Cyber security policies and solutions in the united states

Science, Computer Science

When researchers at the Advanced Research Project Agency invented the precursor to the Internet, they couldn’t have imagined the ubiquitous impact of their creation. Today, the USA and the world rely on the Internet for an exhaustive range of services. This dependence renders us all – individuals, militaries, businesses, schools, governments – vulnerable in the face of a cyber-threat. More than 20 billion devices are expected to be connected to the Internet by 2020. The risks introduced by the growing number and variety of such devices are substantial.

The factors which make Cyber Security one of the most challenging endeavors are:

- Geographical distances and logistical difficulties cease to exist in case of cyber-attacks.
- Cyber-attacks do not come with precursory warnings.
- It is often difficult to track the origin of an attack and therefore difficult to retaliate.
- A cyber-attack proliferates at an unprecedented rate.
- The cyber space can’t be fully controlled or regulated.
- Lack of clarity in legislation.

POLICIES

The United States is committed to an open, secure, interoperable, and reliable Internet that enables prosperity, public safety, and the free flow of commerce and ideas. These qualities of the Internet reflect core American values – of freedom of expression and privacy, creativity, opportunity, and innovation.

In order to entrench a cyber space conducive to the above ideals the United States emphasizes the following guiding principles:

- Information sharing and interagency coordination.
- Build bridges to the private sector recognizing its important role in a comprehensive solution.
- Building alliances, coalitions, and partnerships abroad.

As articulated in the International Strategy for Cyberspace, the United States will continue to respond to cyber-attacks against U. S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U. S. power and in accordance with applicable law and the principle of proportional punishment.

Provide the necessary knowledge, training, and other resources to countries seeking to build technical and cybersecurity capacity.

- Preserve global network security and stability, including the domain name system (DNS).
- Promote and enhance multi-stakeholder venues for the discussion of Internet governance issues.
- Harmonize cybercrime laws internationally by expanding accession to the Budapest Convention.
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet.

SOLUTIONS

- Build and maintain ready forces and capabilities to conduct cyberspace operations:
- Building a competent cyber workforce,
- Improving recruitment and retention,
- Maintaining a persistent training environment,
- Develop and implement exchange programs with the private sector;

Support the initiative for cyberspace education:

- Developing policies to support the Initiative for Cybersecurity Education.
- Working with interagency partners, one or more educational institutions, as well as state and private sector partners, to continue to support innovative workforce development partnerships focused on both the technical and policy dimensions of cybersecurity and cyber defense.

Account for the dynamic nature of cyberspace:

Realize that cyberspace is an immensely evolving domain and to maintain security over a sustained period, constant development is essential. To this end there must be acceleration in R&D and proper identification of evolving cybersecurity risks that affect national security, public health and safety, and economic security.

International sharing of research:

There must be an annual conference of representatives of nations to discuss specific advancements in cyber space both in light of new threats and potential solutions. A journal should be published to provide impetus to transparency and dissemination of information.

OUR CYBERSECURITY IN ACTION

In July 2017, the United States Secret Service, through a synchronized international law enforcement operation, affected the arrest of a Russian national alleged to have operated BTC-e. From 2011 to 2017, BTC-e is alleged with facilitating over $4 billion worth of bitcoin transactions worldwide for cyber criminals engaging in computer hacking, identity theft, Ransomware, public corruption, and narcotics distribution. Researchers estimate approximately 95% of Ransomware payments were laundered through BTC-e.