

State and nonstate actors increasingly exploit the Internet to achieve strategic objectives, while many governments—shaken by the role the Internet has played in political instability and regime change—seek to increase their control over content in cyberspace. The growing use of cyber capabilities to achieve strategic goals is also outpacing the development of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation.

Compounding these developments are uncertainty and doubt as we face new and unpredictable cyber threats. In response to the trends and events that happen in cyberspace, the choices we and other actors make in coming years will shape cyberspace for decades to come, with potentially profound implications for US economic and national security.

In the United States, we define cyber threats in terms of **cyber attacks** and **cyber espionage**.⁶ A cyber attack is a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data. It might range from a denial-of-service operation that temporarily prevents access to a website, to an attack on a power turbine that causes physical damage and an outage lasting for days.

Increasing Risk to US Critical Infrastructure

We judge that there is a remote chance of a major cyber attack against US critical infrastructure systems during the next two years that would result in long-term, wide-scale disruption of services, such as a regional power outage. The level of technical expertise and operational sophistication required for such an attack—including the ability to create physical damage or overcome mitigation factors like manual overrides—will be out of reach for most actors during this time frame. Advanced cyber actors—such as **Russia** and **China**—are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests.

However, isolated state or nonstate actors might deploy less sophisticated cyber attacks as a form of retaliation or provocation. These less advanced but highly motivated actors could access some poorly protected US networks that control core functions, such as power generation, during the next two years, although their ability to leverage that access to cause high-impact, systemic disruptions will probably be limited. At the same time, there is a risk that unsophisticated attacks would have significant outcomes due to unexpected system configurations and mistakes, or that vulnerability at one node might spill over and contaminate other parts of a networked system.

(Continued)