In other domains, the primary threats to national security come from either nation states or transnational actors, such as terrorist organizations. Massive capital resources and personnel are required to build, field, maintain, and operate fighter aircraft, satellites, and ships, but it took only a small and determined organization with simple tools to fly into the World Trade Center buildings on September 11, 2001. Adversaries seek asymmetric advantages and cyberspace provides significant opportunities for obtaining them.

There are a variety of threats to cyberspace operations. The following paragraphs provide a brief description of each category of threat. These threats and others should be considered when conducting cyberspace operations.1

**Nation State Threat.** This threat is potentially the most dangerous because of access to resources, personnel, and time that may not be available to other actors. Other nations may employ cyberspace to attack and conduct espionage against the US. Nation state threats involve traditional adversaries and sometimes, in the case of espionage, even traditional allies. Nation states may conduct operations directly or may outsource third parties to achieve their goals.

**Transnational Actor Threat.** Transnational actors are formal and informal organizations that are not bound by national borders. These actors use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, destabilize confidence in governments, and conduct direct terrorist action.

**Criminal Organization Threat.** Criminal organizations may be national or transnational in nature depending on how they are organized. Criminal organizations steal information for their own use or, in turn, sell it to raise capital.

**Individual or Small Group Threat.** Individuals or small groups of people can illegally disrupt or gain access to a network or computer system—these people are better known as “hackers.” The intentions of hackers vary. Some are peaceful and hack into systems to discover vulnerabilities, sometimes sharing the information with the owners and some have malicious intent. Other hackers have political motivations and use

---

cyberspace to spread their message to target audiences. Another type of hacker desires fame or status, and obtains it by breaking into secure systems or creating malware that creates havoc on commercial or government systems. Malware is the short name for "malicious software." Hackers can also be exploited by the other cyberspace threats, such as criminal organizations, in order to execute concealed operations against specific targets while preserving their identity or create plausible deniability.

In May 05, an unknown subject obtained unauthorized user level access to the Assignments Management System (AMS). Using this access, the subject was able to view information contained within the AMS, but was unable to alter information or gain access to any other Air Force computer systems. Computer records indicate that the subject gained access to AMS via a senior Air Force official's account. The compromised AMS account was set with privileges which allow the user to review any active duty Air Force members' single unit retrieval format (SURF) data from anywhere in the world with an Internet connection. SURF records contain sensitive data, such as assignment history, security clearance, personal identification information, rank, position, and duty status. The subject gained access to the web based account using the "forgot password" function to answer the challenge questions required to change the account password. The challenge questions asked for biographical information on the senior official, which was readily available on the Internet.

Upon review, it was determined that the senior USAF official's account had been used to view the SURF records of 37,069 Air Force members. Log analysis indicates the intrusion initially originated from forty-one different source IP addresses throughout the duration that the compromised account was used by the subject.

Throughout this duration the subject's activity originated from approximately twelve additional US based Internet Protocol (IP) addresses, which were later determined to be open proxies that the subject used to mask their true place of origin. There were no foreign based IP addresses used after the incident was reported. Court order subpoenas were served on all US-based source IP addresses from which the compromised AMS account was accessed; fifty in total. Information obtained via court order subpoenas identified the last known point of the origin. However, local law enforcement indicated that the information required to further identify the subject was no longer available.

—Air Force Office of Special Investigations Brief, June 2005
Traditional Threat. Traditional threats typically arise from states employing recognized military capabilities and forces in well-understood forms of military conflict. Within cyberspace, these threats may be less understood due to the continuing evolution of technologies and methods. Traditional threats are generally focused against the cyberspace capabilities that enable our air, land, maritime, special operations, and space forces and are focused to deny the US military freedom of action and use of cyberspace.

Irregular Threat. Irregular threats can use cyberspace as an unconventional asymmetric means to counter traditional advantages. These threats could also manifest through an adversary’s selective targeting of US cyberspace capabilities and infrastructure. For example, terrorists could use cyberspace to conduct operations against our financial and industrial sectors while simultaneously launching other physical attacks. Terrorists also use cyberspace to communicate anonymously, asynchronously, and without being tied to set physical locations. They attempt to shield themselves from US law enforcement, intelligence, and military operations through use of commercial security products and services readily available in cyberspace. Irregular threats from criminal elements and advocates of radical political agendas seek to use cyberspace for their own ends to challenge government, corporate, or societal interests.

Catastrophic Threat. Catastrophic threats involve the acquisition, possession, and use of weapons of mass destruction (WMD) or methods producing WMD-like effects. While WMD attacks are physical (kinetic) events, they may have profound effects within the cyberspace domain by degrading or destroying key cyber-based systems vital to infrastructure like supervisory control and data acquisition (SCADA) systems. Well-planned attacks on key nodes of the cyberspace infrastructure have the potential to produce network collapse and cascading effects that can severely affect critical infrastructures locally, nationally, or possibly even globally. For example, an electromagnetic pulse could cause widespread damage to segments of the cyberspace domain in which operations must occur.

Disruptive Threat. Disruptive threats are breakthrough technologies that may negate or reduce current US advantages in warfighting domains. Global research, investment, development, and industrial processes provide an environment conducive to the creation of technological advances. The DOD should be prepared for the increased possibility of adversary breakthroughs due to continuing diffusion of cyberspace technologies.

Natural Threat. Natural threats that can damage and disrupt cyberspace include events such as floods, hurricanes, solar flares, lightning, and tornados. These types of events often produce highly destructive effects requiring the DOD to maintain or restore
key cyberspace systems. These events also provide adversaries the opportunity to capitalize on infrastructure degradation and diversion of attention and resources.

**Accidental Threat.** Accidental threats are unpredictable and can take many forms. From a backhoe cutting a fiber optic cable of a key cyberspace node, to inadvertent introduction of viruses, accidental threats unintentionally disrupt the operation of cyberspace. Although post-accident investigations show that the large majority of accidents can be prevented and measures put in place to reduce accidents, accidents should be anticipated.

**Insider Threat.** The "insider" is an individual currently or at one time authorized to access an organization's information system, data, or network. Such authorization implies a degree of trust in the individual. The insider threat refers to harmful acts that trusted insiders might carry out; for example, something that causes harm to the organization, or an unauthorized act that benefits the individual.