The War of Attrition in Cyber-Space or "Cyber-Attacks", "Cyber-War" and "Cyber-Terrorism"

Eduardo Gelbstein

Has over 40 years experience in information systems and technology, both in the private and public sectors. His experience includes being Information Technology Strategy Manager for the British Railways and Director of the United Nations International Computing Centre. He was also an advisor to the United Nations Board of Auditors and the French Cour des Comptes. Ed is currently Adjunct Professor at Webster University Geneva and the author of several books and articles as well as a regular speaker at international conference on security, risk, audit and governance.

Resumo

A Guerra de Atrição no Ciberespaço ou "Ciberataques", "Ciberguerra" e "Ciberterrorismo"

Nos últimos anos tornou-se óbvio que o mundo virtual das bases de dados e do *software* – popularmente denominado como ciberespaço – tem um lado negro. Este lado negro tem várias dimensões, nomeadamente perda de produtividade, crime financeiro, furto de propriedade intelectual, de identidade, *bullying* e outros.

Empresas, governos e outras entidades são cada vez mais alvo de ataques de terceiros com o fim de penetrarem as suas redes de dados e sistemas de informação. Estes vão desde os adolescentes a grupos organizados e extremamente competentes, sendo existem indicações de que alguns Estados têm vindo a desenvolver "*cyber armies*" com capacidades defensivas e ofensivas.

Legisladores, políticos e diplomatas têm procurado estabelecer conceitos e definições, mas apesar da assinatura da Convenção do Conselho da Europa sobre Cibercrime em 2001 por vários Estados, não existiram novos desenvolvimentos desde então.

Este artigo explora as várias dimensões deste domínio e enfatiza os desafios que se colocam a todos aqueles que são responsáveis pela proteção diária da informação das respetivas organizações contra ataques de origem e objetivos muitas vezes desconhecidos.

Abstract

Over the last few years it has become obvious that the virtual world of data and software – commonly referred to as cyberspace, has a dark side. This dark side has many sides, notably loss of worker productivity, financial crime, theft of intellectual property, identity theft, bullying, and more.

Companies, governments and others are increasingly being targeted by largely unknown parties attempting, often successfully, to penetrate their networks and disrupt their information systems and data. These parties range from the individual teenage hacker to highly competent groups, and it is alleged that a growing number of countries are developing "cyber armies" with defensive and offensive capabilities.

Legislators, politicians and diplomats struggle with concepts and definitions (e.g. can malicious software be treated as a weapon?) and, apart from the Council of Europe Convention on Cybercrime issued in 2001, which has been adopted by a small number of countries there are no other treaties.

This article explores the many dimensions of this domain and highlights the challenges faced by practitioners charged with protecting their organization's information assets from unknown attackers with unknown objectives.