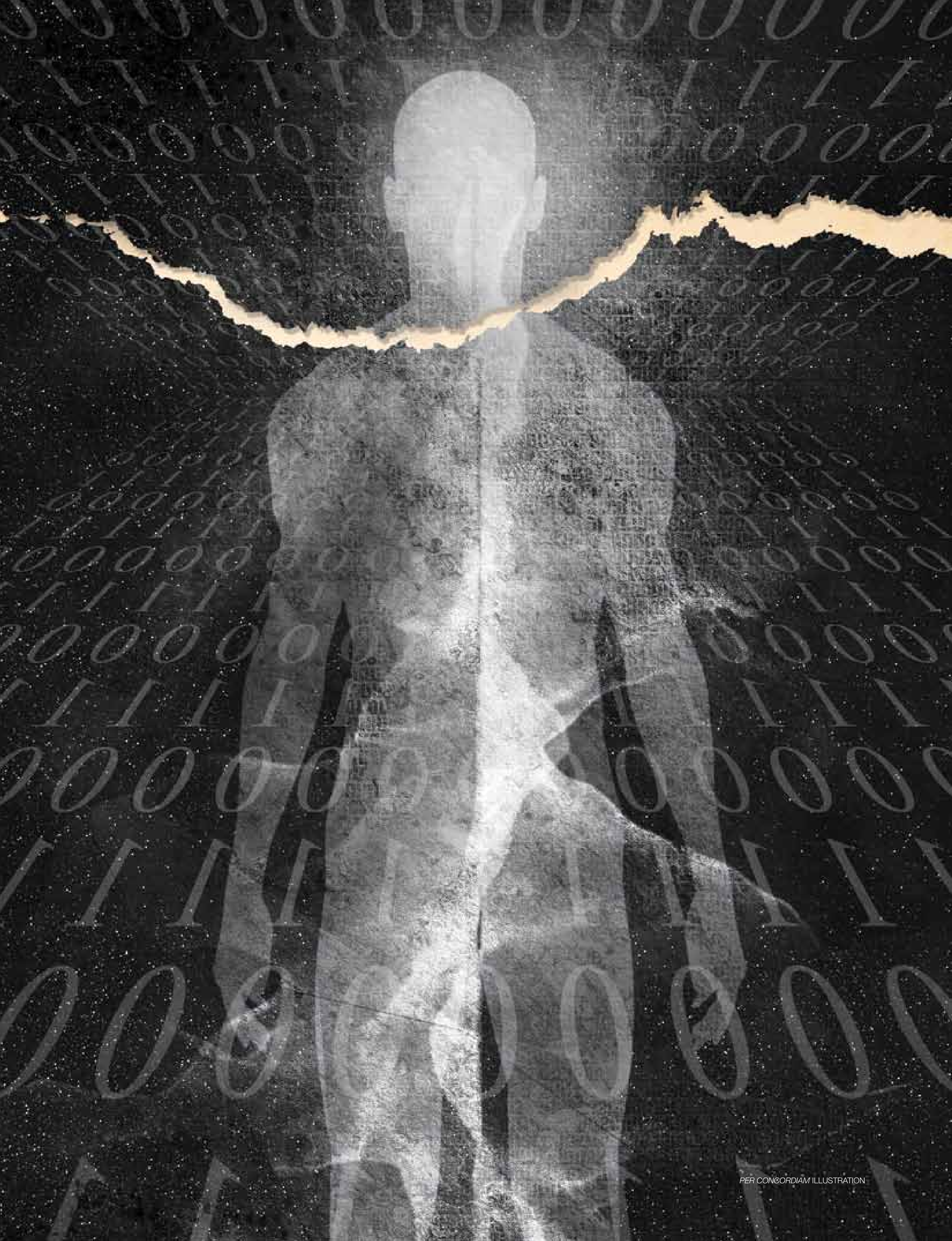


PER CONCORDIAM ILLUSTRATION

HEADING OFF HACKERS

CRIMINALS WIELD COMPUTERS AS CHEAP, ANONYMOUS WEAPONS

KENNETH GEERS
U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

The Internet has changed almost all aspects of human life, including warfare. Every political and military conflict now has a cyber dimension whose size and impact are difficult to predict.

Computers and computer networks have provided a new delivery mechanism that can increase the speed, diffusion and significance of a national security threat. The constant evolution of information technology tends to leave both cyber law and cyber defense breathless. The ubiquity and amplification power of the Internet often make the battles fought there seem more important than events taking place on the ground.

The intangible nature of cyberspace, however, can make the calculation of victory, defeat, and battle damage a highly subjective undertaking. Even knowing whether one is under cyber attack can be a challenge.

National security thinkers are therefore struggling with the complexities of cyber conflict for a wide variety of reasons, including an ignorance of its technical foundations, media-fueled paranoia, and a desire to take advantage of hacking's high return-on-investment before it goes away.

This article seeks to articulate cyber warfare in basic concepts and definitions, enhancing the discussion on cyber defense strategies and tactics.

History

What military officers refer to as the "battlespace" grows more difficult to define and defend over time. Advances in technology are normally evolutionary, but they can be revolutionary, such as when artillery shells reached over the front lines of battle and rockets and airplanes crossed national boundaries. Today, cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, with the added benefit of attacker anonymity.

Every political and military conflict now has a cyber dimension whose size and impact are difficult to predict.

In 1965, Gordon Moore correctly predicted that the number of transistors on a computer chip would double every two years. There has been similar growth in almost all aspects of information technology, including the availability of practical encryption, user-friendly hacker tools, and Web-enabled open source intelligence, or OSINT.

To achieve their objectives, political and military strategists now use and abuse computers, databases and the networks that connect them. In the early 1980s, this concept was already known in the Soviet Union as the Military Technological Revolution. Following the 1991 Gulf War, the Pentagon's Revolution in Military Affairs was almost a household term.

Cyberspace as a war-fighting domain currently favors the attacker, which stands in contrast to our historical understanding of warfare, whereby the defender normally enjoys a significant home field advantage. Further, the terrestrial proximity of adversaries is unimportant because in cyberspace everyone is a next-door neighbor. And there is little moral inhibition to computer hacking because it relates primarily to the use and abuse of computer code. So far, there is little perceived human suffering.

In spite of these advantages for the attacker, many analysts remain skeptical of the seriousness of the cyber threat. In part, this is because a real-world outcome is not guaranteed. In cyber warfare, tactical victories amount to a successful reshuffling of the bits — also known as ones and zeros — inside a computer. At that point, the attacker must wait to see if the intended real-world effects occur.

Motivations for hacking

Experts cite five main reasons for hacking:

- **Vulnerability:** Flaws in the Internet's design allow hackers to secretly read, delete or modify information stored on or traveling between computers. The rapid proliferation of Internet technologies makes it impossible for defenders to keep up with all of the latest attack methods. There are about 100 additions to the Common Vulnerabilities and Exposures, or CVE, database each month. In short, hackers have more paths into a network than its system administrators can protect.
- **Return on investment:** This applies to government, civil society and individuals. A hacker's goals are self-explanatory: the theft of research and development data, eavesdropping on sensitive communications, and the delivery of propaganda behind enemy lines. The elegance of computer hacking lies in the fact that it can be attempted for a fraction of the cost (and risk) of any other information collection or manipulation strategy.
- **Inadequate cyber defense:** Computer network security is still an immature discipline. Traditional security skills are of marginal help in cyber warfare, and it is difficult to retain personnel with marketable technical expertise. Challenging computer investigations are further complicated by the international nature of the Internet. And in the case of state-sponsored cyber operations, law enforcement cooperation is naturally nonexistent.
- **Plausible deniability:** The mazelike architecture of the Internet offers a high degree of anonymity to cyber attackers. Smart hackers route their attacks through countries where the victim's government has poor diplomatic relations or no law enforcement cooperation. Even successful cyber investigations often lead only to another hacked computer. Governments today face the prospect of losing a cyber conflict without even knowing the identity of an adversary.
- **Empowerment of nonstate actors:** The Internet era offers vastly increased participation on the world stage. Governments would like to control international conflict, but globalization and the Internet have considerably strengthened the ability of anyone to follow current events, and have provided a powerful means to influence them. Transnational subcultures now coalesce online, sway myriad political agendas, and do not

AGENCE FRANCE-PRESSE

The computer hacker known as "Mafiaboy," accused of disrupting traffic over the Internet, leaves court following his trial in Montreal in 2001.

AGENCE FRANCE-PRESSE

A man walks inside the Pionen White Mountains high-security computer storage facility of Swedish Internet service provider Bahnhof in Stockholm. The Pionen data center, once a Cold War era nuclear bunker, is one of the most well-protected in the world.

report to a chain of command. A future challenge for world leaders is whether their own citizens could spin delicate international diplomacy out of control.

Hacker targets

There are three basic types of cyber attack, from which all others derive:

• **Confidentiality**: This encompasses any unauthorized acquisition of information, including via "traffic analysis," in which an attacker infers communication content merely by observing communication patterns. Because global network connectivity is currently well ahead of global network security, it can be easy for hackers to steal enormous amounts of information.

Cyberterrorism and cyber warfare may still lie in our future, but we are already living in a golden age of cyber espionage. The most famous case to date is "GhostNet," investigated by Information Warfare Monitor, in which a cyber espionage network of more than 1,000 compromised computers in 103 countries targeted diplomatic, political, economic and military information.

• **Integrity:** This is the unauthorized modification of information or information resources such as a database. Such attacks can involve the "sabotage" of data for criminal, political or military purposes. Cybercriminals have encrypted data on a victim's hard drive, and then demanded a ransom payment in exchange for the decryption key. Governments that censor Google results return part, but not all, of the search engine's suggestions to an end user.

• **Availability:** The goal here is to prevent authorized users from gaining access to the systems or data they require to perform certain tasks. This is commonly referred to as a denial-of-service (DoS), and encompasses a wide range of malware, network traffic or physical attacks on computers, databases and the networks that connect them.

In 2001, "mafiaboy," a 15-year-old student from Montreal, conducted a successful DoS attack against some of the world's biggest online companies, likely causing over $1 billion in financial damage.

Hacker goals

A cyber attack is not an end in itself, but an extraordinary means to a wide variety of ends, limited primarily by the imagination of the attacker.

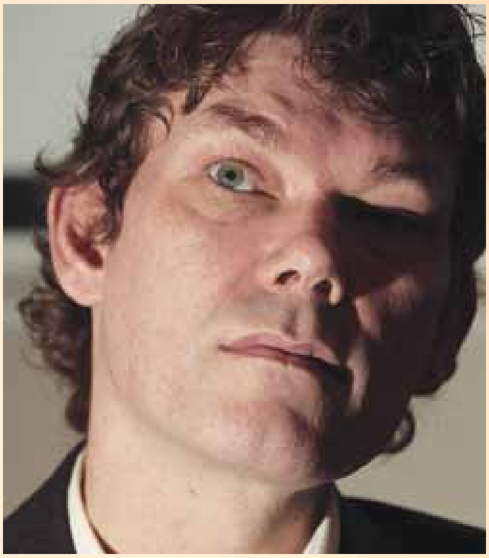
• **Espionage:** Every day, anonymous computer hackers steal vast quantities of computer data and network communications. In fact, it is possible to conduct devastating intelligence-gathering operations, even on highly sensitive political and military correspondence, remotely from anywhere in the world.

• **Propaganda:** Cheap and effective, this is often the easiest and most powerful form of attack. Digital information in text or image format — regardless of whether it is true — can be instantly copied and sent anywhere in the world, even deep behind enemy lines. And provocative information that is censored from the Web can reappear in seconds elsewhere.

• **Denial-of-service (DoS):** The simple goal is to deny the use of data or computers to legitimate users. The most common tactic is to flood the target with so much superfluous data that it cannot respond to real requests for services or information. Other DoS attacks include the

AGENCE FRANCE-PRESSE

AGENCE FRANCE-PRESSE



physical destruction of computer hardware and use of electromagnetic interference designed to destroy unshielded electronics via current or voltage surges.

- **Data modification:** A successful attack on the integrity of sensitive data can mean that legitimate users (human or machine) will make important decisions based on maliciously altered information. Such attacks range from website defacement, which is often referred to as "electronic graffiti," but which can still carry propaganda or misinformation, to the corruption of advanced weapons systems.
- **Infrastructure manipulation:** National critical infrastructures, or CI, are increasingly connected to the Internet. However, because instant response may be required, and associated hardware may have insufficient computing resources, CI security may not be robust. The management of electricity could be especially important for national security planners to evaluate, because electricity has no substitute, and all other infrastructures depend on it. Finally, it is important to note that many CI are in private hands.

If there is a war between major world powers, the first victim of the conflict could be the Internet itself.

Cyber attacks in war

In the future, the ultimate goal of warfare — victory — will not change. And the advice of Sun Tzu and Clausewitz will still apply. However, the tactics of war are radically different in cyberspace, and if there is a war between major world powers, the first victim of the conflict could be the Internet itself.

There will be two broad categories of cyber attacks during a major war:

- **Military forces:** The attacks would be conducted as part of a broader effort to disable the adversary's weaponry and to disrupt military command-and-control systems.

In 1997, the U.S. Department of Defense held a large-scale cyber attack red team exercise called Eligible Receiver. The simulation was a success. As James Adams wrote in Foreign Affairs, 35 National Security Agency personnel posing as North Korean hackers used a variety of cyber-enabled information warfare tactics to "infect the human command-and-control system with a

THE ASSOCIATED PRESS

From far left: An alleged militant with the Global Islamic Media Front is led into a courtroom in Vienna in August 2009. He was sentenced to four years behind bars for producing an Islamic threat video distributed on the Internet.

Scottish hacker Gary McKinnon faces extradition to the U.S. under anti-terrorism laws following his breaching of military computers dating back to 2001. He could face up to 70 years in prison.

The Dalai Lama, Tibet's spiritual leader, responds to reports that a cyber spy network based mainly in China hacked into classified documents stored on computers of the Dalai Lama and Tibetan exiles.

paralyzing level of mistrust. … As a result, nobody in the chain of command, from the president on down, could believe anything."

In 2008, unknown hackers broke into both unclassified and classified computers at U.S. Central Command, the organization that manages both wars in which the U.S. is engaged. The Pentagon was so alarmed by the attack that Chairman of the Joint Chiefs of Staff Michael Mullen personally briefed President George Bush.

In the event of a war between major powers, it is wise to assume that the above-mentioned attacks would pale in comparison to the sophistication and scale of cyber tools and tactics that governments may hold in reserve for a time of national security crisis.

- **Civilian infrastructure:** These would target the adversary's ability and willingness to wage war for extended periods, and may include an adversary's financial sector, industry and national morale.

One of the most effective ways to undermine a variety of these second-tier targets is to disrupt power generation and supply. In May 2009, President Barack Obama made a dramatic announcement: "cyber intruders have probed our electrical grid. … In other countries, cyber attacks have plunged entire cities into darkness." It is believed that these attacks took place in Brazil in 2005 and 2007, affecting millions of civilians, and that the source of the attacks is still unknown.

Referring to theoretical cyber attacks on the financial sector, former U.S. Director of National Intelligence Mike McConnell said his primary concern was not the theft of money, but an attack on the integrity of the financial system itself, designed to destroy public confidence in the security and supply of money.

Today, militaries can exploit global connectivity to conduct a full range of cyber attacks against adversary CI, deep behind the front lines of battle.

Looking to the future

The Internet has changed the nature of warfare. Computers are both a weapon and target. As with terrorism, hackers have found success in pure media hype. As with weapons of mass destruction, it is difficult to retaliate against an asymmetric attack.

On balance, cyber warfare may favor nations robust in IT, but the Internet is a prodigious weapon for a weaker party to attack a stronger conventional foe. And Internet-dependent nations have more to lose when the network goes down.

From a defensive standpoint, nations should invest in technologies that mitigate two key hacker advantages: poor attacker attribution and a high level of asymmetry. The often anonymous nature of computer hacking and its very high return on investment can prevent traditional risk mitigation, such as deterrence and arms control.

At this point in history, many governments may feel compelled to invest in cyber warfare, not only as a way to project national power, but as the only means to defend their presence in cyberspace. □