From the Roman Roads to the Information Superhighway:
Concepts of Deterrence for Cyberspace

Remarks by Senator Robert F. Bennett
Electronic Industry Association
May 7, 2001

The Roman Empire can be reduced to three broad themes:

- Keep the peace: The Romans kept the peace with a well-managed civilian structure and world class military.
- Keep the roads open: Keeping the peace also meant that the roads stayed open for commerce and defense.
- Trade with everyone: The Romans understood commerce and they loved to trade. Their economic empire was built on peace, roads and trade.

I did not come here to give a history lecture, but rather to talk about Internet security. When it comes to the information economy, the knowledge economy, or the new economy, we really are not that different from the Romans.

Americans are fiercely entrepreneurial and we thrive on stability. Entrepreneurial efforts are by their nature disruptive because they challenge the status quo and create new markets. Despite their disruptive nature, entrepreneurs require predictability of rules because they shape their endeavors in response to them. When the rules keep changing, entrepreneurs are left with just disincentives. The more stable the environment, the more analysis available, the better the decisions that can be made.

We – like ancient Rome – are network centric. The only difference is that the Romans built their networks with bricks and paving stones and we use fiber optic cables and routers. The Romans had roads, and we use the information superhighway.

The Roman roads are a very interesting metaphor for the Internet. The Romans built roads to facilitate defense, commerce and the movement of ideas. The barbarians used this same infrastructure against the Romans to launch campaigns against unsuspecting cities and to disrupt trade.

A millennium later, we are looking for ways to protect commerce on the Internet from proliferators of malicious code, virus writers, hackers and sophisticated criminal organizations. In short, we are seeking to ensure, defense, commerce and the flow of information. We are also seeking ways to ensure that the common defense of the nation is sufficiently provided. As a result, we study the capabilities of foreign states -- and they study us. No one wants to be left behind in the information arms race; the stakes are far too high.

If we are to keep the peace in cyber space, keep the global information infrastructure open and facilitate the unrestricted flow of goods and services in the global economy, we must do the following:

Realize that keeping the peace is no longer just the responsibility of the Pentagon. In fact, one could argue that stability in cyberspace cannot be achieved in a traditional geographic sense. Our networks know no boundaries. Unlike the Roman Empire's roads, people, organizations and countries can connect and disconnect from the Internet at a rapid pace.

The Internet poses direct challenges to the principles of keeping peace and roads open. The freedom of the Internet fosters innovation and also creates an infrastructure for launching attacks. Computer network attack capabilities tip the balance in favor of the offense. Just as the Romans' roads gave the barbarians an asymmetrical advantage, the Internet provides certain distinct advantages to the hackers, virus writers, criminal organizations, terrorists and hostile foreign states.

In March 2001, the National Security Advisor, Dr. Condeleeza Rice addressed a gathering of chief information officers and asked them to partner with the federal government to promote better computer security and to prevent computer based attacks against U.S. infrastructures, such as power and telecommunications. Dr. Rice reached back into history and suggested the model of nuclear deterrence as useful one for infrastructure protection. The U.S. won the Cold War by developing defensive capabilities that deterred adversaries from making a strategic strike against the U.S.

I challenge the Internet security community to adopt and redefine deterrence as a model for computer security and infrastructure protection. I suggest a new framework for deterrence based not on nuclear strategy but rather on basic economics. It costs less to protect computer systems than to recover them. I won't bore you with an in-depth macroeconomics discussion, but preventing computer-based attacks contributes to the overall productivity of your organization and the economy as a whole. Government and industry should collaborate to address the following four principles:

(1) robust security practices and industry best practices,

(2) distributed analytical capabilities,

(3) an architecture for warning, and

(4) a flexible response policy.

Deterring computer based attacks is economically sound and makes business sense for corporations and organizations of almost any size. An economy of deterrence – national effort to protect integrity, reliability and integrity of data - promotes stability and continued economic growth. In the end, stability will enable us to

- Keep the peace
- Keep the roads open
- And trade with everyone.

Before I close, I would like to take a brief moment to expand on one of the most pressing challenges we face in infrastructure protection and internet security, the development of a robust distributed analytical capability.

Serious attention must be paid to understanding the indicators of computer-based attacks and the development of predictive warning capabilities. This sounds easy to some, but you know and I know this is the real challenge facing us now for the next decade.

1. Developing analysis and warning capabilities will require three things: industries and the federal government to develop a better understanding of the types of information that needs to be shared;
2. analytical methodologies and procedures to process information and speed attribution of attacks, including the development of a new generation of visualization tools which allow vast quantities of information to be seen and rapidly understood; and
3. narrow, but well-crafted legislative protections such as exemptions from the Freedom of Information Act (FOIA) which will ensure that information shared for the purposes of infrastructure security is protected.

I am studying a variety of information sharing concepts and looking for the effective legislative solutions. I ask you to work with me in developing the appropriate procedures for information sharing between industry and government, as well as, intra-industry information sharing.

Together we can raise awareness about the cost-benefit or the economy of deterring computer based attacks. By ensuring integrity, reliability and availability of information, your business will realize increased efficiency and profitability. On a macro level, "the economy of deterrence," promotes stability and economic growth. It has become popular to say that national security is a shared responsibility. However, I have found that few people know what this really means. I suggest that national security and economic security are closely linked to stability. Stability is may well be the "new common defense" for business in the information age. I repeat: Keep the peace, keep the roads open (or the Internet) and trade with everyone.