engaged in military preparations for Internet warfare. In a recent report to the U.S. Senate the director of the CIA, George Tenet, said that China, Russia, and other states have undertaken "extraordinary" steps to develop an Internet warfare capability.[33] It is difficult to determine the veracity of these reports, however, since heightened and distorted threat construction is a common practice within U.S. military-intelligence circles. What is clear is that the United States itself is actively engaged in such preparations, having gone to great lengths to ensure they receive widespread media exposure.[34] Given the extent of financial, commercial, and other interdependencies between states, however, the prospects of two large states actually assaulting each other in full-blown "electronic warfare" seem remote. Scenarios involving stock exchanges being targeted by *states* with sophisticated electronic tools of warfare fail to account for the "blowback" that would be unleashed on the initiating state itself, as the ripple effects of recent financial crises in Asia demonstrate. More realistic, perhaps, would be sporadic low-level electronic disruptions undertaken by so-called "rogue" states, terrorists, and other non-state actors.

Indeed, numerous and increasing incidents of the latter sort have contributed the most fuel to the rise of this collective image. The most sensational (but least severe) of them have involved the de-facing of webpages, including those of NASA, the CIA, and

---

[33] See "A Prelude to InfoWar," Reuters (24 June 1998).
[34] See James Der Derian, "Global Swarming, Virtual Security, and Bosnia," The Washington Quarterly, (Vol. 19, No. 3, 1996), pp. 45-56; and Douglas Waller, "Onward Cyber Soldiers," Time (August 21, 1995), pp. 30-38.