A Tech Accord
to protect people in cyberspace

Microsoft Policy Papers

Creating a Tech Accord to help protect people in cyberspace

People need to trust technology, the makers of technology, and cyberspace itself. That trust is essential for consumers and enterprises to continue to work, shop, learn and interact online, providing benefits not just for themselves but also for their communities and economies. However, governments are putting this trust at risk by sponsoring an increasing number of cyber-attacks.

Governments must help cultivate trust in cyberspace. Yet it is equally important that technology providers take action to create a trustworthy environment for Internet users. There has never been a greater need for the technology providers – the creators, operators, protectors, and first responders for cyberspace – to agree and champion a common set of principles and behaviors to protect civilians in cyberspace. The time has come for an international Tech Accord.

Industry plays a critical role in keeping cyberspace stable, open and secure

The government and the technology industry must partner on cybersecurity. Governments have unique ways to change behavior of actors in cyberspace – they can negotiate with other countries through diplomatic channels, ban business or trade through economic sanctions, establish cybercrime law, set regulatory requirements, or even undertake military action. However, states alone are simply not capable of managing the risks of cyberspace.

The technology industry plays a key role in keeping the Internet secure for civilians. We are already doing many things – improving security through innovation in our products and services, adapting our practices to proactively and quickly address security risks, as well as using our knowledge of technology to prevent bad behavior. Yet we can and must do more to counter nation state attacks.

It can be difficult for individual technology companies to know when and where to engage on these complex issues. Moreover, no single company can do this alone. Global companies that make technology, provide services, and manage security around the world, and groups that focus on defense, such as the Forum for Incident and Security Response Teams (FIRST), must come together. We must reaffirm our commitment to engage in defense only, never offense. We must also commit to common principles and behaviors that protect citizens and keep the internet secure for all.

The Tech Accord: a collective industry commitment to cybersecurity

A Tech Accord would demonstrate industry's commitment to a common set of principles and behaviors to protect civilians in cyberspace. It could include not only what actions our industry would take or not take, but also shared objectives and collaborative efforts to enhance cyber defense.

The concept of a Tech Accord needs input from a wide range of industry partners, who should move quickly to convene, share ideas, and determine what our shared commitments might be. As a starting point, a Tech Accord could be founded around six common objectives:

1. *No assistance for offensive cyber operations:* Global technology companies should pledge that they will not assist any government in attacking the information infrastructure of any customer anywhere in the world. They should similarly agree that they will not help any government to exploit or undermine commercial, mass-market technology products and services.
2. *Assistance to protect customers everywhere:* Global technology companies should commit to protecting customers by issuing patches for their products and services to all users at the same time and therefore ensure that they do not leave any customers at risk.
3. *Collaboration to bolster first-response efforts:* Global technology companies should commit to partnering to proactively defend against cyberattacks and to minimize the duration and impact of such attacks. Increased collaboration across the sector will increase the effectiveness of our collective response and make the technology ecosystem more secure for users.
4. *Support for governments' response efforts:* Global technology companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.
5. *Coordination to address vulnerabilities:* Global technology companies should commit to work together to address security issues ("vulnerabilities"). Reporting and handling vulnerabilities in a coordinated way will help best protect users while minimizing the risk of vulnerabilities being exploited.
6. *Fighting the proliferation of vulnerabilities:* Global technology companies should commit to not trafficking in cyber vulnerabilities for offensive purposes, nor should they embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes. To counter the threat posed by undisclosed, "zero-day", vulnerabilities available on the black market, the technology industry should leverage publicized bug bounty programs, which provide recognition and compensation for individuals who report bugs, especially those which relate to security vulnerabilities.

Anyone that depends on cyberspace needs to be able to trust the technology on which it relies. While governments need to act themselves, through adoption of a Digital Geneva Convention to protect civilians in cyberspace in times of peace, the technology sector has to take its own steps to increase that trust. After all, we are responsible for owning and operating most of the information infrastructure on which cyberspace relies. As cyberattacks take place, the technology sector as a whole has already become the internet's first responders but we can and should also proactively promote a more peaceful and secure internet for people everywhere. A Tech Accord will help us move forward.