CIBERTERROR & CIBERGUERRA
CYBERTERROR & CIBERWARFARE

SILVA JR., Nelmon J.

RESUMO: A transnacionalização das leis, bem como a ameaça frente ao ciberterror é clara, razão pela qual as Nações devem anteciparem-se aos seus efeitos.
PALAVRAS-CHAVE: Transnacionalização das Leis, Ciberterror. Ciberguerra.

SUMMARY: The transnationalization of law, as well as the threat against cyber terror is aclear reason why the Nations should anticipated up to its effects.
KEYWORDS: Transnacionalization of Law. Cyberterror. Cyberwarfare.

Segundo dados da *Asian School of Cyber Laws*[1], gasta-se atualmente no mundo cerca de US$ 45.000.000,00, no combate ao crime cibernético e seus efeitos, razão pela qual inúmeros países tem-se antecipado na cruzada contra grupo(s) terroristas cibernéticos.

Para Cédric Thévenet, os ataques cibernéticos podem dar-se de três formas básicas:

> *Une attaque physique implique des armes conventionnelles dirigées contre des centres informatiques ou des ensembles de câbles assurant les liaisons; une attaque électronique implique l'utilisation de l'énergie électromagnétique comme une arme. C'est utiliser une impulsion électromagnétique pour surcharger les circuits des ordinateurs, ou, dans une forme moins violente, insérer un flux de code numérique malicieux dans les transmissions micro-onde de l'ennemi; e une attaque Informatique implique généralement l'utilisation de code malicieux comme arme pour infecter des ordinateurs en exploitant certaines failles logicielles.*[2]

Ainda, para o autor existem sete nações que possuem uma política de guerra cibernética, a saber: República Popular da China, Índia, Irã, Coreia do Norte, Paquistão, Rússia e Estados Unidos da América[3]. Sou obrigado a discordar dos dados citados pelo autor, ao analisar o sítio virtual da *International Telecomunication Union – ITU*, em especial daqueles constantes da *Global Cybersecurity Agenda – GCA*.[4]

1 Texto disponível em: http://www.facebook.com/asianschoolofcyberlaws?fref=ts - acesso em 25.06.2013.

2 THEVENET. Cédric., ***CYBER-TERRORISME, MYTHE OU REALITE ?***. Centre d'Etudes Scientifiques de Défense – CESD. 2005. Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/50195426-2006-thevenet-cyberterrorism.pdf

3 *Óp. cit,* p. 16 *usque* 20.

4 http://www.itu.int/osg/csd/cybersecurity/gca/ - acesso em 25.06.2013.

Apenas para entendermos a complexidade do tema em tela, existem mais de setenta formas de agressões cibernéticas: *Anonymizer; ARP cache poisoning; Backdoor; Backscatter; The Blues- Bluebugging, Bluejacking and Bluesnarfing; Buffer overflow; Bullying in Cyberspace; Click fraud; Computer trespass; Cookie Manipulation; Copyright infringement; Crap-flooding; Cyber Stalking; Cyber Terrorism; Cyber Warfare; Data Diddling; Data Leakage; Defamation; DOS / DDOS; DNS poisoning; Easter Eggs; Email Spoofing; Encryption use by terrorists; eShoplifting; Financial Crimes; Fire Sale; Fire Walking; Footprinting; Fraud; Online Gambling; Google based hacking; Griefers; Hactivism; Hijacking; Identity Fraud; Impersonation; Joe – Job; Key stroke Logging; Logic Bomb; Lottery Scam; Mail Bombing; Malware; Nigerian 419 Fraud Scheme; Packet Sniffing; Phishing & Spoofing attacks; Piggy backing; Piracy of Software; Pod Slurping; Poisoning the Source; Pornography; robots.txt file; Port scanning; Rootkits; Salami Theft; Sale of Illegal Articles; Scavenging; Smishing; Social Engineering; Spambot; SQL Injection; Stealware; Time Bomb; Trojan; URL Manipulation; Virus Attack; Web defacement; Vishing; Wire – Tapping; Worm; XSS Attack; Y2K; Zero Day Attack; Zeus;* e *Zombie*.[5]

Percebam que nações, como à exemplo da Índia, investem na formação (gratuita) de profissionais de segurança cibernética, pois segundo suas fontes governamentais, até 2015, serão necessários mais de 4.700 profissionais nesta área.[6] O investimento indiano não pára por aí, através da *Asian School of Cyber Laws*, foi criando num ambiente virtual a República da Cybéria[7], onde assim sedutoramente recrutam seus novos talentos: *Republic of Cyberia is a virtual nation for smart youngsters. We have our own state emblem, our own currency and even our own Government.*

Duas verdades são inquestionáveis: a transnacionalização das leis; e eventual(is) ciber guerra(s) advinda(s) do ciber terrorismo. Face à tais

5 SHAH. Aaushi,. RAVI. Srinidhi,. ***A to Z of Cyber Crime.*** Asian School of Cyber Laws. 2013. Livro disponível em: http://ensaiosjuridicos.files.wordpress.com/2013/06/122592201-cybercrime.pdf

6 http://m.economictimes.com/news/news-by-industry/jobs/around-4-7-lakh-cyber-security-professionals-needed-by-2015-milind-deora/articleshow/17430201.cms – acesso em 25.06.2013.

7 http://www.facebook.com/republic.of.cyberia – acesso em 25.06.2013.

realidades, corretos estão os países que antecipam-se à estas. O que seu País tem feito em relação a isto?

According to the Asian School of Cyber Laws spends is currently the world about U.S.$ 45,000,000.00 in combating cybercrime and its effects, which is why many countries has been anticipated in the crusade against (group(s) cyberterrorists.

To Cédric Thévenet, cyberattacks can gives three basic forms:

> *Une attaque physique implique des armes conventionnelles dirigées contre des centres informatiques ou des ensembles de câbles assurant les liaisons; une attaque électronique implique l'utilisation de l'énergie électromagnétique comme une arme. C'est utiliser une impulsion électromagnétique pour surcharger les circuits des ordinateurs, ou, dans une forme moins violente, insérer un flux de code numérique malicieux dans les transmissions micro-onde de l'ennemi; e une attaque Informatique implique généralement l'utilisation de code malicieux comme arme pour infecter des ordinateurs en exploitant certaines failles logicielles.*

Still, for the author there are seven nations that have a policy of cyber warfare, namely: China, India, Iran, North Korea, Pakistan, Russia and the USA. I am forced to disagree with the data cited by the author, to analyze site of the International Telecommunication Union – ITU, in particular those contained in the GlobalCybersecurityAgenda - GCA.

Just to understand the complexity of the theme in question, there are over seventy forms of cyberattacks: *Anonymizer; ARP cache poisoning; Backdoor; Backscatter; The Blues-Bluebugging, Bluejacking and Bluesnarfing; Buffer overflow; Bullying in Cyberspace; Click fraud; Computer trespass; Cookie Manipulation; Copyright infringement; Crap-flooding; Cyber Stalking; Cyber Terrorism; Cyber Warfare; Data Diddling; Data Leakage; Defamation; DOS / DDOS; DNS poisoning; Easter Eggs; Email Spoofing; Encryption use by terrorists; eShoplifting; Financial Crimes; Fire Sale; Fire Walking; Footprinting; Fraud; Online Gambling; Google based hacking; Griefers; Hactivism; Hijacking; Identity Fraud; Impersonation; Joe – Job; Key stroke Logging; Logic Bomb; Lottery Scam; Mail Bombing; Malware; Nigerian 419 Fraud Scheme; Packet Sniffing; Phishing & Spoofing attacks; Piggy backing; Piracy of Software; Pod Slurping; Poisoning the Source; Pornography; robots.txt file; Port scanning; Rootkits; Salami Theft; Sale of Illegal Articles; Scavenging; Smishing; Social Engineering; Spambot; SQL Injection; Stealware; Time Bomb; Trojan; URL Manipulation; Virus Attack; Web defacement; Vishing; Wire – Tapping; Worm; XSS Attack; Y2K; Zero Day Attack; Zeus; and Zombie.*

Realize that nations, like the example of India, invest in training (free) cyber security professionals, because according to their government sources by 2015 will require more than 4,700 professionals in this área. The Indian investments does not stop there,through the Asian School of Cyber Laws, was creating a virtual environment the Republic of Cyberia, where so seductively

recruit their new talents: *Republic of Cyberia is a virtual nation for smart youngsters. We have our own state emblem, our own currency and even our own Government.*

Two truths are indisputable: the transnationalization of law; and whether(s) cyberwar(s) arising(s) of cyberterrorism. Faced with these realities, Countries that are correct up to anticipate these. What has your Country done about this?