World101
From the Council on Foreign Relations

Transcript: An Overview of Cyberspace and Cybersecurity

It seems impossible to imagine life without the internet, but it was created just decades ago, in 1969.

The United States Defense Department worked with several universities to connect a set of computers through a network called Arpanet, allowing the government and researchers to send scientific information back and forth across the country.

These first users mostly knew and trusted each other, but over the years, with the advent of personal computers, individuals outside the research community started joining the network.

And in 1991, Tim Berners-Lee introduced the World Wide Web, a system for connecting files to each other across the internet, allowing users to easily explore a vast world of information often referred to as cyberspace.

The U.S. government soon outsourced management of the network. A nonprofit organization called ICANN was created to administer the internet's addresses and domains, and private companies sold internet services to users.

The web continued to grow exponentially, becoming the defining feature of modern life, where any user can interact with any other user anywhere, almost instantaneously. Through the internet, businesses, governments, and all types of organizations are able to gather more information, conduct more commerce, and operate more efficiently.

But with these enormous benefits come enormous challenges. The internet was designed by a community that trusted its members to act in good faith. Yet this important tool is no longer in the sole hands of friendly scientists.

Now four billion people—around half the world's population—have internet access. The very connections that make our lives easier also expose us to a world of danger.

Many governments are seeking to tame cyberspace by addressing three major policy issues:

- cybersecurity,
- data privacy,
- and online rights.

Cybersecurity is about building protection against the threats that lurk in cyberspace. We upload tons of personal information to the internet, from photos to credit card numbers. And companies and governments keep intellectual property and top-secret information online too.

But the Internet connects all of us, and some people use it to access our information without permission. This is called “hacking.” Hackers often steal banking information or hold computer systems hostage for financial gain.

But hacking isn’t just a criminal enterprise. Hackers can also work on behalf of governments to conduct cyber espionage, stealing other countries’ sensitive information for economic and military advantage.

Sometimes, governments can use the stolen information as a political weapon. For example, Russian agents hacked the U.S. Democratic National Committee in order to interfere with the 2016 presidential election.

Hackers can also conduct cyberattacks, disrupting or destroying other countries’ computer systems, even potentially causing catastrophic damage in real life. The first such attack was reportedly conducted by the United States and Israel in 2008, when they used the Stuxnet computer virus to destroy one-fifth of Iran’s nuclear centrifuges.

Unlike traditional warfare, there is no international consensus about how governments should and should not act in cyberspace. While some countries, like the United States, may call for others to act responsibly, they resist agreeing to any rules that limit their own cyber capabilities.

Even if there were rules, though—and a country were to break those rules—there’s no shared understanding of how the world should respond to cyber rule-breaking.

Complicating matters, cyberattacks can be nearly impossible to attribute. Hackers often mask their identities and hide their locations by routing attacks through servers in many different countries.

Even if a victimized government does manage to identify its attackers, it may not be able to tell whether the hackers were working as another country’s agents or whether they were working on their own. This is problematic because traditionally countries are deterred from attacking other countries out of fear of retaliation.

But with cyberattacks, if a country doesn’t know who exactly attacked it, then it doesn’t know who to retaliate against. And without the threat of retaliation, countries are more likely to use cyberattacks.

So without the ability to fully deter cyberattacks, it's up to countries, businesses, and individuals to protect themselves, making it harder for hackers to access information without authorization and making systems more resilient to damage when they are hacked.

Improving cybersecurity can be tough for individuals because our information is exposed across cyberspace in ways we may not even know. It's a matter of data privacy, the degree to which a person controls the information they share online.

You may think that you're being careful with your information, but you could be sharing it without realizing. When we visit websites, we often allow them to collect data about our age, location, activities, and much more.

The companies behind those websites can sell that information and create targeted ads that follow us around the internet. And if the information is stolen, those companies have little obligation to inform us.

Data privacy advocates are trying to protect our information online. But there's no global agreement as to how it should be done.

Controlling how digital information is shared is not just a concern for individuals. It's also the focus of certain countries that don't value online rights, the concept that everyone should have the right to full internet access.

Some governments, like China, advocate for cyber sovereignty, arguing that their borders apply to cyberspace and they should be able to control how people and businesses use the internet within their territory.

The United States and its allies disagree with this approach. They support internet freedom, the concept that everyone should be free to express themselves and interact with anyone else, anywhere online—allowing for new ideas to spread freely.

Amid the global disagreement, technological innovation continues to accelerate at a tremendous speed. Billions of items are getting connected to cyberspace—from cars, to kitchen appliances, even surfboards—forming an ever-growing Internet of Things.

This new era of connectivity underscores the need for international arrangements that would encourage responsible cyber practices and discourage harmful ones.

Ideally, these arrangements would persuade governments to act responsibly and do all in their power to stop individuals, companies, and other countries from breaking the cyber rules within their territory.

But we're nowhere close to establishing such arrangements, and they'll only get harder to achieve as our lives become increasingly tangled with the internet, as the threats from cyberspace put our world in greater danger.