Information Warfare - Defense

Incident Classifications

and

Watch Conditions (WATCHCONs)

Class I IW Incidents - Privacy Invasion

Class I IW incidents are characterized by computer intrusions and attempted intrusions from a variety of sources which essentially invade the privacy of individual or organizational computer users of non-classified networks. Class I incidents do not include any evidence of intent to cause damage to the data or networks accessed. This could also be characterized as low-level computer, "hacking." These incidents could come from either domestic or foreign sources.

Class II IW Incidents - Commercial/Industrial Espionage

Class II IW incidents are characterized by concerted attempts or actual penetrations of commercial computer systems to gain unauthorized access to specifically targeted or sensitive information for the purposes of obtaining that information. Class II incidents do not include any evidence of intent to cause damage to the data or networks accessed. These incidents could come from either domestic or foreign sources.

Class III IW Incidents - Military/Government Espionage

Class III IW incidents are characterized by concerted attempts to penetrate, or actual penetrations of military or government computer systems to gain access to and/or steal classified information. Class II incidents do not include any evidence of intent to cause damage to the data or networks accessed. These incidents could come from either domestic or foreign sources Intrusions into unclassified government networks containing sensitive data falls under this category when evidence of foreign involvement or specific targeting is present.

Class IV IW Incidents - Low Level PSYOP/Deception Programs

Class IV IW incidents are characterized by persistent, long term, low level PSYOP or Deception programs which occur at times of mildly increased tension between the United States and an adversary. Typically they include the increase in news items which are favorable to the adversary nations. The original source of these news items may be very difficult to determine

Class V IW Incidents - Commercial Terrorism

Class V IW incidents are characterized by penetrations or concerted attempts to penetrate the computer systems of commercial businesses in an attempt to electronically destroy or degrade those systems or to threaten to destroy computer systems in order to extort money. These incidents could come from either domestic or foreign sources.

Class VI IW Incidents - Civilian and Governmental Infrastructure Terrorism and Attack

Class VI incidents usually occur during a time of impending or ongoing crisis with a foreign power. They can include foreign, state-sponsored PSYOP, Deception, Electronic Warfare against and physical sabotage (destruction) of non-military U.S. government information systems. Class V incidents may also include attacks against the computer systems of key civilian or non-DoD governmental organizations which operate critical elements of the U.S. infrastructure. Those computer attacks may include destructive or degrading electronic codes and viruses or the insertion of false data.

Class VII IW Incidents - Military Infrastructure Terrorism & Attack

Class VII incidents usually occur during a time of impending or ongoing crisis with a foreign power. They can include confirmed foreign, state-sponsored PSYOP, Deception, Electronic Warfare against and physical attack or sabotage (destruction) of U.S military information systems. Class VII incidents also may include attacks against the computer systems of military organizations which operate critical elements of the U.S. military support structure. Those computer attacks may include destructive or degrading electronic codes and viruses or the insertion of false data.

WATCHCON 5 - Operations Normal

No significant IW events. No significant rise in the numbers of small, isolated IW events. May be characterized by a normal level of Class I events.

WATCHCON 4 - Slight Rise In IW Events.

A slightly larger than normal number of IW events have occurred. No significant events which cause major system damage, outages or losses. No correlation of IW events to foreign governments. Characterized by a statistically significant rise in the overall number of Class I events. May also be characterized by suspected Class IV PSYOP or deception events.

OR

A significant IW event has occurred, but purposeful intent vice accidental happenstance cannot be confirmed. May be characterized by a Class II event or events.

WATCHCON 3 - Significant Increase In IW Events.

A significant, confirmed IW event has occurred which causes or has the potential to cause major damage, outages or losses to the U.S. government, military or business. May or may not be accompanied by a slight increase in the number of IW events. No correlation of this major IW event to foreign governments. May be characterized by a rise in the number of Class II, Class III, Class IV or Class V events

WATCHCON 2 - Significant Increase In Attributable IW Events.

A significant, confirmed IW event/s has/have occurred which causes or has the potential to cause major damage, outages or losses to the U.S. government, military or business. This event or events are possibly, or probably correlated to the purposeful activity of a foreign government The overall number of attributable and non-attributable IW events have increased. Characterized by an increase in the number of Class III, Class IV and Class V events. Also characterized by the confirmation of initial Class VI and/or Class VII events being launched by a foreign power. May also be characterized by an increase in the number of Class III and Class IV events.

WATCHCON 1 - Broad Scale, Attributable IW Attacks.

Significant, confirmed IW events have occurred and are occurring. A number of the events are attributable to a hostile, foreign power. The foreign power initiating the events is also involved in hostilities or crisis confrontation with the United States in other political, international or military arenas. Characterized by a large number of Class IV, Class V, Class VI and/or Class VII events.

Key Definitions

Command and Control Warfare: The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict.

C^2 Attack: Prevent effective C^2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C^2 system.

C^2 Protect: Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C^2 system.

Command and Control: The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission.

Computer Network Attack (CNA): Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Counterinformation: Action dedicated to controlling the information realm.

Defense Information Infrastructure (DII): Is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD's local, national, and world-wide information needs. The DII connects DOD mission support, C^2, and intelligence computers through voice, telecommunications, imagery, video-and multi-media services.

Defensive Counterinformation: Actions protecting our military information functions from the adversary.

Global Information Infrastructure (GII): An interconnection of communications networks, computers, databases, and consumer electronics that makes vast amounts of information available to users. It encompasses a wide range of equipment including cameras, scanners, keyboards, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave, nets, switches, televisions, monitors, printers, etc. The GII includes more than the physical facilities used to store, process, and

display voice data, it also includes the personnel who operate and consume the transmitted data.

Information: Facts, data or instructions in any medium or form.

Information Assurance: IO that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Attack: Directly corrupting information without visibly changing the physical entity within which it resides.

Information Environment: The aggregate of individuals, organizations, or systems that collect, process or disseminate information, also included is the information itself.

Information Function: Any activity involving the acquisition, transmission, storage, or transformation of information.

Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority: The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare: Information Operations (IO) conducted during time of crisis or conflict to achieve or promote specific objectives against a specific adversary or adversaries.

Information Warfare - Defense: Protecting the National Information Infrastructure and the Defense Information Infrastructure and interrelated CONUS infrastructures against physical and electronic attacks and ensuring the availability of those infrastructures for commercial and military use.

Military Information Function: Any information function supporting and enhancing the employment of military forces.

National Information Infrastructure (NII): The NII mirrors the GII but is focused on national instead of global networks and systems.

Offensive Counterinformation: Actions against the adversary's information functions.

Special Information Operations (SIO): Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U.S., require a special review and approval process.