them. Spoofing attacks that seek to gain unauthorized access to a space system by emulating an authentic user could permit an intruder to disrupt normal satellite operations.[3] Given the current state of telemetry and spacecraft reliability, an operator might never know whether such an anomaly was an ordinary onboard glitch or the work of a hostile actor.

Figure 11-4
StoptheNATO.org's Netstrike Against NATO campaign.

Cyber attacks are becoming more commonplace. On 28 May 2002 the grassroots Netstrike Against NATO campaign launched a distributed denial-of-service attack against the main website of NATO, coinciding with a meeting of its leaders in Italy.[4] While the US Department of Defense's computer systems have been attacked almost every day for years (estimated at 250,000 times in 1996), the real number of these attacks is difficult to assess because such a small number are actually detected.[5] While the military space assets of the most advanced space-faring states are relatively well protected, not all space security actors enjoy this level of protection, making this type of space negation capability an attractive and relatively low-cost option for many states.

Robotic Manipulation. Satellites are relatively fragile and ungainly systems; they often require devices dedicated to keeping them pointed in the right orientation to ensure their proper operation. Consequently, some satellites could be 'tipped over' by a robotic servicing device from which states they might never recover. Thus, in-orbit robotic manipulators represent a potential space negation capability. Concerns about this capability were expressed by the former Soviet Union over the development of the US space shuttle and its Canadian shuttle remote manipulator system, more commonly known as the Canadarm (see Figure 11-5). However, the likelihood of robotic manipulation systems being used as a space negation capability is remote as it would represent the use of very expensive and complex systems to allow missions that could otherwise be accomplished by less expensive means. This technology is assessed to be limited to the United States, the European Union, Russia, Japan, and Canada.

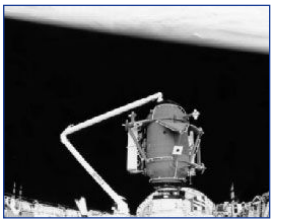

Figure 11-5
Canadarm being used to install the shuttle docking port on Mir.

Permanent or Irreversible Space Negation - Degradation and Destruction

Beyond temporary space system negation efforts, negation may also be undertaken through the application of force to degrade or actually destroy the ground or space segments of an adversary's space systems. Terrestrial satellite control and launch facilities are vulnerable to a wide range of military attacks that could degrade or completely destroy essential components of an actor's space systems or their access to space. Indeed, this approach is widely assessed to be the most cost effective and readily achievable space negation option for most actors. However, attacks against control stations would risk the creation of collateral space debris because satellites without effective ground stations would not receive orbit control or space debris mitigation commands.