Cyber First Principles

Cybersecurity ensures the confidentiality, integrity, and availability of information and information systems. It enables freedom of speech, civil liberties, innovation and free markets—principles that are proven to increase the potential for freedom and opportunity, at home and abroad.

Information networks are a tool that enables the expansion of America’s mutually supportive ideals of human rights, freedom, and opportunity. They help create the conditions for innovation and human prosperity to flourish, while ensuring U.S. national security and world stability. While new technologies can provide hope to millions, they can also be used to create instability and exploit potential vulnerabilities in networks and systems.

THE CHALLENGE

Today, hostile nations, criminal groups, and individuals seek to exploit information networks—like the Internet—to further a variety of national and ideological objectives. America’s banks, energy sector, and intellectual property continue to be routinely targeted by criminal hackers and foreign governments alike. A destabilizing attack on U.S. critical infrastructure would directly threaten American citizens, the U.S. economy, and America’s way of life.

The problem is growing, not shrinking. As people become more dependent upon technology, opportunities for crime, espionage, and physical disruption will increase exponentially. This trend will continue unless we are able to foster an environment where cybersecurity is the rule, not the exception.

4 PRINCIPLES OF CYBER POLICY

I. Cybersecurity is privacy—it protects individuals, companies, and governments from malicious intrusions. Today, some contend that greater security means ceding some degree of personal privacy, or vice versa. This is flawed logic. Privacy is security against unwanted intrusions or disturbances. In essence, privacy and cybersecurity not only work together—they are the same.

When personal information is collected and held by governments and private companies, states and companies can impact the privacy of the individual. When private companies and the government work together to protect information networks, they inevitably share personal information. Privacy requires that the information shared and stored must remain confidential.

Why is this important? Protecting information networks enables security in the real world. State and non-state actors all over the world seek to manipulate information for their own gain. Compromised information means individuals and organizations lose control of their information to actors who they cannot influence. And a loss of network security can easily lead to compromises in physical security, identity security, and political freedom.
Protecting information networks also enables individual freedom. Expanding secure communications helps to strengthen human dignity at home and overseas. Online forums give voice to the politically oppressed and help protect basic human rights. The free flow of information allows new ideas and creativity to flourish, giving people more opportunities to provide for themselves.

Expanding global access to secure information networks is in the interest of our national security. When basic human rights and outlets for grievances are denied, it feeds the conditions for conflict and violence. Extremist groups prey on vulnerable individuals upset by a growing sense of social change and dislocation. The advent of print newspapers helped build community and national identities in the 17th century. When information is denied today, it weakens social and communal bonds and threatens global security.

**What do we do?** America must be willing to hold foreign leaders to the same basic standards of human rights and individual dignity that we expect from our own government. Our international partners deserve our respect, and we should be clear that we cannot achieve maximum global security or individual prosperity without them. But we must also make plain that human rights and dignity are fundamental and apply equally online.

This requires the U.S. to lead by example. America’s adversaries will seek to bend the rules to achieve an upper hand, but the U.S. must be the standard bearer for individual freedom. Large American email and social media platforms are used all across the world and other countries look to us to justify their domestic policies. Even as the U.S. must be vigilant in securing itself against international threats, it must also ensure its domestic policies keep data secure and do not stifle individual rights—at home and abroad.

II. **Cyberspace is a public space.** Ownership over the networks and content that make up cyberspace is decentralized and predominantly operated by non-government entities. It is an open, accessible, and user generated domain that grows constantly and organically. Policies to protect it, therefore, must be designed to match and preserve that distributed architecture.

Yet, cyberspace should not be reserved completely for civilian use. Military, intelligence, and law enforcement agencies leverage these networks to pursue their missions and help protect critical assets. But the greatest benefits of the domain lie in the increased opportunities for education, freedom of speech, and innovation. These ideals must be kept at the center of our policy debates, even as information networks are used for security purposes.

**Why is this important?** The Internet expands access to information and boosts accountability. All people have the right to seek, receive, and convey information and ideas. When information flows freely and freedom of speech is embraced, it creates the conditions that hold governments more accountable, embolden entrepreneurship, and further human rights and dignity.

That is not to say, however, that freedom of speech is without its limits. But the fear that a few will use information networks for reprehensible purposes should not overwhelm the potential for a better life
they provide for millions around the world. Information networks alone do not hold governments accountable or raise families out of poverty, but they do enable those who try.

**What do we do?** The U.S. should advance policies on the international stage that supports the free flow of information. Societies that embrace broad access to information are strengthened. When virtual walls are constructed and access is distributed unevenly, the chances for misunderstanding, misinterpretation, and conflict increase. Conversely, access to information builds a foundation for global peace and human progress.

**III. Protecting cyberspace is a shared responsibility.** No single entity—whether government or private—has the capacity to secure a domain that extends beyond traditional geographic boundaries. In an era where one weak link in the chain can compromise the security of an entire system, all sectors have a role to play in contributing to common security. Cybersecurity requires coordination and cooperation between federal, state, local, and private entities.

**What do we do?** First, the federal government has important responsibilities to address. Civilian agencies must coordinate the protection of our society’s most critical assets. The military must protect its own networks and fulfill its mission of defending the country against sophisticated, destructive attacks against U.S. critical infrastructure. And law enforcement agencies must bring justice to bear when information networks are used to commit a crime. The government also needs to coordinate with our international partners to ensure safe and resilient networks, separate and distinct from the content.

The private sector also has a great stake in fulfilling our nation’s cybersecurity. The majority of critical infrastructure in the United States—everything from power grids to hospitals to large financial institutions—is privately owned. Additionally, private companies collect and store information on U.S. citizens. Securing our most important networks and content requires the private sector to take responsibility for their own security—and that of their customer base.

Finally, individual users have an important role to play in our security architecture. This requires Americans to build a culture of security by making sure end users understand their role in the security solution. From building awareness of commonly used tactics to encouraging people to use more sophisticated passwords, the role of the individual is essential. Individuals must accept responsibility for using information networks in a manner that is respectful of the rights of others and contributes to the security of the whole system.

**IV. We can secure the networks without suppressing content.** By understanding the distinction between information networks and the content travelling over those networks, we can address the threats to the system while preserving individual privacy and freedom.

This distinction is important on the international stage. Other countries will look to U.S. policies to justify their actions. Individual freedom in the 21st century is closely tied to how we govern and use digital technology. Separating the content from the medium sets a precedent that secure information networks are necessary and within reach, but it is not an excuse to suppress individual rights and personal privacy.
Why is this important? *Secure information networks facilitate innovation.* The Internet enables the connections that invigorate economic progress. Together, information and information networks help people rise from poverty and individual dignity through economic independence.

The web’s potential can only be realized if these networks remain open and secure. Allowing the Internet to become compartmentalized will give some nations the opportunity to close off their markets. Under those conditions, entrepreneurs could be denied access to new markets while service providers are charged tariffs just for supporting international traffic.

What do we do? Cyberspace must be protected and available for those who develop new technologies, seek the next cure, and continue to move the needle towards individual freedom. The U.S. should work with international partners to address and mitigate threats to the networks themselves, while leaving content to the individual.

CONTACT INFORMATION

From the Industrial Age to the Information Age, technology has enabled nations to grow and prosper. During the past thirty years, the rapid pace of innovation has allowed for previously unimaginable advancements: companies do business all over the world; oppressed populations are given new outlets for advancing democratic principles; and children have more access to information and greater educational opportunities.

Historically, the security policies that have worked best for America were based on the idea that we should practice the same values abroad that we strive for at home. This is as true in cyberspace as it is in any other domain.

The Truman|CNP Cyberspace & Security Program aims to find a principled approach to cybersecurity policy that will protect American information networks while also enabling human rights, freedom, and opportunity—at home and abroad.

**Matthew Rhoades, Director, Cyberspace & Security Program**
Truman National Security Project & Center for National Policy
MRhoades@TrumanCNP.org