Cyber Threat Source Descriptions

Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above.

- National Governments
- Terrorists
- Industrial Spies and Organized Crime Groups
- Hacktivists
- Hackers
- GAO Threat Table

For the purpose of this discussion, deliberate threats will be categorized consistent with the remarks in the Statement for the Record to the Joint Economic Committee by Lawrence K. Gershwin, the Central Intelligence Agency's National Intelligence Officer for Science and Technology, 21 June 2001. These include: national governments, terrorists, industrial spies, organized crime groups, hacktivists, and hackers. Activities could include espionage, hacking, identity theft, crime, and terrorism.

National Governments

National cyber warfare programs are unique in posing a threat along the entire spectrum of objectives that might harm US interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyber threats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage to U.S. critical infrastructures.

The tradecraft needed to effectively employ technology and tools remains an important limiting factor, particularly against more difficult targets such as classified networks or critical infrastructures. For the next 5 to 10 years, only nation states appear to have the discipline, commitment, and resources t

TLP:WHITE

capabilities to attack critical infrastructures.

Their goal is to weaken, disrupt or destroy the U.S. Their sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack the US economy, full scale attack of the infrastructure when attacked by the U.S. to damage the ability of the US to continue its attacks.

Back to top

Terrorists

Traditional terrorist adversaries of the U.S., despite their intentions to damage U.S. interests, are less developed in their computer network capabilities and propensity to pursue cyber means than are other types of adversaries. They are likely, therefore, to pose only a limited cyber threat. Since bombs still work better than bytes, terrorists are likely to stay focused on traditional attack methods in the near term. We anticipate more substantial cyber threats are possible in the future as a more technically competent generation enters the ranks.

Their goal is to spread terror throughout the U.S. civilian population. Their sub-goals include: attacks to cause 50,000 or more casualties within the U.S. and attacks to weaken the U.S. economy to detract from the Global War on Terror.

Back to top

Industrial Spies and Organized Crime Groups

International corporate spies and organized crime organizations pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent.

Their goals are profit based. Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry using potential public exposure as a threat.

Back to top

Hacktivists

Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-U.S. motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause.

Back to top

Hackers

Although the most numerous and publicized cyber intrusions and other incidents are ascribed to computer-hacking hobbyists, such hackers pose a negligible threat of widespread, long-duration damage to national-level infrastructures. The large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks and even fewer would have a motive to do so. Nevertheless, the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled and malicious hacker attempting and succeeding in such an attack.

In addition, the huge worldwide volume of relatively less skilled hacking activity raises the possibility of inadvertent disruption of a critical infrastructure.

For the purposes of this discussion, hackers are subdivided as follows:

- Sub-communities of hackers
- Script kiddies are unskilled attackers who do NOT have the ability to discover new vulnerabilities or write exploit code, and are dependent on the research and tools from others. Their goal is achievement. Their sub-goals are to gain access and deface web pages.
- Worm and virus writers are attackers who write the propagation code used in the worms and viruses but not typically the exploit code used to penetrate the systems infected. Their goal is notoriety. Their sub-goals are to cause disruption of networks and attached computer systems.
- Security researcher and white hat have two sub-categories; bug hunters and exploit coders. Their goal is profit. Their sub-goals are to improve security, earn money, and achieve recognition with an exploit.
- Professional hacker-black hat who gets paid to write exploits or actually penetrate networks; also falls into the two sub-categories-bug hunters and exploit coders. Their goal is profit.

Nature of the Computer Security Community

Hackers and researchers interact with each other to discuss common interests, regardless of color of hat. Hackers and researchers specialize in one or two areas of expertise and depend on the exchange of ideas and tools to boost their capabilities in other areas. Information regarding computer security research flows slowly from the inner circle of the best researchers and hackers to the general IT security world, in a ripple-like pattern.

Back to top

GAO Threat Table

The following table is an excerpt from NIST 800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security (SME draft), provides a description of various threats to CS networks:

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).

Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized cr using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).

Back to top

TLP:WHITE