

Internet governance toward a national government-based model would contradict many of our policy goals, particularly those to protect freedom of expression and the free flow of online information and ensure a free marketplace for information technology products and services.

- These issues were a core part of the discussions as countries negotiated a global telecommunications treaty in Dubai in December. The contentious new text that resulted led many countries, including the United States, not to sign the treaty because of its language on network security, spam control, and expansion of the UN's role in Internet governance. The negotiations demonstrated that disagreements on these issues will be long-running challenges in bilateral and multilateral engagements.

Internet governance revision based on the state-management model could result in international regulations over online content, restricted exchange of information across borders, substantial slowdown of technical innovation, and increased opportunities for foreign intelligence and surveillance operations on the Internet in the near term.

### *Other Actors*

We track cyber developments among nonstate actors, including terrorist groups, hacktivists, and cyber criminals. We have seen indications that some **terrorist organizations** have heightened interest in developing offensive cyber capabilities, but they will probably be constrained by inherent resource and organizational limitations and competing priorities.

**Hacktivists** continue to target a wide range of companies and organizations in denial-of-service attacks, but we have not observed a significant change in their capabilities or intentions during the last year. Most hacktivists use short-term denial-of-service operations or expose personally identifiable information held by target companies, as forms of political protest. However, a more radical group might form to inflict more systemic impacts—such as disrupting financial networks—or accidentally trigger unintended consequences that could be misinterpreted as a state-sponsored attack.

**Cybercriminals** also threaten US economic interests. They are selling tools, via a growing black market, that might enable access to critical infrastructure systems or get into the hands of state and nonstate actors. In addition, a handful of **commercial companies** sell computer intrusion kits on the open market. These hardware and software packages can give governments and cybercriminals the capability to steal, manipulate, or delete information on targeted systems. Even more companies develop and sell professional-quality technologies to support cyber operations—often branding these tools as lawful-intercept or defensive security research products. Foreign governments already use some of these tools to target US systems.