**Primeira tradução (**<https://www.usip.org/sites/default/files/sr119.pdf>**)**

A potencial ameaça do ciberterrorismo é, obviamente, muito alarmante. Os “hackers”, apesar de não serem motivados pelos mesmos motivos que inspiram os outros terroristas, têm demonstrado que os individuais podem conseguir facilmente acesso a informação sensível.

O crescimento da dependência da nossa sociedade em informação tecnológica gerou uma nova forma de vulnerabilidade, dando aos terroristas a chance de alcançar alvos que, de outra forma, seriam inacessíveis, tais como os sistemas da defesa nacional e a sistemas de controlo de tráfego aéreo. Quanto mais tecnologicamente desenvolvido um país é, o mais vulnerável se torna aos ciberataques.

As noções de ciberterrorismo podem datar desde o início de 1990, quando o uso da Internet despoletou e surgiram vários estudos acerca dos potenciais riscos apresentados pela grande afluência de informação facilmente alcançável.

“Amanhã, os terroristas poderão ser capazes de criar mais danos com um teclado do que com uma bomba” National Academy of Sciences

Dorothy Denning:

O ciberterrorismo é a convergência entre o ciberespaço e o terrorismo. Este refere-se a ataques ilegais e ameaças de ataques a computadores e informações armazenadas com o intuito de intimidar o governo e/ou as pessoas envolvidas devido a objetivos políticos ou sociais. No entanto, para se qualificar como ciberterrorismo, o ataque deve resultar em violência contra pessoas ou propriedades ou, pelo menos, causar grande impacto para gerar medo.

O ciberterrorismo é uma opção atrativa para os terroristas modernos por diversas razões:

* É mais barato do que os métodos tradicionais de terrorismo;
* É mais anónimo;
* A variedade e número de alvos é maior;
* Pode ser conduzido remotamente;
* Tem a capacidade de afetar diretamente um maior número de pessoas.