diffuse development of highly sophisticated public key encryption systems. Today, encryption software with keys in the 1000-bit range are freely distributed over the Internet -- a level of sophistication that would be resistant for decades to even the most advanced network of Cray supercomputers at the service of government security agencies. Although states may set regulations that prohibit the use and export of such technologies, the consensus among most is that "the genie is out of the bottle."[85] At best, prohibitions against encryption use and "key escrow" schemes are contrivances to buy time in a losing battle. The encryption properties of the communications environment clearly "favor" the privacy and network security collective images outlined above.

c. Post-Industrial Global Capitalism. A further boost to the network security collective image is provided by changes in the global political economy, particularly the transnationalization of production and the globalization of finance. Although the full details of the latter are beyond the scope of this paper, they are well documented elsewhere. What is of relevance, however, is that these changes have generated a large constituency of powerful interest groups who support the network security

---

[85] For an excellent analysis along these lines, see Eric Hellweiner, "Electronic Money: A Challenge to the Sovereign State?" Journal of International Affairs (Vol 51, No. 2, Spring 1998), pp. 387-409.

[86] See "Titanic Meeting Stuck at Dock," Wired News (10 June 1998). Of the availability of complex encryption codes outside of the United States, Microsoft CEO Bill Gates said "That's a change in the world of spying and law enforcement that we cannot effect" -- meaning, precisely, that the clock cannot be turned back on encryption technologies. Likewise, the U.S. National Research Council's report, "Cryptography's Role in Securing the Information Society" concluded that " Because cryptography is an important tool for protecting information and because it is very difficult for governments to control, the committee believes that the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run." Kenneth Dam and Herbert Lin, (eds.) Cryptography's Role in Securing the Information Society. National Research Council, (1996).