



SPENCER TOTH SYDOW

Advogado, conferencista, professor de graduação e pós graduação, doutor e mestre em Direito Penal pela Universidade de São Paulo (USP), especialista em Direito Penal Informático, autor de diversos artigos e obras jurídicas.



MARCUS ABREU DE MAGALHÃES

Juiz de Direito em Mato Grosso do Sul; titular da 2ª Vara da Comarca de Costa Rica (MS); Graduado em Economia e Direito pela Universidade de Brasília - UnB; Especialista em Controle de Constitucionalidade e Direitos Fundamentais pela PUC-Rio/IDH Campo Grande/EJUD-TJMS; Com cursos em Enquête économique et financière pela École Nationale de la Magistrature - França; Terrorism and Counterterrorism pela Georgetown University - EUA; Cyberwar, Surveillance and Security pela The University of Adelaide - Austrália e Mestrando em Legal Studies na Ambra College EUA.



V. 04
COLEÇÃO
CYBER
CRIMES

CYBERTERRORISMO:
A NOVA ERA DA CRIMINALIDADE

MARCUS ABREU DE MAGALHÃES | SPENCER TOTH SYDOW



Hoje um terrorista conectado a uma rede social causa com seu atentado enorme impacto político/social. Duas pessoas por meio de mensagens eletrônicas podem se articular para fins delituosos ao mesmo tempo em praticamente qualquer lugar do planeta. A imagem e o relato dos fatos chegam quase que instantânea e simultaneamente aos meios de comunicação de massa.

Marcelo Weitzel Rabello de Souza



ISBN 978-85-8425-996-0
9 788584 259960

COLEÇÃO
CYBERCRIMES

V. 04

MARCUS ABREU DE MAGALHÃES
SPENCER TOTH SYDOW

CYBERTERRORISMO:

A NOVA ERA DA CRIMINALIDADE



A presente obra nos apresenta, nos informa e nos motiva a debater sobre um outro tipo de terrorismo (e conseqüentemente diversas práticas delituosas), pouquíssimo estudado e comentado, mas vulgar em sua aplicação, um exercício de atividade terrorista silenciosa, sem grandes impactos midiáticos, sem o choque da imagem que gera o pânico o temor desorientado. Porém, tão impactante e destruidor quanto. Tão perverso e preocupante, pois com a intercomunicação hoje existente nesse mundo globalizado, praticamente todos os segmentos de uma economia a ele estão sujeitos a ataques como a qualquer cidadão. O ciberterrorismo.



CYBERTERRORISMO

A NOVA ERA DA CRIMINALIDADE



COLEÇÃO

CYBERCRIMES

V. 04

MARCUS ABREU DE MAGALHÃES

SPENCER TOTH SYDOW

CYBERTERRORISMO

A NOVA ERA DA CRIMINALIDADE



Copyright © 2018, D'Plácido Editora.
Copyright © 2018, Marcus Abreu de Magalhães.
Copyright © 2018, Spencer Toth Sydow

Editor Chefe
Plácido Arraes

Produtor Editorial
Tales Leon de Marco

Capa
Leticia Robini de Souza
(Sob imagem de Marcus Hansson via Flickr)

Diagramação
Bárbara Rodrigues

Todos os direitos reservados. Nenhuma parte desta obra pode ser reproduzida, por quaisquer meios, sem a autorização prévia da D'Plácido Editora.



Editora D'Plácido
Av. Brasil, 1843, Savassi
Belo Horizonte - MG
Tel.: 3261 2801
CEP 30140-007

Catálogo na Publicação (CIP)
Ficha catalográfica

MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth;
Cyberterrorismo: a nova era da criminalidade[Coleção Cybercrimes] - 1 reimp.
-Belo Horizonte: Editora D'Plácido, 2018.
Bibliografia
ISBN: 978-85-8425-996-0
1. Direito 2. Direito Penal 3. Direito Digital I. Título II. Direito
CDU343 CDD 341.5

GRUPO
D'PLÁCIDO



*
Rodapé



À Ana Lara pelo apoio e incentivo.

(Marcus)

À Marcelle Sydow, pelo companheirismo infinito.

*Aos meus pais Barbara e Spencer e meus irmãos
Cristina e Thomas.*

À Cecy Tourinho e Alexandre Ares.

*À Ana Lara Camargo de Castro e especialmente ao dedicado
coautor Marcus Abreu de Magalhães.*

(Spencer)





AGRADECIMENTOS

A **José Carlos Couto de Carvalho**, Subprocurador de Justiça Militar; **Roberto Coutinho**, Subprocurador-Geral de Justiça Militar; General de Divisão **Angelo Kawakami Okamura**, Comandante do Comando de Defesa Cibernética (ComDCiber); e Engenheira **Marlene Isidro** ITI e DSIC/GSIPR.

Aos sempre importantes e inspiradores Prof. Dr. Sérgio Salomão Shecaira, Prof. Dr. Renato de Mello Jorge Silveira, Prof. Dr. Alamiro Velludo Salvador Netto, Prof. Dr. Pierpaolo Cruz Bottini e Prof. Dr. Eduardo Saad Diniz, meu agradecimento pelo estímulo na jornada





SUMÁRIO

PREFÁCIO	13
INTRODUÇÃO	17
1. A TERCEIRA ONDA: A ERA DA INFORMAÇÃO	23
2. ADMIRÁVEL MUNDO NOVO: NOVAS AMEAÇAS E NOVOS RISCOS	27
Ataques Cibernéticos.....	37
Ciberterrorismo.....	41
Internet.....	45
3. FOR YOUR EYES ONLY: ARQUIVAMENTO DA INFORMAÇÃO	49
Metadados.....	49
Classificação da Informação.....	54
Classificação das informações no Brasil.....	59
Classificação das informações em outras nações.....	64
Considerações acerca do modelo brasileiro.....	68
4. NINETEEN EIGHTY-FOUR: COLETA DA INFORMAÇÃO	71

Liberdade de Informação versus Segredos de Estado	71
Wikileaks	72
Edward Snowden	80
<i>FISA Court</i>	84
<i>Freios e Contrapesos</i>	87
<i>Controle Judicial</i>	93
<i>Carpenter v. United States</i>	94
<i>American Civil Liberties Union v. James Clapper</i>	95
<i>Wikimedia Foundation v. National Security Agency NSA</i>	96
Anonymous	97
Sigilo da Fonte	103
5. FAHRENHEIT 451: CONTROLE DA INFORMAÇÃO	107
Cifração e Criptografia das Comunicações	108
<i>WhatsApp - interceptação</i>	110
<i>WhatsApp – estudo de caso</i>	120
<i>Telegram – estudo de caso</i>	129
<i>Aplicativos Mensageiros independentes</i>	133
6. A CLOCKWORK ORANGE: DARK WEB - O PORÃO DA REDE	135
Surface Web	135
Deep Web	136
Dark Web	138
7. DO ANDROIDS DREAM OF ELECTRIC SHEEP?: A SOCIEDADE CIBERNÉTICA	143
Ataques cibernéticos	147
Armas cibernéticas	151

<i>Arma cibernética em meio físico - hardware</i>	152
Ferramentas cibernéticas.....	155
ZERO DAY EXPLOIT.....	156
Inteligência e Contraineligência cibernéticas.....	157
Terroristas Cibernéticos.....	158
8. THE CUCKOO`S EGG: DIREITO INTERNACIONAL, GUERRA, ESTADOS	165
Tallinn Manual.....	168
Territorialidade.....	170
Extraterritorialidade	172
Intangibilidade.....	173
Disputas entre Estados	176
Ataques não vinculados a Estados.....	183
Iniciativa Militar no Brasil.....	187
A Coréia do Norte – análise de caso.....	192
9. NEUROMANCER: DIREITO, ESTADO, LIBERDADES E GARANTIAS	195
Controle do Estado.....	195
Fake News e Controle.....	196
Lavagem de Dinheiro.....	220
Iniciativa Civil no Brasil.....	235
ENDGAME: CONCLUSÕES	241
REFERÊNCIAS	245
NOTAS DE FIM	251





PREFÁCIO

Desde 1648, pelo Tratado de Vestfália, que pôs fim a Guerra dos Trinta Anos, estabeleceu-se na ordem internacional a ideia de igualdade e soberania dos Estados.

A criação e solidificação dos Estados, como entidades soberanas com estatuto próprio também é algo recente. Enquanto que identidades étnicas, tribais, clãs, são bem mais antigas e acompanham o homem desde que este se apresentou como agrupamento social.

Histórica e sociologicamente, a evolução é produto de múltiplas mudanças *“cada mudança pode ser considerada uma ruptura (de equilíbrio, de homeostase), e finalmente toda evolução pode ser considerada como desorganização (parcial, local ou geral) seguida de reorganização que por sua vez, e afetada pela nova mudança”* (MORIN, 1984).

Porém, a desorganização faz emergir problemas, conflitos, redistribuição e conseqüentemente novos processos de reorganização. A sociedade para adaptar-se ao crescimento, a inserção de um novo elemento que a ela impõem repercussão, tem de se modificar, o que na hipótese implica em reorganizar para evoluir.

Dito isso, temos uma nova (des) ordem mundial surgida recentemente e ainda se perspectiva de consolidação. Alicerçada basicamente em duas circunstâncias, gera enorme repercussão no conhecimento e conceito referente a segurança social, política e econômica.

A primeira das circunstâncias foi a dissolução do mundo bipolar, tendo como momento emblemático a ocasião da queda do Muro de Berlim. Uma ordem bipolar, com definição clara de autores principais e secundários, sempre tendia ao equilíbrio, ao contrário do mundo multipolar, com vários atores jogando com suas próprias regras, como se transformou o mundo após o fim da chamada Guerra Fria.

O segundo fator, diz respeito ao atual estágio da globalização. Esta nova (des) ordem veio acompanhada da grande evolução trazida pela globalização quanto ao impressionante avanço tecnológico, principalmente mas não exclusivamente, das comunicações, meios de transporte e transações financeiras. Hoje, a tecnologia serve tanto a propósitos civis como a militares.

Hoje um terrorista conectado a uma rede social causa com seu atentado enorme impacto político/social. Duas pessoas por meio de mensagens eletrônicas podem se articular para fins delituosos ao mesmo tempo em praticamente qualquer lugar do planeta. A imagem e o relato dos fatos chegam quase que instantânea e simultaneamente aos meios de comunicação de massa. Tal facilidade também incentiva e alcançam diversas e inauguram outras tantas, além da ofensa terrorista.

Tais transformações repercutiram na abrangência do conceito de geopolítica. BECKER (1995) recoloca em questão o debate sobre o território e o ordenamento. O conceito de território foi muito importante para a ciência geográfica e utilizada no contexto da geopolítica, como ciência da guerra, o que por sua preponderância, deixou outros segmentos da geografia fora do debate, segmentos que apenas ao final do último século retornaram ao conceito de geopolítica.

Como reflexo e consequência da globalização, uma nova geopolítica preocupada com as tensões sociais em paralelo às fronteiras territoriais conhecidas, o nascimento das denominadas fronteiras de vulnerabilidade, decorrentes das interdependências cada vez mais pronunciadas entre os Estados e o alcance que as condutas têm entre eles e seus súditos.

A desestabilizar sistemas políticos ou instituições políticas, desorganizar socialmente, afetar a economia temos a prática cada vez mais frequente da figura do terrorismo.

Muito se escreveu sobre tal temário, seja sob o ponto de vista da segurança pública, dos seus conceitos jurídicos e consequências de ordem processual, porém em obras voltadas via de regra para o dano físico e suas consequências social, o impacto, o aspecto perverso que a imagem ou só mesmo a notícia do atentado homicida produz e o debate jurídico que de tal fato decorre.

A presente obra, por sua vez, nos apresenta, no informa e nos motiva a debater sobre um outro tipo de terrorismo (e consequentemente diversas práticas delituosas), pouquíssimo estudado e comentado, mas vulgar em sua aplicação, um exercício de atividade terrorista silenciosa, sem grandes impactos mediáticos, sem o choque da imagem que gera o pânico o temor desorientado. Porém, tão impactante e destruidor quanto. Tão perverso e preocupante, pois com a intercomunicação hoje existente nesse mundo globalizado, praticamente todos os segmentos de uma economia a ele estão sujeitos a ataques como a qualquer cidadão. O ciberterrorismo.

Mas, o mérito desta obra não se limita ao seu pioneirismo de exclusiva dedicação a ciberterrorismo e os crimes que o circundam. Extremamente didática e abrangente, oferece análise profunda em matrimônio com diversas ocorrências, algumas amplamente divulgadas outras sem tanta divulgação assim, sempre com análises históricas e jurídicas quanto ao ocorrido.

Se é certo que a análise desses casos apresenta especial interesse para esta obra porque demonstra a ineficácia das atuais soluções jurídicas para enfrentar lides envolvendo cibercrimes, ciberterrorismo e mesmo os limites de uso da tecnologia digital, como alertam os autores, é também correto afirmar que será de enorme valia ao jurista pois o seu conteúdo não só poderá, mas deverá também ser sorvido por aquele que por atividade profissional venha a se relacionar ou a se preocupar com tema (seja na área tecnológica, segurança da informação, segurança

pública ou militar, etc.), haja vista que a densidade da obra alcança todos os espectros que circundam os dilemas que envolvem essas novas modalidades criminais.

Tenham todos uma agradável e proveitosa leitura.

Marcelo Weitzel Rabello de Souza
Procurador-Geral da Justiça Militar de 2012 a 2014
Conselheiro do Conselho Nacional do Ministério
Público no biênio 2017-2019



INTRODUÇÃO

O estudo do terrorismo é novo no Brasil, especialmente porque apenas em 2016 surgiu lei específica para tratar do tema, enquanto as primeiras legislações mundiais remontam à década de 1940.

O Brasil, pressionado por organismos internacionais (em especial pelo GAFI – Grupo de Ação Financeira do qual o Brasil faz parte) e à beira de sediar as Olimpíadas, aprovou às pressas a Lei 13.260/2016.

O *cyberterrorism* teve sua primeira definição cunhada em 1998, num contexto militar anglo saxão. Tal precedência ocorreu provavelmente porque os primeiros usos da Internet foram militares (ARPANET) e, seguidamente, universitários e governamentais, dando a tais instituições vantagem no que se refere a testes de infraestrutura, estudo de riscos e pontos fracos e até mesmo usos benéficos, maléficos ou inconvenientes.

Por certo, foi necessário certo desenvolvimento e aceitabilidade da tecnologia de comunicação imaterial, além de sua naturalização e dependência social pelo segmento civil, para que adquirisse a relevância atual no cenário mundial. Com a popularização da tecnologia e sua ubiquidade nos diversos segmentos da vida contemporânea, seja em casa, no lazer, no trabalho ou demais espaços de interação, a Internet tornou-se o principal ambiente, ainda que artificial, de interação social e troca de informações.

Hoje, afirmamos com segurança que condutas cometidas na rede são capazes de afetar significativamente tanto o

usuário¹, individualmente considerado, quanto a coletividade, orientada por comportamentos em grupo, e, assim, aptas a gerar incômodo, pânico ou até mesmo terror. Ações engendradas por instituições, grupos organizados e países adquirem potencial lesivo grandiloquente.

Há espaços (*rectius*, ambientes) comuns na rede aptos a afetar grande parte dos usuários: comunicadores instantâneos, redes sociais, sistemas de telefonia, bancos, portais, revistas, jornais, instituições públicas, órgão de segurança. Assim, é natural que tais *locus* sejam mais vulneráveis e objeto de maior interesse por grupos transgressores.

Quanto mais a sociedade se acostuma à rede – suas funções, seus sites e serviços – mais o ambiente virtual se torna crucial para a rotina e instituições humanas. A importância de sistemas estáveis e confiáveis decorre dos potenciais prejuízos tanto ao segmento virtual quanto ao real da sociedade, pois eventuais ataques à rede irão acarretar impacto direto à coletividade envolvida.

Como o terrorismo busca atingir ambientes em que a coletividade será impactada e a informática enraizou-se por todos os setores cotidianos, a realidade cibernética tornou-se ambiente propício para geração de terror. E assim surgem novos tipos de terror posto que novos valores são incorporados ao plexo jurídico e social.

Ocorre, porém, que há muitos problemas para a conceitualização do próprio terrorismo como conduta basilar. O tema não encontra terreno comum, em verdade, estamos ainda distantes de consenso acadêmico acerca da matéria².

O conceito de geração de terror é controverso e o problema da ausência de termos técnicos se agrava no meio informático pelo fato de haver novos bens jurídicos criados (e ainda não reconhecidos expressamente pela maior parte dos sistemas legais)

¹ Somos hoje, aproximadamente 3,9 bilhões de usuários segundo a Internet Live Statistics. Disponível em <http://www.internetlivestat.com/>. Acesso em 16.04.2018.

² Vide curioso estudo de Schmid, A., & Jongman, A. (1988) no Capítulo 2, nota de rodapé XII.

bem como multiplicidade de novos modos de ataque a bens jurídicos clássicos.

As pesquisas bibliográficas mostram pequeno número de artigos e obras acerca desta temática. Nossas pesquisas bibliográficas, ainda que não exaustivas, indicam grande escassez acadêmica. No SibiUSP (o sistema integrado de bibliotecas da Universidade de São Paulo que possui convênios com Universidades e sistemas de bibliotecas internacionais) a pesquisa pelo termo “*terrorismo*” revelou 153 resultados, sendo apenas 23 resultados em suas buscas em língua portuguesa. Os termos “*cyberterrorismo*” ou “*ciberterrorismo*” retornaram apenas um resultado dentro de um livro coletivo.

O levantamento pelo termo “*ciberterrorismo*” ou “*cyberterrorismo*” feito no Instituto Brasileiro de Ciências Criminais (IBCCrim) – certamente entre os mais respeitados institutos do país – revela 651 registros sob o termo “*terrorismo*” (e respectivas variações em outros idiomas) e 3 artigos apenas, sendo 2 em língua portuguesa (um brasileiro).

Por essa razão, nos socorremos sobremaneira em estudos publicados na Europa e nos Estados Unidos da América do Norte.

Assim como nas demais obras desta coleção *Cybercrimes*, o objetivo dos autores é o de apresentar o argumento de modo crítico e reflexivo, sem a obrigação de exaurir os temas correlatos, as fontes ou apresentar pesquisa bibliográfica completa e que abranja todas as facetas do *cyberterrorismo*, mesmo porque conceito em mutação.

A matéria é complexa e interdisciplinar, criminológica, portanto, pois engloba engenharia, psiquiatria, psicologia, antropologia, sociologia, processamento de dados e até mesmo filosofia do direito e filosofia pura. O objetivo é a provocação do leitor e da ciência penal informática para aperfeiçoamento constante do tema.

Finalmente, por não haver obras sobre o tema em língua portuguesa, o pioneirismo se constrói com a exposição de linhas gerais abertas a melhorias. Por ser inovadora, a obra é criativa e sujeita a erros e mudanças de interpretação.

O método que escolhemos para apresentar o trabalho buscou a informalidade na medida do possível, com inclusão de

fatos e narrativas para incentivar a fluidez na leitura, para propor a abordagem de tópicos por vezes hauridos de disciplinas técnicas em linguagem coloquial.

Como trata-se de tema com viés técnico, sempre que possível recorremos a registros de conceitos e expressões em notas de fim, de acordo com o conhecimento informático que obtivemos ao longo das últimas décadas. Assim, reservamos as notas de rodapé para esclarecimentos mais aprofundados ou curiosidades a respeito do tópico em análise, deixando as referências técnicas para as notas de fim.

Iniciamos apresentando a questão histórica, a dificuldade de conceituação, as diversas formas com as quais o *cyberterrorismo* se aperfeiçoa, a demonstração do *cyberterrorismo* governamental, empresarial, particular, os *lone wolves*, o papel das *fake news* nessa seara, a ideia da lavagem de dinheiro nesse meio, os principais modos de causação de terror e uma análise da legislação existente no Brasil.

Diferentemente dos outros livros da coleção, este é um livro temporal e em constante mudança e atualização. Muitos exemplos de ataques reais são apresentados, bem como episódios de terrorismo e *cyberterrorismo* ocorridos no passado. Muitos ainda ocorrerão, de modo que será necessário sempre trazer às futuras edições as novidades surgidas.

Os autores entrevistaram autoridades militares brasileiras e participaram de Simpósios e cursos sobre os temas “terrorismo”, “contraterrorismo”, “antiterrorismo” e “cyberterrorismo” para melhor inserção no contexto mundial. Também foram lidas dezenas de *papers*, reportagens e sites especializados no tema “prevenção do cyberterrorismo”.

Finalmente, importante esclarecimento acerca da opção pela palavra “cyberterrorismo” no título da obra com a letra “y”, já reincorporada ao vernáculo, mas apenas para topônimos, antropônimos e siglas, o que não é o caso. A palavra em língua portuguesa é “ciberterrorismo” e assim se encontra grafada nos manuais militares e do gabinete de segurança institucional da Casa Civil. Porém, para respeitar a nomenclatura da coleção Cybercrimes, por coerência editorial optamos por manter a

origem grega da palavra, *kybernetiké* ciência de governar, vocábulo derivado do verbo *kybernéo* que significa dirigir, conduzir, pilotar.

No mais, o propósito é conscientizar o leitor da dimensão da problemática que nos cerca e se aproxima a cada dia, o quanto somos e seremos afetados e os meios de mitigar as consequências deletérias: queiramos ou não, a era do terror está aqui.

Agradecemos a atenção e desejamos uma excelente leitura a todos.

Os autores



SPENCER TOTH SYDOW

Advogado, conferencista, professor de graduação e pós graduação, doutor e mestre em Direito Penal pela Universidade de São Paulo (USP), especialista em Direito Penal Informático, autor de diversos artigos e obras jurídicas.



MARCUS ABREU DE MAGALHÃES

Juiz de Direito em Mato Grosso do Sul; titular da 2ª Vara da Comarca de Costa Rica (MS); Graduado em Economia e Direito pela Universidade de Brasília - UnB; Especialista em Controle de Constitucionalidade e Direitos Fundamentais pela PUC-Rio/IDH Campo Grande/EJUD-TJMS; Com cursos em Enquête économique et financière pela École Nationale de la Magistrature - França; Terrorism and Counterterrorism pela Georgetown University - EUA; Cyberwar, Surveillance and Security pela The University of Adelaide - Austrália e Mestrando em Legal Studies na Ambra College EUA.



Hoje um terrorista conectado a uma rede social causa com seu atentado enorme impacto político/social. Duas pessoas por meio de mensagens eletrônicas podem se articular para fins delituosos ao mesmo tempo em praticamente qualquer lugar do planeta. A imagem e o relato dos fatos chegam quase que instantânea e simultaneamente aos meios de comunicação de massa.

Marcelo Weitzel Rabello de Souza



ISBN 978-85-8425-996-0
9 788584 259960

V. 04
COLEÇÃO
CYBER
CRIMES

CYBERTERRORISMO:
A NOVA ERA DA CRIMINALIDADE

MARCUS ABREU DE MAGALHÃES | SPENCER TOTH SYDOW



COLEÇÃO
CYBERCRIMES

V. 04

MARCUS ABREU DE MAGALHÃES
SPENCER TOTH SYDOW

CYBERTERRORISMO:

A NOVA ERA DA CRIMINALIDADE



A presente obra nos apresenta, nos informa e nos motiva a debater sobre um outro tipo de terrorismo (e consequentemente diversas práticas delituosas), pouquíssimo estudado e comentado, mas vulgar em sua aplicação, um exercício de atividade terrorista silenciosa, sem grandes impactos midiáticos, sem o choque da imagem que gera o pânico o temor desorientado. Porém, tão impactante e destruidor quanto. Tão perverso e preocupante, pois com a intercomunicação hoje existente nesse mundo globalizado, praticamente todos os segmentos de uma economia a ele estão sujeitos a ataques como a qualquer cidadão. O ciberterrorismo.