CENTRO UNIVERSITÁRIO DE BRASÍLIA

LEONARDO ALCANFÔR DE PINHO SILVA

TERRORISMO MEDIANTE GUERRA DE INFORMAÇÕES NO DIREITO INTERNACIONAL: UMA BREVE ANÁLISE DE CASOS

BRASÍLIA 2014

CENTRO UNIVERSITÁRIO DE BRASÍLIA

LEONARDO ALCANFÔR DE PINHO SILVA

TERRORISMO MEDIANTE GUERRA DE INFORMAÇÕES NO DIREITO INTERNACIONAL: UMA BREVE ANÁLISE DE CASOS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito no Centro Universitário de Brasília - UniCEUB.

Orientador: Prof. Dr. Daniel Amin Ferraz.

BRASÍLIA 2014

LEONARDO ALCANFOR DE PINHO SILVA

TERRORISMO MEDIANTE GUERRA DE INFORMAÇÕES NO DIREITO INTERNACIONAL: UMA BREVE ANÁLISE DE CASOS

Esta dissertação foi julgada adequada à obtenção do grau de Mestre em Direito e aprovada em sua forma final pelo Curso de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília.

Brasília-DF, de de 2014.

_____

Dr. Daniel Amin Ferraz

_____

Dra. Jamile Bergamaschine Mata Diz

_____

Dra. Maria Edelvacy Pinto Marinho

Dedico este trabalho ao meu avô João.

.

Agradeço o Prof. Dr. Daniel Amin Ferraz por sua brilhante orientação, sem a qual este trabalho não teria sido possível.

“Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety”.

Benjamin Franklin, 1759.

TERRORISMO MEDIANTE GUERRA DE INFORMAÇÕES NO DIREITO INTERNACIONAL: UMA BREVE ANÁLISE DE CASOS

Resumo: O presente estudo busca, por meio da análise de casos, verificar o atual estágio do direito internacional no tocante à regulamentação dos atos de terrorismo virtual praticados mediante guerra de informações. Inicialmente, é feito estudo dos institutos do terrorismo, do terrorismo virtual, e da guerra de informações. Depois, é analisada a tensão entre a competência dos Estados soberanos e a competência da sociedade internacional para proceder a tais apurações e julgamento. Para atingir tal objetivo, é realizado estudo do direito internacional e também do direito pátrio e comparado. Para melhor compreensão do tema, é feita exposição de exemplos, ou seja, de casuística com algumas situações que retratam cenários que podem ser considerados de terrorismo virtual mediante guerra de informações.

Palavras-chave: Terrorismo virtual; guerra de informações; competência jurisdicional.

TERRORISM USING INFORMATION WARFARE IN INTERNATIONAL LAW: A BRIEF CASE ANALYSIS

Abstract: The present study seeks, through the analysis of cases, to verify the current state of international law regarding the regulation of the acts of terrorism committed by information warfare. Then analyzes of the tension between the competence and jurisdiction of sovereign states in international society are made from the perspective of cultural relativism. To achieve this goal, the international law and also the Brazilian and compared law is studied. For better understanding of the topic are presented examples of some situations that depict scenarios that can be considered virtual terrorism through information warfare.

Keywords: Virtual terrorism, information warfare; jurisdiction.

SUMÁRIO

1 Introdução

1.1 Tema

Esta dissertação tem por escopo analisar o terrorismo mediante guerra de informações, no direito internacional, com a apresentação de conceitos doutrinários. Trata-se de esforço acadêmico de conceituar "terrorismo", especificamente o "terrorismo virtual" e a "guerra de informações", e também analisar se a competência para apurar e julgar tais casos deve ser internacional, tendo em vista a natureza de tais atos não obedecer fronteiras nacionais.

1.2 Relevância

Este trabalho se faz relevante na medida em que os conceitos supramencionados são pouco debatidos na doutrina pátria, apesar de possuírem grande importância para o direito internacional.

Os mecanismos convencionais de conflito entre grupos ideológicos distintos[1] são cada vez mais preteridos pelos modernos instrumentos do terrorismo virtual e da guerra de informações, os quais possuem, ao contrário da chamada "guerra convencional" ou os atos terroristas *stricto sensu*, baixa regulamentação no direito internacional.

1.3 Linha de pesquisa

A linha de pesquisa seguida é "Proteção internacional à pessoa humana", dentro da área "Direito internacional". O tema se enquadra em tal linha de pesquisa, na medida em que atos terroristas e guerra de informações podem causar graves transtornos à dignidade da pessoa humana.

Assim, em que pese a guerra estar proscrita no direito internacional – acontecendo o mesmo com alguns atos considerados "terroristas", as nuances intrínsecas a essas modalidades requerem

[1] As expressões "país", "Estado" ou "nação" não seriam adequadas neste contexto, tendo em vista a possibilidade da guerra de informações ser travada entre grupos independentes, ou seja, não necessariamente vinculados a determinado país.

mais atenção do operador do direito internacional, sob pena de serem enquadradas em atos não abrangidos pelo Direito, o que não se vislumbra no atual estágio das relações internacionais. Em outras palavras, é importante discernir entre os dois institutos.

1.4 Problema de pesquisa

O problema de pesquisa é analisar se a competência para apurar e reprimir o terrorismo virtual mediante guerra de informações deve ser Estatal ou internacional, e analisar o atual estágio do direito internacional para lidar com o tema.

O conceito de terrorismo virtual mediante guerra de informações causa confusão no direito internacional, gerando dificuldades na definição da competência e normatização, porém, a mera definição dos institutos da guerra de informações e terrorismo virtual, já será um avanço relevante na medida em que os demais temas são decorrentes dessa premissa.

1.5 Objetivos

O objetivo geral é estudar o terrorismo virtual mediante guerra de informações, e, por meio de pesquisa da normatização existente, verificar o atual estágio do regramento desses fatos – principalmente as regras pertinentes ao direito internacional.

Os objetivos específicos da dissertação ora proposta são dois.

Inicialmente, se buscará analisar o terrorismo virtual mediante guerra de informações, ou seja, será realizada conceituação desses atos.

Em um segundo momento, o objetivo será entender a questão da competência internacional para a apuração e julgamento dos atos decorrentes de terrorismo virtual e guerra de informações, mediante a análise dos tratados e casos existentes sobre o assunto.

1.6 Metodologia de pesquisa

Pretende-se empregar na metodologia a pesquisa documental, tendo em vista o caráter teórico do assunto, com a utilização do método dedutivo, já que algumas premissas serão apresentadas, com base nas quais será feita conclusão.

Inicialmente será realizado estudo do panorama histórico do tema, para contextualizar o assunto. Posteriormente, será feita conceituação de alguns temas para finalmente se analisar o atual cenário da guerra de informações e terrorismo virtual no direito internacional.

Com efeito, casuística e também doutrina estrangeira serão bastante empregados, diante da escassez de doutrina pátria sobre o tema. Além disso, serão observados os tratados pertinentes, ratificados pelo Brasil ou aos quais o país tenha aderido.

1.7 Análise de casos

Serão analisados diversos casos envolvendo guerra de informações ou ataques virtuais, sendo o estudo de tais casos parte imprescindível deste trabalho. O objetivo de tais análises é verificar a situação do direito internacional no tocante à possibilidade de atuar ou de ter atuado nos casos em que seria necessário.

Tal análise se faz importante na medida em que o assunto ainda é pouco debatido na doutrina pátria, especificamente sobre o assunto especializado da guerra de informações no contexto do terrorismo virtual.

1.8 Resultados esperados

Com a pesquisa proposta, espera-se por resultado definir o terrorismo virtual mediante guerra de informações, por meio do estudo de diversas normas internacionais, e depois disso, estabelecer se a competência para apuração e repressão de tais atos deve ser estatal ou internacional.

Com efeito, a definição do terrorismo virtual e da guerra de informações são metas ambiciosas, e que servirão para embasar o estudo da competência ora proposto. Assim, o estudo do terrorismo se faz muito pertinente para o presente trabalho.

2 Terrorismo

2.1 Contexto histórico

2.1.1 Necessidade e pertinência do estudo histórico

Inicialmente, cumpre analisar a conveniência de se realizar um estudo histórico, ainda que introdutório ao tema, em uma dissertação jurídica. Não se busca aqui utilizar a história como argumento, porém como base sobre a qual se iniciará o estudo do tema proposto.

Tal cautela é imprescindível quando se estuda assunto como é a guerra, após a qual quem escreve a história são, invariavelmente, os vencedores[2].

Quando se faz um capítulo sobre a história em pesquisas jurídicas, se deve evitar um estudo superficial, para que o estudo histórico não seja limitado à *triste tarefa de justificar e legitimar o direito atual*[3].

Sobre o assunto, é importante ponderar sobre o papel da história em trabalhos jurídicos[4]:

> *(...) disfarça-se todavia esse ônus empírico , alegando-se que a história do direito oxigena a cultura geral do operador jurídico, que alarga horizontes, que fomenta a compreensão do presente, que explicita a realidade ôntica da experiência jurídica, que revela mistérios, que apresenta exemplos, que prevê tempos vindouros.*

O estudo da história impõe grandes dificuldades[5], geralmente associadas à obtenção de material ou narrativas fidedignas. No caso deste estudo, tais problemas são mitigados, já que a guerra de

---

[2] Em que pese a crítica de Howard Zinn em *A people´s history of the United States*, New York:Harper & Row Publishers, 1980. p. 50.

[3] Ricardo Marcelo Fonseca, Walter Benjamin, a Temporalidade e o Direito, in **A Escola de Frankfurt e o Direito**, págs. 75-86. In: GODOY, Arnaldo Sampaio de Moraes. **Direito e História: uma relação equivocada.** Londrina: Humanidades, 2003. p. 2

[4] Idem, Ibidem, p. 2.

[5] Entre elas as críticas de autenticidade, autoridade, depoimento e reconstituição.

informações e também o terrorismo virtual começaram a ser estudados, efetivamente, nos anos 80.

Deste modo, não se busca criar qualquer tipo de visão histórica que possa favorecer ou prejudicar qualquer argumento, porém simplesmente verificar o advento da utilização da guerra de informações e suas repercussões no direito nacional e principalmente internacional.

2.1.2 História da guerra de informações

A guerra de informações é tão antiga quanto a própria guerra. Tal ensinamento vem de antigo e clássico manual de guerra chinês:

> *(...) faço meus inimigos verem minhas virtudes parecerem fraquezas e minhas fraquezas parecerem virtudes enquanto faço suas virtudes se transformarem em fraquezas e descubro onde estão suas fraquezas*[6].

No entanto, expressão "guerra de informações" no seu sentido atual é relativamente recente – e começou a ser estudada pela doutrina militar nos anos 80[7].

A ênfase inicial era no significado de "information warfare" enquanto "tecnologia" e não "informação". A "informação"[8] que se utilizava era pertinente aos alvos a serem alvejados com precisão cirúrgica, informações essas geradas por satélites e outras fontes de inteligência.

Porém, antes mesmo da expressão ser conceituada pela doutrina militar e deliberadamente utilizada na gestão de informações durante conflitos bélicos, tal gerenciamento de informações já fora relevante em outras ocasiões.

---

[6] TZU, Sun**. A arte da guerra.** Adaptação e prefácio de James Clavell; Tradução de José Sanz. 19ª ed. Rio de Janeiro: Record, 1997. p.19-20.
[7] Campen, Alan D. **The first information war: The story of communications, computers, and intelligence systems in the Persian Gulf War.** Fairfax, VA: AFCEA International Press, 1992. p. 7.
[8] Ibidem.

Com efeito, na Guerra do Vietnam as informações eram disseminadas livremente por jornalistas, muitas vezes enfurecendo a opinião pública, o que foi determinante para o resultado da guerra[9]. As técnicas de gerenciamento de informações foram sendo aprimoradas nos conflitos das Malvinas de 1982 e nas invasões de Granada e do Panamá.

Neste último conflito, foram mostradas na televisão estadunidense desfiles de "panamenhos" supostamente satisfeitos com o resultado da intervenção estrangeira, enquanto a realidade no teatro de operações era absolutamente diversa[10].

Portanto, o termo guerra de informações passou a incluir o controle da mídia e também a utilização de sistemas telemétricos para guiar mísseis. Preocupar-se-á com todos os aspectos da guerra de informações, ou seja, com o terrorismo virtual, que é a infiltração de redes informatizadas para causar danos com motivação ideológica, e também a guerra virtual, que é a manipulação de notícias para obtenção de uma vantagem estratégica – além da guerra tecnológica por meio de *drones* e outros aparatos telemétricos.

Apesar da expressão "guerra de informações" ter surgido nos anos 80 na doutrina militar estadunidense – foi na Guerra do Golfo de 1991 que seus princípios foram utilizados pela primeira vez:[11]

> A Guerra do Golfo foi fundamentalmente diferente de todos os outros conflitos na medida em que o resultado dependeu tanto da administração das informações quando do desempenho do pessoal e dos equipamentos.

Com efeito, o oligopólio que se formou no mercado de redes de notícias nos anos 90[12] fez com que as empresas dominantes no setor de mídia de massa fossem cada vez mais suscetíveis à

---

[9] LOUW, E. **The media and the political process.** London: SAGE Publications, 2005. p.50.
[10] Ibidem.
[11] CAMPEN, Alan D. **The first information war: The story of communications, computers, and intelligence systems in the Persian Gulf War.** Fairfax, VA: AFCEA International Press, 1992. p. 7.
[12] STREET, John. **Mass media, politics and democracy**. Houndmills: Palgrave Macmillan. 2001. p. 103. Alegação aparentemente complexa, porém de fácil constatação: em que pese o cada vez maior número de canais de disseminação de informações, tais como sites de internet, as fontes das quais esses canais obtém suas informações são cada vez menos numerosas.

propagação de ideias propostas pelo governo estadunidense da época, situação essa que chegou ao auge durante os conflitos de setembro de 2001.

2.1.3 História do terrorismo de Estado

Terrorismo de Estado consiste num regime de violência instaurado por um governo, em que o grupo político que detém o poder se utiliza do terror como instrumento de governabilidade, mediante utilização do aparato do Estado para a prática de ataques contra as liberdades individuais e os direitos humanos[13]. Tais atos tipicamente são praticados pelo antigo regime como forma de combater uma revolução[14].

Com efeito, os exemplos são numerosos no sentido de governos totalitários que, ao enfrentarem movimento revolucionários, lançam mão de artifícios denominados terroristas, tais como o democídio[15].

Tendo em vista a dimensão do tema, serão mencionados apenas dois exemplos de terrorismo de Estado.

A. Império Romano

O Império Romano utilizou técnicas terroristas visando baixar o moral dos "bárbaros", ainda que na época não se falasse propriamente de "terrorismo". Utiliza-se o termo "guerra punitiva", que eventualmente acabou sendo substituído por "guerra destrutiva", que acarretava em estupros coletivos e saques.[16]

Entre os inúmeros exemplos, é possível mencionar o caso da morte do Sexto Pompeu Magno Pio, último opositor ao segundo triunvirato. Quando Sexto Pompeu foi finalmente capturado em Mileto,

---

[13] SCHULTZ, Sabrina. **Operação Condor e Terrorismo de Estado: passado, presente e futuro**. Debat: Rev., ISSNe 1980-3532, Florianópolis, Santa Catarina, Brasil. 2006. p. 90.

[14] BAUER, Caroline Silveira. Avenida João Pessoa, 2050 - 3o. andar : **Terrorismo de Estado e ação de polícia política do Departamento de Ordem Política e Social do Rio Grande do Sul (1964-1982)**. Dissertação apresentada à UFRGS, 2006. p. 85

[15] Extermínio de setores da população.

[16] CARR, Caleb. **A assustadora história do terrorismo**. São Paulo: Ediouro Publicações S/A. 2002. p.5.

no ano 35 a.C., deveria ter sido mandado a julgamento, por ser cidadão romano.

No entanto, acabou sendo executado sem qualquer julgamento. Os historiadores debatem se a execução foi responsabilidade de Marco Antônio ou de Marco Tício, tendo excedido este as instruções que lhe tinham sido dadas por aquele.[17]

Em todo caso, a morte de Sexto Pompeu foi contrária ao direito vigente, tendo servido o propósito de desencorajar levantes contrários ao triunvirato.

B. III Reich

O terrorismo de Estado também pode ser exercido mediante guerra de informações, no sentido de disseminar informações que possam manter a população sob controle governamental. Exemplo histórico disso pode ser encontrado no 3º Reich, durante o qual foi totalmente eliminada a liberdade de imprensa, substituída pela propaganda estatal.

O regime nazista inclusive desenvolveu um receptor de rádio a preços módicos para que a população pudesse receber seus noticiários, o *Volksempfänger* (receptor de rádio do povo)[18]. Esse modelo de rádio não possuía capacidade de receber ondas curtas, para que não fosse possível à população ouvir os informes britânicos ou de outro país aliado.

O 3º Reich foi um período de cometimento de inúmeros atos de terrorismo estatal, muitos cometidos pela Schutzstaffel, mais conhecida por sua sigla SS.

---

[17] ROZOIR, Charles du. **Compêndio de História Romana**. Rio de Janeiro:Typ. Imp. e Const. de J. Villeneuve e Comp. 1840. p. 204.

[18] AYLETT, Glenn. **Hitler´s Radio**. Disponível em: <http://www.transdiffusion.org/radio/features/hitlers_radio> . Acessado em 20/12/2012.

A Schutzstaffel teve papel relevante na administração dos campos de concentração[19], onde foram exterminados milhões de judeus.

Além disso, a Schutzstaffel controlava a Gestapo, que era uma polícia secreta que tinha cinco departamentos[20]. O departamento A, apenas para citar um exemplo, servia para reprimir a oposição política, e tinha quatro sub departamentos para cuidar de: (A1) Comunistas; (A2) Contra sabotagem; (A3) Reacionários e Liberais e (A4) Assassinatos.

O terrorismo estatal existente no 3º Reich foi muito amplo, de forma ser impossível listar todos os atos terroristas cometidos naquela época e, além desses, existem inúmeros outros casos de terrorismo estatal na história.

2.2 O problema da legitimação da função da linguagem

Para que o estudo do terrorismo seja feito de modo imparcial, se faz imprescindível levar em consideração o problema da função da legitimação da linguagem no Direito. Com efeito, o poder de nomeação é de grande importância:

> O veredicto do juiz, que resolve os conflitos ou as negociações a respeito de coisas ou de pessoas ao proclamar publicamente o que elas são na verdade, em última instância, pertence à classe dos actos de nomeação ou de instituição, diferindo assim do insulto lançado por um simples particular que, enquanto discurso privado – *idios logos* –, que só compromete o seu autor, não tem qualquer eficácia simbólica.[21]

Deste modo, percebe-se a diferença entre a manifestação de um particular - por exemplo - um jornalista, sobre o enquadramento

---

[19] Redação United States Holocaust Memorial Museum. **Concentration camps**.Disponível em: http://www.ushmm.org/wlc/en/article.php?ModuleId=10005263 Acesso em 23/04/2014.
[20] LONGERICH, Peter. **Heinrich Himmler: A Life**. Oxford:Oxford University Press. 2013. p. 470.
[21] BOURDIEU, Pierre. **O Poder Simbólico**. Tradução de Fernando Tomaz. Ed. Bertrand: Rio de Janeiro. 1998. p. 236.

ou não de um grupo enquanto terrorista, e a declaração do Poder Judiciário no mesmo sentido.

Quando o Estado-Juiz realiza sua função precípua, está a exercer soberania, e dizer, efetivamente, a verdade – efetivando a nomeação.

Neste sentido:

> O direito é a forma por excelência do discurso actuante, capaz, por sua própria força, de produzir efeitos. Não é demais dizer que ele faz o mundo social, mas com a condição de não se esquecer que ele é feito por este. Convém, com efeito, que nos interroguemos acerca das condições sociais – e dos limites – desta eficácia quase mágica, sob pena de cairmos no nominalismo radial (que certas análises de Michel Foucault sugerem) e de estabelecermos que produzimos as categorias segundos as quais construímos o mundo social e que estas categorias produzem este mundo.[22]

Diante da necessidade de legitimação da linguagem, não é possível aceitar, mesmo considerando a importância e a força da jurisprudência, os pronunciamentos jurisdicionais como verdades absolutas se desconexos do contexto social no qual são proferidos.

Com efeito, mesmo se tratando de julgado proferido por tribunais internacionais, sua legitimidade existirá conforme se adeque à realidade ideológica:

> O facto de a produção jurídica, como as outras formas de produção cultural, se realizar num campo está na origem de em efeito ideológico de desconhecimento que os analistas em geral, ao relacionarem diretamente as ideologias com funções coletivas, e até mesmo com intenções individuais, deixam inevitavelmente escapar.[23]

Seguindo tal linha de raciocínio, considera-se que a relação entre o campo jurídico e o campo do poder se dá na estrutura do "jogo", não se tratando de simples efeito de "agregação mecânica":

---

[22] Ibidem. p. 237/238.
[23] Ibidem. p. 253.

> Os efeitos que se geram no seio dos campos não são nem a soma puramente aditiva de ações anárquicas, nem o produto integrado de um plano concreto. A concorrência de que eles são produto exerce-se no seio de um espaço que pode imprimir-lhe tendências gerais, ligadas aos pressupostos inscritos na própria estrutura do jogo de que eles constituem a lei fundamental, como, neste caso particular, a relação entre o campo jurídico e o campo do poder. (...) É a estrutura do jogo e não um simples efeito de agregação mecânica, que está na origem da transcendência, relevada pelos casos de inversão das instituições, do efeito objetivo e coletivo das ações acumuladas.[24]

Deste modo, é imperativo considerar o problema da legitimação da linguagem e sua inevitável influência antes de se fazer uma tentativa de conceituar o terrorismo.

2.3 Conceito de terrorismo

Apesar de não haver consenso sobre a definição do tema, alguns estudiosos se esforçam em conceituar o que seja terrorismo. Com efeito, uma definição doutrinária de terrorismo seria no seguinte sentido:

> "(...) uma forma de violência cujo efeito realiza-se no âmbito psicológico do indivíduo. Seu objetivo é produzir uma reação psicológica no indivíduo: o terror. O terrorismo é um ato de violência que provoca uma comoção social, uma ação social reativa, isto é, ele é uma violência que procura condicionar comportamentos, uma relação de força."[25]

Ocorre que, ainda que diante dessas definições, não é possível diferenciar terrorismo do uso legítimo da força, pois isso tem caráter subjetivo, conforme o caráter relativo dos valores, já estudado acima.

Em outras palavras, em determinado país que tenha sofrido um ataque, os perpetradores podem ser considerados terroristas;

---

[24] Ibidem. p. 254.
[25] PIERRE, Héctor Luís Saint. **As relações civis - militares no Brasil depois dos atentados de 11 de setembro.** Disponível em: http://www.resdal.org/Archivo/d000019b.htm. Acesso em: 19/01/2013.

porém em outro país, ideologicamente alinhado com o pensamento político-religioso que motivou o ataque, os mesmos homens acusados de serem terroristas alhures podem ali ser considerados heróis nacionais.

Além dos esforços da doutrina, no ordenamento jurídico do direito internacional também existem tentativas de se definir o terrorismo.

Admitindo a complexidade de subjetivismo ideológico supra exposta, o *British Terrorism Act of* 2000 assim define o terrorismo:

> (1) Neste Ato "terrorismo" significa o uso ou ameaça de ação onde –
>
> (a) a ação esteja na subseção,
>
> (b) o uso ou ameaça é arquitetado para influenciar um governo ou uma organização governamental internacional ou para intimidar o público ou uma seção do público, e
>
> (c) o uso ou ameaça é feito com o propósito de buscar objetivos políticos, religiosos, raciais ou ideológicos.[26]|[27]

Deste modo, o *British Terrorism Act* admite a necessidade de motivação política, religiosa, racial ou ideológica para a caracterização, cumulativamente com os dois requisitos das alíneas "a" e "b".

2.4 Direito comparado

Serão analisadas as constituições de alguns países latino americanos, no que concerne ao tratamento ao assunto do terrorismo, para efeito de comparação com nossa própria carta magna.

---

[26] An Act to make provision about terrorism; and to make temporary provision for Northern Ireland about the prosecution and punishment of certain offences, the preservation of peace and the maintenance of order. United Kingdom. 20th of July, 2000.

[27] Tradução livre. No original:
(1) In this Act "terrorism" means the use or threat of action where—
(a) the action falls within subsection,
(b) the use or threat is designed to influence the government or an international governmental organization or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause .

Antes disso, ressalte-se a dificuldade inerente ao estudo do direito comparado. Com efeito, é possível diferenciar entre macrocomparação e microcomparação:

> A macrocomparação ocupa-se com os contornos gerais de um sistema, sem se ater a problemas menores ou particulares. Preocupa-se com o modelo judicial, com as fórmulas utilizadas para se administrar a justiça e para se lidar com as questões que emergem da prática forense. A microcomparação, por outro lado, entra-se na preocupação com se estudar os métodos como se resolvem problemas particulares e específicos.[28]

Diante de tais considerações, afirma-se que o estudo a seguir tem cunho microcomparativo, pois se limita a um problema particular e específico.

Além do Brasil, apenas dois países sul americanos tratam explicitamente do tema em suas constituições: Chile e Peru.

O Chile possui em sua Carta Maior o art. 9º, que possui a seguinte redação:

> *ART. 9º O terrorismo, em qualquer de suas formas é, por essência, contrário aos direitos humanos.*[29]

Neste contexto, foi editada a Lei n.º 18.314/84[30], que trata pormenorizadamente do tema, inclusive versando sobre normas processuais e também conceituando o que seriam atos terroristas:

> *Artigo 2º. – Constituirão delitos terroristas, quando cumprirem o disposto no artigo anterior:*
>
> *1.- Os de homicídio sancionados no artigo 391; os de lesões estabelecidos nos artigos 395, 396, 397 e 398; os de sequestro e subtração de menores punidos nos artigos 141 e 142; os de envio de*

---

[28] GODOY, Arnaldo Sampaio de Moraes. **O esperanto jurídico, a utopia da língua normativa universal perfeita e o relativismo do direito.** Rio de Janeiro:Direito, Estado e Sociedade, n.º 41. Jul/dez 2012. p. 56.

[29] Tradução livre. No original: ART. 9º El terrorismo, en cualquiera de sus formas, es por esencia contrario a los derechos humanos.

[30] CHILE. Lei n.º 18.314. Ministerio del Interior. Publicada em 17/05/1984. Disponível em: http://www.leychile.cl/N?i=29731&f=2011-06-21&p=

cartas ou encomendas explosivas do artigo 403 bis; os de incêndio e estragos, descritos nos artigos 474, 475, 476 e 480, e as infrações contra a saúde pública dos artigos 313 d), 315 e 316, todos do Código Penal. Além disso, o descarrilamento previsto nos artigos 105, 106, 107 e 108 da Lei Geral de Ferrovias.

2.- Apoderar-se ou atentar contra um navio, aeronave, trem, ônubus ou outro meio de transporte público em serviço, ou realizar atos que ponham em perigo a vida, integridade física ou a saúde dos passageiros ou tripulantes.

3.- Atentado contra a vida ou integridade física do Chefe de Estado ou outra autoridade política, judicial, militar, policial ou religiosa, ou de pessoas internacionalmente protegidas, em razão de seus cargos.

4.- Colocar, enviar, ativar, jogar, ou atirar detonar bombas ou de engenhos explosivos ou incendiários de qualquer tipo, armas de grande poder destrutivo dispositivos ou tóxico, corrosivo ou infecciosas.

5.- A conspiração quando se visa a prática de crimes para serem classificados como terroristas sob os números acima e no artigo 1°.[31]

Trata-se sem dúvida da legislação mais completa da região, pelo menos até o advento do Novo Código Penal brasileiro, porém não trata da guerra de informações, já que a lei é de 1984, época em que o assunto começava a surgir na doutrina estadunidense.

---

[31] Tradução livre. No original: Artículo 2°.- Constituirán delitos terroristas, cuando cumplieren lo dispuesto en el artículo anterior:

1.- Los de homicidio sancionados en el artículo 391; los de lesiones establecidos en los artículos 395, 396, 397 y 398; los de secuestro y de sustracción de menores castigados en los artículos 141 y 142; los de envío de cartas o encomiendas explosivas del artículo 403 bis; los de incendio y estragos, descritos en los artículos 474, 475, 476 y 480, y las infracciones contra la salud pública de los artículos 313 d), 315 y 316, todos del Código Penal. Asimismo, el de descarrilamiento contemplado en los artículos 105, 106, 107 y 108 de la Ley General de Ferrocarriles.

2.- Apoderarse o atentar en contra de una nave, aeronave, ferrocarril, bus u otro medio de transporte público en servicio, o realizar actos que pongan en peligro la vida, la integridad corporal o la salud de sus pasajeros o tripulantes.

3.- El atentado en contra de la vida o la integridad corporal del Jefe del Estado o de otra autoridad política, judicial, militar, policial o religiosa, o de personas internacionalmente protegidas, en razón de sus cargos.

4.- Colocar, enviar, activar, arrojar, detonar o disparar bombas o artefactos explosivos o incendiarios de cualquier tipo, armas o artificios de gran poder destructivo o de efectos tóxicos, corrosivos o infecciosos.

5.- La asociación ilícita cuando ella tenga por objeto la comisión de delitos que deban calificarse de terroristas conforme a los números anteriores y al artículo 1°.

A carta magna peruana trata do terrorismo em pelo menos dois trechos. No art. 2º, possibilita que as autoridades policiais detenham terroristas por quinze dias, independentemente de ordem judicial:

> *Art. 2º Toda pessoa tem direito:*
>
> *(...)*
>
> *24 A liberdade e à segurança pessoal. E nesse sentido:*
>
> *Ninguém pode ser preso sem ordem escrita emitida pelo juiz ou a polícia em caso de flagrante delito. O detido deve ser apresentado ao tribunal no prazo de 24 horas ou o fim da instância.*
>
> *• Estes prazos não se aplicam aos casos de terrorismo, espionagem e tráfico de drogas.*
>
> *• Nesses casos, a autoridade policial pode realizar a prisão preventiva de suspeitos por um período não superior a 15 dias corridos. Eles informam ao Ministério Público e ao juiz, que pode aceitar a competência antes da expiração deste prazo.*[32]

Além disso, a constituição peruana possibilita, em seu art. 140, a pena de morte para terroristas:

> *Art. 140. pena de morte só pode ser imposta para o crime de traição em tempo de guerra e terrorismo, de acordo com as leis e tratados de que o Peru é uma parte obrigada.*[33]

---

[32] Tradução livre. No original:
Art. 2º Toda persona tiene derecho:
(...)
24 A la libertad y a la seguridad personal. E consecuencia:
Nadie puede ser detenido sino por mandamiento escrito y motivado del Juez o por las autoridades policiales en caso de flagrante delito. El detenido debe ser puesto a disposición del juzgado correspondiente, dentro de las veinticuatro horas o en el término de la isntancia.
• Estos plazos no se aplican a los casos de terrorismo, espionaje y tráfico de drogas.
• En tales casos, las autoridades policiales pueden efectuar la detención preventiva de los presuntos implicados por un término no mayor de quince dias naturales. Deben dar cuenta al Ministerio Público y al juez, quien puede asumir jurisdicción antes de vencido dicho término.

[33] Tradução livre. No original: Art. 140. La pena de muerte solo puede aplicarse por el delito de traición a la patria en caso de guerra, y el de terrorismo, conforme a las leyes y a los tratados de los que el Perú es parte obligada.

Assim, a legislação peruana é definitivamente a mais severa da região.

2.4.1 Patriot Act

Pouco após os ataques terroristas de 2001, os Estados Unidos da América aprovaram a vigência do "Patriot Act"[34], cujo título oficial é

> *UNINDO E FORTALENENDO A AMÉRICA PROVENDO AS FERRAMENTAS APROPRIADAS PARA INTERCEPTAR E OBSTRUIR O TERRORISMO.* [35]

Trata-se de diploma legislativo cuja aplicabilidade se limita aos Estados Unidos da América, mas que merece análise por regular o tema ora estudado.

Tal dispositivo inclui uma definição de quem seja terrorista, para propósito de impedimento de ingresso em território americano. O Patriot Act possui artigo dispondo sobre quem é ou não considerado terrorista:

> SEC. 411. DEFINIÇÕES relacionadas com o terrorismo.
>
> (a) Justificação da Inadmissibilidade -. Seção 212 (a) (3) do Código de Imigração e Nacionalidade (8 USC 1182 (a) (3)) é alterado -
>
> (1) na alínea (B) -
>
> (A) no item (i) -
>
> (i) através da alteração do subitem (IV) como segue:
>
> `` (IV) é um representante (conforme definido no item (v)) de -

[34] ESTADOS UNIDOS DA AMÉRICA. PUBLIC LAW 107–56—OCT. 26, 2001. WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 37. 2001.

[35] Tradução livre. No original: UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM.

`` (aa) uma organização terrorista estrangeira, designado pelo Secretário de Estado ao abrigo da secção 219, ou

`` (bb) um grupo político, social ou outro semelhante, cujo público endosso de atos de atividade terrorista do Secretário de Estado determinou aos Estados Unidos esforços para reduzir ou eliminar as atividades terroristas,";

(ii) na subseção (V), através da inserção de `` ou" após a seção `` 219", e

(iii) adicionando no final as seguintes novas subseções:

`` (VI) tem usado a posição do alienígena de destaque dentro de qualquer país para endossar ou defendem a atividade terrorista, ou persuadir os outros a apoiar a actividade terrorista ou uma organização terrorista, de uma forma que o Secretário de Estado determinou solapa os esforços Estados Unidos para reduzir ou eliminar as atividades terroristas ou

`` (VII) é o cônjuge ou filho de um estrangeiro que é inadmissível nos termos da presente secção, se a atividade fazendo com que o estrangeiro para ser encontrado inadmissível ocorreu nos últimos cinco anos,";[36]

---

[36] Tradução livre. No original: SEC. 411. DEFINITIONS RELATING TO TERRORISM.
(a) Grounds of Inadmissibility.--Section 212(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)) is amended--
(1) in subparagraph (B)--
(A) in clause (i)--
(i) by amending subclause (IV) to read as follows:
``(IV) is a representative (as defined in clause (v)) of--
``(aa) a foreign terrorist organization, as designated by the Secretary of State under section 219, or
``(bb) a political, social or other similar group whose public endorsement of acts of terrorist activity the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities,";
(ii) in subclause (V), by inserting ``or" after ``section 219,"; and
(iii) by adding at the end the following new subclauses:
``(VI) has used the alien's position of prominence within any country to endorse or espouse terrorist activity, or to persuade others to support terrorist activity or a terrorist organization, in a way that the Secretary of State has determined undermines United States efforts to reduce or eliminate terrorist activities, or

Apesar de a definição ter sido incluída no Código de Imigração e Nacionalidade, pois tem repercussão na entrada de terroristas nos Estados Unidos, é aplicada ainda que o terrorista esteja praticando condutas utilizando métodos virtuais ou de guerra de informações.

Interessante observar a última alínea, a qual diz que o filho ou cônjuge do suspeito também são inelegíveis para entrada, o que faz com que a pena passe não a pessoa do condenado, mas a pessoa do suspeito para atingir também sua família.

No mesmo sentido, de que a família do culpado também deve ser considerada culpada, segue o seguinte artigo, que diz claramente que a família do terrorista não pode ser beneficiada ou ajudada em nada:

> SEC. 427. Sem benefícios para os terroristas ou familiares dos terroristas.
>
> Não obstante qualquer outra disposição do presente subtítulo, nada neste subtítulo deve ser interpretado de forma a fornecer qualquer benefício ou alívio -
>
> (1) qualquer indivíduo culpado por um ato terrorista, ou
>
> (2) qualquer membro da família de qualquer indivíduo descrito no parágrafo (1).[37]

Além disso, outro trecho interessante do Patriot Act "afasta a inafastabilidade" da jurisdição, impedindo o uso de habeas corpus ou outros instrumentos jurídicos em favor do estrangeiro suspeito de

---

``(VII) is the spouse or child of an alien who is inadmissible under this section, if the activity causing the alien to be found inadmissible occurred within the last 5 years,";

[37] Tradução livre. No original: SEC. 427. NO BENEFITS TO TERRORISTS OR FAMILY MEMBERS OF TERRORISTS.

Notwithstanding any other provision of this subtitle, nothing in this subtitle shall be construed to provide any benefit or relief to--

(1) any individual culpable for a specified terrorist activity; or

(2) any family member of any individual described in paragraph (1).

atividades terroristas, permitindo somente um procedimento análogo ao habeas corpus, previsto no próprio Ato:

> (b) Habeas Corpus e Revisão Judicial. -
>
> `` (1) De um modo geral -. Revisão judicial de qualquer ação ou decisão relativa a esta seção (incluindo a revisão judicial dos méritos de uma determinação feita na subseção (a) (3) ou
>
> (a) (6)) está disponível exclusivamente em habeas corpus consistentes com esta subseção. Ressalvado o disposto no parágrafo anterior, nenhum tribunal terá competência para rever, por habeas corpus ou de outra forma, qualquer ação ou decisão.[38]

Essa lei relativizou alguns direitos, diminuindo, por exemplo, a burocracia inerente à realização de interceptações telefônicas e ampliando a capacidade das agências de inteligências americanas. Deste modo, é possível dizer que a eliminação de barreiras para a investigação do terrorismo é a parte mais importante do Patriot Act para este estudo.

Investigar atos de terrorismo virtual e guerra de informações é tarefa complexa e, definitivamente, dispendiosa. O Patriot Act aumenta o orçamento às agências de inteligência encarregadas de realizar tais apurações:

> *SEC. 103. Aumento do financiamento para o centro de assistência técnica na Polícia Federal.*
>
> *Está autorizado a ser apropriado para o Centro de Suporte Técnico estabelecido na seção 811 da Antiterrorismo da Lei de Pena de Morte, de 1996 (Lei Pública 104-132) para ajudar a atender às demandas de atividades para combater o terrorismo e apoiar e*

[38] Tradução livre. No original: (b) Habeas Corpus and Judicial Review.--
``(1) In general.--Judicial review of any action or decision relating to this section (including judicial review of the merits of a determination made under subsection (a)(3) or
(a)(6)) is available exclusively in habeas corpus proceedings consistent with this subsection. Except as provided in the preceding sentence, no court shall have jurisdiction to review, by habeas corpus petition or otherwise, any such action or decision.

> *reforçar o apoio técnico e operações táticas do FBI, $200,000,000 dólares para cada um dos exercícios de 2002, 2003 e 2004.*[39]

Além disso, foi criada uma elaborada rede de monitoramento de atividades eletrônicas suspeitas, por meio da expansão da iniciativa nacional de monitoramento de crimes eletrônicos:

> *SEC. 105. << NOTA: 18 USC 3056 nota >> EXPANSÃO DA INICIATIVA DE FORÇA TAREFA DE MONITORAMENTO DE CRIMES ELETRÔNICOS.*
>
> *O Diretor do Serviço Secreto dos Estados Unidos deve tomar medidas adequadas para desenvolver uma rede nacional de forças-tarefa contra o crime eletrônico, com base no modelo de iniciativa contra crimes de New York, em todos os Estados Unidos, com a finalidade de prevenção, detecção e investigação de vários formas de crimes eletrônicos, incluindo potenciais ataques terroristas contra os sistemas de pagamentos financeiros e infra-estrutura crítica.*[40]

O Título II do Patriot Act prevê procedimentos avançados de monitoramento de atividades suspeitas. De fato, a seção 201 amplia as hipóteses de interceptação telefônica e de dados:

> *SEC. 201. AUTORIDADE para interceptar dados, ligações, e as comunicações electrónicas relacionadas com o terrorismo.*
>
> *Seção 2516 (1) do título 18, United States Code, é alterado -*
>
> *(1) pela nova designação parágrafo (p), assim como redesignado pela seção 434 (2) da Lei Antiterrorismo e Pena de*

---

[39] Tradução livre. No original: SEC. 103. INCREASED FUNDING FOR THE TECHNICAL SUPPORT CENTER AT THE FEDERAL BUREAU OF INVESTIGATION.

There are authorized to be appropriated for the Technical Support Center established in section 811 of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132) to help meet the demands for activities to combat terrorism and support and enhance the technical support and tactical operations of the FBI, $200,000,000 for each of the fiscal years 2002, 2003, and 2004.

[40] Tradução livre. No original: SEC. 105. <<NOTE: 18 USC 3056 note.>> EXPANSION OF NATIONAL ELECTRONIC CRIME TASK FORCE INITIATIVE.

The Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems.

> *Morte Efetiva de 1996 (Lei Pública 104-132;. 110 Stat 1274), conforme o parágrafo (r) e (2) através da inserção após o parágrafo (p), assim como redesignado pela seção 201 (3) da Reforma da Imigração Ilegal e Responsabilidade do Imigrante de 1996 (divisão C da Lei Pública 104-208;. 110 Stat 3009-565), a seguinte novo parágrafo: `` (q)* ***qualquer violação criminal*** *da seção 229 (relativo a armas químicas), ou seções 2332, 2332a, 2332b, 2332d, 2339A, 2339B ou deste título (em* ***relação ao terrorismo****), ou". (****GRIFEI****)*[41]

Esse trecho abrange enormemente as possibilidades de interceptação eletrônica e monitoramento realizado pelas agências de inteligência, pois se houver suspeita de que possa se tratar de qualquer violação criminal relacionada a atividade terrorista, se torna possível a interceptação.

Com efeito, o Título V dessa lei removeu diversos obstáculos à investigação de atividades terroristas, tal como o monitoramento eletrônico de informações:

> *SEC. 504. COORDENAÇÃO COM APLICAÇÃO DA LEI.*
>
> *(a) informação, proveniente de um levantamento eletrônico.- Seção 106 da Lei de Vigilância de Inteligência Estrangeira de 1978 (50 USC 1806), é alterado pela adição de no final o seguinte:*
>
> *(k) (1) policiais federais que realizam a vigilância eletrônica para adquirir informações de inteligência estrangeira sob este título poderão consultar os oficiais policiais federais para coordenar os esforços para investigar ou proteger contra-*
>
> *(A) ataque real ou potencial ou outros atos hostis graves de uma potência estrangeira ou um agente de uma potência estrangeira;*

---

[41] Tradução livre. No original: SEC. 201. AUTHORITY TO INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS RELATING TO TERRORISM.

Section 2516(1) of title 18, United States Code, is amended--

(1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and (2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:``(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or".

> *(B) sabotagem ou terrorismo internacional por uma potência estrangeira ou um agente de uma potência estrangeira, ou*
>
> *(C) as atividades de inteligência clandestinas por um serviço de inteligência de rede ou de uma potência estrangeira, ou por um agente de uma potência estrangeira.*

É possível perceber que nos casos de investigações cujo objeto sejam possíveis terroristas, existe grande flexibilidade da legislação:

> (2) Coordenação autorizada nos termos do parágrafo (1) não impede a certificação exigida pela seção 104 (a) (7) (B) ou a entrada de um pedido ao abrigo da secção 105.".
>
> (b) as informações adquiridas de uma busca física.-Seção 305 da Lei de Vigilância de Inteligência Estrangeira de 1978 (50 USC 1825) é alterado, adicionando no final o seguinte:
>
> (k) (1) policiais federais que realizam pesquisas físicas para adquirir informações de inteligência estrangeira sob este título poderão consultar os oficiais policiais federais para coordenar os esforços para investigar ou proteger contra-
>
> (A) ataque real ou potencial ou outros atos hostis graves de uma potência estrangeira ou um agente de uma potência estrangeira;
>
> (B) sabotagem ou terrorismo internacional por uma potência estrangeira ou um agente de uma potência estrangeira, ou
>
> (C) as atividades de inteligência clandestinas por um serviço de inteligência de rede ou de uma potência estrangeira, ou por um agente de uma potência estrangeira.
>
> (2) Coordenação autorizada nos termos do parágrafo (1) não impede a certificação exigida pela seção 303 (a) (7) ou a entrada de um pedido ao abrigo da secção 304." [42]

[42] Tradução livre. No original: SEC. 504. COORDINATION WITH LAW ENFORCEMENT.
(a) INFORMATION ACQUIRED FROM AN ELECTRONIC SURVEILLANCE.—Section 106 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1806), is amended by adding at the end the following:

A seção 814 tem o título “impedimento e prevenção do cyberterrorismo”, realizando previsões, tais como a definição de terrorismo virtual:

> (d) Definições -. Seção 1030 (e) do título 18, Código dos Estados Unidos é
>
> alterada -
>
> (1) no parágrafo (2) (B), através da inserção de ``, incluindo um computador localizado fora dos Estados Unidos, que é utilizado de uma forma que afeta comércio ou de comunicação dos Estados Unidos interestadual ou estrangeiro" antes do ponto e vírgula;
>
> (2) no parágrafo (7), pelo `` marcante e" no final;
>
> (3) pelo parágrafo impressionante (8) e inserindo o seguinte:
>
> `` (8) o termo 'danos' significa qualquer prejuízo para a integridade ou disponibilidade de dados, um programa, um sistema, ou de informação;";
>
> (4) no parágrafo (9), batendo o período no final e inserindo um ponto e vírgula, e
>
> (5), adicionando no final o seguinte:

‘‘(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against—
‘‘(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
‘‘(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
‘‘(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
‘‘(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.’’.
(b) INFORMATION ACQUIRED FROM A PHYSICAL SEARCH.—Section 305 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1825) is amended by adding at the end the following:
‘‘(k)(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against—
‘‘(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
‘‘(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
‘‘(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
‘‘(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 303(a)(7) or the entry of an order under section 304.’’.

`` (10) o termo 'convicção' deve incluir uma condenação ao abrigo da lei de qualquer Estado por crime punível com pena de prisão superior a 1 ano, um elemento que é o acesso não autorizado ou superior a acesso autorizado, a um computador;

`` (11) o termo 'perda' significa qualquer custo razoável para qualquer vítima, incluindo o custo de responder a uma ofensa, a realização de uma avaliação de danos e restaurar os dados, o programa, sistema ou informações à sua condição anterior à infracção e qualquer perda de receita, custos incorridos, ou outros danos conseqüentes incorridos por causa da interrupção do serviço, e

`` (12) o termo 'pessoa' significa qualquer indivíduo, empresa, sociedade, instituição de ensino, instituição financeira, entidade governamental ou entidade jurídica ou outra.".[43]

A seção 816 operacionaliza o aprimoramento do combate ao terrorismo virtual, e realiza previsões de melhorias em treinamento de agentes:

SEC. 816. << NOTA: 28 USC 509 nota >> Desenvolvimento e Suporte de Segurança Cibernética CAPACIDADES forense..

(a) em geral -. O Procurador-Geral deverá estabelecer esses laboratórios regionais de informática forense, como considera o

[43] Tradução livre. No original: (d) Definitions.--Section 1030(e) of title 18, United States Code is amended--

(1) in paragraph (2)(B), by inserting ``, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States" before the semicolon;

(2) in paragraph (7), by striking ``and" at the end;

(3) by striking paragraph (8) and inserting the following:

``(8) the term `damage' means any impairment to the integrity or availability of data, a program, a system, or information;";

(4) in paragraph (9), by striking the period at the end and inserting a semicolon; and

(5) by adding at the end the following:

``(10) the term `conviction' shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

``(11) the term `loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

``(12) the term `person' means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.".

> procurador-geral apropriado, e prestar apoio aos laboratórios de informática forense existentes, a fim de que todos esses laboratórios de informática forense tem a capacidade -
>
> (1) para fornecer exames forenses com relação à evidência de computador apreendidos ou interceptado relativas à atividade criminosa (incluindo ciberterrorismo);
>
> (2) para fornecer treinamento e educação para a Federal, Estadual e agentes da lei locais e do Ministério Público em matéria de inquéritos, análises forenses, e os processos de criminalidade informática (incluindo ciberterrorismo);
>
> (3) para auxiliar Federal, Estadual e aplicação da lei local, em cumprimento Federal, Estadual e leis criminais locais relacionados com a criminalidade informática;
>
> (4) para facilitar e promover a partilha de conhecimentos a aplicação da lei federal e informações sobre a investigação, análise e julgamento de crime de informática com agentes da lei locais e estaduais e do Ministério Público, incluindo o uso de forças-tarefa multijurisdicionais e
>
> (5) para a realização de outras atividades como o procurador-geral considera apropriado.[44]

Além disso, o orçamento também foi drasticamente majorado para a persecução de tais objetivos de treinamento e aperfeiçoamento:

---

[44] Tradução livre. No original: SEC. 816. <<NOTE: 28 USC 509 note.>> DEVELOPMENT AND SUPPORT OF CYBERSECURITY FORENSIC CAPABILITIES.

(a) In General.--The Attorney General shall establish such regional computer forensic laboratories as the Attorney General considers appropriate, and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability--

(1) to provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyberterrorism);

(2) to provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer-related crime (including cyberterrorism);

(3) to assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime;

(4) to facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer-related crime with State and local law enforcement personnel and prosecutors, including the use of multijurisdictional task forces; and

(5) to carry out such other activities as the Attorney General considers appropriate.

> (b) a autorização das dotações. -
>
> (1) Autorização -. Lá fica autorizado a ser apropriado em cada ano fiscal 50 milhões dólares para fins de realização desta seção.
>
> (2) Disponibilidade -. Montantes alocados de acordo com a autorização das dotações no parágrafo (1) permanecerá disponível até gastos.[45]

Apesar do Patriot Act receber duras críticas, principalmente de grupos associados à defesa de direitos humanos, o fato é que desde a sua vigência não foi registrado nenhum ataque terrorista estrangeiro em solo americano[46].

O estudo das diversas modalidades de terrorismo se faz pertinente na medida em que a guerra de informações pode ser praticada em diferentes tipos de atos terroristas.

2.5 Tipologia do terrorismo

Passa-se a analisar brevemente os diversos tipos de terrorismo, com o objetivo de demonstrar que esse fenômeno não é estático, porém está em constante transformação.

Uma importante definição seria no sentido de que[47]:

> (…) terrorismo é definido como violência política em um conflito assimétrico que é projetado para induzir terror e medo psíquico (às vezes indiscriminado), através da vitimização violenta e destruição de alvos não-combatentes (às vezes símbolos icônicos). Tais atos são feitos para enviar uma mensagem a partir de uma organização

[45] Tradução livre. No original: (b) Authorization of Appropriations.--
(1) Authorization.--There is hereby authorized to be appropriated in each fiscal year $50,000,000 for purposes of carrying out this section.
(2) Availability.--Amounts appropriated pursuant to the authorization of appropriations in paragraph (1) shall remain available until expended.

[46] Apesar de terem sido praticados atos terroristas domésticos, muito mais difíceis de serem evitados já que a maioria das relativizações de direitos do Patriot Act se referem a estrangeiros.

[47] BOCKSTETTE, Carsten. **Jihadist Terrorist Use of Strategic Communication Management Techniques.** No. 20 December 2008 ISSN 1863-6039. P. 8. Disponível em http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/occPapers/occ-paper_20 en.pdf. Acessado em 10/05/2013.

> clandestina ilícito. O objetivo do terrorismo é explorar os meios de comunicação, a fim de alcançar publicidade máxima atingível como um multiplicador de força de amplificação, a fim de influenciar o público-alvo (s), a fim de alcançar objetivos políticos de curto e médio prazo e / ou estados finais de longo prazo desejados.[48]

Diante disso, são identificadas as diferentes sub modalidades de terrorismo, ou seja, a tipologia do terrorismo: terrorismo revolucionário; sub-revolucionário; repressivo; internacional; tradicionalista religioso; separatista e criminal, de forma que cada uma dessas modalidades possui subdivisões[49], algumas das quais são estudadas com o intuito de demonstrar que o terrorismo virtual se adapta às diferentes modalidades de atos terroristas.

2.5.1 Terrorismo revolucionário

Trata-se de espécie bastante comum de terrorismo, praticada com fins revolucionários:

> É exatamente o aspecto indiscriminado do ato (a bomba que mata não somente o inimigo de classe, mas qualquer pessoa que, por acaso, se encontre no lugar da explosão) que representa o elemento distintivo entre o terrorismo revolucionário e aquele que se poderia definir como contra revolucionário ou, mais claramente, fascista. Enquanto, em princípio, a ideia revolucionária aceita o atentado político, mas recusa o terrorismo, porque pode atingir além do inimigo também o aliado (...), o aspecto indiscriminado dos resultados da ação é o elemento determinante para fins da escolha terrorista, por parte dos grupos contra revolucionários, os quais desejam criar uma tal situação de incerteza e de medo que cheguem a produzir condições propícias para um golpe de Estado “pacificador”

---

[48] Tradução livre. No original: (…) terrorism is defined as political violence in an asymmetrical conflict that is designed to induce terror and psychic fear (sometimes indiscriminate) through the violent victimization and destruction of noncombatant targets (sometimes iconic symbols). Such acts are meant to send a message from an illicit clandestine organization. The purpose of terrorism is to exploit the media in order to achieve maximum attainable publicity as an amplifying force multiplier in order to influence the targeted audience(s) in order to reach short- and midterm political goals and/or desired long-term end states.

[49] PONTE, Marcos Rosas Degaut. **Terrorismo. Características, tipologia e presença nas relações internacionais.** 1999. Dissertação (Mestrado em Relações Internacionais) Universidade de Brasília, Brasília, p.39. Citado em BOMFIM, Ana Paula Rocha do. **Terrorismo: O Tênue limite do enquadramento enquanto direito de resistência.** 2007. Dissertação (Mestrado em Direito) Centro Universitário de Brasília. p. 56.

> e libertador. Em síntese, enquanto o terrorismo revolucionários (se e quando aceitável) está com as massas, o terrorismo contra revolucionário está contra as massas.[50]

Como forma de terrorismo visa mudança, a guerra de informações pode ser empregada para instigar medo e incerteza na população em relação ao *status quo*.

2.5.2 Terrorismo anárquico

O objetivo do terrorista é eliminar qualquer forma de organização Estatal, modalidade terrorista cujo exemplo é a Facção do Exército Vermelho, criada em 1968 por uma ala radical da Aliança Estudantil Socialista Alemã, que na época cometera uma série de assassinatos, inclusive dos presidentes de dois dos mais importantes bancos alemães à época – Deutsche Bank (Alfred Herrhausen) e Dresdner Bank (Jurgen Ponto).[51]

Ataques terroristas virtuais possuem, em regra, caráter anárquico. Apesar de não ter o intuito ou a capacidade de eliminar a forma estatal de organização social, muitos ataques virtuais visam demonstrar a fragilidade estatal comprometendo estruturas virtuais do governo. Isso acontece quando ativistas anônimos tiram websites do ar, visando desmoralizar as instituições de determinado país.[52]

2.5.3 Terrorismo igualitário

Adotado principalmente por grupos marxistas, esses movimentos buscam impor um novo sistema baseado na igualdade na distribuição de recursos em uma sociedade centralizada.

Como exemplos podem ser citados o Sendero Luminoso do Peru ou o Partido Comunista Malaio.

---

[50] AZEVEDO, Gilvavi Rodrigues. **Terrorismo e movimentos sociais na América Latina: Sendero Luminoso e Movimento dos Trabalhadores Sem Terra (MST).** Univ. Hum., Brasília, v. 6, n. 2, jul./dez. 2009. p. 63.

[51] Ibidem.

[52] Como exemplo é possível mencionar o ataque simultâneos aos sites da CIA, Departamento de Justiça dos EUA, FBI, NASA e MI6, praticados em agosto de 2012, que deixou tais sistemas fora do ar conforme notícia disponível em <http://www.examiner.com/article/anonymous-takes-down-cia-doj-fbi-nasa-mi6> . Acessado em 23/04/2014.

Tal tipo de terrorismo virtual é atualmente praticado por grupos chineses, que desencadearam, por exemplo, a operação Aurora[53], contra diversas empresas ocidentais, ainda que com objetivos não igualitários, mas comerciais.

2.5.4 Terrorismo pluralista

Tem como objetivo a busca de um sistema não autoritário. Como exemplo, podemos citar a Frente Sandinista de Libertação Nacional da Nicarágua[54], criada em 1962 e que visava compor um movimento de resistência contra a ditadura de Anastásío Somoza, que acabou deposto em 1979 por, entre outros motivos, a utilização de técnicas terroristas e de guerrilha.

No contexto virtual, pode ser mencionado o papel das mídias sociais na primavera árabe[55], ainda que o desfecho de tal movimento ainda não seja conhecido ou previsível.

2.5.5 Terrorismo sub revolucionário

Essa modalidade divide-se em "reformista" e "preservacionista". Enquanto aqueles tentam obter maiores benefícios políticos ou autonomia, este visa manter privilégios.

Em tal modalidade não se busca a revolução, mas apenas a modificação de determinados aspectos em determinada sociedade. A guerra de informações é amplamente utilizada neste contexto, já que os grupos que buscam obter ou conservar privilégios utilizam o espaço virtual para disseminar suas ideologias.

---

[53] ZETTER, Kim. **Google Hack Attack Was Ultra Sophisticated, New Details Show**. Disponível em <http://www.wired.com/2010/01/operation-aurora/>. Acesso em 23/04/2014.
[54] WIKIPEDIA. **Frente Sandinista de Libertação Nacional**. Disponível em http://pt.wikipedia.org/wiki/Frente_Sandinista_de_Liberta%C3%A7%C3%A3o_Nacional>. Acessado em 23/04/2014.
[55] KASSIM, Saleem. **Twitter Revolution: How the Arab Spring Was Helped By Social Media**. Disponível em: <http://www.policymic.com/articles/10642/twitter-revolution-how-the-arab-spring-was-helped-by-social-media>. Acessado em 23/04/2014.

2.5.6 Terrorismo repressivo

As ações terroristas são empregadas para restringir determinados grupos, sejam étnicos ou religiosos. Exemplos relevantes seriam o 3º Reich ou a repressão de Stalin.

A guerra de informações foi amplamente utilizada em ambos exemplos.

2.5.7 Terrorismo separatista

Visa, conforme o nome indica, a separação de um grupo social tendo em vista diferenças étnicas ou religiosas com a sociedade na qual está inserido.

Entre os vários exemplos, destacam-se a Frente de Libertação do Quebec, Exército Republicado Irlandês e também a Pátria Basca e Liberdade (ETA).

Muitos desses grupos utilizam tecnologia para propagar suas ideias.

2.5.8 Terrorismo narco-criminal

Mais conhecido como narco terrorismo, utiliza o tráfico de drogas para financiar o promover os objetivos dos grupos produtores e distribuidores de drogas:

> O espectro do narco terrorismo, internacionalmente caracterizado pelo triângulo letal integrado por narcotraficantes, terroristas e contrabandistas de armas, enfatizando atividades do crime organizado nos grandes centos urbanos já atingidos pela migração descontrolada, emerge, na atualidade, como uma ameaça nova e extremamente perigosa à sociedade humana.[56]

[56] PINHEIRO. Álvaro de Souza. **NARCOTERRORISMO - O Flagelo do Século XXI**. Disponível em < http://www.defesanet.com.br/terror/noticia/972/NARCOTERRORISMO---O-Flagelo-do-Seculo-XXI-%C2%A9/>. Acessado em 23/04/2014.

O uso de *bitcoins*[57] para pagamento de drogas enviadas por correios pode ser mencionado como exemplo do uso de tecnologia para o tráfico de drogas, com objetivos terroristas ou comerciais.

2.6 Normatização no Brasil

A Carta brasileira de 1988 trata explicitamente sobre o tema terrorismo em dois momentos.

Com efeito, o art. 4º expõe que *"A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: (...) VIII - Repúdio ao terrorismo e ao racismo."*[58]

Além disso, o art. 5º, que versa sobre as garantias individuais, tem a seguinte redação em seu inciso XLIII:

> *A Lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática da tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evita-los, se omitirem;*[59]

Além desses dois trechos explícitos, em outros momentos a constituição federal trata do assunto de forma implícita. De fato, o art. 5º caput trata do assunto segurança, dentro do qual se insere o tema ora estudado:

> *Todos são iguais perante a Lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito, a vida, a igualdade, a* ***segurança*** *e a propriedade, nos termos seguintes: (****GRIFEI****)*[60]

---

[57] Moeda virtual criptografada e anônima.
[58] BRASIL. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Poder Legislativo, Brasília, DF, 05 jan. 1988. Art. 4º.
[59] BRASIL. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Poder Legislativo, Brasília, DF, 05 jan. 1988. Art.5º, XLII.
[60] BRASIL. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Poder Legislativo, Brasília, DF, 05 jan. 1988. Art.5º, *caput*.

Além disso, o mesmo artigo trata de dois incisos que versam sobre o tema de modo reflexo (grifado):[61]

> *XVI Todos podem reunir-se pacificamente, **sem armas**, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião, anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso a autoridade competente.*
>
> *XVII É plena a liberdade de associação para fins lícitos, **vedados a de caráter paramilitar**.*

Existe no ordenamento pátrio a Lei de Segurança Nacional - Lei n.º 7.170/83[62], que possui a seguinte tipificação penal:

> *Art. 20 - Devastar, saquear, extorquir, roubar, seqüestrar, manter em cárcere privado, incendiar, depredar, provocar explosão, praticar atentado pessoal ou **atos de terrorismo**, por inconformismo político ou para obtenção de fundos destinados à manutenção de organizações políticas clandestinas ou subversivas.*
>
> *Pena: reclusão, de 3 a 10 anos.*
>
> *Parágrafo único - Se do fato resulta lesão corporal grave, a pena aumenta-se até o dobro; se resulta morte, aumenta-se até o triplo.*

Apesar disso, a referida Lei não define o que sejam os **atos de terrorismo**, tendo em vista as dificuldades já expostas em epígrafe, o que faz com que tal norma seja, salvo melhor juízo, uma norma penal em branco – a ser complementada com base em critérios de cunho político e ideológico, já que os tais atos terroristas não são claramente expostos.

No entanto, o anteprojeto do novo Código Penal, apesar de ainda estar sujeito a modificações, traz os seguintes tipos penais:

> ***Terrorismo***

---

[61] BRASIL. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Poder Legislativo, Brasília, DF, 05 jan. 1988. Art. 5º, XVI e XVII.
[62] BRASIL. **Lei n.º 7.170**. Diário Oficial da União, Brasília, DF, 12 dez. 1983.

Art. 239. Causar terror na população mediante as condutas descritas nos parágrafos deste artigo, quando:

I – tiverem por fim forçar autoridades públicas, nacionais ou estrangeiras, ou pessoas que ajam em nome delas, a fazer o que a lei não exige ou deixar de fazer o que a lei não proíbe;

II – tiverem por fim obter recursos para a manutenção de organizações políticas ou grupos armados, civis ou militares, que atuem contra a ordem constitucional e o Estado Democrático; ou

III – forem motivadas por preconceito de raça, cor, etnia, religião, nacionalidade, sexo, identidade ou orientação sexual, ou por razões políticas, ideológicas, filosóficas ou religiosas.

§ 1º Sequestrar ou manter alguém em cárcere privado;

§ 2º Usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos ou outros meios capazes de causar danos ou promover destruição em massa;

§ 3º Incendiar, depredar, saquear, explodir ou invadir qualquer bem público ou privado;

§ 4º Interferir, sabotar ou danificar sistemas de informática e bancos de dados; ou

§ 5º Sabotar o funcionamento ou apoderar-se, com grave ameaça ou violência a pessoas, do controle, total ou parcial, ainda que de modo temporário, de meios de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia e instalações militares:

Pena – prisão, de oito a quinze anos, além das sanções correspondentes à ameaça, violência, dano, lesão corporal ou morte, tentadas ou consumadas.

Ressalte-se a severidade da pena, que pode chegar, na modalidade simples, até 15 aos de reclusão. O artigo ainda prevê uma forma qualificada do crime:

> *Forma qualificada*
>
> *§6º Se a conduta é praticada pela utilização de arma de destruição em massa ou outro meio capaz de causar grandes danos:*
>
> *Pena – prisão, de doze a vinte anos, além das penas correspondentes à ameaça,violência, dano, lesão corporal ou morte, tentadas ou consumadas.*

Caso o ato terrorista seja praticado com armas de destruição em massa, a pena é majorada, podendo chegar, portanto, até vinte anos de reclusão. O artigo prevê, ainda, uma hipótese de exclusão de tipicidade, claramente destinada a prevenir que manifestações populares legítimas sejam tipificadas como atos terroristas:

> *Exclusão de crime*
>
> *§ 7º Não constitui crime de terrorismo a conduta individual ou coletiva de pessoas movidas por propósitos sociais ou reivindicatórios, desde que os objetivos e meios sejam compatíveis e adequados à sua finalidade.*

Além da prática dos atos terroristas, o financiamento também é severamente punido:

> *Financiamento do terrorismo*
>
> *Art. 240. Oferecer ou receber, obter, guardar, manter em depósito, investir ou de qualquer modo contribuir para a obtenção de ativos, bens e recursos financeiros com a finalidade de financiar, custear ou promover a prática de terrorismo, ainda que o atos relativos a este não venham a ocorrer:*
>
> *Pena – prisão, de oito a quinze anos.*

O projeto prevê as situações de favorecimento pessoal e também de escusa absolutória:

> *Favorecimento pessoal no terrorismo*
>
> *Art. 241. Dar abrigo ou guarida a pessoa de quem se saiba ou se tenha fortes motivos para saber, que tenha praticado ou esteja por praticar crime de terrorismo:*
>
> *Pena – prisão, de quatro a dez anos.*
>
> *Escusa Absolutória*
>
> *Parágrafo único. Não haverá pena se o agente for ascendente ou descendente em primeiro grau, cônjuge, companheiro estável ou irmão da pessoa abrigada ou recebida. Esta escusa não alcança os partícipes que não ostentem idêntica condição.*

No caso de ato terrorista praticado em grandes eventos, existe previsão de causa de aumento de pena:

> *Disposição comum*
>
> *Art. 242. As penas previstas para os crimes deste Capítulo serão aumentadas até a metade se as condutas forem praticadas durante ou por ocasião de grandes eventos esportivos, culturais, educacionais, religiosos, de lazer ou políticos, nacionais ou internacionais.*

Deste modo, percebe-se um esforço do legislador penal em estabelecer critérios claros para a tipificação dos denominados atos terroristas.

No ano 2000, foi estabelecido Comitê Especial na Assembleia Geral da ONU com o intuito de estabelecer uma Convenção Global sobre Terrorismo Internacional. No entanto, as negociações não avançaram e ainda não foi definido um critério uniforme, já que o etiquetamento de determinados grupos ou a eleição de certos critérios pode ser conveniente para alguns países em detrimento de outros.

No âmbito do Poder Executivo brasileiro foi criada a Comissão de Relações Exteriores e Defesa Nacional (Creden), que tem a atribuição de "analisar, estudar e propor soluções de governo para temas de segurança". Tal Comissão elaborou três definições de terrorismo[63]. A definição geral trata terrorismo como

> todo ato com motivação política ou religiosa, que emprega força ou violência física ou psicológica, para infundir terror, intimidando ou coagindo as instituições nacionais, a população ou um segmento da sociedade.

A mesma comissão elaborou também a classificação específica, segundo a qual terrorismo seria todo

> ato de devastar, saquear, explodir bombas, sequestrar, incendiar, depredar ou praticar atentado pessoal ou sabotagem, causando perigo efetivo ou dano a pessoas ou bens, por indivíduos ou grupos, com emprego da força ou violência, física ou psicológica, por motivo de facciosismo político, religioso, étnico/racial ou ideológico, para infundir terror com o propósito de intimidar ou coagir um governo, a população civil ou um segmento da sociedade, a fim de alcançar objetivos políticos ou sociais.

Por fim, a Comissão criou a terceira definição, segundo a qual terrorismo seria todo ato no sentido de

> apoderar-se ou exercer o controle, total ou parcialmente, definitiva ou temporariamente, de meios de comunicação ao público ou de transporte, portos, aeroportos, estações ferroviárias ou rodoviárias, instalações públicas ou estabelecimentos destinados ao abastecimento de água, luz, combustíveis ou alimentos, ou à satisfação de necessidades gerais e impreteríveis da população. Trata-se de ação premeditada, sistemática e imprevisível, de caráter transnacional ou não, que pode ser apoiada por Estados, realizada por grupo político organizado com emprego de violência, não importando a orientação religiosa, a causa ideológica ou a motivação

[63] PANIAGO, Paulo de Tarso Resende e outros. **Uma cartilha para melhor entender o terrorismo internacional**. REVISTA BRASILEIRA DE INTELIGÊNCIA. Brasília: Abin, v. 3, n. 4, set. 2007. p. 13.

> política, geralmente visando destruir a segurança social, intimidar a população ou influir em decisões governamentais.

Com a homogeneização da ideologia ocidental, que acarretou inclusive a proscrição da guerra no direito internacional[64], cada vez mais o terrorismo passa a ser entendido como os atos adversos praticados por grupo social com ideologia diversa da dominante.

Os conceitos de terrorismo virtual e guerra de informações são de crucial relevância para a compreensão dos assuntos aqui abordados.

[64] Ressalte-se que RESEK entende haver, nos âmbitos doutrinário e acadêmico, discussão sobre como o direito internacional atuaria na ocorrência de uma Guerra Total, ou iminência da mesma, partindo da premissa que essa hipótese não passa de um "falso problema", pois quando o mundo foi afetado por grandes guerras, os princípios codificados foram esquecidos antes da primeira batalha. (REZEK, Francisco. Direito Internacional: 12.ed. São Paulo: Saraiva, 2010. p. 394)

3. Terrorismo virtual e guerra de informações

3.1 Guerra de informações

Desde os primórdios, as informações tiveram grande importância na conduta da guerra[65]. A história militar contém inúmeros cenários nos quais o emprego de inteligência foi essencial.

Campanhas de propaganda, uma das formas mais primitivas de guerra de informações, tiveram grande relevância nos conflitos mais recentes, e essa chamada "revolução" estratégica impôs que os analistas militares reconsiderassem algumas presunções fundamentais sobre a guerra, nos campos de surpresa estratégica e a natureza do teatro de operações[66].

Existe definição doutrinária de tal[67] revolução:

> A revolução é feita parcialmente na capacidade do uso de armas de precisão e o controle das forças do próprio combatente (em jargão militar "Azul"), mas também e talvez mais significativamente nos avanços tecnológicos envolvendo a busca, processamento e exploração de informações do "Vermelho": o inimigo e seu ambiente.[68]

Se um dos combatentes conseguir obter superioridade sobre seu adversário como resultado de informações, isso reduz significativamente a necessidade de engajamento militar tradicional, diminuindo, assim, a perda de vida e recursos físicos. O otimista prospecto de um campo de batalha virtual, pós humano e estéril, que

---

[65] HANDEL, M.I. **Intelligence and the problem of strategic surprise**. In: Dearth, D.H. & Goodden, R.T. (eds.). Strategic Intelligence: Theory and Application. 2nd. ed. Washington, DC: US Army War College/ Defense Intelligence Agency, 1995. p. 213.

[66] CAMPEN, A.D., Dearth, D.H. & Goodden, R.T. **Cyberwar: Security, Strategy and Conflict in the Information Age**. Fairfax, VA: AFCEA International Press. 1996. p.10.

[67] HERMAN, M. Where hath our intelligence been? The Revolution in Military Affairs. RUSI Journal. 1998. Disponível em < http://www.tandfonline.com/doi/abs/10.1080/03071849808446332?journalCode=rusi20#preview> Acessado em 24/04/2014. p. 62.

[68] Tradução livre. No original: The revolution is held to rest partly on the capabilities for the use of precision weaponry and control of one's own forces (in military terms, 'Blue'), but also and perhaps more significantly on a technological transformation in the gathering, processing and exploitation of information on 'Red': the enemy and his environment.

viria para substituir os métodos tradicionais de combate, tem compreensível apelo tanto para líderes militares quanto políticos – que perdem popularidade perante a opinião pública quando corpos de soldados retornam em caixões dos campos de batalha.

Se essa ainda é uma realidade distante, as tecnologias de gerenciamento de informações possibilitam a administração de imagens emotivas na mídia, fazendo com que a opinião pública se mobilize conforme sejam as necessidades do governante. Exemplo clássico disso foi o envolvimento de forças americanas em Mogadishu, episódio em que foram massacrados milhares de locais, porém a mídia sensibilizou o telespectador ocidental, sendo capaz de criar até mesmo filme e jogos de vídeo game.

Essa "guerra de percepções" tem grande importância no cenário militar atual[69]:

> (…)tornou-se um aspecto fundamental da guerra de informação contemporânea, por vezes referido, em suas manifestações mais exóticos, como "neo-cortical" ou "guerra epistemológica" e que não exige força militar maciça. Guerra baseada na percepção pode ser realizada em um terreno muito mais jogo do que a maioria dos outros aspectos de uma campanha militar tradicional, assim, até certo ponto, corroendo vantagem da força cinética.[70]

Ressalte-se que não se trata aqui do conceito clássico de guerra, definida como "a contenda armada entre Estados, onde cada parte visa proteger seus interesses nacionais",[71] já que a guerra é atualmente considerada proscrita pelo direito internacional:

> 4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a

[69] SZAFRANSKI, R. (1994). **Neo-cortical warfare: the acme of skill?** Fort Leavenworth:Military Review. 1994. p. 41.

[70] Tradução livre. No original: has become a key aspect of contemporary information warfare, sometimes referred to, in its more exotic manifestations, as "neo-cortical" or "epistemological warfare" and one that does not call for massive military muscle. Perception-based warfare can be conducted on a much more level playing field than most other aspects of a traditional military campaign, thereby to some extent eroding kinetic force advantage

[71] SILVA, Roberto Luiz. **Direito Internacional Público**. Belo Horizonte: Del Rey, 2002, p.406.

> dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas.[72]

Na presente situação de massificação da cultura ocidental, as guerras tradicionais são cada vez mais escassas, porém as guerras de informação se propagam cada vez mais.

Se faz necessária a abordagem de alguns conceitos sobre guerra de informações, citando a doutrina militar estadunidense.

O Exército americano define guerra de informações como "ações tomadas para afetar informações e sistemas de informações de um adversário, enquanto defendendo as próprias informações e sistemas de informações". Além disso, a mesma fonte especifica operações de informações como "operações conduzidas durante tempo de crise ou conflito (inclusive guerra) para obter ou promover objetivos específicos contra adversários ou adversário específico".[73]

A Força Aérea Americana possui manual específico, que versa sobre estratégias para a obtenção de superioridade de informações, a qual é definida como "o grau de dominância que permite a forças aliadas a habilidade de coletar, controlar, explorar e proteger informações de forças de oposição efetivas"[74].

De acordo com a mesma fonte, guerras de informações seriam "operações de informações conduzidas para proteger as informações da USAF e sistemas de informações ou conduzidas para atacar e afetar as informações e sistemas de informações de um determinado adversário".[75]

---

[72] Carta das Nações Unidas, art. 2º, IV. Ressalte-se a diferença entre a versão promulgada em Portugal "Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força (...)" e a versão nacional , que emprega a expressão "deverão evitar" ao invés de "deverão abster-se", o que poderia sustentar um argumento no sentido de que o Brasil teria se comprometido a evitar as guerras e não de se abster de praticá-las, debate que teria mais relevância não fosse o histórico pacífico desta República.

[73] STAFF, Chiefs of. **Joint Doctrine for Information Operations**. Washington: Joint Doctrine Publication. 1998. Pg. 13

[74] STAFF, USAF. **USAF Manual for Information Operations**. Washington:USAF. 2005. p. 2-3.

[75] Idem, Ibidem. Pg. 3.

Um detalhe interessante sobre essas definições é que o conceito de guerra de informações pode ser extrapolado para contextos não militares, tais como, por exemplo, Administração de empresas ou qualquer tipo de disputa comercial. Depreende-se tal noção da seguinte definição[76]:

> A guerra de informação é constituída por essas ações destinadas a proteger, explorar, corromper, negar ou destruir informações ou recursos de informação, a fim de alcançar uma vantagem significativa, o objetivo ou a vitória sobre um adversário.[77]

Existem, no entanto, definições mais sucintas, tais como:

> (...) um conflito entre duas partes onde a TI é o principal meio de obtenção de uma vantagem defensiva ou ofensiva. [78]|[79]

Desde modo, existe uma diferença entre guerra de informações e operações de informações, de forma que aquele é gênero do qual este é espécie.

Com efeito, guerra de informações engloba várias situações como, por exemplo, a utilização de sistemas de telemetria para guiar mísseis e também a disseminação de determinada informação para desmoralizar o inimigo.

Para os propósitos deste estudo, o termo guerra de informações será utilizado como sinônimo de operação de informações, englobando tanto os aspectos de sistemas informatizados como as informações de desmoralização ou com outros objetivos psicológicos no teatro de operações.

---

[76] ALGER, J.I. **Introduction to information warfare**. Citado em: SCHWARTAU, W., **Information Warfare. Cyberterrorism: Protecting your Personal Security in the Information Age.** New York: Thunder's Mouth Press. 2ª ed., 1996, p. 8.

[77] Tradução livre. No original: Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective or victory over an adversary

[78] KING, K.. 1996 Citado em: THRASHER, R.D., **Information Warfare Delphi: Raw Results**. 1996. Disponível em: http:/all.net/books/iw/delphi/top.html. Acessado em: 05/12/2012.

[79] Tradução livre. No original: a conflict between two parties where IT is the primary means of obtaining a defensive or offensive advantage

3.2 Atores da guerra de informações

São pelos menos três os atores de um ato envolvendo a utilização bélica de informações: a população, o perpetrador, e o Estado. Conforme observado no terrorismo estatal, o Estado pode ser o perpetrador, mas esse paradigma pode ser modificado no futuro conforme sejam popularizados e simplificados os sistemas e métodos de ataque virtual.

Atualmente, as forças armadas da maioria dos países desenvolvidos dependem de uma rede complexa de informações e sistemas de comunicações para funcionar adequadamente sob o ponto de vista logístico e também em sua função precípua. Isso possibilita que essas forças consigam obter superioridade sobre vetores menos avançados com certa facilidade. No entanto, isso aumenta a vulnerabilidade dessas forças se deparadas com oponentes que, apesar de mais fracos, possuam conhecimento e habilidade para infiltrar e diminuir a eficácia dessas redes de informações.

Tal situação propõe um desafio interessante quanto à determinação da proporcionalidade da resposta a um ataque. Teoricamente um pequeno grupo terrorista composto por hackers[80] poderia criar caos em um oponente muito superior.

A isso se chama "guerra assimétrica" de informações, conceito análogo ao combate entre Davi e Golias, quando existe grande desequilíbrio entre as forças combatentes, mas esse desequilíbrio não é suficiente para impedir a ação dos atacantes.

Esse fenômeno é chamado de "democratização da guerra"[81], pois implica na maior facilidade de acesso aos instrumentos de combate.

---

[80] O termo corretor para esse contexto seria "cracker", porém "hacker" e "cracker" serão utilizados como se tivesse o mesmo significado.

[81] BERKOWITZ, Bruce D. **War logs on.** Foreign Affairs. 2000. Disponível em < http://www.foreignaffairs.com/articles/56039/bruce-d-berkowitz/war-logs-on-girding-america-for-computer-combat>. Acessado em 24/04/2014.

Com o advento da internet, ativistas sociais e políticos obtiveram um espaço sem precedentes para construir uma base de suporte para perseguirem seus ideais[82].

Grupos politicamente alinhados possuem ao seu dispor os meios para propagar campanhas de propaganda digital contra grupos ideologicamente diversos ou com interesses diversos aos seus.

A estrutura organizacional é importante para determinar se um grupo "terrorista" (ou ideologicamente diverso) irá migrar para essa modalidade de ação e em que escala:[83]|[84]

> o perfil sociológico da maioria dos líderes do IRA e ativistas não é propício para o uso de táticas IW / *netwar*, nem sua estrutura celular torna provável que ele iria admitir hackers e crackers em suas fileiras.[85]

Apesar de tal observação, pertinente a um grupo específico, o padrão de mudança existe em diversos outros grupos, que buscam visibilidade por meio de ataques virtuais.

3.3 UIT – União Internacional de Telecomunicações

Qualquer ataque ou ato envolvendo redes de telecomunicações tem implicações na União Internacional de Telecomunicações (UIT), que lida com comunicações internacionais.

A UIT foi precedida pela União Internacional de Telégrafos, cujo escopo era facilitar o tráfego internacional de telegramas, especialmente na Europa. Um dos primeiros objetivos dessa União foi padronizar os sistemas de comunicações marítimos, já que, na época,

---

[82] BROPHY, P. e outros. **Extremism and the Internet.** London: The British Library. British Library Research & Innovation Report. 1999. p. 145.
[83] RATHMELL, A. e outros. **The IW threat from sub-state groups: an interdisciplinary approach. Paper presented at the Third International Symposium, on Command and Control Research and Technology.** Institute for National Strategic Studies-National Defense University. 1997. p. 17.
[84] É feita nesta citação análise sobre a estrutura do IRA – Exército Republicano Irlandês, que é tida pelo autor como não propícia para a execução de ataques virtuais.
[85] Tradução livre. No original: the sociological profile of most IRA leaders and activists is not conducive to the use of IW/netwar tactics, nor does its tight cellular structure make it likely that it would admit freelance hackers and crackers into its ranks.

uma empresa (Marconi Wireless Systems) se recusava a permitir que seus operadores se comunicassem com qualquer estação que não utilizasse equipamentos de sua marca[86].

Alguns regulamentos da UIT possuem aplicabilidade na guerra de informações, no seu sentido tecnológico. Estações de transmissão de um país não podem interferir com estações de outras nações nas suas frequências autorizadas:

> Art. 34. No âmbito de sua legislação nacional, os membros devem esforçar-se por assegurar que as administrações ofereçam e mantenham, na medida do possível, uma qualidade do serviço mínima, correspondente às recomendações pertinentes do CCITT no que respeita:
>
> a) Ao acesso à rede internacional pelos utilizadores que utilizam terminais cuja ligação à rede tenha sido autorizada e que não causem danos às instalações técnicas nem ao pessoal;
>
> (...)

Além disso, o *International Frequency Regulation Board* (IFRB) da UIT trabalha em conjunto com as diversas agências de telecomunicações nacionais para alocar bandas de passagem eletromagnética, evitando, assim, interferência.

Essas informações são de grande importância para evitar interferência proposital, que pode ser, efetivamente, ato de terrorismo virtual.

3.3.1 Liberdade de expressão, terrorismo e o novo regulamento da UIT

O novo texto do regulamento internacional de telecomunicações, aprovado no final de 2012 em Dubai e ainda não internalizado no Brasil, possui alguns trechos polêmicos e pertinentes ao assunto guerra de informações.

---

[86] CODDING. George A. **The International Telecommunication Union**. Leiden, The Netherlands: E. J. Brill. 1952. p. 84.

Com efeito, a internet, atualmente espaço internacional não regulado, passaria a sofrer regulação estatal. De fato, o texto possui o seguinte artigo:

> Art. 41C. Os Estados-Membros devem esforçar-se para tomar as medidas necessárias para evitar a propagação de comunicações electrónicas não solicitadas em massa e minimizar o seu impacto sobre os serviços de telecomunicações internacionais. Os Estados-Membros são incentivados a cooperar nesse sentido.[87]

Além disso, também foi aprovada resolução específica, no âmbito do tratado supra, que traz o seguinte trecho:

> A Conferência Mundial sobre Telecomunicações (Dubai, 2012)
>
> (…)
>
> resolve convidar os Estados Membros
>
> 1 para a reflexão sobre suas respectivas posições na Internet internacional relacionado questões técnicas, de desenvolvimento e de políticas públicas no âmbito do mandato da UIT em vários fóruns da UIT, incluindo, inter alia, a Mundial das Telecomunicações / ICT Policy Forum, a Comissão de Banda Larga para o Desenvolvimento Digital e grupos de estudo da UIT;
>
> (…)[88]

Analisando o tema, é possível inferir uma tensão entre a liberdade da internet e a suposta necessidade de se regular esse espaço para, inclusive, coibir a prática de ilícitos tais como, por exemplo, a guerra de informações.

---

[87] Tradução livre. No original: Art. 41C. Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services. Member States are encouraged to cooperate in that sense.

[88] Tradução livre. No original: The World Conference on International Telecommunications (Dubai, 2012)
(…)
resolves to invite Member States to elaborate on their respective positions on international Internet related technical, development and public-policy issues within the mandate of ITU at various ITU forums including, inter alia, the World Telecommunication/ICT Policy Forum, the Broadband Commission for Digital Development and ITU study groups;
(…)

Com o inevitável advento da guerra de informações, a tendência é de aumento na regulação da internet, hoje considerada um espaço livre e aberto.

Com efeito, o Marco Civil da Internet, atualmente Projeto de Lei n.º 2.126/2011[89], prevê a "preservação da estabilidade, segurança e funcionalidade da rede, por meio de (...)" e também faz extensas previsões sobre o sigilo de dados e informações.

3.4 Soberania e guerra de informações

A ideia de soberania é um dos pilares da organização do sistema internacional de países.

O conceito clássico de soberania é a prerrogativa que possui o Estado de se determinar, isto é, de definir seu próprio destino. Isso significa o poder do Estado de impor comportamentos, determinar sanções, enfim, exercer jurisdição sobre seu território sem interferência de qualquer ente da comunidade internacional. Não haveria nenhuma entidade acima do Estado soberano – que exerce sobre seu território jurisdição geral e exclusiva.[90]

No entanto, muito se escreve sobre uma suposta crise da soberania no sentido clássico, crise esta alimentada por diversos fatores, entre os quais, a disseminação rápida das informações.

3.4.1 Liberdade de expressão vs segurança nacional

O art 5º, IV e XXI, da Constituição Federal prevê a liberdade de expressão:

> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
>
> (...)
>
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

[89] Atualmente já aprovado pelas Casas Legislativas, pendente publicação.
[90] REZEK, José Francisco. **Direito Internacional Público – curso elementar**. 10. ed. rev. e atual. São Paulo: Saraiva, 2005. p. 161-162.

(...)

O próprio inciso IV veda o anonimato, para possibilitar responsabilidade no caso de excesso no exercício desse direito. No mesmo sentido, o mesmo art. 5º, em seu inciso V, assegura o direito de resposta e de indenização:

> V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem;

No entanto, o art. 215 da própria Carta de 1988 protege a cultura nacional:

> Art. 215. O Estado garantirá a todos o pleno exercício dos direitos culturais e acesso às fontes da cultura nacional, e apoiará e incentivará a valorização e a difusão das manifestações culturais.
>
> § 1º - O Estado protegerá as manifestações das culturas populares, indígenas e afro-brasileiras, e das de outros grupos participantes do processo civilizatório nacional.

Existe, portanto, tensão entre os dois direitos supra mencionados: o direito à liberdade de expressão e o direito à segurança nacional.

Com o advento das redes virtuais de comunicação, o direito à liberdade de expressão é amplamente utilizado, e deve de fato ser garantido, como se pretende com o recém aprovado marco civil da internet.

No entanto, caso o direito à liberdade de expressão seja garantido sem limites, será possível a disseminação de ideias contrárias aos interesses da segurança nacional, tais como, por exemplo: a formação de grupos de extermínio, nazistas, crime organizado, etc.

Seja o direito à segurança nacional exercido muito arduamente, a censura poderá prejudicar o livre intercâmbio de ideias entre os cidadãos.

Assim, se faz necessário ponderar a importância dos dois direitos constitucionais, para que nenhum deles seja totalmente sacrificado em detrimento do outro.

3.4.2 Soberania no controle de informações

Em 1957, a então União Soviética lançou com sucesso o SPUTNIK, primeiro satélite artificial. Ao invés de projetar a humanidade para o espaço, o invento fez com que o homem se voltasse para si mesmo, já que o satélite de comunicações iniciou não somente a "era espacial", mas também, efetivamente, a "revolução da globalização da informação".[91]

Os acadêmicos da época sugeriram diversas aplicações dos satélites para as comunicações internacionais:

> Com o auxílio de satélites artificiais, programas televisivos de Moscou poderão ser facilmente transmitidos não somente a qualquer ponto da União Soviética, mas também para longe de suas fronteiras.[92]

Naquela época, surgiram preocupações causadas pela evidente relativização da soberania de informações, se um país pudesse transmitir propaganda[93] diretamente aos lares de outros países.

Essa preocupação acabou levando, em 15/11/1972, que a UNESCO adotasse a "Declaration of Guiding Principles on the Use of satellite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange", cujos arts. 2º e 6º possuem o seguinte teor:

> Art. 2º

---

[91] NAISBITT, John. **Megatrends**. New York: Warner Books, Inc. 1982. p.12.
[92] NORDENSTRENG, Kaarle e outros. **National Sovereignty and International Communication.** New Jersey: Ablex Publishing Co. 1979. p. 129.
[93] No sentido de propaganda ideológica ou política.

> 1. Transmissão de satélite deve respeitar a soberania e a igualdade de todos os Estados.
>
> 2. Radiodifusão por satélite deverá ser apolítica e conduzida no pleno respeito pelos direitos das pessoas singulares e entidades não-governamentais, como reconhecido pelos Estados e o direito internacional.
>
> Art. 6º
>
> (…)
>
> 2. Cada país tem o direito de decidir sobre o conteúdo dos programas educacionais transmitidos por satélite para o seu povo e, nos casos em que tais programas são produzidos em cooperação com outros países, para participar de seu planejamento e de produção, em pé de igualdade.[94]

Esse artigo demonstra a seriedade da preocupação com o assunto, porém é o art. 9º que expressa a medida da consternação que a relativização da soberania de informação ocasionava então:

> 1. A fim de alcançar os objectivos estabelecidos nos artigos anteriores, é necessário que os Estados, tendo em conta o princípio da liberdade de informação, alcançar ou promover acordos anteriores sobre transmissão via satélite direto para a população de outros que não o país de origem de países a transmissão.[95]

Apesar da declaração supra ser de 1972 e a questão da disseminação de imagens de televisão por satélite ter se tornado irrelevante face ao advento da transmissão de imagens pela internet, o

---

[94] Tradução livre. No original: Art. 2º
1.Satellite broadcasting shall respect the sovereignty and equality of all States.
2. Satellite broadcasting shall be apolitical and conducted with due regard for the rights of individual persons and non-governmental entities, as recognized by States and international law.
Art. 6º
(…)
2. Each country has the right to decide on the content of the educational programmes broadcast by satellite to its people and, in cases where such programmes are produced in co-operation with other countries, to take part in their planning and production, on a free and equal footing.

[95] Tradução livre. No original: In order to further the objectives set out in the preceding articles, it is necessary that States, taking into account the principle of freedom of information, reach or promote prior agreements concerning direct satellite broadcasting to the population of countries other than the country of origin of the transmission.

fato é que o problema permanece relevante, na medida em que alguns Estados tentam manter sua soberania de informações.

Apesar de se tratar de um assunto importante, não se pretende aqui debater o mérito da atual e relevante discussão sobre a crise da soberania em face do sistema internacional.

Busca-se, no entanto, determinar a influência da guerra de informações na soberania dos Estados. Por exemplo, quando se entra em território chinês, o art. 3º do formulário de aduana prevê como itens proibidos:

> (…)matérias impressas, filmes, fotos, discos, filmes, cassetes de áudio, vídeo-cassete, VCD, DVD, e outro meio de armazenamento de computador que são prejudiciais para a política chinesa, a economia, a cultura e a moralidade. [96]|[97]

Com isso, o Estado chinês exerce controle sobre as informações que entram em seu território por meio físico, e de fato também faz isso quando controla mecanismos de busca de internet, fato amplamente divulgado na mídia.[98] Se isso pode ser considerado exercício soberano do controle sobre as informações que entram no país, também pode ser considerado medida arbitrária e antidemocrática de cerceamento das liberdades individuais dos cidadãos.

É difícil imaginar outra saída para a detenção da soberania de informações, e a consequente manutenção de uma situação de vigilância e preparação contra ataques com informações, sem ser a limitação do tráfego de dados estrangeiros.

Estudados os fundamentos teóricos da guerra de informações e do terrorismo virtual, se faz pertinente a análise da

---

[96] Formulário chinês de imigração. Obtido em http://www.tju.edu.cn/ico_site/oic_english/IFS/PFS/201204/t20120426_154794.htm. Acesso em 5/04/2013.

[97] Tradução livre. No original: printed matters, films, photos, records, movies, audio-tapes, video-tapes, VCD, DVD, and other computer storage medium that are harmful to Chinese politics, economy, culture and morality.

[98] BBC, Redação. **China 'blocks Google news site'.** Disponível em: http://news.bbc.co.uk/2/hi/technology/4056255.stm. Acesso em 7/04/2013.

normatização internacional de tais atos, ou seja, dos tratados internacionais que tratem do assunto terrorismo.

Como sequer existem tratados que versem sobre o tema terrorismo virtual ou guerra de informações, analisaremos todos os tratados que abordem, ainda que genericamente, o assunto terrorismo, tentando observar alguma peculiaridade de interesse ao tema deste trabalho em cada um deles.

4 Marco regulatório internacional sobre combate ao terrorismo

4.1. Competência: Estatal ou Internacional

Duas soluções se apresentam para o problema da apuração e julgamento de atos considerados terroristas empregando meios virtuais ou de informações: a competência Estatal, ou seja, exercida pelo país vitimado; ou a competência internacional.

A solução local seria no sentido de que o país que seja vítima de um ato de terrorismo virtual ou de informações seja o responsável por apurar e levar a julgamento os perpetradores. Tal sistema foi observado na maioria dos casos de apuração e julgamento de pessoas consideradas terroristas.

Como exemplo, é possível citar a captura, julgamento e execução de Adolf Eichmann e também a execução de Osama Bin Laden.

No primeiro exemplo, Eichmann, oficial alemão da 2ª Guerra Mundial que serviu na SS, unidade de elite responsável por propagar o terror na comunidade judia na Alemanha, foi morar na Argentina com documentos falsificados depois da guerra.

No entanto, como era acusado pelo Estado de Israel por crimes de guerra, o mesmo foi capturado e retirado clandestinamente da Argentina por agentes da Mossad[99], tendo sido levado a julgamento e posterior execução em Israel.[100]

Apesar de se tratar de um criminoso de guerra, percebemos a total ausência de respeito às normas internacionais e à soberania Argentina, de forma que o Estado de Israel, vítima dos atos perpetrados por Eichmann, se encarregou da apuração, captura, transporte, julgamento e execução do alemão.

---

[99] Instituto de Inteligência e Operações Especiais de Israel.
[100] AHARONI, Zvi e DIETL, Wilhelm. **Operation Eichmann: The Truth About the Pursuit, Capture and Trial.** London: Arms and Armour. 1997. p. 52.

Já o segundo exemplo trata da recente morte de Osama Bin Laden, tido como responsável pelos ataques de 2001 e por uma guerra de propaganda que se arrastou por mais de uma década.

Os esforços de apuração foram empreendidos por agências de inteligência americanas, e a operação "Neptune Spear" foi lançada de bases americanas no Afeganistão, um país então ocupado pela superpotência, tendo como objetivo neutralizar Bin Laden, que, segundo tais fontes de inteligência, estaria se escondendo em uma casa em Bilal Town, Abbottabad, no Paquistão.

Apesar da operação ter sido bem sucedida, culminando com a morte do terrorista, existiu total desconsideração da soberania do Paquistão, que somente foi informado da invasão de seu território após a conclusão do ataque.[101]

A ação foi obviamente considerada legítima pelos EUA, onde existe uma lei que autoriza o Presidente dos Estados Unidos da América a "usar todos os meios necessários e força apropriada contra as nações, organizações ou pessoas que ele considere ter planejado, autorizado, praticado ou auxiliado nos ataques terroristas ocorridos em setembro de 2001".[102]

No entanto, é patente a falta de envolvimento da sociedade internacional se o próprio país onde foi realizada a operação sequer tomou conhecimento do fato.

Os direitos humanos possuem relação com a paz, e vinculação indissociável à democracia, de forma que a universalização

---

[101] BBC, Redação. **Osama Bin Laden, al-Qaeda leader, dead – Barack Obama**. Revista BBC News. May 2, 2011.Disponível em: <http://www.bbc.co.uk/news/world-us-canada-13256676> Acessado em 13 de junho de 2013.

[102] Resolução conjunta do Congresso americano. 18/09/2001. Tradução livre. No original: to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001 (…)

dos direitos humanos reside nos diversos instrumentos legais internacionais.[103]

A Comissão Interamericana de Direitos Humanos se ocupou em produzir instrumentos legais para prevenir e reprimir o terrorismo, como, por exemplo, a Convenção Americana dos Direitos Humanos[104], que, em seu art. 4º, versa sobre o direito à vida:

> Artigo 4º - Direito à vida
>
> 1. Toda pessoa tem o direito de que se respeite sua vida. Esse direito deve ser protegido pela lei e, em geral, desde o momento da concepção. Ninguém pode ser privado da vida arbitrariamente.
>
> 2. Nos países que não houverem abolido a pena de morte, esta só poderá ser imposta pelos delitos mais graves, em cumprimento de sentença final de tribunal competente e em conformidade com a lei que estabeleça tal pena, promulgada antes de haver o delito sido cometido. Tampouco se estenderá sua aplicação a delitos aos quais não se aplique atualmente.
>
> 3. Não se pode restabelecer a pena de morte nos Estados que a hajam abolido.
>
> 4. Em nenhum caso pode a pena de morte ser aplicada a delitos políticos, nem a delitos comuns conexos com delitos políticos.
>
> 5. Não se deve impor a pena de morte a pessoa que, no momento da perpetração do delito, for menor de dezoito anos, ou maior de setenta, nem aplicá-la a mulher em estado de gravidez.
>
> 6. Toda pessoa condenada à morte tem direito a solicitar anistia, indulto ou comutação da pena, os quais podem ser concedidos em todos os casos. Não se pode executar a pena de morte enquanto o pedido estiver pendente de decisão ante a autoridade competente.

A outra possibilidade seria, efetivamente, que a apuração e julgamento dos atos terroristas fosse de competência internacional. Com efeito, se os atos de terrorismo virtual e de informações possuem repercussão internacional, parece lógico que a apuração e julgamento também fossem.

Immanuel Kant considera existirem algumas premissas essenciais para que exista paz entre os Estados. Como efeito, o autor

---

[103] AMARAL, Alberto. **Os direitos humanos e as intervenções humanitárias em face da luta contra o terrorismo**. In VIEIRA, Oscar Vilhena. **DIREITOS HUMANOS. Estado de Direito e a construção da paz**. São Paulo: Quartier Latin, 2005. p. 58.

[104] BRASIL. **Decreto n.º 678**, de 6 de novembro de 1992, publicado no Diário Oficial da União em 9 de novembro de 1992.

entende que "não deve considerar-se como válido nenhum tratado de paz que se tenha feito com a reserva secreta de elementos para uma guerra futura"[105].

Neste sentido, Kant caracteriza os tratados internacionais como simples armistícios, ou adiamento das hostilidades, já que todos mantém exércitos permanentes prontos para o combate.

Deste modo, se faz necessária uma efetiva paz perpétua, e não um adiamento de hostilidades entre os Estados e também entre os diferentes grupos ideológicos existentes.

São três as formas de direito necessários para garantir a paz perpétua de Kant:

> Surge agora a questão que concerne ao essencial do propósito da paz perpétua: «O que a natureza faz neste desígnio em relação ao fim que a razão apresenta ao homem como dever, portanto para a promoção da sua intenção moral, e como a natureza fornece a garantia de que aquilo que o homem deveria fazer segundo as leis da liberdade, mas que não faz, fique assegurado de que o fará, sem que a coacção da natureza cause dano a esta liberdade e, decerto, de harmonia com as três relações do direito público, o direito político, o direito das gentes e o direito cosmopolita.» – Quando digo que a natureza quer que isto ou aquilo ocorra não significa que ela nos imponha um dever de o fazer (pois tal só o pode fazer a razão prática isenta de coacção), mas que ela própria o faz, quer queiramos quer não (fata volentem ducunt, nolentem trahunt ['o destino guia o que voluntariamente se sujeita, arrasta aquele que se recusa]).[106]

Para obter a paz, além de tais premissas, Kant expõe ser necessário que o direito das gentes seja fundamentado numa federação de Estados livres, fazendo uma analogia entre a comunidade internacional e o estado de natureza:

---

[105] KANT, Immanuel. **A Paz Perpétua. Um Projecto Filosófico**. Universidade da Beira Interior, Covilhã, 2008. p.4.
[106] Ibidem, p.28.

> Os povos, enquanto Estados, podem considerar-se como homens singulares que, no seu estado de natureza (isto é, na independência de leis externas), se prejudicam uns aos outros já pela sua simples coexistência e cada um, em vista da sua segurança, pode e deve exigir do outro que entre com ele numa constituição semelhante à constituição civil, na qual se possa garantir a cada um o seu direito. Isto seria uma federação de povos que, no entanto, não deveria ser um Estado de povos.[107]

Para Kant, portanto, é com a cooperação entre os Estados, dispostos em uma federação, que seria possível obter a paz perpétua.

Para garantir a paz perpétua, a solução federalista de Kant não se confunde com um governo central universal:

> A ideia do direito das gentes pressupõe a separação de muitos Estados vizinhos, entre si independentes; e, embora semelhante situação seja em si já uma situação de guerra (se uma associação federativa dos mesmos não evitar a ruptura das hostilidades), é todavia melhor, segundo a ideia da razão, do que a sua fusão por obra de uma potência que controlasse os outros e se transformasse numa monarquia universal; porque as leis, com o aumento do âmbito de governação, perdem progressivamente a sua força, e também porque um despotismo sem alma acaba por cair na anarquia, depois de ter erradicado os germes do bem.[108]

Isso acontece porque Kant entende que existem obstáculos para a integração total dos povos, e que tais barreiras são naturais:

> (...) a natureza quer outra coisa. – Serve-se de dois meios para evitar a mescla dos povos e os separar: a diferença das línguas e das religiões14 ; esta diferença traz, sem dúvida, consigo a inclinação para o ódio mútuo e o pretexto para a guerra.[109]

---

[107] Ibidem, p.15.
[108] Ibidem, p.30.
[109] Ibidem, p.30.

Kant verifica então a necessidade de maior aproximação ideológica entre os grupos sociais para que exista, efetivamente, tal federação de Estados com a consequente paz perpétua:

> (...) com o incremento da cultura e a gradual aproximação dos homens de uma maior consonância nos princípios leva à conivência na paz, a qual se gera e garante não através do enfraquecimento de todas as forças, como acontece no despotismo (cemitério da liberdade), mas mediante o seu equilíbrio, na mais viva emulação.[110]

Se Kant já que considerava, em 1795, que a obtenção da paz perpétua somente seria possível no contexto internacional, ou seja, não seria possível se deixada a cargo de cada Estado isoladamente, com muito mais razão imagina-se que o problema do terrorismo virtual mediante guerra de informações, para quem as fronteiras são transponíveis em frações de segundo, somente pode ser enfrentado mediante cooperação internacional entre os Estados.

O risco de se manter a competência para apuração e julgamento de atos terroristas praticados mediante terrorismo virtual e guerra de informações se dá na medida em que uma país específico confere direitos e garantias a seus cidadãos e estrangeiros residentes em seu território[111], porém pode ser construído um argumento no sentido de que os estrangeiros não residentes não possuiriam tais garantias.

Com efeito, tal raciocínio, ainda que não esteja concatenado com os princípios e diretrizes do direito internacional, certamente fundamentará a defesa da existência do PRISM, codinome do esforço de agências de inteligências estadunidenses realizam, aproveitando-se do monopólio americano de serviços virtuais tais como e-mail e redes sociais, para coletar massivamente dados de estrangeiros.

---

[110] Ibidem, p.30.

[111] Exemplo disso é o art. 5º, caput, da nossa Constituição Federal de 1988: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos **brasileiros e aos estrangeiros residentes no País** a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes (...) (**GRIFEI**)

Caso tal competência estivesse a cargo de organismos internacionais, seria razoável imaginar que cidadãos de todos os países do mundo, e não apenas estadunidenses, fossem considerados pessoas possuidoras de direitos e não objetos de investigação como atualmente acontece sob o conturbado programa PRISM.

Deste modo, devendo ser internacional a competência para apuração e julgamento de tais atos, passamos a analisar brevemente cada tratado que verse, ainda que genericamente, sobre terrorismo, tentando realizar, quando possível, ligação entre os tratados e o tema ora estudado.

4.2 Tratados internacionais anteriores aos efeitos dos ataques terroristas de 11 de setembro de 2001

Existem atualmente diversos tratados e resoluções internacionais que versam sobre o tema terrorismo, de forma que serão estudados isoladamente algum deles, em especial sua pertinência à temática abordada.

O ataque terrorista aos Estados Unidos da América de setembro de 2001 foi um marco para o assunto, de forma que serão analisados os tratados anteriores e depois os posteriores a tal data.

4.2.1 Convenção referente às Infracções e a certos outros Actos cometidos a bordo de Aeronaves (1963)

Por se tratar de um documento de 1963, não abrange a possibilidade de terrorismo virtual, já que naquela época as aeronaves não contavam com os sofisticados sistemas aviônicos atuais, que permitem a operação automatizada dos aviões.

Além disso, o complexo sistema de controle de tráfego aéreo, dependente de inúmeros sistemas computadorizados e de radares, seria severamente prejudicado na hipótese de um ataque virtual.

4.2.2 Convenção para a Repressão da Captura Ilícita de Aeronaves (Haia, 1970);

Essa convenção também é da época em que a maior preocupação dos passageiros era ter o avião sequestrado e os "terroristas" demandarem que o comandante pousasse em Miami ao invés de Havana.

No entanto, diante do cenário atual, no qual aeronaves são utilizadas como armas de destruição em massa, essa convenção ganha importância.

4.2.3 Convenção para Prevenir e Punir os Atos de Terrorismo Configurados em Delitos Contra as Pessoas e a Extorsão Conexa, Quando Tiverem Eles Transcendência Internacional[112] (Washington, 02/02/1971)

Este tratado foi internalizado mediante publicação no Diário Oficial da União no dia 07/04/1999, apesar de ter vigência no âmbito internacional desde 8 de março de 1973. Assim, o decreto passou a ter vigência no Brasil depois de 26 anos de já ter aplicabilidade internacional.

Trata-se de importante convenção, que tem entre seus objetivos prevenir e punir o terrorismo:

> *Artigo 1*
>
> *Os Estados Contratantes obrigam-se a cooperar entre si, tomando todas as medidas que considerem eficazes de acordo com suas respectivas legislações e, especialmente, as que são estabelecidas nesta Convenção, para prevenir e punir os atos de terrorismo e, em especial, o seqüestro, o homicídio e outros atentados contra a vida e a integridade das pessoas a quem o Estado tem o dever de proporcionar proteção especial conforme o direito internacional, bem como a extorsão conexa com tais delitos.*

[112] BRASIL. **Decreto n.º 3.018,** de 6 de abril de 1999. Diário Oficial da União - Seção 1 - 7/4/1999, Página 3.

Na hipótese do perpetrador brasileiro cometer o ato terrorista no exterior, não há do que se falar em extradição, porém na aplicação do artigo 5º do tratado ora analisado:

> *Artigo 5*
>
> *Quando não proceder a extradição solicitada por algum dos delitos especificados no Artigo 2 em virtude de ser nacional a pessoa reclamada ou mediar algum outro impedimento constitucional ou legal, o Estado requerido ficará obrigado a submeter o caso ao conhecimento das autoridades competentes, para fins de processo como se o ato houvesse sido cometido em seu território. A decisão que adotarem as referidas autoridades será comunicada ao Estado requerente. Cumprir-se-á no processo a obrigação que se estabelece no Artigo 4.*

Este artigo é de grande importância na medida em que os atos possuam repercussão em países estrangeiros e o terrorista seja nacional.

4.2.4 Convenção para a Repressão de Actos Ilícitos contra a Segurança da Aviação Civil (Montreal, 1971);

Nesta convenção, vislumbra-se a possibilidade de cometimento de ato de terrorismo virtual na hipótese negritada do artigo abaixo:

> *ARTIGO 1.º*
>
> *1. Comete uma infracção penal quem ilícita e intencionalmente:*
>
> *a) Pratique contra uma pessoa um acto de violência a bordo de uma aeronave em voo susceptível de pôr em perigo a segurança da aeronave; ou*

> *b) Destrua uma aeronave em serviço ou lhe cause danos que tornam incapaz para o voo ou que, por sua natureza, constituam um perigo para a segurança da aeronave em voo; ou*
>
> *c) Coloque ou faça colocar numa aeronave em serviço, por qualquer modo, um engenho ou substâncias capaz de destruir aquela aeronave, ou de lhe causar danos que a tornam incapaz para o voo, ou de lhe causar danos que, por sua natureza, constituam um perigo para a segurança da aeronave em voo; ou*
>
> *d) Destrua ou cause danos às instalações ou serviços da navegação aérea ou perturbe o seu funcionamento, ou tais actos, por sua natureza, constituam um perigo para a segurança das aeronaves em voo;*
>
> ***e) Comunique informações de que tenha conhecimento que são falsas, pondo assim em perigo a segurança de uma aeronave em voo.***
>
> *2. Igualmente comete uma infracção penal quem:*
>
> *a) Tente cometer qualquer das infracções penais mencionadas no n.º 1 do presente artigo; ou*
>
> *b) Seja cúmplice de uma pessoa que comete ou tenta cometer qualquer das referidas infracções penais.*

Isso acontece na medida em que um ato virtual que poderia prejudicar o bom andamento da navegação aérea se dá mediante a comunicação de informações falsas.

Evidente que o intuito do legislador foi, efetivamente, penalizar as informações falsas passadas oralmente via rádio, já que uma pessoa poderia, simulando ser um controlador de tráfego aéreo, determinar vetores que fariam com que uma aeronave colidisse contra uma montanha, por exemplo.

No entanto, qualquer disseminação de informação falsa pode ser enquadrada neste artigo, como, por exemplo, a adulteração de parâmetros dos computadores da aeronave.

4.2.5 Convenção sobre a Prevenção e Repressão de Infracções contra Pessoas gozando de Protecção Internacional, incluindo os Agentes Diplomáticos (Nova Iorque, 1973);

Nesse tratado, são feitas previsões para que os perpetradores de atos praticados contra agentes diplomáticos e outras pessoas que tenham proteção internacional sejam efetivamente punidos. Tais atos são:

> *Artigo 2 º*
>
> *1.O prática intencional de:*
>
> *(a) Um assassinato, seqüestro ou outro ataque contra a pessoa ou a liberdade de uma pessoa internacionalmente protegida;*
>
> *b) Um violento ataque contra as instalações oficiais, alojamentos privados ou os meios de transporte de uma pessoa protegida internacionalmente possam por em perigo a sua pessoa ou a liberdade;*
>
> *(c) A ameaça de cometer tal atentado;*
>
> *(d) Uma tentativa de cometer tal atentado, e*
>
> *(e) Um ato que implique a participação como cúmplice em tal ataque será feito por cada Estado Parte um crime sob sua lei interna.*
>
> *2.Cada Estado Parte deverá tornar esses crimes puníveis com penas adequadas que levem em conta sua gravidade.*
>
> *3.Os n.os 1 e 2 do presente artigo em nada derrogar as obrigações dos Estados Partes em direito internacional a tomar todas as medidas adequadas para prevenir outros ataques à integridade física, à liberdade ou à dignidade de uma pessoa protegida internacionalmente.* [113]

[113] Tradução livre. No original: Article 2
1.The intentional commission of:
(a) A murder, kidnapping or other attack upon the person or liberty of an internationally protected person;
b) A violent attack upon the official premises, the private accommodation or the means of transport of an internationally protected person likely to endanger his person or liberty;

Esse tratado denomina os atos ilícitos como infrações, já que podem ser considerados crimes, ou atos terroristas, a depender do contexto.

4.2.6 Convenção europeia para a repressão do terrorismo (Strasbourg, 1977);

Essa Convenção regional estabelece que nenhum dos atos por ela considerados terroristas poderão ser tidos como de cunho político:

> Artigo 1.º
>
> Para efeitos de extradição entre os Estados Contratantes, nenhuma das infracções a seguir mencionadas será considerada como uma infracção política, como uma infracção conexa a uma infracção política ou como uma infracção inspirada por móbil político:
>
> a) As infracções compreendidas no campo da aplicação da Convenção para a Repressão da Captura Ilícita de Aeronaves, assinada na Haia em 16 de Dezembro de 1970;
>
> b) As infracções compreendidas no campo da aplicação da Convenção para a Repressão de Actos Ilícitos Dirigidos contra a Segurança da Aviação Civil, assinada em Montreal em 23 de Setembro de 1971;
>
> c) As infracções graves constituídas por um ataque contra a vida, a integridade física ou a liberdade das pessoas que gozem de protecção internacional, inclusive os agentes diplomáticos;
>
> d) As infracções comportando o rapto, a detenção de reféns ou o sequestro arbitrário;

(c) A threat to commit any such attack;
(d) An attempt to commit any such attack; and
(e) An act constituting participation as an accomplice in any such attack shall be made by each State Party a crime under its internal law.
2.Each State Party shall make these crimes punishable by appropriate penalties which take into account their grave nature.
3.Paragraphs 1 and 2 of this article in no way derogate from the obligations of States Parties under international law to take all appropriate measures to prevent other attacks on the person, freedom or dignity of an internationally protected person.

> e) As infracções comportando a utilização de bombas, granadas, foguetões, armas de fogo automáticas ou cartas ou embrulhos armadilhados, na medida em que essa utilização apresente perigo para quaisquer pessoas;
>
> f) A tentativa de cometer uma das infracções acima citadas ou a participação como co-autor ou cúmplice de uma pessoa que comete ou tenta cometer uma tal infracção.

Os únicos atos contra a vida que não envolvem explosivos ou armas automáticas que são considerados, são aqueles praticados contra pessoas que gozem de proteção internacional, inclusive os agentes diplomáticos.

4.2.7 Convenção contra a Tomada de Reféns (Nova Iorque, 1979);

Aqui são feitas disposições no sentido de que os perpetradores de sequestros sejam punidos criminalmente segundo o direito interno. O único trecho no qual é feita menção sobre terrorismo é o preâmbulo, que deixa claro que o escopo do tratado é, efetivamente, disciplinar sequestros com motivações ideológicas, que naturalmente não se confunde com o sequestro criminoso, que busca conseguir dinheiro da família da vítima:

> *Convencidos de que urge desenvolver uma cooperação internacional entre os Estados, com vistas à elaboração e a adoção de medidas eficazes para a prevenção, a repressão e a punição de quaisquer atos de tomada de reféns, enquanto manifestações de terrorismo internacional,*[114]
>
> *(..)*

[114] BRASIL. **Decreto n.º 3.517**, de 20 de junho de 2000. Publicado no Diário Oficial da União em 21/06/2000.

4.2.8 Convenção sobre a proteção física dos combustíveis nucleares (Viena, 1980);

Este diploma internacional tem grande importância, já que um ataque nuclear é assunto de grande preocupação internacional, pois teria potenciais consequências desastrosas.

A guerra de informações pode ser um instrumento importante no tocante à utilização de meios nucleares, motivo pelo qual a convenção sobre a proteção das instalações nucleares é, efetivamente, relevante.

Além disso, os combustíveis nucleares são matéria prima de uma eventual bomba atômica. Diante dessas preocupações, a convenção define o que seja transporte nuclear internacional em seu art. 1º, “c”:

> c) "Transporte nuclear internacional" significa o transporte de uma remessa de materiais nucleares por qualquer meio de transporte destinado a ultrapassar as fronteiras do território do Estado em que tem origem, desde a sua partida de uma instalação do expedidor, nesse Estado, até à sua chegada a uma instalação do destinatário, no território do Estado de destino.

O artigo 3º trata sobre a segurança desses combustíveis, que devem ser mantidos em níveis seguros de radiação:

> Artigo 3.º
>
> Cada Estado Parte tomará as necessárias disposições, em conformidade com a sua legislação nacional e em consonância com o direito internacional, para que, sempre que tal seja exequível, no decurso de um transporte nuclear internacional, os materiais nucleares que se encontrem no seu território ou a bordo de um navio ou de um avião sob a sua jurisdição, desde que tal navio ou avião participe no transporte com destino ou proveniente desse Estado, sejam protegidos de acordo com os níveis enunciados no anexo I.

A cooperação internacional é estabelecida nos casos de desaparecimento de materiais nucleares:

> Artigo 5º
>
> (…)
>
> 2 - No caso de furto, roubo ou de qualquer outra obtenção ilícita de materiais nucleares, ou de credível ameaça de um desses actos, os Estados Partes deverão, de acordo com a sua legislação nacional, fornecer cooperação e auxílio, de todas as formas possíveis, com vista à recuperação e protecção de tais materiais, a qualquer Estado que o solicite. Especialmente:
>
> a) Um Estado Parte tomará as medidas necessárias para informar, logo que possível, aos outros Estados que lhe pareçam interessados a ocorrência de qualquer furto, roubo ou outra obtenção ilícita de materiais nucleares, ou de credível ameaça de um desses actos, e para informar, quando necessário, as organizações internacionais;
>
> b) Quando necessário, os Estados Partes interessados trocarão informações entre si ou com as organizações internacionais a fim de proteger os materiais nucleares ameaçados, verificar a integridade dos contentores de expedição ou recuperar os materiais nucleares ilicitamente desviados e deverão:
>
> i) Coordenar os seus esforços por via diplomática ou outras vias acordadas;
>
> ii) Fornecer assistência, se para tal forem solicitados;
>
> iii) Assegurar a restituição dos materiais nucleares roubados ou em falta, em sequência dos factos anteriormente mencionados.
>
> As formas de implementação desta cooperação serão determinadas pelos Estados Partes interessados.
>
> (...)

São previstas condutas que devem ser punidas pelo direito nacional, no tocante aos combustíveis nucleares:

Artigo 7.º

1 - A prática intencional de um dos actos seguintes:

a) Receber, deter, utilizar, ceder, alterar, alienar ou dispersar materiais nucleares, sem autorização legal e provocando ou podendo provocar a morte ou ferimentos graves a outrem ou danos consideráveis em bens;

b) Furto ou roubo de materiais nucleares;

c) Desvio ou qualquer outra apropriação fraudulenta de materiais nucleares;

d) Exigência de entrega de materiais nucleares por ameaça, recurso à força ou qualquer outra forma de intimidação;

e) Ameaça:

i) De utilizar materiais nucleares para provocar a morte ou ferimentos graves a outrem ou causar danos consideráveis em bens;

ii) De cometer uma das infracções descritas na alínea b) a fim de coagir uma pessoa singular ou colectiva, uma organização internacional ou um Estado a praticar ou a abster-se de praticar um acto;

f) Tentativa de cometer uma das infracções descritas nas alíneas a), b) ou c); e

g) Participação numa das infracções descritas nas alíneas a) a f);

é considerada, por cada Estado Parte, como uma infracção punível pelo seu direito nacional.

2 - Cada Estado Parte aplicará às infracções previstas no presente artigo sanções apropriadas, tendo em conta a gravidade da sua natureza.

4.2.9 Convenção regional para a eliminação do terrorismo da associação da Ásia do Sul (Katmandú, 1987);

Trata-se de outra Convenção regional, similar às já estudadas.

A cooperação entre as agências governamentais é prevista nos seguintes termos:

> Artigo VIII
>
> 1. Os Estados Contratantes, sujeito às suas leis nacionais, darão a maior assistência mútua no âmbito de processos instaurados relativamente às infracções referidas no artigo I ou concordar com nos termos do artigo II, incluindo o fornecimento de todas as provas em sua disposição necessária para o processo.
>
> 2. Os Estados Contratantes devem cooperar entre si, na medida permitida por suas leis nacionais, por consultas entre os órgãos competentes, a troca de informações, inteligência e experiência e outras medidas de cooperação que possam ser apropriados, com vista à prevenção de atividades terroristas com medidas de precaução.[115]

4.2.10 Convenção para a Repressão de Actos Ilícitos contra a Segurança da Navegação Marítima (Roma, 1988);

A palavra “terrorismo” é mencionada cinco vezes, porém todas no preâmbulo e nenhuma vez no texto do tratado. Com efeito:

> (...)

[115] Tradução livre. No original: Article VIII

1. Contracting States shall, subject to their national laws, afford one another the greatest measure of mutual assistance in connection with proceedings brought in respect of the offences referred to in Article I or agree to in terms of Article II, including the supply of all evidence at their disposal necessary for the proceedings.
2. Contracting States shall cooperate among themselves, to the extent permitted by their national laws, thought consultations between appropriate agencies, exchange of information, intelligence and expertise and such other cooperative measures as may be appropriate, with a view to prevention of terrorist activities thought precautionary measures.

PROFUNDAMENTE PREOCUPADOS com a escalada mundial de atos de terrorismo em todas as suas formas, que põem em risco e tiram vidas humanas inocentes, comprometem as liberdades fundamentais e prejudicam seriamente a dignidade dos seres humanos,

(...)

RECORDANDO a resolução 40/61 da Assembléia Geral das Nações Unidas, de 9 de dezembro de 1985, que, entre outras disposições, "conclama a que todos os Estados, unilateralmente e em cooperação com outros Estados, bem como os órgãos relevantes das Nações Unidas, contribuam para a eliminação progressiva das causas que constituem a base de terrorismo internacional e dediquem especial atenção a todas as situações, inclusive o colonialismo, o racismo e situações que impliquem violações em massa e flagrantes dos direitos humanos e das liberdades fundamentais e todas aquelas que impliquem ocupação estrangeira, que possam dar surgimento ao terrorismo internacional e pôr em risco a paz e a segurança internacionais",

(...)

RECORDANDO, ALÉM DISSO, que a resolução 40/61 "inequivocamente condena, como criminosos, todos os atos, métodos e práticas de terrorismo, onde quer que e por quem quer que sejam praticados, inclusive aqueles que ponham em risco as relações amigáveis entre Estados e sua segurança",

RECORDANDO TAMBÉM QUE, pela resolução 40/61, a Organização Marítima Internacional foi convidada a "estudar o problema do terrorismo a bordo ou contra navios, com vistas a fazer recomendações sobre medidas adequadas",[116]

(...)

[116] BRASIL. **Decreto n.º 6.136**, de 26 de junho de 2007. Publicado no Diário Oficial da União em 27/06/2007.

No corpo do tratado são feitas previsões de condutas puníveis e também cooperação internacional para a punição dos perpetradores de atos contra embarcações.

4.2.11 Protocolo para a Repressão de Actos Ilícitos de Violência nos Aeroportos ao Serviço da Aviação Civil[117] (Montreal, 1988);

O trecho relevante desse tratado é o artigo 2º:

> *ARTIGO II*
>
> *1. Acrescente-se ao Artigo I da Convenção o seguinte parágrafo 1 bis:*
>
> *"1 bis. Qualquer pessoa comete um crime se, ilícita e intencionalmente, utilizando qualquer artefato, substância ou arma:*
>
> *a) executa um ato de violência contra uma pessoa em um aeroporto que preste serviço à aviação civil internacional, que cause ou possa causar lesões graves ou a morte; ou*
>
> *b) destrói ou causa graves danos às instalações de um aeroporto que preste serviço à aviação civil internacional ou a uma aeronave que não esteja em serviço e esteja situada no aeroporto, ou perturba os serviços do aeroporto,*
>
> *se esse ato coloca em perigo ou pode colocar em perigo a segurança do aeroporto".*
>
> *(...)*

A importância desse protocolo é que ele amplia o alcance da Convenção para a Repressão de Atos Ilícitos contra a Segurança da Aviação Civil (Montreal, 23 de setembro de 1971), para proteger também as instalações aeroportuárias.

Isso é importante porque apesar de ainda ser tecnicamente impossível derrubar um avião remotamente por meio de recursos telemáticos, é plenamente viável, e, a depender do estágio da infra

---

[117] BRASIL. **Decreto n.º 2.611,** de 2 de junho de 1998, publicado no Diário Oficial da União em 03/06/1998.

estrutura de determinado país, não muito difícil, derrubar um avião por meio do comprometimento da estrutura aeroportuária, se incluído neste contexto o sistema de controle de tráfego aéreo.

Deste modo, um ato neste sentido pode ser considerado terrorismo virtual, a ser disciplinado pelo protocolo em epígrafe.

4.2.12 Convenção interamericana contra a fabricação e o tráfico ilícito de armas de fogo, munições, explosivos e outros materiais correlatos (Washington, 1997);

Tem como objetivo[118] coibir a fabricação ilícita e o tráfico[119] de armas de fogo.

4.2.13 Convenção Internacional para a Repressão de Atentados Terroristas à Bomba (Nova Iorque, 1997);

O preâmbulo dessa convenção, que eu seu nome traz a palavra “terrorista”, emprega esse termo algumas vezes, inclusive se referindo a ato terrorista como “criminoso”:

> Recordando também a Declaração sobre Medidas para Eliminar o Terrorismo Internacional, que consta do anexo da resolução 49/60 da Assembléia-Geral, de 9 de dezembro de 1994, na qual, entre outros, "os Estados Membros das Nações Unidas reafirmam solenemente e de forma inequívoca sua condenação a todos os atos, métodos e práticas terroristas, por considerá-los criminosos e injustificáveis, seja onde for ou quem for que os cometa, incluídos os que colocam em perigo as relações de amizade entre os Estados e os povos, e ameaçam a integridade territorial e a segurança dos Estados";[120]

O objetivo da convenção é disciplinar a conduta do terrorista que utiliza explosivos:

> Artigo 2

---

[118] BRASIL. **Decreto n.º 3.229**, de 29 de outubro de 1999. Publicado no Diário Oficial da União em 03/11/1999.
[119] Todo tráfico é ilícito.
[120] BRASIL. **Decreto n.º 4.394,** de 26 de setembro de 2002. Publicado no Diário Oficial da União em 27.9.2002.

> 1. Comete um delito no sentido desta Convenção qualquer pessoa que ilícita e intencionalmente entrega, coloca, lança ou detona um artefato explosivo ou outro artefato mortífero em, dentro ou contra um logradouro público, uma instalação estatal ou governamental, um sistema de transporte público ou uma instalação de infra-estrutura:
>
> a) Com a intenção de causar morte ou grave lesão corporal; ou
>
> b) Com a intenção de causar destruição significativa desse lugar, instalação ou rede que ocasione ou possa ocasionar um grande prejuízo econômico.
>
> 2. Também constitui delito a tentativa de cometer qualquer dos delitos enumerados no parágrafo 1.
>
> 3. Também constitui delito:
>
> a) Participar como cúmplice nos delitos enunciados nos parágrafos 1 ou 2; ou
>
> b) Organizar e dirigir outros na perpetração dos delitos enunciados nos parágrafos 1 e 2; ou
>
> c) Contribuir de qualquer outra forma na perpetração de um ou mais dos delitos enunciados nos parágrafos 1 ou 2 por um grupo de pessoas que atue com um propósito comum; essa contribuição deverá ser intencional e ocorrer seja com a finalidade de colaborar com a atividade ou o propósito delitiva genérico do grupo, seja com o conhecimento da intenção do grupo de cometer o delito ou delitos de que se trate.

É no artigo 5º da convenção que se encontra interessante dispositivo, pertinente ao estudo do terrorismo mediante guerra de informações:

> Artigo 5
>
> Cada Estado Parte adotará as medidas necessárias, inclusive, quando for o caso, a adoção de legislação interna, para garantir que atos criminosos compreendidos no âmbito desta Convenção, em

> especial os que pretendam ou tenham o propósito de criar um estado de terror na população em geral, em um grupo de pessoas ou em determinadas pessoas, não se possam, em nenhuma circunstância, justificar por considerações de natureza política, filosófica, ideológica, racial, étnica, religiosa ou de qualquer natureza semelhante e sejam apenados de forma consistente com sua gravidade.

Os Estados contratantes devem, portanto adotar medidas para garantir que os atos terroristas não possam ser justificados por considerações ideológicas.

Isso traz implicações complexas tendo em vista o relativismo cultural, já que um Estado democrático não tem como punir aquele que é apoiado pelo povo, sob pena de perder sua legitimidade.

A opção restante é, portanto, uma guerra de propaganda, para que o motivo "político, filosófico, ideológico, racial, étnico, religioso ou de qualquer natureza semelhante" seja visto como impertinente pela sociedade – nacional e também internacional.

4.2.14 Convenção árabe para a repressão do terrorismo, assinada em reunião da Secretaria Geral da Liga dos Estados Árabes (Cairo, 1998);

Trata-se de uma convenção regional para a repressão do terrorismo, que faz inclusive uma tentativa de definição do que seja terrorismo:

> 2. Terrorismo
>
> Qualquer ato ou ameaça de violência, quaisquer que sejam seus motivos ou propósitos, que ocorre no avanço de uma agenda criminal individual ou coletiva e procuram semear o pânico entre as pessoas, causando medo de prejudicá-los, ou colocando suas vidas, a liberdade ou a segurança em perigo, ou tentando causar danos ao meio ambiente ou às instalações públicas ou privadas ou de

> propriedade ou de ocupar ou tomá-los, ou tentar comprometer um dos recursos nacionais.. [121]

A convenção árabe também disciplina o intercâmbio de informações, fazendo, inclusive, menção direta aos meios de comunicação e emprego de guerra de informações ("propaganda") utilizados pelos terroristas:

> Artigo 4 º
>
> (...)
>
> I. Troca de informações
>
> 1. Estados Contratantes comprometem-se a promover o intercâmbio de informações entre e dentre elas sobre:
>
> (a) As atividades e os crimes dos grupos terroristas e de seus líderes e membros, sua sede e treinamento, os meios e as fontes pelas quais são financiados e armados, os tipos de armas, munições e explosivos utilizados por eles, e outros meios de agressão, assassinato e destruição;
>
> (b) Os meios de comunicação e propaganda utilizados por grupos terroristas, o seu modus operandi, os movimentos de seus líderes e membros, e os documentos de viagem que eles usam. [122]

[121] Tradução livre. No original: 2. Terrorism
Any act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking to sow panic among people, causing fear by harming them, or placing their lives, liberty or security in danger, or seeking to cause damage to the environment or to public or private installations or property or to occupying or seizing them, or seeking to jeopardize a national resources.

[122] Tradução livre. No original: Article 4
(...)
I. Exchanging of information
1. Contracting States shall undertake to promote the exchange of information between and among them concerning:
(a) The activities and crimes of terrorist groups and of their leaders and members; their headquarters and training; the means and sources by which they are funded and armed; the types of weapons, munitions and explosives used by them; and other means of aggression, murder and destruction;
(b) The means of communication and propaganda used by terrorist groups, their modus operandi; the movements of their leaders and members; and the travel documents that they use.

4.2.15 Convenção sobre a Marcação dos Explosivos Plásticos para efeitos de Detecção (Montreal, 1998);

Tendo em vista a dificuldade em se detectar explosivos plásticos, essa convenção[123] traz uma tabela contendo marcadores que servem como agentes de detecção, que devem estar presentes em qualquer explosivo plástico.

4.2.16 Tratado de cooperação entre os membros de Estados da comunidade dos Estados independentes para lugar contra o terrorismo (Minsk, 1999);

A peculiaridade dessa recente Convenção é ter definido o "terrorismo tecnológico":

> "Terrorismo Tecnológico" - o uso ou a ameaça do uso de armas nucleares, radiológicas, químicas ou bacteriológicas (biológicas) armas ou seus componentes, os microrganismos patogénicos, substâncias radioativas ou outras substâncias nocivas para a saúde humana, incluindo a apreensão, colocando para fora de operação ou destruição de armas nucleares, químicas ou outras instalações que representem um perigo acrescido tecnológicas e ambientais e os sistemas de serviços públicos de cidades e outras localidades habitadas, se esses atos são cometidos com o propósito de minar a segurança pública, aterrorizando a população ou influenciar as decisões do autoridades, a fim de alcançar fins políticos, mercenário ou qualquer outro, bem como as tentativas de cometer um dos crimes listados acima para os mesmos fins e levando, financiamento ou agindo como o instigador, acessório ou cúmplice de uma pessoa que comete ou tenta cometer tal crime; [124]

---

[123] BRASIL. **Decreto n.º 4.021**, de 19 de novembro de 2001. Publicado no Diário Oficial da União em 20/11/2001.

[124] Tradução livre. No original: "Technological terrorism" - the use or threat of the use of nuclear, radiological, chemical or bacteriological (biological) weapons or their components, pathogenic micro-organisms, radioactive substances or other substances harmful to human health, including the seizure, putting out of operation or destruction of nuclear, chemical or other facilities posing an increased technological and environmental danger and the utility systems of towns and other inhabited localities, if these acts are committed for the purpose of undermining public safety, terrorizing the population or influencing the decisions of the authorities in order to achieve political, mercenary or any other ends, as well as attempts to commit one of the crimes listed above for

4.2.17 Convenção da Organização de Unidade Africana (OUA) na prevenção e na luta contra o terrorismo, aprovado em Argel, em 14 de julho de 1999;

Da mesma forma que no tratado da Liga Árabe, a cooperação entre os Estados é disciplinada nessa Convenção:

> 1. Os Estados Partes comprometem-se a reforçar o intercâmbio de informações entre eles em relação a:
>
> (a) atos e crimes cometidos por grupos terroristas, seus líderes e elementos, respectivas sedes e campos de treinamento, seus meios e as fontes de financiamento e de aquisição de armas, os tipos de armas, munições e explosivos utilizados, e outros meios em seu poder;
>
> (b) os métodos e as técnicas utilizadas pelos grupos terroristas, o comportamento desses grupos, o movimento de seus líderes e elementos, bem como seus documentos de viagem de comunicação e propaganda. [125]

Assim, a cooperação deve abranger a questão da utilização de informações para atividades terroristas, já que os métodos de propaganda devem ser monitorados e suas informações trocadas pelos Estados signatários.

4.2.18 Convenção Internacional para a Repressão do Financiamento do Terrorismo (Nova Iorque, 1999).

Essa convenção possui uma abordagem diferenciada em relação a todas as outras até aqui estudadas, na medida em que se

---

the same purposes and leading, financing or acting as the instigator, accessory or accomplice of a person who commits or attempts to commit such a crime;

[125] Tradução livre. No original: 1. States Parties undertake to strengthen the exchange of information among them regarding:
(a) acts and crimes committed by terrorist groups, their leaders and elements, their headquarters and training camps, their means and sources of funding and acquisition of arms, the types of arms, ammunition and explosives used, and other means in their possession;
(b) the communication and propaganda methods and techniques used by the terrorists groups, the behaviour of these groups, the movement of their leaders and elements, as well as their travel documents.

buscou repreender os métodos utilizados pelos terroristas, e aqui o objetivo é cortar os recursos.

Com efeito, enquanto o objetivo é evitar a ação por meio de explosivos, aeronaves ou combustíveis nucleares, por exemplo, o que se busca com essa convenção é evitar que os terroristas tenham condições financeiras de lançar seus ataques.

Isso é ressaltado no preâmbulo[126]:

> Observando que a Declaração sobre Medidas para Eliminar o Terrorismo Internacional incentivou, ainda, os Estados, a reverem urgentemente o âmbito das disposições legais internacionais vigentes para a prevenção, repressão e eliminação do terrorismo em todas as suas formas e manifestações, com o propósito de assegurar a existência de uma ampla estrutura jurídica que abranja todos os aspectos da matéria,
>
> Relembrando a resolução da Assembléia Geral 51/210, de 17 de dezembro de 1996, parágrafo 3, inciso (f), na qual a Assembléia exortou os Estados a adotarem providências para obstar e neutralizar, por meio de medidas internas apropriadas, o financiamento, que direto ou indireto, de terroristas e organizações terroristas por organizações que tenham, ou aleguem ter, fins filantrópicos, sociais ou culturais, ou que estejam, ainda, engajadas em atividades ilegais tais como tráfico de armas e de drogas e extorsão, inclusive a exploração de pessoas para fins de financiamento de atividades terroristas e, em particular, a considerarem, quando pertinente, a adoção de medidas reguladoras para obstar e neutralizar movimentações de fundos supostamente destinados a fins terroristas, sem ameaçar, de qualquer forma, movimentações de capital legítimas e, por fim, a intensificarem o intercâmbio de informações sobre a movimentação desses fundos,

Especificamente neste trecho do preâmbulo, tal enfoque é ressaltado:

---

[126] BRASIL. **Decreto n.º 5.640**, de 26 de dezembro de 2005. Publicado no Diário Oficial da União em 27/12/2005.

> Considerando que o financiamento do terrorismo é objeto de séria preocupação para a comunidade internacional como um todo,
>
> Observando que o número e a gravidade de atos terroristas internacionais dependem do financiamento que os terroristas venham a obter,
>
> Observando, ainda, que os instrumentos jurídicos multilaterais vigentes não abordam expressamente esse financiamento,

Diante da dificuldade de se definir o que seja terrorismo, a convenção simplesmente informa que o ato praticado tiver sido definido em um dos tratados nela listados, ou que tenha causado dano visando intimidar uma população ou obrigar um governo a agir ou abster-se de agir:

> Artigo 2
>
> 1. Qualquer pessoa estará cometendo um delito, em conformidade com o disposto na presente Convenção, quando, por qualquer meio, direta ou indiretamente, ilegal e intencionalmente, prover ou receber fundos com a intenção de empregá-los, ou ciente de que os mesmos serão empregados, no todo ou em parte, para levar a cabo:
>
> a) Um ato que constitua delito no âmbito de e conforme definido em um dos tratados relacionados no anexo; ou
>
> b) Qualquer outro ato com intenção de causar a morte de ou lesões corporais graves a um civil, ou a qualquer outra pessoa que não participe ativamente das hostilidades em situação de conflito armado, quando o propósito do referido ato, por sua natureza e contexto, for intimidar uma população, ou compelir um governo ou uma organização internacional a agir ou abster-se de agir.

4.3 Tratados internacionais posteriores aos efeitos dos ataques terroristas de 11 de setembro de 2001

Após os ataques terroristas de 11 de setembro de 2001 foram aprovadas pelo menos duas normas internacionais, quais sejam:

a resolução 1.373/2001 e a convenção interamericana contra o terrorismo.

Ao contrário das normas previamente analisadas, os dois diplomas a seguir possuem enfoque mais enfático, visando não apenas combater a pontos específicos ou regionais, mas desmantelar as organizações terroristas:

4.3.1 Resolução 1.373/2001

Logo após os ataques terroristas aos EUA de setembro 2001, o Conselho de Segurança das Nações Unidas – do qual o Brasil não fazia parte naquela época sequer em assento rotativo – adotou a Resolução 1.373/2001, a qual dispõe sobre diversas providências a serem adotadas em retaliação aos "terroristas", tais como, por exemplo seu artigo 1º:

> *1. Decide que todos os Estados devem:*
>
> *a)prevenir e reprimir o financiamento de atos terroristas;*
>
> *b)criminalizar o fornecimento ou captação deliberados de fundos por seus nacionais ou em seus territórios, por quaisquer meios, diretos ou indiretos, com a intenção de serem usados ou com o conhecimento de que serão usados para praticar atos terroristas;*
>
> *c)congelar, sem demora, fundos e outros ativos financeiros ou recursos econômicos de pessoas que perpetram, ou intentam perpetrar, atos terroristas, ou participam em ou facilitam o cometimento desses atos. Devem também ser congelados os ativos de entidades pertencentes ou controladas, direta ou indiretamente, por essas pessoas, bem como os ativos de pessoas e entidades atuando em seu nome ou sob seu comando, inclusive fundos advindos ou gerados por bens pertencentes ou controlados, direta ou indiretamente, por tais pessoas e por seus sócios e entidades;*
>
> *d)proibir seus nacionais ou quaisquer pessoas e entidades em seus territórios de disponibilizar quaisquer fundos,*

> *ativos financeiros ou recursos econômicos ou financeiros ou outros serviços financeiros correlatos, direta ou indiretamente, em benefício de pessoas que perpetram, ou intentam perpetrar, facilitam ou participam da execução desses atos; em benefício de entidades pertencentes ou controladas, direta ou indiretamente, por tais pessoas; em benefício de pessoas e entidades atuando em seu nome ou sob seu comando.*

Essa resolução dispõe sobre outras várias diretrizes, fornecendo instrumentos para o combate ao terrorismo.

4.3.2 Convenção interamericana contra o terrorismo (Bridgetown, 2002)

Traz em seu art 4º a previsão de cooperação entre as autoridades competentes no tocante ao intercâmbio de informações, de forma não muito diferente à já vista em outras convenções regionais acima estudadas:

> c) Medidas que assegurem que as autoridades competentes dedicadas ao combate dos delitos estabelecidos nos instrumentos internacionais enumerados no Artigo 2 tenham a capacidade de cooperar e intercambiar informações nos planos nacional e internacional, em conformidade com as condições prescritas no direito interno. Com essa finalidade, cada Estado Parte deverá estabelecer e manter uma unidade de inteligência financeira que seja o centro nacional para coleta, análise e divulgação de informações relevantes sobre lavagem de dinheiro e financiamento do terrorismo. Cada Estado Parte deverá informar o Secretário-Geral da Organização dos Estados Americanos sobre a autoridade designada como sua unidade de inteligência financeira.[127]

A diferença aqui foi o enfoque dado à área de inteligência financeira.

---

[127] BRASIL. **Decreto n.º 5.639**, de 26 de dezembro de 2005. Publicado no Diário Oficial da União em 27/12/2005.

Como foi possível analisar, cada uma dessas convenções internacionais traz algum aspecto interessante e pertinente ao tema ora estudado.

Além dos tratados, existe também que defenda a aplicabilidade de uma variação do princípio jurídico da precaução, tão conhecido do Direito Ambiental, a outros temas envolvendo catástrofes, tal como o terrorismo:

> Quando os riscos ensejam cenários terríveis, faz sentido tomar medidas especiais para eliminar tais riscos, mesmo quando a informação disponível não permita aos reguladores que façam um julgamento confiável sobre a probabilidade que o cenário de fato aconteça[128]. [129]

A Segunda Guerra do Iraque é utilizada como exemplo da aplicação de tal princípio:

> (...) os Estados Unidos seguiram um tipo de princípio da precaução após os ataques de 11/9, respondendo a riscos que não eram prováveis de ocorrer. A Guerra do Iraque foi publicamente defendida com fundamento no princípio da precaução: mesmo que nós não tivéssemos certeza que Saddam Hussein tivesse armas de destruição em massa, ou que as utilizaria caso as tivesse, a guerra seria justificada enquanto meio de eliminar a ameaça.[130|131]

Se faz necessária a análise de alguns casos concretos nos quais a guerra de informações foi empregada, dentro ou não do contexto de terrorismo virtual, para verificar se a legislação internacional supra exposta foi aplicada ou poderia ter sido aplicada de alguma maneira.

---

[128] SUNSTEIN. Cass R. **Worst-Case Scenarios**. Cambridge:Harvard University Press. 2007. p. 119.
[129] Tradução livre. No original: When risks have catastrophic worst-case scenarios, it makes sense to take special measures to eliminate those risks, even then existing information does not enable regulators to make a reliable judgment about the probability that the worst-case scenarios will occur.
[130] SUNSTEIN. Cass R. **Worst-Case Scenarios**. Cabridge:Harvard University Press. 2007. p.123.
[131] Tradução livre. No original: the United States has followed a kind of Precautionary Principle in the aftermath of the 9/11 attacks, responding to risks that were not likely to occur. The Iraq War was publicly defended by reference to the Precautionary Principle: Even if we could not be certain that Saddam Hussein had weapons of mass destruction, or would use them, the war might be justified as a way of eliminating the threat.

Com efeito, além do debate teórico envolvendo conceituação de terrorismo, e também a análise da doutrina sobre guerra de informações e terrorismo virtual, se faz necessário estudar alguns casos onde tais instrumentos tenham sido utilizados.

5. Casuística e condições de operacionalidade

Serão estudadas algumas situações nas quais foi empregado o instrumento da guerra de informações, seja em situações classificadas pela opinião pública como atos de terrorismo, ou atos "legítimos" de guerra.

Ressalte-se o relativismo de valores, de forma que um estudo de caso pode ser tido como verdadeira salvação do mundo para o ocidente, mas interpretado como um ato terrorista para o país atingido.

Isso se justifica na medida em que, considerando-se a complexidade dos ataques envolvendo guerra de informações, são os países desenvolvidos que possuem capacidade de empregar essas técnicas.

5.1 Programa nuclear iraniano

Existem suspeitas de que a República Islâmica do Irã estaria desenvolvendo um programa nuclear[132], o qual alega possuir fins pacíficos. O ocidente demonstra ceticismo em relação a essa informação, principalmente considerando que o Irã possui imensas reservas de petróleo, energia muito mais barata do que a nuclear.

O conflito Árabe-Israelense se expandiu para a realidade virtual, com ataques e contra-ataques documentados nos sítios eletrônicos de ambos os lados. São exemplos de uma prática que nos últimos anos vem se tornando cada vez mais comum.

Apesar de ações militares já terem sido tomadas contra o programa nuclear iraniano no passado, serão analisados alguns ataques virtuais e de informações já empreendidos.

---

[132] GLADSTONE, Rick. **Nuclear Program Talks Could Resume, Iranian Official Says.** New York Times, Edição on-line. Disponível em: <http://www.nytimes.com/2013/07/18/world/middleeast/nuclear-program-talks-could-resume-iranian-official-says.html?ref=nuclearprogram&_r=0>. Acessado em 22/05/2013.

5.1.1 Guerra de informações

Inicialmente cabe salientar a existência do Tratado de Não Proliferação de Armas Nucleares[133], assinado pelo Irã em 1968, cujos três pilares são: 1. A não proliferação; 2. Desarmamento; 3. O direito para o uso pacífico da tecnologia nuclear.

Ressalte-se que esse tratado tem por escopo manter o poder nuclear com as nações que já possuem um arsenal, proibindo que os outros países tenham a mesma situação militar.

Para assegurar que os programas nucleares estejam sendo desenvolvidos com fins pacíficos, foi criada a Agência Nacional de Energia Atômica - IAEA[134] para inspecionar as instalações nucleares dos diversos países que desenvolvem esse tipo de energia.

Para desenvolver energia nuclear com fins pacíficos, assim como para produzir artefatos nucleares, é necessário enriquecer urânio, coisa que inúmeros países ocidentais fazem cotidianamente, inclusive o Brasil.

No relatório da IAEA[135], o Irã é acusado de não prestar cooperação à agência de fiscalização:

> 62. Enquanto a Agência continua a verificar o não desvio de material nuclear declarado nas instalações nucleares e LOFS declaradas pelo Irã em seu Acordo de Salvaguardas, como o Irã não está oferecendo a cooperação necessária, inclusive por não implementar o seu Protocolo Adicional, a Agência é incapaz de fornecer garantias credíveis sobre a ausência de material nuclear não declarado e

[133] BRASIL. Decreto n.º 2.864. Diário Oficial da União. Brasília/DF, 08/12/1998.
[134] A IAEA – International Atomic Energy Agency tem sede em Viena e é um fórum intergovernamental para a cooperação científica e técnica do uso pacífico da tecnologia nuclear.
[135] Implementation of the NPT Safeguards Agreement and relevant provisions of Security Council resolutions in the Islamic Republic of Iran. 21/02/2013. Derestricted 6 March 2013. Disponível em: < http://www.isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Safeguards_report_--_21_Feb_2013.pdf>. Acessado em 18/12/2012.

> atividades no Irã, e, portanto, concluir que todo o material nuclear no Irã é em atividades pacíficas.[136]

É óbvio que a IAEA não pode dizer com 100% de certeza não existir material nuclear não declarado em nenhum país do mundo, pois nenhuma agência tem capacidade de monitorar todo o território mundial para fazer essa negativa universal.

Mas o fato é que o ocidente lançou uma campanha de propaganda[137] para transformar esses relatórios, inconclusivos já que não confirmam nem excluem nada, em verdades de que o Irã estaria produzindo armas nucleares, para legitimar perante a opinião pública futura ação militar.

O interessante é que a imprensa iraniana também faz sua campanha de propaganda, e, mediante citação do mesmo relatório, cujo trecho copiado acima diz claramente não haver cooperação iraniana, produz uma reportagem cujo título é "IAEA admits Iran nuclear energy program peaceful"[138]:

> "O Irã tem um acordo global com a AIEA e o Irã está sujeito às resoluções do Conselho de Segurança da ONU que são juridicamente vinculativos. Este é o padrão ", Diretor Geral da AIEA Yukiya Amano disse em uma conferência de imprensa conjunta com o secretário de Relações Exteriores indiano Ranjan Mathai na quarta-feira.[139]

A reportagem chega a mencionar as acusações feitas por outros países, retrucando:

---

[136] Tradução livre. No original: While the Agency continues to verify the non-diversion of declared nuclear material at the nuclear facilities and LOFs declared by Iran under its Safeguards Agreement, as Iran is not providing the necessary cooperation, including by not implementing its Additional Protocol, the Agency is unable to provide credible assurance about the absence of undeclared nuclear material and activities in Iran, and therefore to conclude that all nuclear material in Iran is in peaceful activities.

[137] http://topics.nytimes.com/top/news/international/countriesandterritories/iran/nuclear_program/index.html. Acessado em 03/03/2013.

[138] PRESSTV, Redação. **IAEA admits Iran nuclear energy program peaceful** .Disponível em: <http://www.presstv.ir/detail/2013/03/13/293451/iran-nuclear-activities-peaceful-amano/>. Acessado em 03/03/2013.

[139] Tradução livre. No original: Iran has a comprehensive agreement with the IAEA and Iran is subject to UN Security Council resolutions which are legally binding. This is the standard," IAEA Director General Yukiya Amano said at a joint press conference with Indian Foreign Secretary Ranjan Mathai on Wednesday.

> Os Estados Unidos, Israel e alguns de seus aliados acusam repetidamente o Irã de perseguir objetivos não-civis em seu programa de energia nuclear.
>
> Irã rejeita as acusações, argumentando que, como um compromisso signatário do Tratado de Não Proliferação Nuclear (TNP) e membro da AIEA, tem o direito de usar tecnologia nuclear para fins pacíficos.
>
> Além disso, a AIEA realizou várias inspecções de instalações nucleares do Irã, mas nunca encontrou qualquer prova de que o programa nuclear civil do Irã foi desviado para a produção de armas nucleares.[140]

Só o tempo esclarecerá qual lado está agindo de boa fé nesta questão, mas o fato é que a crise ainda não chegou a seu desfecho.

5.1.2 Stuxnet

Com o aprofundamento do conflito de informações, em junho de 2010 foi descoberta a existência de um *worm*[141] especializado em infectar computadores operando com sistemas Windows e atacar equipamento e software industrial da Siemens, especificamente o tipo de equipamento utilizado nas usinas iranianas para monitorar processos de enriquecimento de urânio[142].

A empresa de segurança virtual Symantec estima que 60% dos computadores infectados no mundo estejam localizados no Irã[143], e que somente os equipamentos nucleares tenham sido afetados, já que

---

[140] Tradução livre. No original: The United States, Israel, and some of their allies have repeatedly accused Iran of pursuing non-civilian objectives in its nuclear energy program.
Iran rejects the allegations, arguing that as a committed signatory to the nuclear Non-Proliferation Treaty (NPT) and a member of the IAEA, it has the right to use nuclear technology for peaceful purposes.
In addition, the IAEA has conducted numerous inspections of Iran's nuclear facilities but has never found any evidence showing that Iran's civilian nuclear program has been diverted to nuclear weapons production.

[141] Tipo de vírus de computador.

[142] McMILLAN, Robert . "**Siemens: Stuxnet worm hit industrial systems**". Revista Computerworld. 16 Set 2010. Disponível em < http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems> Acessado em 23/10/2013.

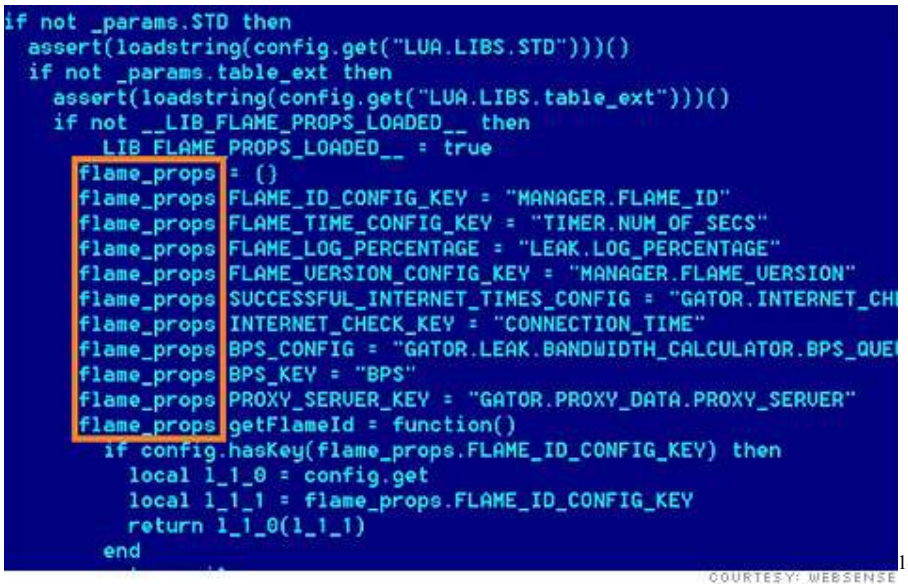
[143] MACLEAN, William. "**UPDATE 2-Cyber attack appears to target Iran-tech firms**". Reuters, 24 set 2010. Disponível em < http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N1OI20100924> Acessado em 20/12/2013.

esse worm possui a capacidade de se instalar em qualquer computador, mas somente afeta os alvos compatíveis.

É possível comparar tal instrumento virtual com equipamentos tradicionais de combate, de forma que um especialista defende que o worm é tão avançado que era como "a utilização de um F-35 em um teatro de operações na primeira guerra mundial"[144].

Os sistemas de defesa iranianos não tiveram a menor chance de se defender e o programa nuclear iraniano sofreu estagnação, já que o *worm* mudou a velocidade de giro das centrífugas, o que influenciou a qualidade do enriquecimento do urânio e, além disso, desgastou os rolamentos do equipamento, que vão precisar de substituição ou reparos[145].

5.1.3 Flame



[146]

Imagem: Agence France-Presse

[144] Ibidem.
[145] WORSTALL, Tim. **Stuxnet Was a Joint US/ Israeli Project** Disponível em: <http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/>. Acessado em 05/01/2013.
[146] GOLDMAN, David. **Super-virus Flame raises the cyberwar stakes**. Disponível em: <http://money.cnn.com/2012/05/30/technology/flame-virus/index.htm>. Acessado em 05/01/2013.

O conflito não se estabilizou. O gráfico acima refere-se a um *spyware*, ou seja, um vírus espião cujo propósito é obter dados de sistemas computadorizados. Esse programa específico foi descoberto pelas autoridades iranianas em 2012, porém, ele operava pelo menos desde 2010 nos computadores e sistemas iranianos.

Apesar de nenhuma autoridade americana ou israelense admitir, especula-se[147] que o vírus tenha sido desenvolvido por agências de inteligência desses países, pois o programa possui a capacidade de infectar os sistemas automatizados existentes nas instalações nucleares iranianas, e gravar todas as informações, transformando, inclusive, câmeras e microfones em gravadores remotos e enviando as informações para o operador do ataque.

As informações obtidas por esse instrumento servem para monitorar o programa nuclear iraniano, e também para planejar e coordenar esforços militares ou de outros ataques virtuais. Além disso, o próprio flame possui capacidade de provocar prejuízo em sistemas Siemens, exatamente iguais àqueles utilizados pelas centrífugas automatizadas do Irã.

O Flame tem capacidade de provocar danos 20 vezes maiores do que o stuxnet[148].

Acontece que, conforme já exposto, o vírus foi descoberto pela autoridades iranianas. Quando uma bomba explode no campo de batalha, não pode mais ser utilizada. Até mesmo os *drones*, avançados robôs aéreos americanos, possuem mecanismos de autodestruição caso sejam abatidos em território hostil, exatamente para que sua tecnologia não seja analisada pelo oponente.

---

[147] THE TELEGRAPH, Redação. **Flame virus 'created by US and Israel as part of intensifying cyber warfare'.** Disponível em: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9343141/Flame-virus-created-by-US-and-Israel-as-part-of-intensifying-cyber-warfare.html>. Acessado em 07/01/2013.

[148] SCHMULOVICH, Michal. **Iran 'Thunderstruck' by AC/DC computer virus**. Disponível em: http://www.timesofisrael.com/iranian-nuclear-plants-thunderstruck-by-acdc-playing-virus/> Acessado em 09/02/2013.

No entanto, quando um código de computador é descoberto pelo inimigo, ele tem a possibilidade de fazer engenharia reversa no programa, e utilizá-lo para seus próprios fins. Essa é uma preocupação crescente na área de segurança de redes:

> “Na guerra, quando uma bomba explode ele detona, em guerra cibernética, malware continua indo e se proliferando ", disse Roger Cressey, vice-presidente sênior da segurança consultoria Booz Allen Hamilton, em uma conferência de segurança cibernética Bloomberg realizada em Nova York no mês passado.
>
> "Uma vez que um pedaço de malware é lançado na natureza, o que acontece com esse código e sua capacidade?" acrescentou. "Coisas como Stuxnet estão sofrendo engenharia reversa".
>
> Uma vez que está lá fora, o código também pode ficar nas mãos dos cidadãos ou terroristas com um conhecimento sofisticado de codificação de software. É por isso que alguns defensores da segurança cibernética estão pedindo ao governo dos EUA para melhor proteger-se contra uma "guerra de código" total que alguns vêem como inevitável.
>
> "A coisa mais aterrorizante é que os governos não têm mais o monopólio sobre essa capacidade", disse Tom Kellerman, o ex-comissário do conselho de segurança cibernética do presidente Obama, na conferência Bloomberg. "Tem códigos por aí que colocam essa capacidade nas mãos de qualquer um."[149|150]

Percebe-se que tudo isso aconteceu ao arrepio de qualquer regulamentação do direito internacional. Com efeito, nenhum país ou

---

[149] GOLDMAN, David. **Super-virus Flame raises the cyberwar stakes**. Disponível em: <http://money.cnn.com/2012/05/30/technology/flame-virus/index.htm>. Acessado em 05/01/2013.

[150] Tradução livre. No original: In warfare, when a bomb goes off it detonates; in cyberwarfare, malware keeps going and gets proliferated," said Roger Cressey, senior vice president at security consultancy Booz Allen Hamilton, at a Bloomberg cybersecurity conference held in New York last month.
"Once a piece of malware is launched in wild, what happens to that code and its capability?" he added. "Things like Stuxnet are being reverse-engineered."
Once it's out there, the code get also get into the hands of citizens or terrorists with a sophisticated knowledge of software coding. That's why some cybersecurity advocates are calling on the U.S. government to better protect itself against an all-out "code war" that some see as inevitable.
"The terrifying thing is that governments no longer have a monopoly on this capability," said Tom Kellerman, former commissioner of President Obama's cyber security council, at the Bloomberg conference. "There is code out there that puts it in anyone's hands.

pessoa sequer assume a autoria desses programas maliciosos, de forma que tais ataques extremamente nocivos à infra estrutura de países não são abrangidos pelo direito internacional.

5.1.4 Thunderstruck

O chefe de uma empresa de segurança virtual da Finlândia, recebeu e-mails de um cientista iraniano narrando um fato curioso:

> "Estou te escrevendo para dizer que nosso programa nuclear foi mais uma vez comprometido e atacado por um novo worm que explora vulnerabilidades e conseguiu desligar nossa instalação em Natanz e outra instalação em Qom. De acordo com o email enviado por especialistas, eles acreditam que uma ferramenta hacker "Metasploit" foi utilizada. Os hackers tiveram acesso ao nosso VPN. Os sistemas automatizados e equipamento Siemens foram atacados e desligados. Não sei muito sobre os detalhes, pois sou cientista e não programador. Além disso, teve música alta tocando a noite toda. Acredito que tenha sido Thunderstruck, do AC/DC."[151]

Não foi a primeira vez que heavy metal foi utilizado como tática de confronto, já que em 2010, forças especiais americanas colocaram *Metallica* e *Thin Lizy* durante confrontos com tropas do Talibã em Marjah. As músicas eram tocadas por muitas horas com o intuito de cansar os talibãs, que detestam esse tipo de música[152]:

> "O Talibã detesta essas músicas", disse o Sargento das forças especiais americanas. "Alguns populares reclamam mas é uma maneira de fazê-los decidir com quem estão. Além disso, os fuzileiros navais ficam motivados." Aparentemente, quando forças rebeldes começaram a atirar contra soldados americanos em Marjah um veículo blindado com "caixas de som potentes" começou a tocar

[151] Tradução livre. No original: I am writing you to inform you that our nuclear program has once again been compromised and attacked by a new worm with exploits which have shut down our automation network at Natanz and another facility Fordo near Qom. According to the email our cyber experts sent to our teams, they believe a hacker tool Metasploit was used. The hackers had access to our VPN. The automation network and Siemens hardware were attacked and shut down. I only know very little about these cyber issues as I am scientist not a computer expert. Here was also some music playing randomly on several of the workstations during the middle of the night with the volume maxed out. I believe it was playing 'Thunderstruck' by AC/DC.

[152] MICHAELS, Sean. **US forces fight Taliban with heavy metal** . Disponível em : <http://www.guardian.co.uk/music/2010/apr/07/us-forces-fight-taliban-metal>. Acessado em 02/03/2013.

> as músicas, rock e heavy metal tão alto que podia ser ouvido a dois quilômetros de distância. As músicas continuaram a tocar por várias horas..[153]

Esse vírus que infectou os computadores das instalações nucleares iranianas passou a desligar os sistemas automatizados, e ligar a música “Thunderstruck”, da banda AC/DC, no meio da noite.

Não existem informações sobre demais danos que esse vírus específico possa ter causado.

5.1.5 Legitimidade dos ataques

Apesar de não haver confirmação de qualquer autoridade sobre a origem dos ataques, os recursos necessários para realizar esse tipo de programa deixam muito claro que não se trata de nenhum indivíduo, mas de governos ou corporações.

Como não se vislumbra que corporação alguma tenha interesse lucrativo em sabotar instalações nucleares iranianas, os suspeitos que sobram são alguns poucos Estados com capacidade de realizar esses sofisticados ataques.

Deste modo, considerando-se que em nenhum momento a IAEA diz claramente existir arsenal nuclear no Irã, que por sua vez alega desenvolver tecnologia para a produção pacífica de energia, e tendo em vista o fato de não se tratar de um ataque formal, já que nenhum país assumiu a autoria dos atos perpetrados, poderiam, e são, efetivamente, considerados terroristas pelo Irã, que se considera vítima dessa situação:

> O Secretário do Conselho Supremo para o Cyber Espaço Mehdi Akhavan Bahabadi disse no Domingo que o Iran, como uma das

[153] Tradução livre. No original: Taliban hate [this] music," said a US special forces sergeant. "Some locals complain but it's a way to push them to choose [sides]. It's motivating marines as well." Apparently, when rebel forces start firing on American soldiers in Marjah, an armoured vehicle with "powerful speakers" fires up the tunes, blaring rock and heavy metal so loudly that it can be heard two kilometres away. The tactical playlist continues for several hours.

> maiores vítimas do terrorismo virtual, condena quaisquer medidas para promover tais ataques.[154|155]

No entanto, graças à efetividade da guerra de informações empreendida, o fato é que a opinião pública ocidental não condena esses atos, supostamente terroristas – pelo contrário, os enxergam como convenientes, pois possuem o condão de evitar ação militar direta, poupando, assim, vidas ocidentais.

5.2 Batalha de Mogadishu (1993)

5.2.1 Contexto do teatro de operações

No dia 3 de outubro de 1993, uma força americana composta por 160 soldados de elite tentaram invadir uma reunião do alto comando somaliano, para capturar os presentes, inclusive o general Mohamed Farrah Aidid, principal Senhor da Guerra da época, que inclusive recebeu treinamento na conhecida Academia Militar Frunze, frequentada apenas pela elite dos estrategistas da antiga União Soviética e seus aliados.[156]

No entanto, durante a operação, dois helicópteros americanos que davam apoio foram abatidos por forças somalianas, de forma que o foco da missão passou a ser resgatar os tripulantes.

Durante dois dias de luta, foram mortos 18 soldados americanos, e entre 1.500 e 3 mil homens[157] somalianos, o que, estima-se, equivaliam a um terço da força total da milícia somaliana.

Havia forças do Paquistão e Malásia apoiando os americanos, porém as fatalidades do lado estadunidense foram pequenas:

---

[154] THE FREE LIBRARY, Redação. **Official Calls Iran Main Victim of Cyber Terrorism**. Disponível em: <http://www.thefreelibrary.com/Official+Calls+Iran+Main+Victim+of+Cyber+Terrorism.-a0305291573 > Acessado em 02/02/2013.

[155] Tradução livre. No original: Secretary of Iran's Supreme Council of Cyberspace Mehdi Akhavan Bahabadi said here on Sunday that Iran, as one of the biggest victims of cyber terrorism, condemns any moves to promote such attacks.

[156] AHMED, Abdul. **Brothers in Arms Part I .** Disponível em: <http://wardheernews.com/Articles_2011/Oct/29_Brothers_in_Army_abdul.pdf> Acessado em 02/02/2013.

[157] Estimativas obtidas dos canais de comunicação, motivo da ampla variação.

> O Pentágono informou inicialmente cinco soldados americanos foram mortos, mas o número era realmente 18 soldados americanos mortos e 73 feridos. Dois dias depois, um soldado de 19, Delta operador SFC Matt Rierson, foi morto em um ataque de morteiro. Entre as forças da ONU, um malaio e um paquistanês morreu, sete malaios e dois paquistaneses ficaram feridos.[158|159]

Ressalte-se que a qualquer observador seria razoável imaginar que o confronto foi uma vitória americana absoluta.

5.2.2 Terror e brutalidade

Apesar dos números estarrecedores, que indicam total massacre dos somalianos, que perderam milhares de homens, os corpos dos 18 americanos foram mutilados e arrastados pelas ruas da cidade de Mogadishu, e parte dessas cenas de barbaridade acabaram sendo filmadas pelas redes de televisão americanas, que mostraram tudo em seus telejornais[160].

5.2.3 Guerra de informações

Apesar da devastadora e inquestionável vitória militar americana, se observados os números, a opinião pública, diante dessas imagens de soldados mortos sendo arrastados pelas ruas, se voltou contra as ações americanas da Somália:

> Fotos de somalianos arrastando corpos de soldados norte-americanos com zombaria pelas ruas de Mogadíscio, transmitidas pela CNN nos Estados Unidos acabaram por alienar a opinião pública em relação à permanência de tropas americanas na Somália.

---

[158] RICHBURG. Keith. **Somalia Battle Killed 12 Americans, Wounded 78**. Disponível em: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700747.html. Acessado em 05/02/2013.

[159] Tradução livre. No original: The Pentagon initially reported five American soldiers were killed, but the toll was actually 18 American soldiers dead and 73 wounded. Two days later, a 19th soldier, Delta operator SFC Matt Rierson, was killed in a mortar attack. Among U.N. forces, one Malaysian and one Pakistani died; seven Malaysians and two Pakistanis were wounded.

[160] Algumas fotos, vencedoras do Pulitzer de 1994, podem ser vistas em <http://iconicphotos.wordpress.com/2010/03/10/u-s-marine-dragged-through-mogadishu/>. Acessado em 23/04/2014.

> As forças dos EUA se retiraram, e Aideed, essencialmente, venceu a guerra da informação.[161|162]

Diante disso, o então presidente Bill Clinton determinou, em 6 de outubro de 1993, que todos os movimentos contra Aidid cessassem, e em 24 de abril de 1994, Boutros-Ghali admitiu a derrota e declarou o término da missão das Nações Unidas.[163]

Esse episódio serviu para demonstrar que a guerra de informações pode se desenvolver mesmo sem qualquer aparato tecnológico, e nem sempre a nação com mais recursos prevalece, já que um senhor da guerra somaliano venceu o poderoso exército estadunidense utilizando a própria mídia de massa americana como instrumento de guerra de informação.

Por causa daqueles poucos corpos mutilados sendo mostrados na CNN, a Somália virou um paraíso para extremistas e terroristas, além de ter proporcionado, mediante caos social, o retorno dos piratas marítimos.

5.3 Conexão Holanda

Em 2008, foi desencadeada uma operação da Polícia Federal brasileira em conjunto com a polícia holandesa e o FBI, que culminou com a prisão do brasileiro Leni de Abreu Neto e do holandês Nordin Nasiri.

A prisão, em território holandês, aconteceu no momento em que os dois homens realizavam a seguinte transação dentro do aeroporto de Amsterdã: o holandês entregava um CD contendo o

---

[161] LIBICKI, Martin. "**What is Information Warfare?",** artigo para o Institute for National Strategic Studies. Disponível em <http://212.150.54.123/inter_ter/noncon/infowar.htm> Acessado em 02/03/2013.

[162] Tradução livre. No original: Photos of jeering Somalis dragging corpses of U.S. soldiers through the streets of Mogadishu transmitted by CNN to the United States ended by souring TV audiences at home in the U.S. on staying in Somalia. U.S. forces left, and Aideed, in essence, won the information war.

[163] RUTHERFORD, Ken. **Humanitarianism under fire: the US and UN intervention in Somalia**. Sterling:Kumarian Press. 2008. p. 167–168.

código fonte do programa “Shadow”, em troca de uma mala contendo 25 mil Euros.[164]

5.3.1 Shadow

Trata-se de um “botnet”, ou seja, um programa automático de controle que, uma vez que consegue infectar um computador, passa a controlá-lo, de forma que o operador remoto adquire privilégio de administrador e pode, sem que o dono do PC infectado sequer perceba, atuar como um “computador zumbi”.

No caso do Shadow, o computador infectado passa e enviar milhares de e-mails por dia, em geral contendo *spam*, ou seja, propagandas, motivo pelo qual os serviços desses *spammers* são contratados por empresas de marketing em países onde não exista punição para a conduta como, por exemplo, o Brasil.[165]

5.3.2 Conspiração

As autoridades do estado americano de Louisiana, diante das provas geradas pela investigação do FBI acabaram indiciando o brasileiro por *conspiracy*[166] e pedindo inclusive a extradição do brasileiro.

Em caso de condenação pela justiça americana, Leni de Abreu Neto estará potencialmente sujeito a uma pena privativa de liberdade de até cinco anos e pode ter que pagar multa de pelo menos 250 mil dólares ou o equivalente ao prejuízo das vítimas ou o lucro que ele tenha obtido.[167]

---

[164] SALVADORI, Fausto. **A queda do Rei do spam** . Disponível em: http://revistagalileu.globo.com/Revista/Galileu/0,,EDR86914-7943,00.html>. Acesso em 02/02/2013.

[165] MILAGRE, José Antônio. **A criminalização do Spam no Brasil. O que muda no marketing?** Disponível em: < http://www.ecommercebrasil.com.br/eblog/2013/10/03/criminalizacao-spam-brasil-muda-marketing/> Acessado em 23/04/2014.

[166] Crime previsto na legislação americana, similar, porém diferente da associação criminosa, pois não exige que se associem três ou mais pessoas, bastando que se associem duas ou mais pessoas.

[167] STAFF, Department of Justice. **Brazilian Man Charged in Conspiracy to Infect More Than 100,000 Computers Worldwide with Malicious Software**. Disponível em: <http://www.justice.gov/opa/pr/2008/August/08-crm-739.html> Acessado em 03/03/2013.

Ressalte-se que se trata de um brasileiro que foi preso na Holanda, mas a lei a ser aplicada ao caso será a americana, diante do vácuo da legislação internacional sobre o assunto.

5.4 Drones

Diante da crise financeira de 2008, que ainda assola a economia de diversos países, o orçamento militar dos EUA foi atingido com reduções drásticas[168]. Isso acontece porque o estímulo à economia demanda recursos que seriam gastos militares.

Contudo algumas áreas do orçamento de defesa não foram atingidas, e uma dessas áreas são os gastos em pesquisa e desenvolvimento de *drones* e guerra de informações[169].

5.4.1 Ascenção das máquinas

O avanço na aviação no último século foi tão rápido que só se passaram 63 anos entre o célebre vôo de Santos Dummont em seu famoso 14-Bis, em 1906 até 1969, data em que o homem pousou na Lua.

A necessidade militar sempre foi o principal elemento que levou ao desenvolvimento de aeronaves cada vez mais velozes e eficientes, porém tudo indica que neste século, os aviões serão diferentes em um aspecto elementar.

O Lockheed Martin F-35 Joint Strike Fighter, mais moderno e recente avião de guerra americano, é uma aeronave cara, com o custo unitário de mais de 150 milhões de dólares[170].

---

[168] AMADEO, Kimberly. **Current U.S. Military Budget: How Defense Spending Affects the Economy .** Disponível em: <http://useconomy.about.com/od/usfederalbudget/p/military_budget.htm> Acessado em 10/03/2013.

[169] ALEXANDER, David. **New U.S. military strategy focuses on cyberwarfare, unmanned drones**. Disponível em: <http://news.nationalpost.com/2012/01/06/new-u-s-military-strategy-focuses-on-cyberwarfare-unmanned-drones/> Acessado em 13/02/2013.

[170] THE ECONOMIST, Redação. **The last manned fighter**. Disponível em: <http://www.economist.com/node/18958487> Acessado em 15/03/2013.

Não são muitos os alvos inimigos que se pode destruir em uma guerra que custem muito mais do que isso. Deste modo, faria pouco sentido mandar um avião de 150 milhões de dólares em uma missão para destruir um alvo que custe uma fração disso, caso o avião seja abatido. Além disso, existe o risco dos pilotos serem capturados.

Por esses motivos, o F-35 é tido como o último avião de caça tripulado da história da aviação militar americana. Tal noção existe na medida em que acredita-se que as próximas gerações de vetores sejam não tripuladas, e isso já começa a acontecer atualmente, ainda que de forma incipiente.

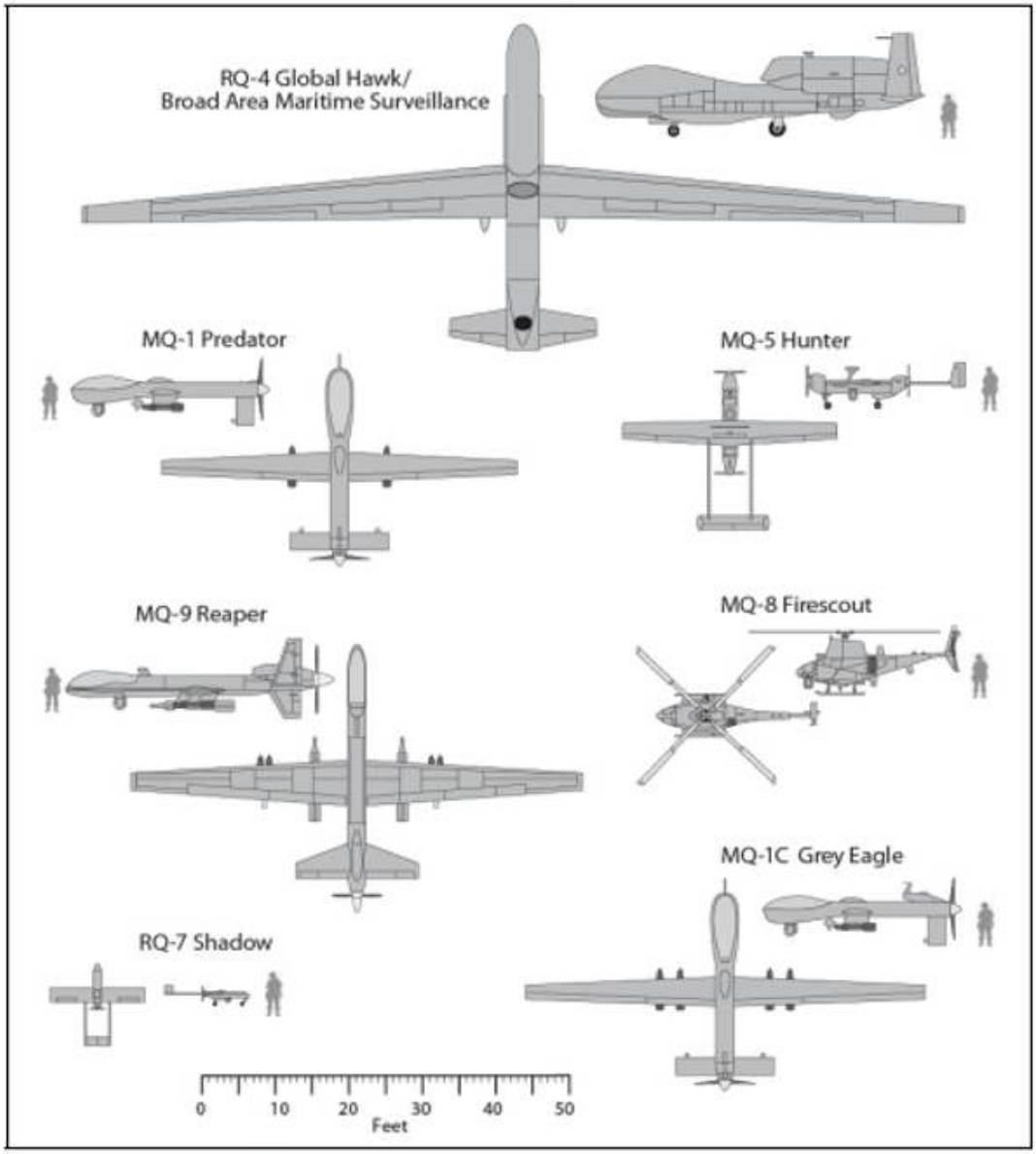
Estima-se que atualmente 31% das aeronaves da Força Aérea Americana sejam *drones*[171]. Esses aviões são mais leves e possuem maior autonomia do que aviões tripulados, e, caso sejam abatidos, ninguém morre – já que o piloto está em uma estação de comando e controle a milhares de distância do *drone* e do teatro de operações.

Esses são os drones mais utilizados atualmente:[172]|[173]

[171] ACKERMAN, Spender. **Almost 1 In 3 U.S. Warplanes Is a Robot**. Disponível em: < http://www.wired.com/dangerroom/2012/01/drone-report/> Acessado em 20/03/2013.

[172] SAENZ, Aaron. **THE ERA OF ROBOTIC WARFARE HAS ARRIVED – 30% OF ALL US MILITARY AIRCRAFT ARE DRONES** . Disponível em: <http://singularityhub.com/2012/02/09/the-era-of-robotic-warfare-has-arrived-30-of-all-us-military-aircraft-are-drones/> Acessado em 20/03/2013.

[173] Tradução da legenda do gráfico, indissociável do mesmo: "Fonte: Escritório Parlamentar de Orçamento. Opções de políticas para sistemas de vôo não tripulados. Publicação 40B3. Washington, DC, Junho de 2011. Observações: Todas as aeronaves são desenhadas na mesma escala. A silhueta da figura é o de um soldado com seis pés de altura, também desenhado na mesma escala.



Source: Congressional Budget Office, *Policy Options for Unmanned Aircraft Systems*, Publication 4083, Washington, DC, June 2011.

Notes: All aircraft are drawn to the same scale. The silhouette figure is a 6-foot-tall soldier, also drawn to scale.

As vantagens de se utilizar *drones* são muitas: custos menores, autonomia maior, risco de perda de vida inexistente. No entanto, existem algumas dificuldades na utilização desse tipo de vetor. Veja-se, a seguir.

5.4.2 Drones e guerra de informações

Quando *drones* são utilizados contra inimigos tecnologicamente inferiores, o resultado é excelente sob o ponto de vista militar e de custos. Essas aeronaves, comandadas remotamente por pilotos em alguma base americana, conseguem pilotar esses vetores, que atingem seus alvos seja no Afeganistão ou no Iraque.

Caso o *drone* seja abatido por uma bateria antiaérea, o prejuízo é pequeno e não existe perda de vida humana, ou a necessidade de complexas e caríssimas missões de resgate de tripulantes.

No entanto, quando o adversário possui um nível tecnológico mais avançado, esse cenário muda drasticamente. Como os *drones* são pilotados remotamente, ou seja, o piloto está nos Estados Unidos e o *drone* no Oriente Médio, por exemplo, a comunicação é feita via satélite entre os dois, e existe um atraso entre o momento em que o piloto dá o comando e o mesmo é executado pelo *drone*. Esse atraso varia com a distância, mas, no caso do Oriente Médico, é de pouco mais de um segundo.[174]

Enquanto esse atraso é imperceptível em missões de reconhecimento, e tolerável em missões de bombardeio, torna o *drone* indefeso contra aviões de combate que venham a interceptá-lo. Deste modo, ainda que os *drones* sejam difíceis de ser detectados por radar, tendo em vista suas formas não convencionais, o fato é que se for feito contato visual com uma aeronave tripulada, o *drone* será abatido sem qualquer dificuldade, pois um segundo é uma eternidade em um *dogfight*.

Além disso, quando se enfrenta oponentes tecnologicamente avançados, pode haver um ataque contra o satélite que transmite o sinal de comando aos *drones*, ou então o próprio sinal que os controla

[174] SHARKEY, Noel. **Say no to killer robots** . Revista The Engineer. 11 mar 2013. Disponível em: <http://www.theengineer.co.uk/military-and-defence/opinion/say-no-to-killer-robots/1015720.article> Acessado em 21/03/2013.

pode ser interceptado, decifrado e modificado, de forma que o inimigo passaria a ter controle sobre a esquadrilha de *drones*, os inutilizando ou, pior, os fazendo se voltar contra seus antigos mestres.[175]

Deste modo, os *drones* são muito úteis contra adversários com tecnologia rústica, porém praticamente inúteis contra inimigos tecnologicamente avançados.

5.4.3 Drones autônomos

Para evitar as desvantagens de não poder participar em combate aéreo devido ao atraso no recebimento dos sinais (*lag* ou *delay*) e o risco de ter o sinal interceptado e modificado, a próxima geração de *drones* provavelmente será totalmente autônoma.[176]

Os próximos *drones*, alguns dos quais já voam em fase experimental, serão capazes de decolar, navegar até o teatro de operações, identificar o inimigo, decidir se irá atacar, atacar, retornar para a base e pousar, tudo sem qualquer intervenção humana.

O *drone* "Tarantis", por exemplo, da Força Aérea Real Britânica, é um bombardeiro autônomo, capaz de fazer todas as ações acima, sem qualquer operador remoto. Somente no momento do ataque o *drone* solicita autorização à base, porém isso pode ser alterado com uma linha de programação. Além disso, a aeronave é invisível para radares e possui capacidade para desempenhar diversos tipos de bombardeio, inclusive de natureza termo nuclear.[177]

---

[175] UAV DRONE, Redação. **UAV DRONE UNMANNED AERIAL VEHICLE**. Disponível em: < http://uav-drone.net/anti-drone-uav.htm#.U1gtA6L7nvY>. Acesso em 23/04/2014.

[176] VERKAIK, Robert. **Set for take-off: Britain's deadly superdrone that picks its own targets but experts warn plane could mark the start of 'robot wars'**. Disponível em: <http://www.dailymail.co.uk/news/article-2268909/Taranis-Britains-deadly-superdrone-picks-targets.html> Acessado em 24/03/2013.

[177] GRAY, Richard. **British stealth drone to undergo first test flight** . Disponível em: <http://www.telegraph.co.uk/news/uknews/defence/9797738/British-stealth-drone-to-undergo-first-test-flight.html> Acessado em 25/03/2013.

5.4.4 Aspectos éticos

Quando o tomador de decisões não é um ser humano, porém um computador, e a decisão a ser tomada é a de exterminar ou não vidas humanas, algumas questões éticas são levantadas.

Há quem diga que um robô pode ser mais ético no campo de batalha do que os seres humanos[178], pois não possui emoções, tais como a necessidade de vingança.

Existe ponto de vista no sentido de estabelecer-se regras e código de condutas para os equipamentos militares autônomos, de forma a fazer com que esses *drones* respeitem as normas do direito internacional:

> (…)"Governador ético", um nome inspirado pelo governador mecânico para o motor a vapor, que garantiu que os motores potentes comportado de forma segura e dentro dos limites pré-definidos de desempenho. Da mesma forma, um governador ético seria garantir que o comportamento do robô iria ficar dentro de limites pré-definidos éticas. Por exemplo, para os robôs militares autônomos, esses limites que incluem princípios decorrentes das Convenções de Genebra e outras regras de engajamento que os seres humanos usam. Robôs civis teriam diferentes conjuntos de limites específicos para os seus fins.[179|180]

Seguindo o raciocínio, as máquinas precisariam de emoções para modificar comportamentos lógicos que levariam ao extermínio:

> Uma das emoções mais importantes para os robôs têm que ser culpa, que um robô seria "sentir" ou produzir sempre que viola suas

---

[178] ARKIN, Ronald C. **The Case for Ethical Autonomy in Unmanned Systems**. Disponível em: <http://www.cc.gatech.edu/ai/robot-lab/online-publications/Arkin_ethical_autonomous_systems_final.pdf> Acessado em 23/04/2014.

[179] ZYGA, Lisa. **How to make ethical robots** . Revista PHYS ORG. 12 mar 2012.Disponível em: <http://phys.org/news/2012-03-ethical-robots.html> Acessado em 02/04/2013.

[180] Tradução livre. No original: “ethical governor,” a name inspired by the mechanical governor for the steam engine, which ensured that the powerful engines behaved safely and within predefined bounds of performance. Similarly, an ethical governor would ensure that robot behavior would stay within predefined ethical bounds. For example, for autonomous military robots, these bounds would include principles derived from the Geneva Conventions and other rules of engagement that humans use. Civilian robots would have different sets of bounds specific to their purposes.

> restrições éticas impostas pelo governador, ou quando criticado por um ser humano. Filósofos e psicólogos consideram a culpa como um motivador fundamental do comportamento moral, uma vez que leva a modificações de comportamento com base nas conseqüências das ações anteriores. Os pesquisadores aqui propor que, quando o valor a culpa de um robô ultrapassa determinados limites, as capacidades do robô podem ser temporariamente restritas.[181|182]

Em resumo, tal teoria impõe que a ética dos campos de batalha possa melhorar com o advento das máquinas de guerra autônomas:

> (…) se os robôs pudessem atuar como modelos em situações em que os seres humanos têm dificuldade em agir de acordo com os padrões morais, isso poderia reforçar positivamente o comportamento ético das pessoas, mas essa é uma hipótese não comprovada (…)[183|184]

No entanto, existem opiniões em sentido diametralmente oposto, determinando que o uso de máquinas de guerra retira o freio moral que é uma nação ter que mandar seus cidadãos para o combate, onde correm o risco de serem mortos:

> E agora nós possuímos uma tecnologia que remove as últimas barreiras políticas à guerra. O apelo mais forte de sistemas não-tripulados é que não temos de enviar o filho ou filha de alguém em perigo. Mas quando os políticos podem evitar as conseqüências políticas da carta de condolências – e o impacto que as baixas militares têm sobre os eleitores e os meios de comunicação – não

---

[181] Ibidem.

[182] Tradução livre. No original: One of the most important emotions for robots to have would be guilt, which a robot would "feel" or produce whenever it violates its ethical constraints imposed by the governor, or when criticized by a human. Philosophers and psychologists consider guilt as a critical motivator of moral behavior, as it leads to behavior modifications based on the consequences of previous actions. The researchers here propose that, when a robot's guilt value exceeds specified thresholds, the robot's abilities may be temporarily restricted.

[183] Ibidem.

[184] Tradução livre. No original: if robots could act as role models in situations where humans have difficulty acting in accord with moral standards, this could positively reinforce ethical behavior in people, but that's an unproven hypothesis.

> vão mais tratar os assuntos previamente pesados de guerra e paz da mesma forma. [185][186]

Como não haveria risco algum na guerra, a mesma seria cada vez mais comum:

> Durante os primeiros 200 anos da democracia americana, engajar-se em combate e sofrer risco - pessoal e político – andaram de mãos dadas. Na era dos *drones*, não é mais o caso.[187][188]

Além disso, no sistema americano, alega o autor, o presidente da república necessita de autorização para mandar tropas agirem. Isso não acontece com os *drones*, motivo pelo qual o presidente americano ordena milhares de missões de todo tipo sem sequer dar conhecimento ao Congresso:

> O Congresso não desapareceu de todas as decisões sobre a guerra, apenas das que importam. Na mesma semana em que drones americanos estavam realizando o seu ataque aéreo não autorizado 145 na Líbia, o presidente notificou o Congresso que ele havia implantado 100 tropas de operações especiais para uma parte diferente da África.
>
> Devemos agora aceitar que as tecnologias que removem os seres humanos a partir do campo de batalha, a partir de sistemas não-tripulados como o Predator para armas cibernéticas, como o worm de computador Stuxnet, estão se tornando o novo padrão na guerra.
>
> E, goste ou não, o novo padrão que nós estabelecemos para eles é que os presidentes precisam buscar a aprovação somente para

---

[185] SINGER, Peter W. **Do Drones Undermine Democracy?** Jornal NY Times. Disponível em: <http://www.nytimes.com/2012/01/22/opinion/sunday/do-drones-undermine-democracy.html?pagewanted=all> Acessado em 05/04/2013.

[186] Tradução livre. No original: And now we possess a technology that removes the last political barriers to war. The strongest appeal of unmanned systems is that we don't have to send someone's son or daughter into harm's way. But when politicians can avoid the political consequences of the condolence letter — and the impact that military casualties have on voters and on the news media — they no longer treat the previously weighty matters of war and peace the same way.

[187] Ibidem.

[188] Tradução livre. No original: For the first 200 years of American democracy, engaging in combat and bearing risk — both personal and political — went hand in hand. In the age of drones, that is no longer the case.

> operações que enviam as pessoas para o perigo - não para aqueles que envolvem travando uma guerra por outros meios.[189|190]

O fato é que os ataques com *drones* não custam sangue americano, e, por isso, são vistos com simpatia por grande parte da opinião pública americana.

5.4.5 O direito de ser morto por seres humanos

Diante desse quadro de crescente mecanização e automatização dos sistemas informatizados de combate, um tema que poderá ser debatido no futuro é o suposto direito de ser morto por seres humanos, e não por máquinas autônomas – ou seja, o direito de ser morto por uma decisão humana e não por um algoritmo computadorizado:[191]

> Alguém poderia argumentar que, se o resultado for superior a decisão humana, e daí? Alternativamente, pode-se sugerir que atribuir a responsabilidade final para o "governador ético" ainda a deixa com seus proprietários. Aqui eu sugiro que seja a resposta não seria suficiente para captar a importância do julgamento ético. Resultados importam eticamente, fundamentalmente porque se referem ao conceito de responsabilidade. Isso só se torna possível com o julgamento. Além disso, os engenheiros de um "governador ético" presumivelmente têm alguma responsabilidade, mas para o que exatamente? Será que eles não apenas fornecem os algoritmos para a ação, ao invés de julgar as circunstâncias relevantes? Literalmente, neste deslocamento menor, o adversário tornou-se um ponto de dados, ao invés de um assunto 'digno' de julgamento. Sua morte seriam as consequências de uma consulta algorítmica

---

[189] Ibidem.

[190] Tradução livre. No original: We must now accept that technologies that remove humans from the battlefield, from unmanned systems like the Predator to cyberweapons like the Stuxnet computer worm, are becoming the new normal in war.
And like it or not, the new standard we've established for them is that presidents need to seek approval only for operations that send people into harm's way — not for those that involve waging war by other means.

[191] How the advent of autonomous drones will affect our conception of ethics by Rutger Kaput on March 29, 2013 in Law, Political Theory, Terrorism and Security. <http://politicsinspires.org/how-the-advent-of-autonomous-drones-will-affect-our-conception-of-ethics>. Acessado em 05/04/2013.

> produzindo um determinado resultado, ao invés de julgamento, independentemente de quão terrível. [192]

Tal direito subjetivo faz sentido na medida em que seres humanos, ao contrário de máquinas, podem ser responsabilizados por suas condutas.

Com efeito, o papel dos *drones* aumenta rapidamente no cenário militar, e, se 10 anos atrás falar de um robô autônomo realizando decisões de vida ou morte no campo de batalha era algo absolutamente limitado a filmes de ficção científica, essa é uma realidade cada vez mais perturbadora, situada no contexto da guerra virtual e de informações.

Esse assunto deve ser objeto de estudo do direito internacional, principalmente na medida em que países não alinhados e grupos terroristas tenham acesso a tais sistemas, o que é inevitável conforme os custos de desenvolvimento baixem e os programas se popularizem.

---

[192] Tradução livre. No original: One might argue that if the outcome is superior to human decision, why bother? Alternatively one might suggest that the ultimate responsibility for the 'ethical governor' still relies with its owners. Here I suggest that either response would fail to capture the importance of judgment for ethics. Outcomes matter ethically, fundamentally so because they refer to the concept of responsibility. This only becomes possible with judgment. Moreover, the engineers of an 'ethical governor' would presumably bear some responsibility; but for what exactly? Would they not merely provide the algorithmic possibilities for action, rather than pass actual judgment in the relevant circumstances? Quite literally, in this minor shift, the adversary has become a data point, rather than a subject 'worthy' of judgment. His death would be the consequences of an algorithmic query yielding a particular result, rather than of judgment, regardless how terrible.

6 Conclusão

Foi feita a análise teórica do assunto terrorismo de maneira genérica e também o estudo específico da guerra de informações e do terrorismo virtual.

Também foram analisados os tratados internacionais existentes que versam sobre o tema terrorismo, ainda que nada falem sobre terrorismo virtual ou guerra de informações. A análise de tais diplomas foi feita de modo a fazer alguma ligação entre eles e o assunto ora estudado.

Depois disso, foram analisados os casos de atos envolvendo o uso de guerra de informações para a prática de atos que podem ser considerados terroristas.

Diante disso, percebe-se claramente que, mesmo tendo sido aprimorado após 2001, o ordenamento jurídico internacional existente é absolutamente insuficiente para disciplinar os atos praticados mediante o emprego de tais instrumentos.

Não existe um tratado sequer que verse sobre o tema específico da guerra de informações, e os ataques são praticados livremente pelos vários atores. Quando um *hacker* isolado ou um país não alinhado pratica um ataque, trata-se de terrorismo virtual; quando a Força Aérea dos Estados Unidos da América pratica um ataque, trata-se de defesa nacional, existindo até manuais para disciplinar as várias estratégias possíveis.

Neste assunto a sociedade internacional encontra-se, salvo melhor juízo, em estado anárquico.

Conforme se “popularizem” os ataques virtuais, tecnológicos, ou de informações, seja por meio da maior utilização de *worms* ou *drones*, a necessidade de maior regulamentação internacional se tornará cada vez mais evidente.

Atualmente, conforme verificado nos exemplos já expostos, o cenário é de grande sofisticação dos métodos de ataques virtuais ou de informações e, exceto pelo senhor da guerra somaliano, que usou a imprensa estadunidense contra seu próprio país, ou métodos empregados são caríssimos: ataques informatizados empregando pessoal altamente especializado ou caríssimos *drones*.

Deste modo, como as grandes potências são os atuais perpetradores dos atos de terrorismo virtual e guerra de informações, é bastante provável que tais atos permaneçam impunes e não regulados pelo direito internacional até quando se "popularizem" o suficiente para serem praticados por grupos "terroristas", indivíduos ou forças armadas tecnologicamente primitivas contra tais potências.

Quando esse momento chegar, é provável que os órgãos internacionais criem tratados capazes de criminalizar tais condutas, estabelecendo regras claras para apuração e julgamento dos atos de terrorismo virtual praticados mediante guerra de informações.

7 Referências bibliográficas

ACKERMAN, Spender. **Almost 1 In 3 U.S. Warplanes Is a Robot**. Disponível em: < http://www.wired.com/dangerroom/2012/01/drone-report/> Acessado em 20/03/2013.

AHARONI, Zvi e DIETL, Wilhelm. **Operation Eichmann: The Truth About the Pursuit, Capture and Trial**. London: Arms and Armour. 1997.

AHMED, Abdul. **Brothers in Arms Part I .** Disponível em: <http://wardheernews.com/Articles_2011/Oct/29_Brothers_in_Army_abdul.pdf> Acessado em 02/02/2013.

ALEXANDER, David. **New U.S. military strategy focuses on cyberwarfare, unmanned drones**. Disponível em: <http://news.nationalpost.com/2012/01/06/new-u-s-military-strategy-focuses-on-cyberwarfare-unmanned-drones/> Acessado em 13/02/2013.

AMADEO, Kimberly. **Current U.S. Military Budget: How Defense Spending Affects the Economy .** Disponível em: <http://useconomy.about.com/od/usfederalbudget/p/military_budget.htm> Acessado em 10/03/2013.

ARKIN, Ronald C. **The Case for Ethical Autonomy in Unmanned Systems**. Disponível em: <http://www.cc.gatech.edu/ai/robot-lab/online-publications/Arkin_ethical_autonomous_systems_final.pdf> Acessado em 23/04/2014.

AYLETT, Glenn. **Hitler´s Radio**. Disponível em: <http://www.transdiffusion.org/radio/features/hitlers_radio> . Acessado em 20/12/2012.

AZEVEDO, Gilvavi Rodrigues. **Terrorismo e movimentos sociais na América Latina: Sendero Luminoso e Movimento dos Trabalhadores Sem Terra (MST).** Univ. Hum., Brasília, v. 6, n. 2, jul./dez. 2009. p. 63.

BAUER, Caroline Silveira. **Avenida João Pessoa, 2050 - 3o. andar** : **Terrorismo de Estado e ação de polícia política do Departamento de Ordem Política e Social do Rio Grande do Sul (1964-1982)**. Dissertação apresentada à UFRGS, 2006.

BBC, Redação. **China 'blocks Google news site'**. Disponível em: http://news.bbc.co.uk/2/hi/technology/4056255.stm. Acesso em 7/04/2013.

BBC, Redação. **Osama Bin Laden, al-Qaeda leader, dead – Barack Obama**. Revista BBC News. May 2, 2011. Disponível em: <http://www.bbc.co.uk/news/world-us-canada-13256676> Acessado em 13 de junho de 2013

BERKOWITZ, Bruce D. **War logs on.** Foreign Affairs. 2000. Disponível em < http://www.foreignaffairs.com/articles/56039/bruce-d-berkowitz/war-logs-on-girding-america-for-computer-combat>. Acessado em 24/04/2014.

BOBBIO, Norberto. **Dicionário de Política**. Vol. 2. 5ª ed. Brasília: Ed. Universidade de Brasília.

BOCKSTETTE, Carsten. **Jihadist Terrorist Use of Strategic Communication Management Techniques.** No. 20 December 2008 ISSN 1863-6039. P. 8. Disponível em

http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/occPapers/occ-paper_20 en.pdf. Acessado em 10/05/2013.

BOMFIM, Ana Paula Rocha do. **Terrorismo: O Tênue limite do enquadramento enquanto direito de resistência.** 2007. Dissertação (Mestrado em Direito) Centro Universitário de Brasília.

BOURDIEU, Pierre. O Poder Simbólico. Tradução de Fernando Tomaz. Ed. Bertrand: Rio de Janeiro. 1998.

BROPHY, P. e outros. Extremism and the Internet. London: The British Library. British Library Research & Innovation Report. 1999.

BRASIL. **Constituição da República Federativa do Brasil**. Diário Oficial da União, Poder Legislativo, Brasília, DF, 05 jan. 1988.

BRASIL. **Lei n.º 7.170**. Diário Oficial da União, Brasília, DF, 12 dez. 1983.

BRASIL. **Decreto n.º 3.018,** de 6 de abril de 1999. Diário Oficial da União - Seção 1 - 7/4/1999, Página 3.

BRASIL. **Decreto n.º 2.611,** de 2 de junho de 1998, publicado no Diário Oficial da União em 03/06/1998.

BRASIL. **Decreto n.º 3.517**, de 20 de junho de 2000. Publicado no Diário Oficial da União em 21/06/2000.

BRASIL. **Decreto n.º 678**, de 6 de novembro de 1992, publicado no Diário Oficial da União em 9 de novembro de 1992.

BRASIL. **Decreto n.º 6.136**, de 26 de junho de 2007. Publicado no Diário Oficial da União em 27/06/2007.

BRASIL. **Decreto n.º 4.021**, de 19 de novembro de 2001. Publicado no Diário Oficial da União em 20/11/2001.

BRASIL. **Decreto n.º 3.229**, de 29 de outubro de 1999. Publicado no Diário Oficial da União em 03/11/1999.

BRASIL. **Decreto n.º 4.394,** de 26 de setembro de 2002. Publicado no Diário Oficial da União em 27.9.2002.

BRASIL. **Decreto n.º 5.640**, de 26 de dezembro de 2005. Publicado no Diário Oficial da União em 27/12/2005.

BRASIL. **Decreto n.º 5.639**, de 26 de dezembro de 2005. Publicado no Diário Oficial da União em 27/12/2005.

CAMPEN, A.D., Dearth, D.H. & Goodden, R.T. **Cyberwar: Security, Strategy and Conflict in the Information Age**. Fairfax, VA: AFCEA International Press. 1996.

CAMPEN, Alan D. **The first information war: The story of communications, computers, and intelligence systems in the Persian Gulf War.** Fairfax, VA: AFCEA International Press, 1992.

CARR, Caleb. **A assustadora história do terrorismo**. São Paulo: Ediouro Publicações S/A. 2002.

CHILE. Lei n.º 18.314. Ministerio del Interior. Publicada em 17/05/1984. Disponível em: http://www.leychile.cl/N?i=29731&f=2011-06-21&p=

CODDING. George A. **The International Telecommunication Union**. Leiden, The Netherlands: E. J. Brill. 1952.

ESTADOS UNIDOS DA AMÉRICA. PUBLIC LAW 107–56—OCT. 26, 2001. WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 37. 2001.

GLADSTONE, Rick. **Nuclear Program Talks Could Resume, Iranian Official Says.** New York Times, Edição on-line. Disponível em: <http://www.nytimes.com/2013/07/18/world/middleeast/nuclear-program-talks-could-resume-iranian-official-says.html?ref=nuclearprogram&_r=0>. Acessado em 22/05/2013.

GODOY, Arnaldo Sampaio de Moraes. **Direito e História: uma relação equivocada.** Londrina:Humanidades. 2003.

GODOY, Arnaldo Sampaio de Moraes. **O esperanto jurídico, a utopia da língua normativa universal perfeita e o relativismo do direito.** Rio de Janeiro:Direito, Estado e Sociedade, n.º 41. Jul/dez 2012..

GOLDMAN, David. **Super-virus Flame raises the cyberwar stakes**. Disponível em: <http://money.cnn.com/2012/05/30/technology/flame-virus/index.htm>. Acesado em 05/01/2013.

GRAY, Richard. **British stealth drone to undergo first test flight** . Disponível em: <http://www.telegraph.co.uk/news/uknews/defence/9797738/British-stealth-drone-to-undergo-first-test-flight.html> Acessado em 25/03/2013.

HANDEL, M.I. Intelligence and the problem of strategic surprise. In: Dearth, D.H. & Goodden, R.T. (eds.). Strategic Intelligence: Theory and Application. 2nd. ed. Washington, DC: US Army War College/ Defense Intelligence Agency, 1995.

HERMAN, M. **Where hath our intelligence been? The Revolution in Military Affairs**. RUSI Journal. 1998. Disponível em < http://www.tandfonline.com/doi/abs/10.1080/03071849808446332?journalCode=rusi20#preview> Acessado em 24/04/2014.

KANT, Immanuel. **A Paz Perpétua. Um Projecto Filosófico**. Universidade da Beira Interior, Covilhã, 2008.

KASSIM, Saleem. Twitter Revolution: **How the Arab Spring Was Helped By Social Media**. Disponível em: <http://www.policymic.com/articles/10642/twitter-revolution-how-the-arab-spring-was-helped-by-social-media>. Acessado em 23/04/2014.

LIBICKI, Martin. "**What is Information Warfare?",** artigo para o Institute for National Strategic Studies. Disponível em <http://212.150.54.123/inter_ter/noncon/infowar.htm> Acessado em 02/03/2013.

LONGERICH, Peter. Heinrich Himmler: A Life. Oxford:Oxford University Press. 2013.

LOUW, E. **The media and the political process.** London: SAGE Publications, 2005.

MACLEAN, William. **"UPDATE 2-Cyber attack appears to target Iran-tech firms"**. Reuters, 24 set 2010. Disponível em < http://www.reuters.com/article/2010/09/24/security-cyber-iran-idUSLDE68N1OI20100924> Acessado em 20/12/2013.

McMILLAN, Robert . "**Siemens: Stuxnet worm hit industrial systems". Revista Computerworld.** 16 Set 2010. Disponível em < http://www.computerworld.com/s/article/9185419/Siemens_Stuxnet_worm_hit_industrial_systems> Acessado em 23/10/2013.

MICHAELS, Sean. **US forces fight Taliban with heavy metal** . Disponível em : <http://www.guardian.co.uk/music/2010/apr/07/us-forces-fight-taliban-metal>. Acessado em 02/03/2013.

MILAGRE, José Antônio. **A criminalização do Spam no Brasil. O que muda no marketing?** Disponível em: < http://www.ecommercebrasil.com.br/eblog/2013/10/03/criminalizacao-spam-brasil-muda-marketing/> Acessado em 23/04/2014.

MONTESQUIEU, Charles Louis Secondat, Barón de. **O Espírito das leis**. Tradução de Fernando Henrique Cardoso e Leôncio Martins Rodrigues. 2. ed. São Paulo: Abril Cultural, 1979.

NAISBITT, John. **Megatrends**. New York: Warner Books, Inc. 1982.

NORDENSTRENG, Kaarle e outros. **National Sovereignty and International Communication**. New Jersey: Ablex Publishing Co. 1979.

PANIAGO, Paulo de Tarso Resende e outros. **Uma cartilha para melhor entender o terrorismo internacional**. REVISTA BRASILEIRA DE INTELIGÊNCIA. Brasília: Abin, v. 3, n. 4, set. 2007.

PIERRE, Héctor Luís Saint. **As relações civis - militares no Brasil depois dos atentados de 11 de setembro.** Disponível em: http://www.resdal.org/Archivo/d000019b.htm. Acesso em: 19/01/2013.

PINHEIRO. Álvaro de Souza. **NARCOTERRORISMO - O Flagelo do Século XXI**. Disponível em < http://www.defesanet.com.br/terror/noticia/972/NARCOTERRORISMO---O-Flagelo-do-Seculo-XXI-%C2%A9/>. Acessado em 23/04/2014.

PRESSTV, Redação. IAEA admits Iran nuclear energy program peaceful .Disponível em: <http://www.presstv.ir/detail/2013/03/13/293451/iran-nuclear-activities-peaceful-amano/>. Acessado em 03/03/2013.

R.D. Thrasher, **Information Warfare Delphi: Raw Results**. Disponível em: http:/all.net/books/iw/delphi/top.html. Acessado em: 05/12/2012.

RATHMELL, A. e outros. **The IW threat from sub-state groups: an interdisciplinary approach**. Paper presented at the Third International Symposium, on Command and Control Research and Technology. Institute for National Strategic Studies-National Defense University. 1997.

REZEK, Francisco. **Direito Internacional**: 12.ed. São Paulo: Saraiva, 2010.

REZEK, José Francisco. **Direito Internacional Público – curso elementar**. 10. ed. rev. e atual. São Paulo: Saraiva, 2005.

RICHBURG. Keith. **Somalia Battle Killed 12 Americans, Wounded 78**. Disponível em: http://www.washingtonpost.com/wp-dyn/content/article/2006/08/07/AR2006080700747.html. Acessado em 05/02/2013.

ROZOIR, Charles du. Compêndio de História Romana. Rio de Janeiro:Typ. Imp. e Const. de J. Villeneuve e Comp. 1840.

RUTHERFORD, Ken. **Humanitarianism under fire: the US and UN intervention in Somalia**. Sterling:Kumarian Press. 2008.

SAENZ, Aaron. **THE ERA OF ROBOTIC WARFARE HAS ARRIVED – 30% OF ALL US MILITARY AIRCRAFT ARE DRONES** . Disponível em: <http://singularityhub.com/2012/02/09/the-era-of-robotic-warfare-has-arrived-30-of-all-us-military-aircraft-are-drones/> Acessado em 20/03/2013.

SALVADORI, Fausto. **A queda do Rei do spam** . Disponível em: http://revistagalileu.globo.com/Revista/Galileu/0,,EDR86914-7943,00.html>. Acesso em 02/02/2013.

SCHMULOVICH, Michal. **Iran 'Thunderstruck' by AC/DC computer virus**. Disponível em: http://www.timesofisrael.com/iranian-nuclear-plants-thunderstruck-by-acdc-playing-virus/> Acessado em 09/02/2013.

SCHULTZ, Sabrina. **Operação Condor e Terrorismo de Estado: passado, presente e futuro**. Debat: Rev., ISSNe 1980-3532, Florianópolis, Santa Catarina, Brasil. 2006.

SCHWARTAU, W., Information Warfare. Cyberterrorism: Protecting your Personal Security in the Information Age. New York: Thunder's Mouth Press. 2ª ed., 1996

SHARKEY, Noel. **Say no to killer robots** . Revista The Engineer. 11 mar 2013. Disponível em: <http://www.theengineer.co.uk/military-and-defence/opinion/say-no-to-killer-robots/1015720.article> Acessado em 21/03/2013.

SILVA, Roberto Luiz. **Direito Internacional Público**. Belo Horizonte: Del Rey, 2002.

SINGER, Peter W. **Do Drones Undermine Democracy?** Jornal NY Times. Disponível em: <http://www.nytimes.com/2012/01/22/opinion/sunday/do-drones-undermine-democracy.html?pagewanted=all> Acessado em 05/04/2013.

STAFF, Chiefs of. Joint Doctrine for Information Operations. Washington: Joint Doctrine Publication. 1998.

STAFF, Department of Justice. **Brazilian Man Charged in Conspiracy to Infect More Than 100,000 Computers Worldwide with Malicious Software**. Disponível em: <http://www.justice.gov/opa/pr/2008/August/08-crm-739.html> Acessado em 03/03/2013

STAFF, USAF. USAF Manual for Information Operations. Washington:USAF. 2005.

STREET, John. Mass media, politics and democracy. Houndmills: Palgrave Macmillan. 2001.

SUNSTEIN. Cass R. **Worst-Case Scenarios**. Cambridge:Harvard University Press. 2007.

SZAFRANSKI, R. (1994). **Neo-cortical warfare: the acme of skill?** Fort Leavenworth:Military Review. 1994.

THE ECONOMIST, Redação. **The last manned fighter**. Disponível em: <http://www.economist.com/node/18958487> Acessado em 15/03/2013.

THE FREE LIBRARY, Redação. **Official Calls Iran Main Victim of Cyber Terrorism**. Disponível em: <http://www.thefreelibrary.com/Official+Calls+Iran+Main+Victim+of+Cyber+Terrorism.-a0305291573 > Acessado em 02/02/2013

THE TELEGRAPH, Redação. **Flame virus 'created by US and Israel as part of intensifying cyber warfare'**. Disponível em: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9343141/Flame-virus-created-by-US-and-Israel-as-part-of-intensifying-cyber-warfare.html>. Acessado em 07/01/2013

THRASHER, R.D., **Information Warfare Delphi: Raw Results**. 1996. Disponível em: http:/all.net/books/iw/delphi/top.html. Acessado em: 05/12/2012.

TZU, Sun**. A arte da guerra.** Adaptação e prefácio de James Clavell; Tradução de José Sanz. 19ª ed. Rio de Janeiro: Record, 1997.

UAV DRONE, Redação. UAV DRONE UNMANNED AERIAL VEHICLE. Disponível em: < http://uav-drone.net/anti-drone-uav.htm#.U1gtA6L7nvY>. Acesso em 23/04/2014.

UNITED STATES HOLOCAUST MEMORIAL MUSEUM. **Concentration camps**. Disponível em: http://www.ushmm.org/wlc/en/article.php?ModuleId=10005263 Acesso em 23/04/2014.

VERKAIK, Robert. **Set for take-off: Britain's deadly superdrone that picks its own targets but experts warn plane could mark the start of 'robot wars'**. Disponível em: <http://www.dailymail.co.uk/news/article-2268909/Taranis-Britains-deadly-superdrone-picks-targets.html> Acessado em 24/03/2013.

VIEIRA, Oscar Vilhena. **DIREITOS HUMANOS. Estado de Direito e a construção da paz**. São Paulo: Quartier Latin, 2005.

WIKIPEDIA. Frente Sandinista de Libertação Nacional. Disponível em http://pt.wikipedia.org/wiki/Frente_Sandinista_de_Liberta%C3%A7%C3%A3o_Nacional>. Acessado em 23/04/2014.

WORSTALL, Tim. **Stuxnet Was a Joint US/ Israeli Project** Disponível em: <http://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/>. Acessado em 05/01/2013.

ZETTER, Kim. Google Hack Attack Was Ultra Sophisticated, New Details Show. Disponível em <http://www.wired.com/2010/01/operation-aurora/>. Acesso em 23/04/2014.

ZYGA, Lisa. **How to make ethical robots** . Revista PHYS ORG. 12 mar 2012.Disponível em: <http://phys.org/news/2012-03-ethical-robots.html> Acessado em 02/04/2013.