms of time, money, and people. It adds to the cost of the delivered capability. Security also lengthens delivery schedules because it takes longer to write a computer program without the flaws which make it vulnerable.

Perhaps the overarching reason for not implementing security is that the public, industry, and government did not perceive a threat sufficient to warrant the extra cost to embed security into hardware and software. For example, not realizing that a mountainside switch was on the rail line that the US Army uses to transport its main battle tanks to a seaport during hostilities, a Conrail railroad employee might ask, “Why would anyone want to attack a switch?” Not only is security expensive, it is prohibitively costly if it is considered after the fact. One

IBM study stated that it would cost ten times more to retrofit security into a system than it would if it was considered from the beginning.

Potential vulnerabilities are also frequently overlooked by the government in its use of commercial-off-the-shelf (COTS) products. The rationale for their use is two-fold. First, COTS provides strong capabilities at reasonable cost. Not only do these strong capabilities enable businesses to make a profit, but in addition the government does not bear the long-term costs of the resources to develop the products. Second, COTS upgrades and new products are more timely. However, the typical software product, portions of which are developed overseas in countries that either are or may be US competitors, contains several million lines of code. Determining whether such software contains any malicious code is economically infeasible and practically impossible. To do so would require a line-by-line code check as well as an understanding of how the lines of code interact. There is no artificial intelligence program that does this. It requires skilled people and time; indeed, more people and time than it takes to write the software in the first place.

Complexity is a hallmark of modern software. There are at least 300 security features in Windows NT, for example, that can be turned on and off. Adversaries constantly probe for weaknesses. It takes just one weakness not detected and resolved in one system to make all users connected to it vulnerable to exploitation and attack. Because of the trusted relationship between systems and networks in our highly interconnected infrastructure, achieving and maintaining control over our environment is very difficult.

The distributed routing design of the Internet means that there is no central point of control and thus no single-point-of-failure. This creates a highly reliable telecommunications system because an enemy or accident must disable every Internet node to disrupt traffic. Paradoxically, this high reliability carries with it an associated security vulnerability—every participating Internet node computer is a decision-maker, with full routing information and authority and access to the information stream. Accordingly, access to any Internet node will give a hostile or criminal element access to Internet traffic.

Also, with no centralized control, Internet entities do not naturally make use of information correlated from diverse sources to evaluate the intentions of their traffic—hostile traffic that conducts a distributed computer network attack is not recognized as such and thus allowed unimpeded passage. In direct analogy to covert, spread spectrum communications that spread wireless information over a number of radio frequencies to disguise transmissions, distributed Internet attacks use coordinated connections and communications from disparate locations to disguise the activity or objectives of the attack. These distributed attacks

ultimately make use of flaws in the operating system or applications software, just as with any other computer “hack.” Often, however, the distributed exploit is not obvious because individual steps are taken by different remote computers and each step is, in and of itself, relatively innocuous.

### **Methods of Computer Network Attack**

Perhaps the greatest vulnerability of any computer system is the human element. Most people still use family names or other easy-to-remember passwords, or use more difficult passwords but write them down in an easily accessible location near the computer. While some hackers may attack only by the Internet, a sophisticated and persistent threat dedicated to compromising a computer system will attempt to surveil the system physically and electronically. Information gathered from conventional forms of surveillance and analysis is very effective in determining which type of intrusion will be the most successful. Insiders, of course, are the greatest threat to any computer system—they have authorized access.

If physical access is obtained, both information gathering and actual system compromise are significantly easier. Hackers may gain physical access to a company’s computers through employment as a janitor or temporary secretary—or they may simply be a client or customer who is left alone near a computer momentarily. Once they gain physical access to a computer, hackers can immediately download or corrupt information, or install sniffer software to collect it. A sniffer is a program that runs in the background of the target machine, collecting information, such as passwords or credit card numbers, during normal operations. It generally requires a return visit to retrieve the collected information, but these programs may be quite small and difficult to detect.

Physical access also allows hackers to plant conventional recording devices that will collect information. For example, an audio recording of an impact printer may allow the printed characters to be recreated. Similarly, devices planted in nearby offices can record an entire document when it is transmitted by electronic bursts to a laser printer. Hackers may also learn relevant information by simply collecting trash from the curbside.

Finally, hackers may use social engineering techniques to learn information that compromise a computer system. Social engineering takes advantage of the fact that most people endeavor to be honest and helpful. Unless an enterprise has taken steps to educate its user base to the vulnerabilities represented by releasing seemingly innocuous information, social engineering gathers attack design information very effectively. Typically, a perpetrator will call on an over-worked employee, either in person or by telephone, invent a plausible need-to-know

excuse, and ask for relevant information. They may also offer a free magazine subscription in return for answering a few survey questions. Or, they may actually send free software (which contains malicious code) to try out on a computer. A trained practitioner in social engineering will usually obtain at least unclassified system details, but often passwords and sensitive information can also be obtained.

Seemingly innocuous information can also be very useful, leading to ease of access through system configuration details, personnel information, or guessed passwords. Public records, such as a company's website, or public business relationships allow a significant amount of information to be collated for use against the target. This information may point to a vulnerable electronic interface or an insecure business partner with full access. These elements of friendly information (EFI) may be insignificant in isolation, but can generate considerable weight when collected and pieced together.

Aside from the vulnerabilities exposed by a lack of discipline and compliance of the user base, computer network attacks ultimately rely upon flaws in software, and these type of attacks are greatly enhanced in an Internet environment because of the robust and flexible access and communications paths that the Internet represents. The incongruous truth is that, in spite of a carefully crafted public image of total control over others' information systems, the hacker is precisely limited to what the inadvertent holes the software design process leaves behind allow him or her to do.

Flaws in software design take many forms. Since large software packages contain many million lines of source code,<sup>5</sup> the law of averages guarantees many flaws in logical construction, reduction to source lines, typographical errors, and ill-defined interfaces between code developed by many different groups, at different times, and in different places. The hacker community lives to find and exploit these inevitable flaws and they are very good at doing so, but they cannot normally create holes *a priori* for their own use.<sup>6</sup>

Buffer overflows, for example, are a common vulnerability in all software. They require specific knowledge of the targeted operating system, but are powerful in that they allow arbitrary code (i.e., malicious programs) to be executed. Buffer overflows occur when data written to a pre-sized memory buffer exceeds the buffer's allocated space. The excess data then overwrites other memory areas. This can occur when a user response is longer than the software designer expected. Intentional buffer overflows attempt to write the perpetrator's code into the computer's instructions. Implementation of this exploit is routine; however, it must be precisely written, aligned, and sized so that it falls on a specific memory location.

The majority of flaws in any software package simply represent sand in the gears, disrupting or halting operation in generally unpredictable ways. A large percentage of these purely disruptive flaws are useful for Denial Of Service (DOS) attacks. The defining characteristic of a DOS attack flaw is the element of control. The DOS must be activated by an external action over which the perpetrator has control. As with any compromise of a computer system, access to exercise this control is crucial. Unfortunately, DOS flaws are legion, due to the pervasive instabilities in common operating system and application software packages.

In a DOS attack, triggering the flaw simply disables the target computer in some way, denying the services of that machine to the owner or intended user. Combined with extortion or other kinetic or IW attacks that the target computer was designed to monitor or prevent, DOS can be a useful component of many IW attacks. In the hacker community, which is largely a socially-based merit system, there are very few "brownie points" awarded for DOS attacks because they are so commonly available and easy to perpetrate.

One method for conducting a DOS attack is to transmit malformed data, which is data in a format that isn't expected by the target. For example, sending a negative value where the programmer assumed a positive value would always be received. Although the result of a malformed data packet is generally undetermined, the common result is to crash the target, thus denying service.

A small percentage of the inherent flaws in a software package are useful for more purposefully directed attacks. These include, in order of increasing severity: destruction of data (vandalism), viewing protected data (read capability), modifying data (read/write capability), and control of the system (administrative rights or root access). Of particular importance are exploits that allow a normal user to increase his assigned rights on the network to more powerful levels. These exploits allow a hacker who gains access to the network at any level to make himself an administrator, with full rights to every aspect of the system and data.

Hackers have the innate advantage, and they work together. The collegial, intellectual nature of the hacker community and of the Internet in general guarantees that many hundreds of hours are spent by malicious individuals to develop and improve existing, published exploits. Websites, chat rooms, private electronic bulletin board systems, and other services which cater to the malicious hacker number in the thousands. Hundreds of pre-designed exploits are categorically listed by operating system and software application on public electronic forums (e.g., see [www.rootshell.com](http://www.rootshell.com)<sup>7</sup>). Many more exploits exist or are in development in private venues, though private exploits are published coincident with news of the first major attack using the exploit.

## **Defending Against Computer Network Attack**

Effective computer security demands constant vigilance by all users, system administrators, and commanders—and depends upon an integrated security program that protects against hardware, software, and social engineering attacks. The cornerstone of all computer security programs is situational awareness, training, and education. “Security through obscurity,” i.e., not worrying about flaws buried in millions of line of code, is a very poor choice for network defense. Unauthorized access must be prevented through an active, layered defense, erecting sequential electronic defenses, which include intrusion detection systems. This strategy allows the defender to detect intruders in the information-gathering stage that precedes every significant information attack. The Achilles’ heel of this approach is that human operators must monitor intrusion detection systems for full effectiveness. This is a thankless task of reviewing scores of perfectly legitimate electronic transactions looking for the one obscure, innocent looking interchange that might indicate an attack. This time-consuming and boring task requires considerable technical skill and patience—a difficult combination.

## **The Application of International Law in Cyberspace**

There has been no evolution of international law to govern or prohibit State activities in cyberspace such as computer network attack. Indeed, maintaining a credible ability to project military force in cyberspace is a lawful and fundamentally important aspect of deterrence and maintenance of international peace and security. Existing international law, however, does govern the conduct of computer network attack and other State activities in cyberspace. While these international law norms do not explicitly address information operations, information warfare, computer network attack, or other State activities in cyberspace, they do prohibit the entire range of State activities that causes certain effects. Accordingly, it is critically important that all State activities in cyberspace, especially those conducted by the military and the intelligence community, be reviewed by assigned government counsel.

Until a legal regime matures that comprehensively addresses State activities in cyberspace, which is highly unlikely anytime in the near future, legal advisers must principally conduct an effects-based analysis of international law to determine the lawfulness of State activities in cyberspace. State activities must comply with the law of conflict management and the international peacetime regime, and, during times of armed conflict, the law of war.

Under the law of conflict management, all State activities in cyberspace must comply with the Charter of the United Nations. Unless otherwise authorized by the Security Council under its Chapter VII authority, Article 2(4) of the Charter prohibits the threat or use of force by any State against the territorial integrity or political independence of another State except in individual or collective self-defense as authorized by international law and recognized by Article 51 of the Charter. Customary international law requires that all use of force authorized under the law of conflict management be necessary and proportional.

Although unlawful under the domestic law of most States, the peacetime regime of international law permits espionage, but the unique nature of computer network attack, which allows remote electronic access, undermines the deterrent value of national law. Of grave concern is that many forms of computer espionage may be considered a hostile act or a demonstration of hostile intent, thereby causing a State to use military force in response. There are many other peacetime norms that govern State activities in cyberspace. The 1982 United Nations Convention on the Law of the Sea, for example, prohibits any act conducted in the territorial sea aimed at collecting information to the prejudice of the defense or security of the coastal State; any act of propaganda aimed at affecting the defense or security of the coastal State; and any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State. Similarly, peacetime telecommunications treaties such as the 1982 Nairobi Convention prohibit harmful interference with radio navigation services, and the 1976 INMARSAT Convention requires that its telecommunications infrastructure be used only for peaceful purposes.

Law of war principles embodied in the Geneva and Hague conventions as well as customary international law apply to State activities in cyberspace during armed conflict. For example, the universally accepted general principle that the “right of belligerents to adopt means of injuring the enemy is not unlimited” certainly places many restraints on the conduct of cyber warfare. Similarly, the principles of military necessity, unnecessary suffering, proportionality, distinction, and collateral damage also apply.

More detailed analyses of these and many other applicable international norms are provided later in this volume by other authors who are noted experts in international law. There are a number of issues, however, which remain unclear under international law. For example, what State activities in cyberspace constitute a use of force prohibited by the law of conflict management? What are peaceful purposes? Can hostile military activities which are tantamount to a use of force conducted in self-defense as recognized by Article 51 of the Charter of the United Nations be peaceful within the meaning of the INMARSAT

Convention? In modern society, the military is heavily dependent upon the civilian infrastructure, especially the telecommunications infrastructure. To what extent is the civilian telecommunications infrastructure a lawful target because a military relies upon it in some way for command and control or computer network attack? What about the Internet nodes of a State that is not a party to a conflict; is its telecommunications infrastructure a lawful target? Is a cyberattack against the critical infrastructures of an “undefended” city prohibited by the Hague Convention even if no physical destruction ensues? How do we regulate computer espionage to avoid the appearance of a hostile act or a demonstration of hostile intent without outlawing espionage completely? A legal review of these and the many other unresolved issues must be conducted in the context of the fundamental principle of international law and sovereignty which provides “that which is not prohibited is permitted.” Legal advisers must also understand and embrace the Internet technology of binary mathematics and electronic circuitry which forms the foundation of digital warfare.

### **The Future of Technology, Law, and Warfare**

While the future of technology, law, and warfare is uncertain, it is very clear that technology will continue to drive profound changes in the nature and conduct of 21st century warfare, and that international law, by its very nature, will always lag behind. The international community does not yet understand, much less agree, on how existing international law applies to State activities in cyberspace. An international consensus on a comprehensive regulation of State activities in cyberspace is very unlikely, and States must continue to regulate these activities by their own domestic laws and rules of engagement. In crafting their domestic norms, States must remember, however, that State practice will shape the evolution of international law that will in turn permit or prohibit future activities in cyberspace by all States.

The unintended consequences of computer network attack are also uncertain. For most, the notions of computer network attack and digital warfare conjures up visions of precision warfare, but these visions are far from reality. Information systems are constructed from flawed building materials. All operating systems, software applications, and hardware architectures contain many flaws that can be exploited by computer network attack—and the variations on how they can be combined represent almost an infinite number of vulnerabilities and unintended responses to unauthorized intrusions. Unauthorized access, such as during a computer network attack, therefore, has a relatively high probability of inducing instability into the target system. Without a complete and

accurate modeling of the target system, the uncertainty in predicting the exact primary, secondary, and subsequent order effects of a computer network attack is large. Obviously estimates of distinction, proportionality, and collateral damage are very tenuous when predicated on uncertain estimates of effects.

An exact determination of the uncertainty of a computer network attack is calculable, given *complete* information about the information systems involved, but such a calculation would become quickly outdated due to the fast pace of software development. Reasonable estimates that account for incomplete information are also possible, but these estimates are even more difficult and short-lived since minor changes to a system configuration can have dramatic effects on the results of a particular attack. Estimating the effects of a computer network attack will continue to be risky and inaccurate until the operating systems and applications, for the attacker as well as the target, achieve a reasonable measure of stability. Scenarios where a computer network attack on a military information system disables a linked civilian system that controls water purification, for instance, are very plausible.

The Information Environment (IE) is the new battlespace of the 21st century. The IE is the interrelated set of information, information infrastructure, and information-based processes. Information is data, information, and knowledge—and the information infrastructure is the hardware, software, and transport media used during information-based processes created when storing, manipulating, and transferring information. Denying, degrading, or destroying a select subset of the IE can have significant repercussions in one or more critical infrastructures and can be more effective than physical destruction. Manipulation of the IE now offers the potential to obtain political and military objectives without the use of kinetic weapons. Indeed, control of the IE may be far more effective than physical attack, and may be able to prevent future hostilities.

States must develop a national strategy to defend their own IEs and affect the international IE to successfully attain political and military objectives. Such a strategy requires breaking with traditional organizing, equipping, training, and warfighting strategy. Political support, along with appropriate planning guidance, strategy, and force structure, must be developed. The philosophical insights and intellectual understanding of such a national IE strategy are in their nascent stages and need further development.

Existing information systems have not begun to scratch the surface of the capabilities for self-aware behavior. In ten years, these systems will make practical use of what we have learned in both neural networks and artificial intelligence to model human thinking more closely. This means both that our information systems will modify their own behavior in response to past experience and that the

larger the network, the more effective this behavior will be. They will be capable of detecting and correcting defects in their own hardware, minor imperfections in their own software codes, damage due to neglect, vandalism, or war, and obvious errors in the judgment of their operators.

For information warfare, the potential of self-aware behavior is overwhelming. We could, for example, teach a distributed information system to gather information from a target network *exactly* as a series of a certain number of legitimate users would use the system, i.e., their intrusion detection software will not be able to distinguish between the two events. Or the attack could model an attack on the enemy network from 600 saboteurs in 200 locations, causing the target network to disconnect vast subnets. This would exacerbate the degradation of the target network's self-aware functions, denying it the information it needs to discriminate further fictional attacks from real events (the speed and accuracy of a neural net is directly related to the size of the net).

On the battlefield, individual warfighters will be connected to vast information resources to enable effective decision-making and coordination of troops. Forward observers will be automated and equipped with sensors that dwarf a human's information collecting hardware. Indeed, humans may not need to inhabit the kinetic battlefield at all.

Defensive capabilities will reap similar advantages, at some point pitting their software and processing skill against ours. With rapid software and hardware development likely to continue, a quickly escalating arms race in technology weapons is possible. Lagging behind in this race might be as deadly as losing an arms race in kinetic weapons, but the time scales will be much, much shorter.

The United States currently enjoys a distinct technological advantage. The most likely scenario is that this will continue and technical developments will generally tend to open the disparity in capability between us and our enemies, to our favor. Commercial development pressures will drive this naturally, although military applications need to be carefully identified as new technologies present new offensive and defensive possibilities. This creative ruminating is not trivial and must not be cursory—the selection process that produces technologists ensures that they are creative. The weapons they design will exploit non-obvious niches in new technologies.

At present, however, the instability of present operating systems and our dependence upon them, paradoxically leaves us more vulnerable to information warfare and computer network attack than less technically developed nations. Malicious code, HERF weapons, EMP, and other less sophisticated attacks could wreak great havoc in our technological society. This "Blue Book," and the conference on which it is based, is a tremendous step toward an international

understanding of the implications of information technology on a State's national security, the information environment, and the underlying international legal issues.

---

### Notes

1. STEPHEN BULL, *AN HISTORICAL GUIDE TO ARMS & ARMOR* 7 (1991).
2. Advanced Research Project Administration NETwork—later renamed DARPA NET: Defense Advanced Research Project Administration NETwork, although ARPA had always been a Department of Defense entity with military objectives.
3. M.L. YOUNG AND J.R. LEVINE, *INTERNET FAQs: ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS* 22–24 (1995).
4. National Science Foundation NETwork. The NSFNET was initiated to handle the increasing volume of traffic as the ARPANET became more and more popular. NSFNET also solved a number of technical headaches inherent in the original design of the ARPANET, and so eventually the ARPANET was phased out completely.
5. The Windows NT™ operating system, for instance, contains roughly fifty million lines of source code.
6. A notable exception is, of course, when the hacker works for a software development firm—a not infrequent case. Even in this case, inserting a “backdoor” providing access to the software after deployment is not trivial. The software development enterprise has layers of testing in place to catch such defects. While these layers of testing are far from foolproof, such a hacker has a slightly lower than even chance of success. Failure typically results in termination of employment, making repeated attempts statistically meaningless.
7. These sites are free and are extensively cross-referenced. The primary belief that motivates the maintainers of these sites is that full disclosure of all exploitable flaws is the only way for intelligent system administrators to ensure robust information systems security.