

Abstract
NATO Cyber Defense Conference

“Cyber Risk from a Homeland Security Perspective”

Andrew Cutts
Director, Cybersecurity Policy
U.S. Department of Homeland Security

Cyberspace and malicious cyber activity have both evolved rapidly. The evolution is such that even defending against the current state constantly leaves us behind the threat. We’ve got to anticipate where the threat *will* be. We’ve got to think – and act – well in advance.

But how can one anticipate a future threat, especially one that has evolved so quickly, with any degree of confidence? Maybe it’s not as difficult as it appears. From a strategic perspective, the cyber threat has to exist somewhere along a defined threat continuum.

On one end of that threat continuum, the low-consequence end, is the nuisance kind of malware found on the Internet. At the other end is attack by a sophisticated and motivated nation-state adversary who is willing and able to use cyber attacks to destroy critical information infrastructure. In between are other threats including cyber crime, terrorist activity, and nation-state activities short of conflict.

The cyber threat we now face, and its commensurate risks, started at one end of this continuum – the nuisance end. But in a relatively brief timeframe – a couple of decades – it has escalated toward the other end, comprising attacks that could pose serious risks to national and economic security. So the cyber threat vector is clear: it’s headed in the wrong direction. And this vector is not likely to change until or unless the perceived cost of cyber attacks outweighs their perceived benefit.

Given that, the key question for those with national cyber defense responsibilities is no longer “where’s the threat going to be?” but rather, “how do we defend against the most serious cyber attacks?” And importantly, “how long do we have to develop that defense, in an environment in which that is a great deal more difficult than offense?”

How does an advanced country, dependent upon information networks for economic growth, build an effective cyber defensive against cyber risks on the far end of the consequence spectrum, while at the same time supporting profitable business models and maintaining essential civil liberties? An effective approach, much like the threat itself, needs to be multifaceted. It requires a common perception of risks and clearly assigned responsibility for managing them. It requires a deep intellectual framework for thinking about and solving an inherently complex problem – one that supports the needs of decision-makers in both industry and government. Above all, it requires truly effective teamwork and partnerships between government and the private sector.