

(Continued)

- ▶ Within the past year [2012], in a denial-of-service campaign against the public websites of multiple US banks and stock exchanges, actors flooded servers with traffic and prevented some customers from accessing their accounts via the Internet for a limited period, although the attacks did not alter customers' accounts or affect other financial functions.
- ▶ In an August 2012 attack against Saudi oil company Aramco, malicious actors rendered more than 30,000 computers on Aramco's business network unusable. The attack did not impair production capabilities.

Eroding US Economic and National Security

Foreign intelligence and security services have penetrated numerous computer networks of US Government, business, academic, and private sector entities. Most detected activity has targeted unclassified networks connected to the Internet, but foreign cyber actors are also targeting classified networks. Importantly, much of the nation's critical proprietary data are on sensitive but unclassified networks; the same is true for most of our closest allies.

- ▶ We assess that highly networked business practices and information technology are providing opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive US national security and economic data. This is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena.
- ▶ It is very difficult to quantify the value of proprietary technologies and sensitive business information and, therefore, the impact of economic cyber espionage activities. However, we assess that economic cyber espionage will probably allow the actors who take this information to reap unfair gains in some industries.

Information Control and Internet Governance

Online **information control** is a key issue among the United States and other actors. However, some countries, including Russia, China, and Iran, focus on "cyber influence" and the risk that Internet content might contribute to political instability and regime change. The United States focuses on cyber security and the risks to the reliability and integrity of our networks and systems. This is a fundamental difference in how we define cyber threats.

The current multi-stakeholder model of Internet governance provides a forum for governments, the commercial sector, academia, and civil society to deliberate and reach consensus on Internet organization and technical standards. However, a movement to reshape