



» XI Congresso Luso Afro Brasileiro de Ciências Sociais
Diversidades e (Des)igualdades
Salvador, 07 a 10 de agosto de 2011.
Universidade Federal da Bahia (UFBA) - PAF I e II
Campus de Ondina

XI Congresso Luso Afro Brasileiro de Ciências Sociais
Salvador da Bahia, 07 a 10 de Agosto de 2011

**CIBERTERRORISMO: TERRORISMO VIRTUAL? UMA ABORDAGEM
TERRITORIAL AO FENÓMENO TERRORISTA NO CIBERESPAÇO**

Maria Francisca Saraiva

Núcleo de Investigação Tecnologia, Sociedade e Governança - CAPP
ISCSP, Universidade Técnica de Lisboa, Portugal
Email: msaraiva@iscsp.utl.pt

Introdução

As sociedades estão cada vez mais abertas e dependentes dos sistemas informáticos. A inter-conectividade que as caracteriza torna-as vulneráveis a ataques cibernéticos por parte de actores maliciosos.

No espectro dos ataques cibernéticos, destacam-se como principais preocupações estratégicas o ciberterrorismo, o cibercrime e a ciberguerra.

Neste contexto, pretende-se, com o presente texto, dar a conhecer as principais características e desafios colocados pelo ciberterrorismo à segurança dos Estados.

O tema central deste texto é a importância da noção de terrorismo híbrido enquanto modelo de interpretação do fenómeno ciberterrorista, discutindo-se a possibilidade de ocorrência no ciberespaço de um terrorismo simultaneamente cibernético e convencional que pode ser combatido tanto no ciberespaço como fora deste espaço estratégico.

Com este exercício procuramos abandonar a ideia de um terrorismo cibernético puramente “virtual”.

A natureza do terrorismo

O terrorismo é um fenómeno antigo.



» XI Congresso Luso Afro Brasileiro de Ciências Sociais

Diversidades e (Des)igualdades

Salvador, 07 a 10 de agosto de 2011.

Universidade Federal da Bahia (UFBA) - PAF I e II
Campus de Ondina

O conceito de terrorismo, por seu lado, é muito discutido e controverso.

No ambiente da Guerra Fria, os terrorismos (tradicionais) eram considerados um subproduto estratégico da competição ideológica entre os blocos militares.

No 11 de Setembro, a discussão mudou de tom, começando a falar-se da hipótese de ocorrerem ciberataques em resposta às medidas de retaliação dos Estados Unidos e dos seus Aliados no Afeganistão (Vatis, 2001) e do uso preventivo da força na “guerra” contra o terrorismo.

Hoje o contra-terrorismo conta com menos adeptos e a prática dos Estados em relação ao terrorismo e seus patrocinadores parece hesitar entre o modelo pré-11 de Setembro e o modelo pós-11 de Setembro, defendido pelos Estados Unidos (Reinold, 2011).

Não obstante as incertezas em relação ao assunto, por terrorismo continua a entender-se “o uso intencional ou a ameaça do uso da violência contra civis ou alvos civis, com objectivos políticos” (Ganor, 2001, p.6). Neste sentido, podemos concluir que os actos terroristas se situam no espectro das violências políticas exteriores à lógica da guerra (Kilcullen, 2005, p.606) sendo, entre outras coisas, uma arma usada pelos mais fracos contra os mais fortes num quadro de conflitualidade hostil.

A posição assumida neste texto está de acordo com a visão de Vacca (2006, p. 443), de que o terrorismo tem tido regra geral pouco impacto político nas sociedades e quando tem impacto político é frequente produzir um efeito contrário ao desejado pelos movimentos terroristas.

No entanto, a utilização do ciberespaço como vector privilegiado da condução de acções terroristas emergiu recentemente como uma nova ameaça à segurança dos Estados, favorecendo a necessidade de acções de aprofundamento de uma cultura de segurança tanto ao nível nacional como internacional.

Terrorismo em Ambiente Virtual

A palavra ciberterrorismo foi inventada em 1980 por Barry Collin, um investigador sénior do *Institute for Security and Intelligence*, sedado na Califórnia (Ribeiro; Amaral, 2004, p.33).



O ciberterrorismo, à semelhança do cibercrime, é uma importante expressão da democratização no acesso às tecnologias informáticas e, em particular, à utilização da Internet no ciberespaço.

Como refere Mark Pollitt,

“Esta forma de terrorismo é um ataque premeditado, politicamente motivado, contra informação, sistemas de computadores, programas de computadores e dados que resulta em violência contra agentes não combatentes por parte de grupos subnacionais ou agentes clandestinos” (1997, p.1)”.

Parece óbvio que, para o autor, o ciberterrorismo é simplesmente a capacidade de usar o computador para aterrorizar e nada mais do que isso.

É curiosa esta definição de Pollitt, tendo em conta que a palavra ciberterrorismo encerra uma elevada densidade de significação, ao conjugar num mesmo referente dois medos particularmente presentes na sociedade internacional contemporânea: o temor pelo desconhecido e complexo, relacionado com as novas tecnologias, e o medo do terror terrorista (Embar-Seddon, 2002, p.1033).

Com efeito, as novas tecnologias de informação põem em evidência a necessidade de averiguar de que modo onexo entre terror, informação e tecnologia vai marcar os terrorismos do futuro (Der Derian, 2003, p.445).

Ainda assim, algumas questões precisam ser previamente clarificadas.

No debate do ciberterrorismo a retórica política invoca frequentemente um Pearl Arbour Digital, como um cenário catastrófico de desorganização social provocado pelas novas tecnologias de informação e comunicação. A posição assumida nesta comunicação rejeita as referências que empolam estes medos, procurando recentrar o problema do ciberterrorismo no que é a sua principal característica, a (baixa) probabilidade do fenómeno vir a ocorrer num futuro próximo (Nunes, 2004; Weisman, 2005).

Não existem dados precisos sobre a ocorrência de incidentes terroristas no ciberespaço (Denning, 2009), podendo aceitar-se que nunca ocorreu um ataque deste género.



Além disso, como veremos um pouco mais adiante, esta opção revela-se problemática para a maioria dos grupos terroristas.

Mas, apesar do debate em torno do ciberterrorismo chamar a atenção para o seu carácter de ameaça potencial, no caso dos Estados Unidos o ciberterrorismo assume contornos particulares.

Com efeito, na liderança da revolução tecnológica e sem inimigos junto às suas fronteiras, os Estados Unidos surgem como o país mais vulnerável aos ataques virtuais. Em larga medida, esta vulnerabilidade resulta da Transformação da Defesa das forças armadas norte-americanas e da superioridade tecnológica que os Estados Unidos pretendem alcançar com este processo. As novas guerras assimétricas, tanto na sua versão clássica, quanto na versão *on line*, devem, acima de tudo, ser entendidas como uma resposta estratégica dos outros actores a esta supremacia militar dos Estados Unidos.

Por seu lado, os terroristas tradicionais ver-se-ão cada vez mais envolvidos em aventuras no ciberespaço porque os alvos das suas acções são a cada dia que passa mais controlados ou protegidos, ou ambas as coisas, por computadores.

Em relação à presença de actores maliciosos no ciberespaço, algumas questões precisam ser consideradas.

A primeira é que há diferentes motivações para cometer ciberataques.

Assim, o ciberterrorista não é um *hacker* (pirata informático), que movido pelo desafio e curiosidade consegue um acesso não autorizado a um sistema de computadores, nem tão pouco pratica *cracking*, que é uma actividade criminosa, maliciosa, que consiste em roubar ou alterar dados, frequentemente a troco de dinheiro. Estes indivíduos fazem *cracking* por motivos políticos (Cavelty, 2007).

Para além disso, e mais importante do que tudo o resto, o uso dos meios digitais com objectivos organizativos (informação, comunicação, comando e controlo) nada tem que ver com o uso de comunicações digitais para cometer actos de terror, sendo importante destringir os usos legais dos usos criminosos do espaço virtual.

Podemos concluir que um ciberterrorista executa ataques através das tecnologias de computadores ou pela *Internet* contra redes, sistemas, ou infra-estruturas suportadas por



computadores ou redes (Dunnigan, 2003), incluindo víruses, cavalos de tróia e outro software malicioso, com o objectivo de coagir a população ou um governo para atingir objectivos políticos ou ideológicos. Os actos terroristas são normalmente perpetrados contra sistemas de informação e comunicação, centrais eléctricas, de produção, armazenamento e transporte de gás e petróleo, serviços governamentais e de emergência.

Verifica-se assim que ao contrário do que é muitas vezes veiculado, os ciberataques terroristas não se confundem com outros usos das tecnologias de informação e comunicação, como a propaganda terrorista em páginas na *internet* e grupos de conversação, a captação de financiamentos *on line* para os movimentos ou quando funciona como veículo de comunicação rápida e barata entre os simpatizantes do grupo. Em resultado disso, a Internet é mais uma ferramenta ao serviço das causas terroristas e não o modelo do grupo terrorista do futuro.

O ciberterrorismo como terrorismo territorializado

Para abordar este assunto há que ter em conta o tema das cibersegurança nas agendas de segurança.

O conceito de protecção de infra-estruturas críticas é essencial para se perceber este ponto, em razão da presença de actores maliciosos no ciberespaço com capacidade para debilitar a segurança nacional e económica de um país.

Por outro lado, tem sido notório, em alguns meios políticos, uma clara preocupação com as movimentações de grupos terroristas em ambiente virtual porque devido à interconectividade global em que vivemos, qualquer sistema ligado à rede global pode vir a constituir-se como um alvo potencial de ataque ciberterrorista ou de outro actor hostil presente no ciberespaço (Everard, 2001, p.103).

Sobre este ponto, diríamos que pese embora os novos riscos tecnológicos associados à utilização livre deste espaço virtual serem reais, não se vislumbra que o uso da Internet para infligir grave danos em termos de perda catastrófica de vidas humanas ou destruição física associadas aos actos mais violentos do terrorismo convencional venha a ser um instrumento de eleição para a generalidade dos movimentos terroristas.



Neste sentido, o alarme social em torno do ciberterror é exagerado, resultando do medo do desconhecido combinado com a ignorância (falta de informação e desinformação) em relação a estes temas.

Porém, é uma ameaça potencial que não pode ser totalmente descartada, pelo que importa perceber melhor o seu *modus operandi*.

Como se sugeriu atrás, a intenção é o critério fundamental para aferir se ocorreu um ataque (ciber)terrorista, concretizando-se num ataque por computador politicamente motivado e perpetrado para intimidar ou coagir um governo ou a população para se atingir um determinado objectivo político.

Neste aspecto, e em comparação com os conflitos cinéticos, os conflitos *on line* tornam menos perceptível o contraste entre conflitos armados/actividades criminosas/terrorismo/simples falhas no sistema¹. Assim, o que distingue um *cracker* de um Estado que executa operações ofensivas usando as técnicas dos *crackers*? As operações no ciberespaço de um *hacker* adolescente ou de um ciberterrorista não têm natureza militar, mas o que não pode ignorar-se é que os computadores, *modems*, telefones e *software* são iguais para todos os actores que navegam na *www*.

A verdade é que a *Internet* é uma rede de redes onde ninguém sabe quem é o outro (Matusitz, 2008, p.195). Não há um centro e as localizações são múltiplas num ambiente operacional que ultrapassa as fronteiras da soberania e dilui a distinção defesa/segurança interna. Acima de tudo, os cibertiques terroristas podem ser controlados remotamente, no anonimato, são baratos, não envolvem a manipulação de explosivos e evitam missões suicidas. Terão sempre ampla cobertura mediática.

Como se verifica, parece tratar-se de um terrorismo virtual de difícil prevenção e combate porque a *Internet* é ubíqua, permite ataques a partir de qualquer parte do mundo.

No entanto, a análise empreendida até aqui deixa de lado alguns aspectos que vale a pena mencionar e que estão relacionados com a questão dos efeitos do terrorismo, dando-se desta forma resposta à questão de saber se os ciberataques causam danos



políticos ou económicos graves ou mesmo irreversíveis aos países afectados (Stohl, 2006, p.229).

Do nosso ponto de vista, é fácil apercebermo-nos que existe uma certa inter-influência entre o mundo imaterial e o mundo territorial na análise do ciberterrorismo, em pelos menos dois sentidos diferentes.

Em primeiro lugar, no ciberespaço circula informação numérica, virtual, que inter-age com as infra-estruturas físicas podendo provocar efeitos destruidores de natureza material. De facto, os resultados da acção terrorista perpetrada através de fios e dígitos são tangíveis do ponto de vista físico – podem matar não combatentes e provocar a destruição da propriedade (Ellis, 2001, p.7). Existe aqui uma semelhança com as tecnologias que aumentam o poder de ataque das armas convencionais, no sentido em que no ciberespaço os grupos responsáveis pelos ataques parecem maiores e mais poderosos do que na realidade são, fazendo crer que podem desferir ataques em qualquer momento ou lugar.

É pois de concluir que os ataques por computador podem criar efeitos disruptivos em certa medida comparáveis aos actos tradicionais de terrorismo, em termos do medo que provocam na sociedade.

Por outro lado, e em segundo lugar, importa dizer que em determinadas situações estes ciberataques não constituem actos hostis isolados, surgindo frequentemente como poderosos multiplicadores de força, precursores de ataques que ocorrem posteriormente com utilização formal da força no contexto de uma operação terrorista tradicional, ou em simultâneo com esta, sendo utilizados para atingir o efeito de surpresa e provocar o caos (desorientação temporária).

Este aspecto não constitui novidade no estudo do fenómeno terrorista.

Historicamente os terroristas sempre estudaram os padrões de comunicação dos inimigos antes de os atacarem (Matusitz, op.cit., p.187), com o objectivo de provocar efeitos disruptivos nas suas comunicações. No passado, os grupos terroristas recorriam a técnicas de decepção durante o ataque (idem, p.187), com o objectivo de induzir em erro o inimigo acerca das suas próprias capacidades e intenções, manipulando a realidade para levar o inimigo a decidir num sentido que lhes poderia ser favorável.



Ora, a decepção também está presente na Internet, na medida em que esta permite esconder o real e mostrar ao mesmo tempo o falso (idem, p.187).

Temos então que concluir que o sucesso operacional das operações terroristas pode aconselhar a manutenção dos métodos tradicionais, pelo que a cibertecnologia só será usada se esta alternativa for mais interessante que as outras possibilidades de ataque, muitas vezes em combinação com o *modus operandi* tradicional, e que o ciberterrorismo tem sempre uma dimensão territorial, quando entra em contacto com o mundo físico, ao nível dos efeitos que provoca.

Conclusão

Este texto procurou contribuir para a delimitação do fenómeno do ciberterrorismo no espectro das ameaças depois de 1989.

A principal conclusão é que o terrorismo contemporâneo ocupa um lugar mais amplo no espectro dos conflitos, em parte por causa da possibilidade de ameaças ciberterroristas às infra-estruturas críticas dos países mais desenvolvidos.

Em segundo lugar, julgamos ter demonstrado que no ciberespaço o cibercrime e o *hacking* são actividades mais frequentes e mais preocupantes que as acções que grupos terroristas possam estar a planear neste espaço operacional.

Vimos, com efeito, que enquanto as armas de tipo convencional destroem as estruturas físicas, as armas lógicas destroem as estruturas lógicas e as armas comportamentais, ou semânticas, destroem a confiança dos utilizadores nos sistemas de informação e na rede e influenciam a interpretação da formação que circula. O que significa que no mundo cibernético o ciberterrorismo é uma ameaça potencial com uma utilidade política muito relativa para a generalidade dos movimentos terroristas.

Na realidade, ao longo do texto foi possível tornar clara a ideia de que o ciberterrorismo é essencialmente um terrorismo híbrido, num duplo sentido.

Em primeiro lugar, é importante ter em conta que os ataques no ciberespaço não têm capacidade autónoma para produzir efeitos devastadores, o que os coloca em desvantagem em relação aos métodos físicos tradicionais. Neste sentido não é



» XI Congresso Luso Afro Brasileiro de Ciências Sociais

Diversidades e (Des)igualdades

Salvador, 07 a 10 de agosto de 2011.

Universidade Federal da Bahia (UFBA) - PAF I e II
Campus de Ondina

expectável que se concretizem como actos hostis isolados, funcionando antes como multiplicadores de força de ataques físicos tradicionais.

Por outro lado, esta, como outras ameaças cibernéticas, não é totalmente virtual, na medida em que o terror virtual pode resultar em morte e/ou destruição de propriedade. Esta realidade física, concreta e observável, confere ao ciberterror uma dimensão real e territorial, permitindo combater este uso indevido do ciberespaço tanto no plano cibernético como fora deste espaço estratégico.

Finalmente, é óbvio que a abordagem territorial do fenómeno terrorista no ciberespaço, por si só, não resolve todos os problemas da utilização ilegal do ciberespaço, nomeadamente o problema da identificação do actor malicioso, aspecto que pode condicionar senão mesmo inviabilizar uma resposta atempada a estes desafios à segurança nacional dos Estados.

Neste texto, optámos por não desenvolver esta questão de importância crucial para o combate e prevenção do ciberterrorismo, interessando-nos sobretudo desconstruir a ideia, profundamente errada, de que o ciberterrorismo é uma forma de terrorismo puramente “virtual”.

Referências Bibliográficas

- CAVELTY, Myrian Dunn, “Critical Information Infrastructure: Vulnerabilities, Threats, and Responses”, *Disarmament Forum*, Vol.3 (2007), pp.15-22.
- DENNING, Dorothy E., “Terror’s Web: How the Internet is Transforming Terrorism”, in Y. Jewkes and M. Yar (eds.), *Handbook of Internet Crime*, Cullompton: William Publishing, 2009.
- DER DERIAN, James, “The Question of Information Technology in International Relation”, *Millennium*. Vol.32: 3 (2003), pp.441-456.
- DUNNIGAN, James F. *How to make War: a Comprehensive Guide to Modern Warfare for the Post-Cold War Era*. 4th ed. New York: Quill, 2003.



- ELLIS, Bryan W., *The International Legal Implications and Limitations: What Are Our Options?*. Carlisle Barracks, Pennsylvania: Us Army War College (USAWC Strategy Research Project), Abril 2001.
- EMBAR-SEDDON, Ayn, “Cyberterrorism: Are We Under Siege?”. *American Behavioral Scientist*, Vol.45: 6 (Feb 2002), pp.1033-1043.
- EVERARD, Jerry. *Virtual States: The Internet and the Boundaries of the Nation-State*. 1st ed. rep. London: Routledge, 2001.
- GANOR, Boaz, “Is One Man’s Terrorist Another Man’s Freedom Fighter?”, *ICT Papers on Terrorism*, Herzliya, [Israel]: The International Institute for Counter-Terrorism/ The Interdisciplinary Center, 2002.
- KILCULLEN, David J, “Countering Global Insurgency”. *The Journal of Strategic Studies*, Vol.28: 4 (2005), pp.597-617.
- MATUSITZ, Jonathan, “Similarities Between Terrorist Networks in Antiquity and Present-Day Cyberterrorist Networks”, *Trends in Organized Crime*, Vol.11 (2008), pp.83-199.
- NUNES, Paulo Viegas, “Ciberterrorismo: Aspectos de Segurança”. Lisbon Conference on Defence and Security: Terrorism as a Global Threat-Models and Defence Strategies, Instituto da Defesa Nacional, 1-2 Julho 2004.
- POLLITT, Mark M., “Cyberterrorism: Fact or Fancy?”. *Proceedings of the 20th National Information Systems Security Conference*, Outubro de 1997, pp.287, disponível em <<http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>>, acedido em 3 de Junho de 2011.
- REINOLD, Theresa, “State Weakness, Irregular Warfare, and the Right to Self-Defense Post-9/11”, *AJIL*, Vol.105: 2 (2011), pp.244-286.
- RIBEIRO, Gonçalo Baptista; AMARAL, Feliciano, “Ciberterrorismo: a Nova Forma de Criminalidade do Século XXI: Como Combatê-la”. *Proelium*. VI Série: 1, (2004), pp.29-64.
- STOHL, Michael, “Cyber Terrorism: a Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?”, *Crime, Law and Social Change*, Vol.46 (2006), pp.223-238.
- VACCA, John R., *Guide to Wireless Network Security*, New York: 2006.



» XI Congresso Luso Afro Brasileiro de Ciências Sociais

Diversidades e (Des)igualdades

Salvador, 07 a 10 de agosto de 2011.

Universidade Federal da Bahia (UFBA) - PAF I e II
Campus de Ondina

VATIS, Michael A., *Cyberattacks During the War on Terrorism: a Predictive Analysis*,
Hannover: Dartmouth College, Institute for Security Technology Studies,
2011.

WEISMAN, Gabriel, “Cyberterrorism: the Sum of All Fears”, *Studies in Conflict &
Terrorism*, Vol.25 (2005), pp.129-141.