Alexandre Peres Teixeira

PODER, TECNOLOGIA E DIREITO!

A Força Cibernética e a disrupção nos principais paradigmas de sustentação do Direito aplicado aos Conflitos Armados



DIALÉTICA
EDITORA

MIOLO_Poder, Tecnologia e Direito - 2_1 02/12/2024 02:21:44

PODER, TECNOLOGIA E DIREITO!

A Força Cibernética e a disrupção nos principais paradigmas de sustentação do Direito aplicado aos Conflitos Armados

MIOLO_Poder, Tecnologia e Direito - 2.indd 1 26/04/2024 11:12:02

CONSELHO EDITORIAL



Alexandre G. M. F. de Moraes Bahia
André Luís Vieira Elói
Antonino Manuel de Almeida Pereira
António Miguel Simões Caceiro
Bruno Camilloto Arantes
Bruno de Almeida Oliveira
Bruno Valverde Chahaira
Catarina Raposo Dias Carneiro
Christiane Costa Assis
Cíntia Borges Ferreira Leal
Claudia Lambach
Cristiane Wosniak
Eduardo Siqueira Costa Neto
Elias Rocha Gonçalves
Evandro Marcelo dos Santos
Everaldo dos Santos Mendes
Fabiani Gai Frantz
Fabíola Paes de Almeida Tarapanoff
Fernando Andacht
Flávia Siqueira Cambraia
Frederico Menezes Breyner
Frederico Perini Muniz
Giuliano Carlo Rainatto
Gláucia Davino
Helena Maria Ferreira
Hernando Urrutia
Izabel Rigo Portocarrero
Jamil Alexandre Ayach Anache
Jean George Farias do Nascimento
Jorge Douglas Price
Jorge Manuel Neves Carrega
José Carlos Trinca Zanetti
Jose Luiz Quadros de Magalhaes
Josiel de Alencar Guedes
Juvencio Borges Silva
Konradin Metze
Laura Dutra de Abreu
Leonardo Avelar Guimarães
Lidiane Mauricio dos Reis
Ligia Barroso Fabri
Lívia Malacarne Pinheiro Rosalem
Luciana Molina Queiroz
Luiz Carlos de Souza Auricchio
Luiz Gustavo Vilela
Manuela Penafria
Marcelo Campos Galuppo
Marco Aurélio Nascimento Amado
Marcos André Moura Dias
Marcos Antonio Tedeschi
Marcos Pereira dos Santos
Marcos Vinício Chein Feres
Maria Walkiria de Faro C Guedes Cabral
Marilene Gomes Durães
Mateus de Moura Ferreira
Mauro Alejandro Baptista y Vedia Sarubbo
Milena de Cássia Rocha
Mirian Tavares
Mortimer N. S. Sellers
Nígela Rodrigues Carvalho
Paula Ferreira Franco
Pilar Coutinho
Rafael Alem Mello Ferreira
Rafael Vieira Figueiredo Sapucaia
Rayane Araújo
Regilson Maciel Borges
Régis Willyan da Silva Andrade
Renata Furtado de Barros
Renildo Rossi Junior
Rita de Cássia Padula Alves Vieira
Robson Jorge de Araújo
Rogério Luiz Nery da Silva
Romeu Paulo Martins Silva
Ronaldo de Oliveira Batista
Susana Costa
Sylvana Lima Teixeira
Vanessa Pelerigo
Vitor Amaral Medrado
Wagner de Jesus Pinto

Alexandre Peres Teixeira

PODER, TECNOLOGIA E DIREITO!

A Força Cibernética e a disrupção nos principais paradigmas de sustentação do Direito aplicado aos Conflitos Armados



DIALÉTICA
EDITORA

MIOLO_Poder, Tecnologia e Direito - 2.indd 3 26/04/2024 11:12:08

Todos os direitos reservados. Nenhuma parte desta edição pode ser utilizada ou reproduzida – em qualquer meio ou forma, seja mecânico ou eletrônico, fotocópia, gravação etc. – nem apropriada ou estocada em sistema de banco de dados, sem a expressa autorização da editora.

Copyright © 2024 by Editora Dialética Ltda.
Copyright © 2024 by Alexandre Peres Teixeira.

DIALÉTICA
EDITORA

/editoradialetica
@editoradialetica
www.editoradialetica.com

EQUIPE EDITORIAL

Editores
Profa. Dra. Milena de Cássia de Rocha
Prof. Dr. Rafael Alem Mello Ferreira
Prof. Dr. Tiago Aroeira
Prof. Dr. Vitor Amaral Medrado

Coordenadora Editorial
Kariny Martins

Produtora Editorial
Júlia Noffs

Controle de Qualidade
Maria Laura Rosa

Capa
Larissa Brito

Diagramação
Larissa Brito

Preparação de Texto
José Rômulo

Revisão
Responsabilidade do autor

Auxiliar de Bibliotecária
Laís Silva Cordeiro

Assistentes Editoriais
Rafael Andrade
Ludmila Azevedo Pena
Thaynara Rezende

Estagiários
Giovana Teixeira Pereira
Maria Cristiny Ruiz



Dados Internacionais de Catalogação na Publicação (CIP)

T266p Teixeira, Alexandre Peres.

Poder, Tecnologia e Direito! : "a força cibernética e a disrupção nos principais paradigmas de sustentação do direito aplicável aos conflitos armados" / Alexandre Peres Teixeira. – São Paulo : Editora Dialética, 2024.
964 p.

Bibliografia.
ISBN 978-65-270-2000-4

1. Poder. 2. Tecnologia. 3. Direito. 4. Força cibernética. I. Título.

CDD-340

Mariana Brandão Silva - Bibliotecária - CRB -1/3150

Dedico este trabalho acadêmico às pessoas que foram importantes na minha jornada até aqui. Em primeiro lugar para minha mãe, Edina Peres Teixeira, carinhosamente conhecida como Bibi, que partiu recentemente, deixando um vazio angustiante nos nossos corações.

Dona Bibi, sem nenhuma dúvida, foi o maior exemplo de resiliência que presenciei na minha vida, dela também herdei esta importante característica, que todo ser humano necessita possuir, principalmente atualmente, vivendo neste mundo louco e incerto. Gostaria de dedicar também ao meu querido pai, Adalberto Teixeira, que lutou muito para que eu pudesse estar aqui hoje, vivendo este momento ímpar. Infelizmente, ele também já nos deixou!

Para minha querida, linda e maravilhosa esposa, Hellen Bianca, também consigno esta dedicatória, por toda paciência, carinho, cuidado e atenção para comigo, nestes últimos quatro, intermináveis, anos de doutoramento. Aos meus queridos filhos, Bernardo e Sofia, minhas fontes de inspiração, que sofreram juntamente comigo, neste difícil processo. Ambos são a razão pela qual eu não desisto nunca e, enquanto conseguir respirar, não desistirei! Vocês são meus preciosos presentes, vindos diretamente do coração do Pai.

Dedico também aos meus queridos irmãos Débora, Danielle e Cláudio, pelo incentivo constante e apoio incondicional.

MIOLO_Poder, Tecnologia e Direito - 2.indd 5 26/04/2024 11:12:03

MIOLO_Poder, Tecnologia e Direito - 2.indd 6 26/04/2024 11:12:03

"O aspecto mais triste da vida agora é o fato de a ciência ser capaz de reunir conhecimento mais rapidamente do que a sociedade é capaz de reunir sabedoria."
(Isaac Asimov)

MIOLO_Poder, Tecnologia e Direito - 2.indd 8 26/04/2024 11:12:03

LISTA DE ABREVIATURAS E SIGLAS

AAP-6	Glossário de Termos e Definições oficial da OTAN
ARPA	Agência de Projetos de Pesquisa Avançada do Pentágono
ARPANET	*Advanced Research Projects Agency Network*
ASEAN	Associação de Nações do Sudeste Asiático
CAI	Conflito Armado Internacional
CANI	Conflito Armado não Internacional
CAs	*Certification Authority*
CBM	*Confidence-building measures*
CBM	Medidas de Construção de Confiança
CCD COE	Centro de Excelência em Defesa Cibernética Cooperativa da OTAN
CERTs	Equipes para proteção de sistemas de informação críticos
CIA	Agência Central de Inteligência
CIJ	Corte Internacional de Justiça
CSNU	Conselho de Segurança das Nações Unidas
DICA	Direito Internacional dos Conflitos Armados
DIH	Direito Internacional Humanitário
DNS	*Domain Name System*
DoD	Departamento de Defesa dos Estados Unidos
ENIAC	*Integrator And Calculator*
EU	União Europeia
EUA	Estados Unidos da América
HTTP	*Hyper Text Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICPD	Instituto CEUB de Pesquisa e Desenvolvimento
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*

ISP	*Internet Service Provider*
TCP	*Transmission Control Protocol*
LBDN	Livro Branco de Defesa Nacional
NATO CCD COE	Centro Cooperativo de Excelência em Defesa Cibernética
NSA	Agência de Segurança Nacional
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
RF	Rádio Frequência
TCP/IP	*Transfer Control Protocol/Internet Protocol*
UN GGE	*United Nations Group of Governmental Experts*
UNGGE	Grupo de Especialistas Governamentais da ONU
UNICEUB	Centro Universitário de Brasília
URL	*Uniform Resource Locator*

APRESENTAÇÃO

É com grande satisfação e orgulho que apresento livro fruto da pesquisa doutoral desenvolvida por Alexandre Peres acerca do tema da força cibernética e dos conflitos armados. Ultrapassar as barreiras acadêmicas ao mesclar inovação, ciência jurídica e conflitos armados, temas nada óbvios numa pesquisa doutoral, revela a determinação de Alexandre ao longo de quatro anos desafiadores, ampliados pelo advento da grave pandemia da COVID-19, na superação das adversidades que o acompanharam até a conclusão desta obra.

Desde o princípio, ao aceitar a orientação desta pesquisa, sabia que teríamos um profícuo período de descobertas interessantes, debates acalorados, um levantamento de dados documentais e bibliográficos exaustivo e custoso. Estes últimos escassos, de difícil catalogação, motivo que não esmoreceu este doutor em sua jornada.

Alexandre, com inquestionável sucesso, conseguiu superar com dedicação, trabalho árduo e tranquilidade os compromissos e desafios de uma pesquisa científica séria. Hoje, seu livro nos brinda com reflexões sólidas sobre o Direito Internacional aplicado aos Conflitos Armados. Não tenho dúvida de que o leitor de "*Poder, Tecnologia e Direito: A Força Cibernética e a Disrupção nos Principais Paradigmas de Sustentação do Direito Aplicável aos Conflitos Armados*" encontrará nestas páginas ideias instigantes de como o direito regulará os fenômenos advindos da utilização do ciberespaço nos conflitos armados.

Saliento a honra em ter orientado tal pesquisa cuja grande contribuição para a academia brasileira já tem gerado impactos positivos no debate sobre o tema. Sinto a sensação de dever cumprido na qualidade de orientadora. Agora, inauguramos uma nova fase de investigações científicas aprofundando o escopo anterior. Neste momento, não mais na qualidade de orientadora, mas de amiga, desejo a todos e todas uma excelente leitura e reflexão.

Liziane Paixão Silva Oliveira

Professora Titular do Programa de Mestrado e Doutorado do UniCEUB
Orientadora da Pesquisa

MIOLO_Poder, Tecnologia e Direito - 2.indd 12 26/04/2024 11:12:03

PREFÁCIO

No século XXI, os Estados, os atores não estatais e os indivíduos enveredaram por um novo caminho para solver suas desavenças e enfrentamentos. O desenvolvimento da Internet impactou-os, juntamente a sociedade humana, de maneira imponderável, possibilitando mudanças massivas nas comunicações, no comércio e nos próprios conflitos.

No cenário hodierno, as conflagrações armadas presenciam, cada vez mais, o advento não só de intervenientes e protagonistas até então inexistentes, mas de novas tecnologias bélicas resultantes do contínuo desenvolvimento tecnológico na área de defesa. Das tecnologias robóticas ao ataque cibernético, perpassando pelos drones, pelas armas energéticas, satélites e armas espaciais, mudanças radicais ocorreram nos campos de batalha e teatros de operação de guerra, que questionam a efetiva aplicação de princípios outrora estabelecidos pelo Direito Internacional Humanitário, na medida em que suas execuções são ainda mais difíceis de esquadrinhar sob a égide do ordenamento legal exógeno.

E é sobre este contexto intricado e caótico, que o Doutor Alexandre Peres Teixeira lança o presente livro que tenho a honra de prefaciar: "*Poder, Tecnologia e Direito: A Força Cibernética e a Disrupção nos Principais Paradigmas de Sustentação do Direito Aplicável aos Conflitos Armados.*"

Trata-se da investigação para a obtenção do título de Doutor, agora editada em livro, que perscruta e reflete o aprofundado mergulho intelectivo, lançando luzes sobre a intricada ordem legal, tanto interna quanto internacional vigente, a propósito de um tema polêmico e festejado na atualidade: a problemática da incidência do Direito nas Operações Cibernéticas de Guerra.

Por certo, as tendências que afetam as pugnas contemporâneas estão a ocorrer em âmbito social, militar e estratégico, portanto, a compreensão de tais fenômenos impõe a compreensão das complexidades jurídicas decorrentes destes novos tipos de hostilidades.

A questão assume contornos complexos, porquanto articula com a ponderação dos postulados norteadores do Direito da Guerra. E nisto reside o ineditismo da obra! Está-se diante de um primoroso trabalho científico que examina detidamente o Direito Internacional Humanitário, alçado à *canon* magno em diversas Cartas Políticas, com ênfase em um *novel* tipo de batalha: a cibernética.

O autor conduz, entre outros aspectos, a uma apreciação crítica sobre a fonte mais importante do *Jus ad Bellum,* refletido na Carta da ONU, com vistas a descortinar sua omissão em aspectos de relevo, a exemplo das modalidades precisas que regem o uso da força em caso de legítima defesa.

Nesta conjuntura, a alentada pesquisa, aqui publicada, traz como cerne, para além da análise aprofundada das diversas nuances das pugnas em ambiente virtual, o descortínio da insuficiência do Direito Internacional clássico, inadaptável aos fenômenos jurídicos advindos na Era da Informação e a consequente utilização maliciosa do ciberespaço que, para muitos internacionalistas, constitui a "quinta dimensão da guerra", excluída que está do enquadramento das leis referentes ao século passado.

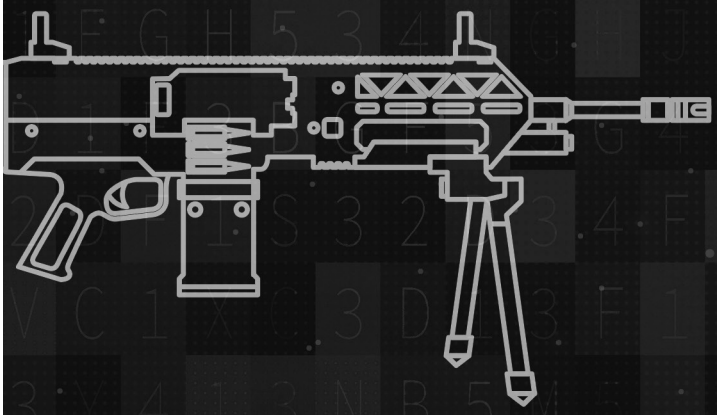
O impacto nos paradigmas jurídicos desta contenda belicosa de ineditismo inconteste, à evidência, tem modificado pilares, nuances, matizes e dimensões legais edificadas pela Sociedade das Nações. E, para aguçar ainda mais o interesse dos ávidos, é exposta a divergência entre doutrinadores da matéria, brilhantemente referenciados pelo Doutor Alexandre Peres, acerca da necessidade da criação de um Direito Internacional Cibernético, em que a normatividade do ciberespaço deveria ser concebida separadamente da ordem estatal e internacional.

Sem dúvidas, a obra brinda o leitor com uma construção doutrinal vigorosa que transcende o contributo teórico-dogmático para servir de norte aos magistrados, juristas e estudiosos a propósito da sensível interlocução entre o alvedrio e o mister dos Estados-nação ao dizer o Direito Humanitário e os Direitos Humanos - que nele se imbricam - e o pior flagelo que assola a Humanidade. Nela, arquétipos carcomidos pelo tempo são revisitados, matizados por uma *práxis cuja* tensão permite almejar bem mais do que o prevalecimento de uma ordenação coativa de convivência na Sociedade Mundial, permite, sobretudo, reivindicar o aprimoramento do brado civilizatório!

Que o presente livro encontre leitores instigados pelo conhecimento e prontos para se envolverem em uma jornada cerebral instigante!

Brasília, 10 de fevereiro de 2024

Maria Elizabeth Guimarães Teixeira Rocha
Ministra do Superior Tribunal Militar





SUMÁRIO

INTRODUÇÃO | 25

CAPÍTULO 1: O PODER NA ERA DO CYBER | 55

1.1 PODER: O PODER DO ESTADO E O DOMÍNIO CIBERNÉTICO | 60

1.1.1 O Poder Nacional | 64

1.1.2 O Poder Cibernético | 73

1.2 SOBERANIA: A SOBERANIA NA ERA DA INFORMAÇÃO | 81

1.2.1 Considerações sobre a noção clássica de soberania | 88

1.2.2 A Soberania cibernética | 99

1.3 PÓS-TERRITORIALIDADE: A PÓS-TERRITORIALIDADE E A DISRUPÇÃO DO MODELO WESTFALIANO | 121

1.3.1 O fenômeno cibernético da Pós-territorialidade | 125

1.3.2 Disrupção: violência quando o limite não é a destruição | 133

1.3.3 "Disruptivo" ou "Destrutivo"?| 136

1.3.4 Tipos de disrupção | 139

1.4 CONCLUSÃO PARCIAL | 142

CAPÍTULO 2: TECNOLOGIA – O CIBERESPAÇO, SUA FORÇA E O NOVO TIPO DE CONFLITO DO SÉCULO XXI | 147

2.1 O POTENCIAL OCULTO DA FORÇA CIBERNÉTICA| 150

2.2 O CIBERESPAÇO E SUAS PECULIARIDADES | 163

2.2.1 Desvendando o ciberespaço | 171

2.2.2 Um breve histórico sobre o surgimento do ciberespaço | 173

2.2.3 O que é o ciberespaço: em busca de uma definição | 179

2.2.3.1 A abordagem teórico-filosófica | 181

2.2.3.2 A abordagem técnico-científica | 189

2.2.3.2.1 A Arquitetura do Ciberespaço | 204

2.2.3.3 A abordagem geopolítica | 222

2.3 A GUERRA CIBERNÉTICA | 238

2.3.1 Correntes doutrinárias sobre guerra cibernética | 250

2.3.1.1 Alarmistas | 255

2.3.1.1.1 Análise da corrente alarmista | 257

2.3.1.1.2 Resumo do conceito de guerra cibernética da corrente alarmista | 260

2.3.1.2 Céticos | 261

2.3.1.2.1 Análise da corrente cética | 263

2.3.1.2.2 Resumo do conceito de guerra cibernética da corrente cética| 265

2.3.1.3 Realistas | 267

2.3.1.3.1 Análise da corrente realista | 269

2.3.1.3.2 Resumo do conceito de guerra cibernética da corrente realista| 272

2.3.1.4 Sintetizando uma definição para a Guerra Cibernética | 273

2.3.1.5 Definindo as variáveis da corrente sintetizada | 274

2.3.2 A Taxonomia das operações cibernéticas maliciosas | 276

2.3.2.1 Ajustando a terminologia | 278

2.3.2.2 Características peculiares das operações cibernéticas | 283

2.3.2.2.1 A dependência nacional e a interconectividade | 284

2.3.2.2.2 O anonimato | 285

2.3.2.2.3 A simplicidade, rapidez e facilidade de uso | 286

2.4 CONCLUSÃO PARCIAL | 287

CAPÍTULO 3: O DIREITO — O EMERGENTE DIREITO INTERNACIONAL CIBERNÉTICO | 293

3.1 A LEGITIMAÇÃO DO PODER PELO DIREITO E O CONCEITO DE ORDEM PÚBLICA | 299

3.1.1 O conceito tripartido de ordem pública | 302

3.1.2 Em busca de uma Ordem Pública Internacional | 306

3.2 DESAFIOS À NORMATIZAÇÃO DO CIBERESPAÇO | 316

3.2.1 Construindo normas para o ciberespaço | 323

3.2.2 As principais maneiras de criação de normas para o ciberespaço | 328

3.2.2.1 Normas cibernéticas surgindo por Tratados | 336

3.2.2.2 Normas cibernéticas surgindo por Costumes | 346

3.2.2.3 Normas cibernéticas surgindo por Princípios Gerais de Direito | 359

3.3 O PAPEL DA ONU E DA OTAN NO PROCESSO DE NORMATIZAÇÃO DO CIBERESPAÇO | 361

3.3.1 A ONU e os trabalhos do UNGGE | 361

3.3.2 A OTAN e os Manuais de Tallinn | 369

3.3.2.1 O Manual de Tallinn 2.0: a primeira fonte de direito internacional cibernético (soft law) | 373

3.3.2.2 A dinâmica de construção do Manual de Tallinn 2.0 | 378

3.4 AS PRINCIPAIS ZONAS CINZENTAS DO EMERGENTE DIREITO INTERNACIONAL CIBERNÉTICO | 380

3.4.1 Soberania: regra ou princípio? | 384

3.4.2 O Princípio da Devida Diligência | 392

3.4.3 O desafio da Atribuição no ciberespaço | 397

3.4.4 A Intervenção Ilícita | 401

3.5 CONCLUSÃO PARCIAL | 405

CAPÍTULO 4: A DISRUPÇÃO — O IMPACTO DO CIBERESPAÇO NOS PARADIGMAS DE SUSTENTAÇÃO DO DIREITO INTERNACIONAL APLICADO AOS CONFLITOS ARMADOS | 415

4.1 O *JUS AD BELLUM* E O PARADIGMA DO USO DA FORÇA NA ERA DA INFORMAÇÃO | 424

4.1.1 Análise Preliminar dos Conceitos Clássicos | 430

4.1.1.1 Da Guerra Justa ao "Pacto de Briand Kellog": os esforços fracassados para coibir a guerra total | 430

4.1.1.2 A Carta das Nações Unidas e a proibição do uso da força | 442

4.1.1.2.1 O ataque armado | 450

4.1.1.2.2 O direito à legítima defesa | 454

4.1.1.3 Os Conceitos ambíguos na Carta da ONU | 457

4.1.1.3.1 Força como violência armada | 458

4.1.1.3.2 Força como coerção | 460

4.1.1.3.3 Força como Interferência | 466

4.1.2 Novos conceitos da Era da Informação: Ataques cibernéticos sob a perspectiva do *Jus ad Bellum* | 471

4.1.2.1 O "uso da força" e o "ataque armado" no ciberespaço | 482

4.1.2.2 Tipos de abordagem que a doutrina emergente tem considerado para enquadramento das operações cibernéticas | 491

4.1.2.2.1 Abordagem baseada em instrumentos | 491

4.1.2.2.2 Abordagem baseada no alvo | 493

4.1.2.2.3 Abordagem baseada em efeitos | 497

4.1.2.3 O Teste Schmitt e o "uso da força" pelo Manual de Tallinn 2.0 | 502

4.1.2.4 Um conceito de Ataque Armado Cibernético | 515

4.1.2.5 A abordagem do Manual de Tallinn 2.0 sobre Ataque Cibernético | 522

4.1.2.6 A atribuição dos Ataques Cibernéticos | 529

4.2 O *JUS IN BELLO* E OS PARADIGMAS DO EMPREGO DA FORÇA CONTRA PESSOAS | 531

4.2.1 Os paradigmas do uso da força pelo Estado contra pessoas | 545

4.2.1.1 Base Jurídica e Características dos dois Diferentes Paradigmas | 547

4.2.1.1.1 Os regimes jurídicos internacionais que regem o uso da força em conflitos armados | 548

4.2.1.1.2 Os paradigmas da condução das hostilidades e de aplicação da lei | 552

4.2.1.1.3 Principais diferenças entre a condução das hostilidades e os paradigmas de aplicação da lei | 557

4.2.2 Diferença entre civil e combatente e os reflexos no regime protetivo | 562

4.2.2.1 Civil | 564

4.2.2.2 Combatentes | 567

4.2.3 Operações Cibernéticas e *Jus in bello* | 578

4.2.3.1 Segmentação de alvos no Ciberespaço | 580

4.2.3.1.1 Pessoas | 581

4.2.3.1.2 Objetos | 582

4.2.4 A importância dogmática do Princípio da Distinção para o contexto cibernético | 589

4.2.5 O *Leveé* en Masse cibernético | 600

4.2.5.1 Bases históricas do instituto jurídico | 600

4.2.5.2 A "cibermobilização" e o Levée en Masse do Século XXI | 603

4.2.5.3 Aspectos jurídicos do Levée en Masse cibernético | 608

4.2.5.3.1 Espontaneamente | 610

4.2.5.3.2 Habitantes do território invadido | 612

4.2.5.3.3 Território desocupado | 613

4.2.5.3.4 Portar armas abertamente | 615

4.2.5.3.5 Respeitar os costumes da guerra | 618

4.2.5.4 A visão do Manual de Tallinn 2.0 sobre o Levée en Masse cibernético | 620

4.2.6 A participação de civis em hostilidades cibernéticas | 622

4.2.6.1 Critérios de análise da Participação de Civis em Hostilidades | 635

4.2.6.1.1 Limite do dano | 636

4.2.6.1.2 Afetar adversamente as operações militares ou capacidade de uma parte no conflito | 638

4.2.6.1.3 Causar morte, lesão ou destruição a pessoas ou objetos protegidos contra os ataques diretos | 639

4.2.6.1.3 Ligação Causal Direta | 646

4.2.6.1.4 Condução das hostilidades, esforço geral de guerra e atividades de manutenção da guerra | 647

4.2.6.1.5 Causalidade direta e indireta | 649

4.2.6.1.6 Causalidade direta em operações coletivas | 650

4.2.6.1.7 Proximidade causal, temporal e geográfica | 651

4.2.6.1.8 O Nexo Beligerante | 653

4.2.6.1.9 Conceitos básicos | 654

4.2.6.1.10 Nexo beligerante e intenção subjetiva | 655

4.2.6.1.11 Relevância prática do nexo beligerante | 656

4.2.6.1.12 Determinação prática do nexo beligerante | 659

4.2.6.2 Início e fim da Participação Direta de Civis nas Hostilidades | 660
4.2.6.2.1 Medidas Preparatórias | 661
4.2.6.2.2 Desdobramento e retorno | 662
4.2.6.3 A noção de "função de combate contínuo" | 664
4.2.7 Operações Cibernéticas e a Lei da Neutralidade | 668
4.3 CONCLUSÃO PARCIAL | 670

CAPÍTULO 5 - A REALIDADE: ESTUDO DE CASOS SOBRE OPERAÇÕES CIBERNÉTICAS MALICIOSAS RECENTES QUE ENVOLVERAM ESTADOS | 679

5.1 CASO 1 – ESTÔNIA 2007: UMA SOCIEDADE SOB O CHOQUE E O PAVOR | 681
5.1.1 Resumo dos fatos ocorridos | 683
5.1.2 Análise técnica do caso | 690
5.1.2.1 Matriz de Análise Técnica do Caso 1 | 691
5.1.2.2 Síntese da análise técnica | 692
5.1.3 Análise política do caso e atribuição de autoria | 693
5.1.4 Análise jurídica do caso | 699
5.2 CASO 2 – O *STUXNET* E A MANIFESTAÇÃO CINÉTICA DA FORÇA CIBERNÉTICA | 704
5.2.1 Resumo dos fatos ocorridos | 706
5.2.2 Análise técnica do caso | 710
5.2.2.1 Matriz de Análise Técnica do Caso 2 | 711
5.2.2.2 Síntese da análise técnica | 712
5.2.3 Análise política do caso e atribuição de autoria | 715
5.2.4 Análise jurídica do caso | 719
5.3 CASO 3 – A INTERFERÊNCIA NAS ELEIÇÕES DE 2016 DOS EUA: A DISRUPÇÃO NO LIMITE DA DEMOCRACIA | 723
5.3.1 Resumo dos fatos ocorridos | 729
5.3.1.1 A Atuação da Inteligência Russa | 729
5.3.1.2 O trabalho sujo da Cambridge Analítica | 733
5.3.2 Análise técnica do caso | 735

5.3.2.1 Matriz de Análise Técnica do Caso 2 | 735

5.3.2.2 Síntese da análise técnica | 736

5.3.3 Análise política do caso e atribuição de autoria | 742

5.3.4 Análise jurídica do caso | 749

5.3.4.1 Os impactos jurídicos na democracia | 751

5.3.4.2 Os reflexos no direito internacional | 760

5.4 CASO 4 – DESAFIANDO O *JUS IN BELLO*: O EXÉRCITO DE TI DA UCRÂNIA | 770

5.4.1 Resumo dos fatos ocorridos | 777

5.4.2 Análise técnica do caso | 793

5.4.2.1 Matriz de Análise Técnica do Caso 4 | 793

5.4.2.2 Síntese da análise técnica | 794

5.4.3 Análise política do caso e atribuição de autoria | 803

5.4.4 Análise jurídica do caso | 811

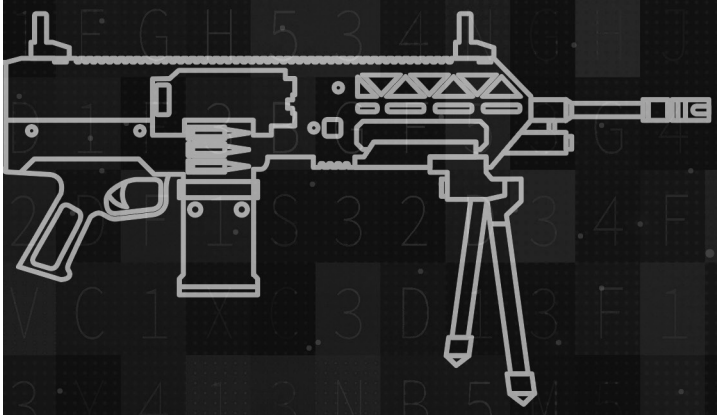
5.5 ALGUMAS CONSIDERAÇÕES FINAIS SOBRE RESPONSABILIZAÇÃO | 833

5.5.1 Gravidade Jurídica e Gravidade Relativa de Situações e Casos de Conduta Criminosa no Ciberespaço | 856

5.6 CONCLUSÃO FINAL | 858

REFERÊNCIAS | 873

PÓSFACIO | 959





INTRODUÇÃO

"Estamos criando um exército de TI. Precisamos de talentos digitais. Todas as tarefas operacionais serão dadas aqui: https://t.me/itarmyofuraine. Haverá tarefas para todos. Continuamos a lutar na frente cibernética. A primeira tarefa está no canal para especialistas cibernéticos." (tradução nossa)

Mykhailo Fedorov
(Vice Primeiro-Ministro da Ucrânia, em 23/02/2022)

"Por conseguinte, do ponto de vista da Cibernética, o mundo é um organismo, nem tão rígido ao ponto de que qualquer mudança em algum aspecto o faça perder sua identidade, nem tão frouxamente articulado que qualquer coisa possa acontecer."

Norbert Wiener
(1956)

"*A suprema arte da guerra é derrotar o inimigo sem lutar.*"

Suz Tzu
(500 AC)

O acelerado incremento da tecnologia, no pós-Guerra Fria, tornou propício o início da chamada Era da Informação[1] ou era digital. Com a chegada desse tempo, a história vivenciou sua terceira revolução industrial, e a comunicação ganhou velocidade impressionante. No meio técnico-científico informacional[2], as transformações ocorreram de forma a impactar, contundentemente, a dinâmica e a vida das sociedades. A velocidade dos fluxos econômicos, sociais, culturais, linguísticos, entre outros, ampliou-se em ritmo exponencial, deflagrando uma sucessão de

1 PENA, R. F. A. Era da informação. UOL, Goiânia, 2013. Disponível em: http://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 12 fev. 2022.

2 O conceito de meio técnico-científico informacional está relacionado com o processo de formação e integração espacial, ocasionado pelas técnicas digitais, bem como com a maneira a qual ele modifica o espaço Idem.

MIOLO_Poder, Tecnologia e Direito - 2.indd 25 26/04/2024 11:12:05

novas revoluções a cada instante. Dessa forma, o ciberespaço[3] passa a ser parte integrante das interações sociais, comerciais, econômicas e jurídicas que se realizam em seus diferentes níveis[4].

O ciberespaço se constitui em uma fronteira desconhecida a ser explorada e estudada, principalmente pelo Direito. Por esse fato, o livro dedica uma seção inteira para analisar a arquitetura do ambiente informacional[5]. Com sua construção peculiar, ele engloba um número imenso

3 A expressão *cyberspace* é atribuída a William Gibson e foi cunhada na obra de ficção Neuromancer, publicada em 1984, em Nova Iorque, pela Editora Ace Books. Compõe uma trilogia e explora a relação entre o homem e a máquina; recebeu os principais prêmios de produção literária de ficção científica e serviu de base para o filme Matrix, no qual o ator Keanu Reaves entra no ciberespaço e conecta seu sistema nervoso central a um computador. SALDAN, E. **Os desafios jurídicos da guerra no espaço cibernético**. 2012. 118 f. Dissertação (Mestrado em Direito Constitucional)- Instituto Brasiliense de Direito Público, Brasília, 2012.

4 Existem três níveis de espaço a serem considerados na grande rede virtual. O primeiro nível é o espaço físico, onde as pessoas habitam e convivem, cada um governado por um único Estado-Nação. Dentro desse nível, as pessoas devem obedecer às leis de onde estão fisicamente localizadas. É o nível-base da jurisdição da Internet, vinculando a pessoa ao espaço físico que habita. O segundo nível é o dos provedores de acesso, na realidade, o primeiro nível de jurisdição da Internet em si. O provedor é a conexão entre o mundo físico e o virtual e, na maioria dos casos, abriga, em seu bojo, muitas comunidades virtuais, sendo um verdadeiro "país virtual". O terceiro nível é o dos domínios e das comunidades que ultrapassam fronteiras nacionais por meio dos provedores. Dentro desse nível, há várias comunidades virtuais que operam sem respeitar fronteiras internacionais ou de outros provedores. O domínio seria o endereço e a forma pela qual determinada comunidade virtual apresenta-se na rede. DYSON, E. **Release 2.0:** a design for living in the digital age. Estados Unidos: Broadway Books, 1997.

5 No desenvolvimento da tese serão encontradas expressões como: "ciberespaço", "espaço cibernético" ou "ambiente informacional", cujos significados estão relacionados ao meio composto por parafernália de Tecnologia de Informação (TI), dividido em camadas, operado por um ser humano com finalidades mais variadas possíveis (a descrição detalhada do ciberespaço será realizada no segundo capítulo do livro); "força cibernética", cujo significado está relacionado com o efeito obtido pelo uso malicioso do ciberespaço, que é capaz de causar disrupção, (por meio de efeitos primários), danos físicos, ou danos imateriais, (que se equiparam a danos físicos), por meio de efeitos secundários e terciários; "cibercinéticos", que se trata de um neologismo trazido para a língua pátria em decorrência dos novos fenômenos da Era da Informação, e cujo significado está relacionado com a fronteira existente entre a porção virtual de uma operação cibernética e os seus efeitos materiais no mundo real; "operações cibernéticas maliciosas", cujo significado está relacionado com a conduta na qual o ser humano, patrocinado ou não por um Estado nação, utiliza-se das capacidades do espaço cibernético para a realização de condutas que visem causar danos, materiais ou imateriais, contra outros Estados soberanos ou seus *proxies*; "crimes

MIOLO_Poder, Tecnologia e Direito - 2.indd 26 26/04/2024 11:12:05

de redes e periféricos, que estão ligados por uma infraestrutura física, distribuída por todo planeta. Entretanto, sem programas, aplicativos e bancos de dados, tal parafernália técnica não se prestaria à sua finalidade. Bem como não se pode olvidar que o ser humano[6] é o principal ator em todo este processo, não apenas porque se trata do mentor, do criador e do arquiteto principal deste paradigma complexo[7], apresentado à raça humana, fruto da genialidade e do trabalho inovador, mas também por ser o responsável por fazer rodar este audacioso mecanismo conhecido como ciberespaço, que tem o potencial de gerar uma força ainda muito pouco conhecida e explorada: a força cibernética.

A força cibernética, desde a sua gênese, tem exercido forte influência nas relações de poder que moldam a sociedade internacional. Neste sentido, impactando no poder, esse novo fenômeno causa também influência, consequentemente, na ordem jurídica, tanto nacional, como internacional. A tecnologia, associada ao poder, possui um viés especificamente disruptivo, capaz de causar desordem, em decorrência do surgimento de fenômenos jurídicos que, até então, eram novos para a ciência jurídica. Poder, tecnologia, Direito e disrupção compõem uma nova cadeia de fenômenos jurídicos que urgem a pesquisa acadêmica de

cibernéticos da esfera comum", cujo significado está relacionado aos os crimes comuns, que estão normatizados nos ordenamentos jurídicos nacionais, são perpetrados com a finalidade de obtenção de vantagem patrimonial financeira ou qualquer vantagem de ordem pessoal, inclusive aquelas de conteúdo sexual; e "crimes cibernéticos internacionais", cujo significado pode estar relacionado com graves violações de Direitos Humanos, graves violações do Direito Internacional Humanitário (DIH), condutas criminosas que atentem contra a paz e a segurança internacionais e, em geral, crimes da competência material do Tribunal Penal Internacional (TPI).

6 O ciberespaço é um espaço artificial, criado por humanos para fins humanos. Sem usuários humanos, o ciberespaço estagnaria, cairia em ruínas e eventualmente deixaria de existir. A menos que algo mais possa assumir a manutenção e o desenvolvimento da infraestrutura e do conteúdo cibernéticos, o humano continua sendo uma parte importante do ciberespaço (OTTIS, R.; LORENTS, P. Cyberspace: Definition and Implications. INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 5., 2010. Dayton. **Anais [...]**, Dayton, OH, US: Reading: Academic Publishing Limited, p 267-270, 2010. Disponível em: https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/. Acesso em: 16 jul. 2023).

7 Quando se considera a quantidade de nós que existem na internet, fica claro porque o ciberespaço é considerado algo extremamente complexo. Segundo Ottis e Lorents, a União Internacional de Telecomunicações estima que quase um quarto da população mundial está conectada a Internet, enquanto mais de 60% está conectada a telefones celulares. Idem.

MIOLO_Poder, Tecnologia e Direito - 2.indd 27 26/04/2024 11:12:05

alto nível. Exatamente tentando contribuir com o debate acadêmico sobre este importante tema, este trabalho dedica um capítulo para a análise de cada aspecto específico dessa cadeia lógica.

Desde o surgimento da sociedade internacional, os Estados buscam um posicionamento vantajoso no concerto das nações e se utilizam de relações de poder para isto. A Soberania do Estado nação figura como o grande paradigma que sustenta as prerrogativas de jurisdição territorial desses entes dotados de personalidade jurídica de direito internacional. Entretanto, a disputa pelo poder é a marca de um sistema que vive, constantemente, sendo testado, desafiado e desconsiderado. Desta forma, o conflito é uma consequência inconteste desta relação interestatal, instável e volátil. Mas o Direito se apresenta, neste contexto, como elemento estabilizador da ordem pública, que busca sempre obter uma resposta assertiva para os fenômenos jurídicos que se apresentam no âmbito das jurisdições nacionais e da internacional.

Os consagrados critérios para evidência de jurisdição e soberania dos Estados, estabelecidos após a assinatura dos Tratados de Westfalia, têm sido frontalmente questionados pela dinâmica pós-territorial inaugurada com a chegada da Era da Informação. Em virtude da facilidade, rapidez e alcance possibilitados pela utilização do ambiente informacional, as condutas *contra lege*, de caráter extraterritorial, fazem com que os conflitos de leis no espaço se tornem uma preocupação para os Estados nacionais. Não apenas os crimes cibernéticos, que invadem esfera patrimonial individual e coletiva, mas também os crimes contra a paz e segurança internacionais, as violações contra a proteção internacional da pessoa humana e os crimes específicos da competência material do Tribunal Penal Internacional (TPI), figuram no rol de alcance das operações cibernéticas maliciosas.

Pelos séculos, o Direito vem atuando como elemento de moderação e estabilidade de uma ordem internacional marcada por desequilíbrio e arbitrariedade. O uso da força pelos Estados, desde a sua gênese incontrolável, até a obtenção definitiva de sua tutela, pela sociedade internacional, sempre figurou como ferramenta de imposição de vontades e de busca de vantagens competitivas para os Estados. Neste caminho, tendo deixado muito sangue de seres humanos para trás, o controle do uso da força foi finalmente alcançado pelos comandos do Direito e pacificado, por meio de normatização própria, representada pela Carta da Nações Unidas e demais títulos legais, aceitos de forma consensual pelos Estados.

MIOLO_Poder, Tecnologia e Direito - 2.indd 28 26/04/2024 11:12:05

O contexto tecnológico, para o qual foram levantadas as regras que normatizam o uso da força, não era similar ao contexto atual, no qual o planeta está inserido, neste século marcado pelo advento da Era da Informação. O estado de coisas se transformou inegavelmente, gerando caducidade ou enfraquecimento das normas contidas na Carta da ONU, isso também, decorrente de uma distribuição de poder totalmente incoerente com a realidade deste século. Grande parcela das normas existentes na esfera de regulação do uso força está relacionada com um tipo de força caracterizada pela violência cinética, causada pelos meios de combate. Desde os primórdios dos combates militares entre Estados até o surgimento do ciberespaço e sua utilização como ferramenta de combate, as lutas sempre foram caracterizadas por uma delimitação espacial, por uma visível materialização de meios de combate e pela existência física de atores no terreno.

Entretanto, o despertar da força cibernética e sua utilização para este tipo de atividade bélica veio agregar instabilidade, incerteza e insegurança jurídica em um cenário que já era extremamente difícil, controverso e instável. A real possibilidade de se conseguir alcançar objetivos políticos, econômicos e psicossociais sem a necessidade de utilização de portifólio militar clássico, evitando-se, assim, a exposição ao escrutínio da sociedade internacional, parece ter virado obsessão de um grupo de Estados, que têm se mostrado contumazes em buscar seus objetivos particulares a despeito do que preconiza a ordem internacional.

Em 2013, o general Valery Gerasimov, chefe do Estado-Maior da Rússia, publicou um importante artigo de revista no qual observou que as linhas entre guerra e paz estavam se tornando tênues, enfatizando o crescimento do uso de meios não militares para se alcançar objetivos políticos e estratégicos. Segundo o general, tal uso tem se mostrado mais eficiente e bem-sucedido do que "o uso tradicional da força". Como exemplo de sua assertiva o general citou as "revoluções coloridas", no norte da África (por exemplo, a Revolução Jasmim da Tunísia de 2010-11) e a Primavera Árabe (2011), tendo também citado a forma pela qual uma "guerra no domínio cibernético" poderia ser um meio-chave de intervenção estrangeira, gerando o "caos interno, catástrofe humana e até mesmo uma guerra civil"[8]. Por outro lado, o ex-Diretor de Inteligência Nacional

8 GERASIMOV, V. S. The Value of Science Is in the Foresight: new challenges demand rethinking the forms and methods of carrying out combat operations. **Military review**, Kansas, v. 96, p. 23, 2016, p. 25. Disponível em: https://www.semanticscholar.org/paper/The-Value-of-Science-Is-in-the-Foresight%3A-New-the-Gerasimov/a132e441825bd5314b7135af33ac643bed422e7e. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 29 26/04/2024 11:12:05

dos Estados Unidos da América (EUA), Mike McConnell comparou as consequências potenciais dos ciberataques destrutivos modernos àquelas produzidas por armas de destruição em massa[9].

O uso do ciberespaço como ferramenta de guerra tem mostrado efeitos imprevisíveis. Suas características *sui generis* atribuem ao domínio cibernético qualidades e vantagens que os meios e métodos convencionais não possuem. Furtividade, anonimização, possibilidade de operação remota e longínqua, flexibilidade, versatilidade e baixíssimo custo, quando comparado com os meios convencionais, fazem do ciberespaço uma opção irrecusável para seus utilizadores. Somado a isso, a inexistência de uma normatização específica e pacífica, capaz de estabelecer critérios de governança para seus usuários. Sem nenhuma dúvida, o ciberespaço figura como uma opção militar vantajosa e letal, mas também disponível para qualquer ser humano, de qualquer parte do planeta, que queira se aventurar e tomar parte em hostilidades cibernéticas.

Neste sentido, a reunião da letalidade, de um meio de guerra potencialmente destrutivo, com a possibilidade de uso por pessoas não afetadas diretamente pelos combates das zonas de guerra, gera um problema sério para o escopo limitativo e protetivo do Direito Internacional Humanitário (DIH), também conhecido como *jus in bello*, bem como afeta diretamente a base tradicional do *jus ad bellum*, que foi construída para limitar o uso da força nas relações internacionais. Nesse processo, percebe-se que tanto o paradigma do monopólio da força, decorrente da soberania externa, como o monopólio da soberania interna do Estado nação sofrem influência com os efeitos disruptivos do ciberespaço. Cabendo ressaltar que os paradigmas militares, considerados para a construção da Carta da ONU, já estão ultrapassados pela evolução dos métodos e meios de guerra e pela capacidade de disrupção trazida pela Era da Informação, com o advento do ciberespaço.

Entretanto, como será explorado neste livro, o processo de adaptação do Direito posto aos fenômenos jurídicos criados pelo uso da tecnologia da informação (TI), principalmente no que tange ao uso

9 ROLLINS, J.; HENNING, A. C. Comprehensive National Cybersecurity Initiative: Legal Authorities And Policy Considerations. **Congressional Research Service**, CRS Report for Congress: Prepared for Members and Committees of Congress, 2009. Disponível em: https://obamawhitehouse.archives.gov/files/documents/cyber/Congressional%20Research%20Service%20%20CNCI%20%20Legal%20Authorities%20and%20Policy%20Considerations%20%28March%202009%29.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 30 26/04/2024 11:12:05

malicioso realizado pelos Estados para as ações de combate, no curso dos conflitos armados, tem sido muito mais assertivo do que o processo de adaptação do Direito aos fenômenos jurídicos que ocorrem em tempos de paz, com o uso da mesma tecnologia. Isto, pelo fato de a doutrina estar evoluindo no sentido de considerar o ciberespaço como um meio, uma ferramenta capaz de infringir danos cinéticos no mundo real. Com isto, tem sido criado o padrão da "escala e dos efeitos" para as operações cibernéticas maliciosas destrutivas. Desta forma, compara-se o efeito da operação cibernética ao efeito similar de uma arma cinética e classifica-se a ação dentro de um padrão que varia de mero "uso da força" até o "ataque armado", que enseja direito de legítima defesa ao ofendido.

Cabe ressaltar que uma arma convencional é utilizada para causar efeitos cinéticos no alvo, seja o alvo uma pessoa, uma instalação ou qualquer objeto material. Uma vez causados os efeitos, caracterizados estão os danos, e estes, se forem causados em desacordo com a norma, ficarão ao alcance do Direito. Quando se utiliza uma arma cibernética, seus efeitos podem ser percebidos em três níveis diferentes: no nível primário, no secundário e no terciário. Nesse caminho, tais efeitos podem causar danos no mundo material. Uma vez causados os efeitos, em forma de danos físicos, caso não estejam em conformidade com a norma, tais danos serão alcançados pelo Direito da mesma forma que os danos causados pelos meios convencionais são. Para condutas realizadas em situações de conflitos armados, o regime competente será o do DIH.

O grande problema jurídico surge quando operações cibernéticas maliciosas disruptivas, que não atinjam o limite de danos materiais, são executadas fora do contexto dos conflitos armados, em tempo de paz, causando efeitos secundários e terciários que possam se equiparar aos efeitos de uso da força. Mesmo que não cause o dano físico material, dependendo da escala e dos efeitos da operação, se a conduta não for justificável pelo Direito, os autores podem responder, tanto pela jurisdição nacional do país alvo, quanto pela jurisdição do Direito Internacional, e o Estado pode ser responsabilizado por cometimento de ato ilícito na esfera internacional. Para este tipo de operação, o ciberespaço possui características que dificultam a atribuição de responsabilidades, causando dificuldades à persecução penal.

As operações cibernéticas maliciosas disruptivas, que não causam danos físicos, mas impactam de forma negativa a vida das socieda-

MIOLO_Poder, Tecnologia e Direito - 2.indd 31 26/04/2024 11:12:05

des dos países vítimas de tais operações, inauguram uma nova forma de violência, capaz de gerar efeitos extremamente nocivos para seus alvos. Se executadas por Estados, tais condutas se revestem de uma gravidade sem precedentes, principalmente se forem direcionadas a minar e enfraquecer expressões de poder no Estado-alvo. Neste sentido, casos reais, que serão apresentados no quinto capítulo deste livro, demonstrarão efeitos devastadores impostos às expressões econômicas, militares, psicossociais, científicas e tecnológicas dos países alvos.

Tais ações são denominadas de operações de zona cinzenta e se utilizam de brechas existentes, que são decorrentes de interpretações errôneas ou tendenciosas das fracas normas que estão sendo importadas do Direito Internacional Geral para o emergente Direito Internacional Cibernético. Estados oportunistas se valem para explorar tais brechas, na busca de seus próprios interesses e em detrimento dos interesses e valores buscados pela sociedade internacional. Desta forma, a base existente para a normatização do uso da força, bem como aquela que busca a responsabilização de Estados e indivíduos por atos ilícitos, cometidos na esfera internacional, não está totalmente aderente aos novos fenômenos apresentados pela Era da Informação. Se por um lado, o Estado protagoniza condutas maliciosas e se posiciona como réu, ao desconstruir os padrões normativos do *Jus ad Bellum*, por outro, ele figura como vítima da atuação controversa e, em princípio ilegal, de civis que tomam parte de hostilidades cibernéticas utilizando-se de um padrão pouco ortodoxo e desconstruindo padrões normativos do *Jus in bello*. Este é o tipo de guerra que emerge no horizonte do século XXI.

A guerra silenciosa, sorrateira e sub-reptícia, operacionalizada mesmo em tempos de paz e normalidade institucional, contra as jurisdições nacionais, é uma realidade da atual conjuntura internacional. Contra esta guerra, o Direito ainda não possui remédios totalmente testados e aprovados pela prática e pelo costume. No decorrer deste trabalho serão abordadas questões importantes, relacionadas ao tema que se propõe explorar, que servirão para ilustrar tamanho do abismo normativo no qual o Direito Internacional se encontra, em decorrência do mau uso do ciberespaço pelos Estados. Como Draper[10] afirma: "[...] a dicotomia entre os propósitos do direito da guerra e a natureza da guerra é, provavelmente, o mais agudo ponto de tensão entre o direito e a vida". Apesar da natureza

10 DRAPER, G. I. A. D. The implementation and enforcement of the Geneva Conventions of 1949 and of the two additional protocols of 1979, Recueil des Cours. **The Hague Academy of International Law**, The Netherlands, v. 164, n. III, 1979, p. 10.

MIOLO_Poder, Tecnologia e Direito - 2.indd 32 26/04/2024 11:12:05

paradoxal de ambos os conceitos, no século XXI, tendo em vista a evolução do poder letal dos meios de combate, o Direito atua como elemento de moderação e limitação, possuindo um valor inestimável para a história dos conflitos armados e, na atual conjuntura, está sendo desafiado por um tipo de guerra obscura, que transcende a sua capacidade de abordagem. Sendo assim, não se pode deixar de responder com assertividade aos desafios impostos pela inovação tecnológica.

Como afirma Roscini[11], os tratados de Direito Internacional existentes, bem como as normas consuetudinárias, podem ser estendidos, por analogia e interpretação, às operações cibernéticas, mesmo que o tema não seja contemplado, expressamente, nestes títulos legais. Também não se pode excluir que disposições específicas do Direito Internacional consuetudinário ainda estejam em processo de desenvolvimento, em relação a pelo menos certos aspectos da condução de operações cibernéticas pelos Estados. Posto isto, ressalta-se que no presente livro é sustentada a ideia-chave de que a base normativa posta, para regular as ações e as condutas, de Estados e pessoas físicas, perpetradas com a utilização da força cibernética, não se encontra em condições de fornecer segurança jurídica à ordem internacional, principalmente nos casos em que a força cibernética é utilizada por Estados e/ou seus *proxies* com finalidade geopolítica maliciosa e de forma disfarçada. Portanto, na carência de base normativa positivada[12] que regule, processe e puna comportamentos impróprios de Estados e pessoas por eles patrocinadas, principalmente em situação de paz, brechas são abertas para que crimes internacionais, bem como graves violações contra a pessoa humana sejam perpetradas, em nível nacional e internacional.

Desde a Batalha de Solferino, em 1859, vem sendo construída a base normativa que regula as condutas de Estados durante as hostilida-

11 ROSCINI, M. **Cyber operations and the use of force in international law**. Oxford: Oxford University Press, 2014.

12 Sem a existência de base normativa para cobrir os fenômenos jurídicos decorrentes de condutas maliciosas perpetradas pelo ciberespaço, tanto a responsabilização do Estado por ação ilícita na esfera internacional, como a responsabilização penal internacional individual das pessoas envolvidas ficam prejudicadas, podendo gerar impunidade e o incentivo de novas condutas. Neste sentindo deve se ressaltar que, tendo em vista as peculiaridades do ciberespaço, qualquer pessoa, de qualquer parte do planeta, pode se envolver em hostilidades cibernéticas, durante o curso dos conflitos armados. Tal conduta invade a esfera do Direito Internacional Humanitário (DIH) e causa problemas relacionados ao conteúdo normativo dedicado à proteção de civis contra os ataques diretos.

MIOLO_Poder, Tecnologia e Direito - 2.indd 33 26/04/2024 11:12:05

des dos conflitos armados. Tal compêndio, inicialmente sustentado pelo Costume, foi consolidado naquilo que hoje se conhece como "Direito de Genebra", cujo escopo principal é o de limitar o emprego dos meios de violência, por parte dos beligerantes, e proteger as pessoas que não tomam parte das hostilidades dos efeitos dos combates.

O princípio internacional da proteção da pessoa humana, erguido e consolidado em decorrência de sofrimento e morte causados a milhões de seres humanos, na história dos combates nos últimos séculos, que tem seu fundamento no princípio da humanidade, traduz-se na base de sustentação da proteção oferecida pelo DIH. Neste sentido, durante o curso dos conflitos armados, civis que não tomam parte das hostilidades ativas não devem ser alvos de ataques diretos, devendo ser protegidos durante o curso das operações de combate. Tal estado de coisas só se modifica em caso dos civis, por própria vontade, resolverem tomar parte das hostilidades e, consequentemente, renunciar a proteção atribuída pelo DIH a esta classe de pessoas.

Entretanto, o advento do ciberespaço tem modificado, de forma significativa, o acesso de civis às hostilidades ativas. A base, ainda em construção, do Direito Internacional Humanitário Cibernético considera o caso das hostilidades cibernéticas, que se dão com a utilização do ciberespaço, como ferramenta de combate, no curso dos conflitos armados. Tais hostilidades podem se materializar, com a realização de operações maliciosas com efeitos "cibercinéticos" que buscam a causação de danos físicos, por meio dos efeitos diretos, secundários ou terciários; ou então, por operações que, apesar de não romperem a barreira do dano físico, causem danos lógicos capazes de influenciar nas operações militares.

Desta forma, o envolvimento de civis nas hostilidades cibernéticas, no curso dos conflitos armados, se apresenta como uma ruptura do paradigma que busca a proteção da população civil e dos civis em geral. Exemplos reais, que estão ocorrendo no conflito entre Rússia e Ucrânia, figuram como grande preocupação para o Comitê Internacional da Cruz Vermelha (CICV). Registros de mídia aberta e uma pequena quantidade de artigos acadêmicos apontam para a larga participação de civis e grupos privados não estatais nas ações beligerantes do conflito. Tendo como verdadeiras tais suposições, fato é que, além de se transformarem em verdadeiros objetivos militares, sendo passíveis de sofrerem ataques diretos (inclusive com meios cinéticos), tais pessoas também se tornam

MIOLO_Poder, Tecnologia e Direito - 2.indd 34 26/04/2024 11:12:05

elegíveis a sofrerem a persecução penal pelos crimes que cometerem com suas condutas, inclusive crimes de guerra.

Ao abordar a questão do crime, cabe ressaltar que, apesar da pesquisa ter identificado que o ciberespaço figura também como ferramenta para realização de condutas criminosas ilícitas, fora da situação de conflito armado e por parte de grupos privados, ou de pessoas físicas entre si, que se utilizam do ciberespaço para a perpetração de crimes cibernéticos da esfera comum que visam o lucro patrimonial ou o dano material fortuito. Tais condutas criminosas da esfera comum, por sua vez, não serão objeto de análise no desenvolvimento deste livro, que se prenderá à análise de condutas ilícitas de Estados, que possam gerar responsabilização na esfera internacional; nas condutas cometidas por pessoas físicas, patrocinadas e autorizadas por Estados, que possam gerar responsabilização penal, em situação de paz; e nas condutas de civis que tomam parte das hostilidades, no curso dos conflitos armados.

Cabe ressaltar que a abordagem de crimes cibernéticos da esfera comum não será privilegiada neste trabalho, em virtude do autor acreditar que a persecução penal, para este tipo de crime cibernético, está bem delineada e coberta por títulos legais das jurisdições nacionais, bem como por instrumentos normativos internacionais que cuidam da temática, sendo tal persecução, realizada pelas jurisdições nacionais, com cooperação entre jurisdições. Desta forma, acredita-se que a utilização do ciberespaço para a perpetração de crimes cibernéticos comuns não gera zonas cinzentas ou lapsos de aplicação da lei que possam fomentar a impunidade.

Já o crime perpetrado pelo Estado e por seus *proxies*, além de impactar negativamente na esfera das jurisdições nacionais, contém elementos de estraneidade que reportam para a ruptura de normas e tratados internacionais, relacionados com a tutela da paz e da segurança internacional, com o DIH e com a proteção internacional dos direitos humanos. Da mesma forma, as condutas cibernéticas realizadas por civis, durante o curso dos conflitos armados, geram reflexos na proteção internacional da pessoa humana e devem ser objeto de análise do Direito.

Desta forma, acredita-se que, por sua posição de prepotência, o Estado possui a capacidade de, não apenas se esquivar da justa responsabilização, como também de encobrir e dificultar a responsabilização de indivíduos que atuem com seu mandato. E igualmente, não se faz capaz

MIOLO_Poder, Tecnologia e Direito - 2.indd 35 26/04/2024 11:12:05

de realizar a persecução penal dos civis que participem diretamente das hostilidades, sem a devida pacificação do tema perante a ordem internacional. Cabe ressaltar que, pela ausência de normatização pacífica, muitas condutas perpetradas por Estados e seus *proxies* são processadas pelas jurisdições nacionais, tendo como base a lei interna, que, na maioria dos casos, não possui a força necessária, isto é, a extraterritorial, para responder com assertividade e fazer justiça.

Em relação ao que será abordado no primeiro capítulo do livro, ressalta-se que, ao dedicar o presente trabalho de pesquisa à investigação de tema de caráter inovador para a academia jurídica, cujo objeto de análise é a manifestação da força cibernética, foi necessária uma busca detalhada sobre correlação que existe entre os conceitos de poder, especificamente referindo-se ao poder do Estado, com o conceito de soberania e de Direito, no que tange ao Direito Internacional especificamente. A análise das expressões do poder figura como tema central do capítulo, assim como sua relação com a força cibernética, que vai gerar o conceito de poder cibernético. Desta forma, se pode observar que existe uma sensível diferença na manifestação da força cibernética nas expressões do poder nacional de um Estado soberano. Se no mundo real as ações de força são exclusivamente realizadas por meio da expressão militar do poder, no mundo virtual, em contrapartida, a força cibernética possui a capacidade de influenciar e se fazer sentir em quaisquer das expressões do poder do Estado (política, econômica, militar, psicossocial, científica e tecnológica), conforme será abordado com mais detalhes na primeira seção do capítulo inaugural.

Cabe também ressaltar que o Princípio da Soberania, abordado com detalhes na segunda seção do capítulo 1, que está intimamente relacionado com o Poder Nacional, tem sido de importância fundamental para as relações internacionais, até os dias atuais. Verdade é que, após este marco espacial e temporal, estabelecido pela Paz de Westfália, o recurso da força por parte dos Estados veio sofrendo ingerências diretas e sucessivas, por parte da recém-criada sociedade internacional. Neste sentido, o ciberespaço tem proporcionado o surgimento de novos atores, que colocam a soberania do Estado nação em debate. O trabalho aborda as principais reações que estão sendo constatadas, vindas por parte da instituição Estado, em decorrência da chamada "soberania cibernética".

A terceira seção, do capítulo 1, dedica-se a apresentar, ainda que de forma não muito profunda, o fenômeno da pós-territorialidade. Per-

MIOLO_Poder, Tecnologia e Direito - 2.indd 36 26/04/2024 11:12:05

ceber-se-á que o ciberespaço tem, como uma de suas principais características, a possibilidade de atuação pós-territorial. Tal peculiaridade tem sido de extrema importância para o enfraquecimento da soberania do Estado nação. Pode-se dizer que os efeitos disruptivos da tecnologia da informação exercem influência direta no fortalecimento do viés pós-territorial que ameaça a jurisdição interna dos Estados nacionais.

O segundo capítulo do livro, seguindo a trilha proposta, aborda a Tecnologia! Na sua primeira seção, se apresenta o potencial obscuro da força cibernética, elencando alguns exemplos reais que demonstram os efeitos sinistros, cinéticos e disruptivos, que podem ser causados com o uso malicioso da força cibernética. Em seguida, na segunda seção, serão exploradas as nuances do ciberespaço, com a finalidade de situar o leitor em relação à natureza fática do ambiente informacional. A proposta aqui é que se tenha um direcionamento do terreno complexo no qual o Direito terá que navegar. A seção se inicia com uma visita à estrutura do ciberespaço, analisando suas principais definições e abordagens, caminhando por suas camadas[13], para que se tenha a percepção dos locais, espaços, heurísticas e programas que são utilizados para condutas que não se coadunam com o Direito. Nesta viagem, será percebido que todas as camadas do ciberespaço estão ao alcance dessa área do saber, para efeito de estudo e normatização. A segunda seção, do segundo capítulo, demonstrará a dificuldade de se definir o que realmente é o ciberespaço, enumerando as abordagens que variam num espectro que vai desde a teórico-filosófica até a geopolítica, passando pela abordagem técnico-científica. Independentemente de qual abordagem seja considerada, a composição do ciberespaço é imutável: trata-se de uma superposição de camadas, que englobam o portfólio físico, a estrutura lógica e o agregamento humano, sem o qual não existe operação cibernética.

A atuação geopolítica do Estado, pelo ciberespaço, surgiu com contundência no século XXI e figura, atualmente, como uma das grandes preocupações da sociedade internacional, ataques cibernéticos são realizados hodiernamente. Dado o custo relativamente barato do conhecimento tecnológico necessário, tais ataques cibernéticos podem ser montados por governos hostis ou vários tipos de atores não estatais, desde empresas privadas até organizações militantes, gangues

13 O número de camadas que compõe o ciberespaço varia de autor para autor, mas para a presente obra foram consideradas três principais camadas: a física, a lógica e a social, pois são as camadas que estão expostas para a análise no Manual de Tallinn 2.0, uma das principais fontes de estudo desta tese, ainda que em nível de *soft law*.

MIOLO_Poder, Tecnologia e Direito - 2.indd 37 26/04/2024 11:12:05

criminosas ou outros grupos armados não estatais. Nesse contexto, os doutrinadores do Direito muitas vezes se apressaram em usar a expressão corriqueira no senso comum "Guerra Cibernética" ou "Armas Cibernéticas", levantando assim a necessidade de saber se o princípio da proibição do uso da força sob o Artigo 2(4) da Carta da ONU se aplicaria aos ataques cibernéticos que são executados diariamente, inclusive em tempo de paz[14].

Desta forma, a terceira seção, do capítulo 2, se prestará para a análise do fenômeno da guerra cibernética, sem adentrar demais nos aspetos técnicos de TI. A taxonomia da guerra cibernética será discutida, uma vez que se faz importante a compreensão de como a literatura está classificando este novo fenômeno. Serão apresentadas as correntes doutrinárias que tentam abordar o tema, bem como as principais características que fazem do ciberespaço o perfeito campo de batalha da guerra cibernética. Sobre isto, Hughes e Colarik[15] descobriram que de 159 artigos a respeito da guerra cibernética, 103 (65%) falharam em oferecer uma definição explícita acerca desta. Ashraf[16] afirma que existem muitas definições diferentes, e muitas vezes contraditórias, que variam desde a crença na inexistência da guerra cibernética até certeza de que a guerra cibernética é uma ameaça existencial. Este amplo espectro de incerteza contribui para que a abordagem jurídica do fenômeno seja prejudicada, limitando as análises teóricas e dificultando a construção de políticas públicas que possam trazer segurança jurídica para a utilização do ciberespaço[17].

Cabe ressaltar que se optou pela apresentação de uma análise do impacto da tecnologia no contexto da guerra, não tão profunda, no que tange aos aspectos técnicos mais específicos, mas que

14 HENRY, Etienne. The Falklands/Malvinas War – 1982. *In*: CORTEN, Olivier; RUYS, Tom (eds). **International Law and the Use of Force**: A Case-Based Approach. Oxford: Oxford University Press 2018, p. 368.

15 HUGHES, D.; COLARIK, Andrew. The Hierarchy of Cyber War Definitions. *In*: PACIFIC ASIA WORKSHOP ON INTELLIGENCE AND SECURITY INFORMATICS. 12., 2017, Spring. **Anais [...]**, Springer, 2017, p. 15-33.

16 ASHRAF, Cameran. Defining cyberwar: towards a definitional framework. **Defense & Security Analysis**, Londres, v. 37, n. 3, 2021, p. 274-294, Disponível em: https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141. Acesso em: 25 jul. 2023.

17 LIFF, A. P. Cyberwar: A New 'Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, London, v. 35, n. 3, 2012, p.401-28.

MIOLO_Poder, Tecnologia e Direito - 2.indd 38 26/04/2024 11:12:05

fosse suficiente para se atingir uma definição aceitável. Além de expor a composição em camadas e delinear as principais características disruptivas do ciberespaço, pelo fato deste ambiente ser um terreno pouco explorado pela academia, principalmente pela área do Direito. Durante os trabalhos de pesquisa, teve-se a nítida impressão de que, por ser um tema extremamente inovador, ele não é tratado com muita relevância por juristas e operadores do Direito, em nível nacional. Decorrente disto, a esmagadora fonte de consulta utilizada na pesquisa está em idioma estrangeiro, com grande parte das citações expostas por tradução livre, pelo autor.

No terceiro capítulo será analisado o Direito, mais precisamente a importância do Direito para a manutenção da paz de segurança internacionais, por meio da construção da ordem pública internacional, que seja capaz de manter a estabilidade do planeta. Serão também abordados os movimentos iniciais do processo de emergência do Direito Internacional Cibernético, que figura como uma peça importante para a conjuntura da Era da Informação. A intenção é que se tenha uma compreensão do estado atual que se encontra o processo de normatização do ciberespaço. Para se atingir esse propósito, a primeira seção do capítulo discorre sobre a legitimação do poder pelo Direito e o conceito de ordem pública. Na segunda seção serão analisados os desafios que existem no caminho da normatização, focando-se nas questões, políticas e jurídicas, que influenciam os esforços de normatização. Em seguida, na terceira seção, serão apresentadas as ações realizadas pela ONU e pela OTAN no sentido de construir uma base normativa que seja capaz atender às necessidades da sociedade internacional. Neste sentido, serão analisadas as ações do Grupo de Especialistas Governamentais para assuntos de TI (UNGGE), criado pela ONU para discutir medidas de comportamento dos Estados no ciberespaço. Em seguida serão tecidos comentários sobre o Manual de Tallinn 2.0, única fonte de doutrina consolidada sobre Direito Internacional Cibernético existente, ainda que em nível de *soft law*. Na última seção do capítulo serão apresentadas algumas considerações sobre as principais zonas cinzentas existentes no conjunto de regras que tentam estabelecer comportamentos dos Estados no ciberespaço.

O capítulo 3 tem como um de seus objetivos demonstrar que, apesar de os esforços para a construção de uma base jurídica comum

MIOLO_Poder, Tecnologia e Direito - 2.indd 39 26/04/2024 11:12:05

aos Estados terem sido iniciados nos anos 1990[18], o atual arcabouço jurídico do sistema internacional[19], por ser insipiente e agregar pouco consenso em relação às questões de Direito Internacional aplicado ao ciberespaço, mostra-se inapto para gerir os conflitos que surgem na dimensão cibernética. Tal fato tem sido grande preocupação da Organização das Nações Unidas (ONU), desde a década de 1990, pois tem reflexo direto na manutenção de uma ordem internacional que seja capaz de assegura a paz e a estabilidade.

Seguindo os trabalhos da ONU, a Organização do Tratado do Atlântico Norte (OTAN), por meio do Centro Cooperativo de Excelência em Defesa Cibernética (NATO CCD COE), encomendou a produção de dois manuais que tratassem das regras relacionadas à utilização do ciberespaço, por parte dos Estados. O primeiro manual foi criado em 2013, mas restringiu sua abordagem às operações cibernéticas realizadas em situação de conflito armado, sob o regime do Direito Internacional Humanitário (DIH). A edição do segundo manual, lançado em 2017, abordou diversos regimes jurídicos, inclusive para operações cibernéticas realizadas em tempo de paz. Atualmente, o manual de 2017 é considerado uma das primeiras fontes de doutrina de Direito Internacional aplicado às operações cibernéticas, mas ainda em nível de *soft law*, por não ter o caráter vinculativo para os Estados.

No que tange à normatização das operações cibernéticas, existe dificuldade para a construção de um marco jurídico consensual[20],

18 SCHMITT, M. N. Computer network attack and the use of force in international law: thoughts on a normative framework**Columbia Journal of Transnational Law**, New York, v. 37, n. 7, 1999. Disponível em: https://ssrn.com/abstract=1603800. Acesso em: 17 fev. 2023.

19 O sistema internacional é formado por um vasto conjunto de tratados e convenções que se ocupam em manter a paz e a segurança internacionais. Os principais documentos estão reunidos em conjuntos conhecidos como direito de Genebra, direito de Haia, direito de New York, fazendo parte, também, os costumes internacionais. STOCKBURGER, P. Z. Known unknowns: State Cyber Operations, Cyber Warfare, and the jus ad bellum. **American University International Law Review**, New York, v. 31, n. 4, 2016. Disponível em: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.com.br/&httpsredir=1&article=1898&context=auilr. Acesso em: 25 fev. 2023.

20 Para Lotrionte e Tikk, atualmente não se pode apenas olhar para as normas de uma perspectiva legal, porque nem todas as normas foram testadas na prática e, portanto, requerem uma avaliação de políticas para determinar sua relevância, contexto e escopo de aplicação. LOTRIONTE, C.; TIKK, E. (Co-chairs). Applicability of international law to cyberspace & Characterization of cyber incidents. **Cyber Norms**

MIOLO_Poder, Tecnologia e Direito - 2.indd 40 26/04/2024 11:12:05

que possa encontrar respaldo na sociedade internacional e pacificar o uso de tais operações entre os Estados. Para Kanuck[21], o consenso de uma perspectiva global sobre essas questões é essencial, "[...] porque nenhuma política declaratória ou interpretação legal específica de uma única nação será vinculante para a comunidade internacional". Além disso, segue o autor afirmando que "[...] a lei será apenas um fator na determinação de como os Estados vão gerir os conflitos cibernéticos entre si no futuro"[22].

Para Schmitt[23], além da incerteza quanto aos parâmetros legais precisos da guerra cibernética, existe o fato de que o Direito internacional público é, por natureza, "uma criatura dinâmica, sendo que seu conteúdo, interpretação e aplicação evoluem com o tempo, em resposta à transformação do ambiente de segurança para o qual se aplica". Paralelamente, as questões de evolução das leis internacionais, as operações no ciberespaço podem ser realizadas totalmente à margem da regulação jurídica. As denominadas zonas cinzentas já demonstraram sua utilidade, para Estados partidários da utilização de operações maliciosas.

O quarto capítulo pode ser considerado a alma desta obra, pois nele será analisada, efetivamente, a Disrupção. Figurando como uma reunião entre Política, Tecnologia e Direito, o capítulo aborda, de forma direta, os efeitos disruptivos do ciberespaço nos paradigmas do *jus ad bellum* e do *jus in bello*, por meio da análise dos principais institutos jurídicos relacionados a estes paradigmas: o instituto jurídico do uso da força, que em sentido amplo é a base de sustentação do *jus ad bellum*; e o instituto jurídico do emprego da força contra pessoas, em conflitos armados, que em sentido estrito é a base de sustentação do *jus in bello*. Neste sentido, o capítulo apresenta uma análise profunda, sobre o ponto de vista do Direito Internacional dos Conflitos Armados, acerca da quebra dos principais paradigmas que regem o *Jus ad bellum* e o *Jus in*

Workshop 2.0, [*S.l.*], 2012. Disponível em: https://citizenlab.ca/cybernorms2012/panel3 summary.pdf. Acesso em: 12 fev. 2023.

21 KANUCK, S. Sovereign discourse on cyber conflict under international law. **Texas Law Review**, Texas, v. 88, p. 1571-1597, 2010. Disponível em: https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Kanuck.pdf. Acesso em: 17 fev. 2023, p. 1571.

22 Idem, p. 1571.

23 SCHMITT, M. N. The Law of Cyber Warfare: Quo Vadis? **Stanford Law & Policy Review**, Stanford, v. 25, p.269-299, 2014a. Disponível em: https://ssrn.com/abstract=2320755. Acesso em: 25 jul. 2023, p. 271 – tradução nossa.

MIOLO_Poder, Tecnologia e Direito - 2.indd 41 26/04/2024 11:12:05

bello. Na primeira seção será demonstrado que toda base normativa construída para normatizar o instituto do uso da força foi construída sob o paradigma de emprego da força militar cinética, sendo este fato uma das primeiras inconsistências jurídicas desveladas pela pesquisa. Inconsistência que impacta frontalmente o trabalho de adaptação da base posta aos novos fenômenos jurídicos decorrentes do uso da força cibernética com ênfase no *Jus ad Bellum*, atentando-se para a conceituação de ataque armado cibernético e legítima defesa cibernética.

Os primeiros esforços de codificação das regras costumeiras, que tinham como escopo a normatização da guerra, foram realizados com as Conferências de Haia de 1899 e 1907. Entretanto, em decorrência da existência de múltiplas soberanias, com os mais variados interesses, a fraca normatização não foi capaz de evitar a eclosão do Primeiro Conflito Armado generalizado. Ao término da Primeira Guerra Mundial, um grande esforço foi realizado para a criação de uma Organização Internacional que fosse capaz de tutelar a paz e a segurança internacionais e assim foi criada a Liga da Nações. Porém, por possuir uma fraca base normativa, que não proibia que a força fosse utilizada pelos Estados como ferramenta de relações internacionais, a empreitada não logrou êxito e a Segunda Guerra Mundial eclodiu com maior violência ainda. Cabe registrar a existência do Pacto de Briand Kellog (1928) que, desde 1928, figura como o documento base para que a guerra fosse definitivamente proibida na sociedade internacional.

Após o fracasso da Sociedade das Nações, o planeta conheceu o segundo grande conflito generalizado, que foi caracterizado por um grande derramamento de sangue, inclusive de civis. Somente após este grande revés, a sociedade internacional foi capaz de consolidar parte do direito costumeiro e positivá-lo em dois grandes blocos, o Direito de Nova York e o Direito de Genebra, que vigoram até os dias atuais, procurando manter a paz e a estabilidade internacionais. Neste caminho, ressalta-se que o principal título legal que aborda o uso da força pelos Estados é a Carta da ONU, principalmente o seu artigo 2º, inciso 4º. Outro importante artigo, para o presente trabalho, é o artigo 51º, que versa sobre o direito de legítima defesa.

O instituto do uso da força, tutelado pela Carta da ONU, tem suas raízes no direito costumeiro, na era das chamadas "guerras justas". Durante grande parte da história das guerras, o recurso para se utilizar a força como ferramenta de relações internacionais era considerado um direito para os Estados ou entes soberanos. Fundamentada em preceitos religiosos, a te-

MIOLO_Poder, Tecnologia e Direito - 2.indd 42 26/04/2024 11:12:05

oria da guerra justa começou a perder força com o fim da guerra dos 30 anos e a assinatura do conjunto de Tratados que ficou conhecido como "A Paz de Westfália". Esse conjunto de Tratados foi responsável por inaugurar uma nova dinâmica nas relações entre os Estados, uma vez que reconhecia a territorialidade como evidência de soberania do Estado.

Finalmente, a Carta da ONU, que pode ser citada como o caso de sucesso da Sociedade Internacional, limitou e proscreveu o uso da violência armada como forma de solução de controvérsias internacionais. Entretanto, construída sob uma base dogmática que vigorava em 1945, a Carta da ONU não atende, de forma assertiva, às necessidades que surgiram com a criação do ciberespaço. A grande zona cinzenta surge na definição do que exatamente é uma "Força", nos termos da Carta, que seja capaz de ativar os comandos proibitivos do artigo 2º, inciso 4º, bem como de acionar o artigo 51º, que se refere ao direito de legítima defesa. Pela doutrina corrente, a única força capaz de acionar os comandos da Carta é a força armada de portifólio militar.

Para que se tenha uma base de comparação relacionada aos institutos jurídicos válidos para a atualidade, naquilo que tange ao *Jus ad Bellum*, será realizada uma análise detalhada da Carta da ONU, sem esquecer de se referir às controvérsias e ambiguidades que impactarão na normatização do uso da força cibernética. Desta forma, o trabalho também discorrerá sobre o uso da força cibernética, um conceito que foi criado pelo autor, por adaptação do conceito de uso da força, contido na Carta da ONU. Para que se chegue à discussão sobre tal conceito, inicialmente será abordada a evolução histórica do instituto jurídico que proscreveu o uso da força nas relações internacionais.

Em seguida, a segunda seção do quarto capítulo aborda a questão da proteção de civis, outorgada pelas normas de *Jus in bello* e consolidadas no Direito de Genebra. Além de trazer os principais conceitos jurídicos que caracterizam as figuras do combatente e do civil, a seção discorrerá também sobre as características e condições, estabelecidas pelo Comitê Internacional da Cruz Vermelha (CICV), para que um civil possa perder a proteção contra os ataques diretos e possa sofrer persecução penal pelas condutas realizadas durante o tempo que estiver tomando parte das hostilidades ativas. Mais precisamente, serão elencadas duas situações específicas que possuem relevância para o contexto das hostilidades cibernéticas: a situação do civil participando de um *Leveé en Masse* e a situação do civil participando diretamente das hostilidades ativas. O foco desta análise será a busca de paralelos entre as situações de hostilidades

MIOLO_Poder, Tecnologia e Direito - 2.indd 43 26/04/2024 11:12:05

cinéticas e hostilidades cibernéticas, com a finalidade de avaliar se existe compatibilidade entre o Direito posto pelo compêndio de Genebra e as particularidades das condutas realizadas pelo ciberespaço.

Sobre esta questão, Kilovaty[24] afirma que a emergência do ciberespaço como instrumento de guerra exacerba as lacunas e ambiguidades que já existem no DIH. Um fator particularmente agravante é o aumento do envolvimento de civis em ataques cibernéticos. Neste sentido, civis, em conflitos armados modernos, podem desempenhar um papel ativo quando se trata desses ataques, pois atuam como contratados privados realizando operações cibernéticas ofensivas e defensivas. Embora a noção tradicional de conflito armado inclua membros das Forças Armadas regulares ("combatentes"), esse paradigma não é mais o caso no campo de batalha moderno, devido ao crescente envolvimento de civis em hostilidades cibernéticas[25].

Cabe ressaltar que este livro, além de focar-se na análise do Direito da guerra aplicado às relações internacionais cibernéticas, também terá como foco, em uma segunda fase, a análise de questões de *Jus in bello*, referentes à ação de civis, que executam condutas, supostamente ilícitas, com a utilização do ciberespaço, contra Estados nacionais, no curso de conflitos armados. Neste caminho, no que tange inicialmente às relações entre Estados, cabe ressaltar que a globalização deu lugar à participação de outros atores, além do Estado, na dinâmica das relações internacionais e trouxe desafios para o exercício de soberania[26], no contexto internacional. O ciberespaço desconstruiu a relevância das fronteiras estatais, erguidas segundo o paradigma westfaliano[27], fazendo crescer a importância da

24 KILOVATY, I. Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under Humanitarian Law. **Michigan Telecommunications nad Technology Law Review**, Michigan, v. 23, n. 1, 2016. Disponível em: https://repository.law.umich.edu/mttlr/vol23/iss1/3. Acesso em 22 set. 2023.

25 Idem.

26 Poder de um Estado para criar e aplicar, nos limites do seu território, as leis que considerar adequadas, sem sofrer interferências externas de outros Estados ou de organismos internacionais. É um dos fundamentos da República Federativa do Brasil, nos termos do artigo 1º da Constituição Federal. O artigo 17 da Lei de Introdução às Normas do Direito Brasileiro (Lei nº 12.376/2010) dispõe sobre a ineficácia de atos e leis estrangeiras ofensivos à soberania, à ordem pública e aos bons costumes no Brasil.

27 Segundo esse paradigma, o Estado-Nação exerce soberania e jurisdição sobre os ocupantes de um território definido por fronteiras físicas reconhecidas pela comunidade internacional. MELLO, op. cit.

MIOLO_Poder, Tecnologia e Direito - 2.indd 44 26/04/2024 11:12:06

cooperação internacional para a mitigação de conflitos. Além de abrir a possibilidade de que atores comuns tenham acesso às hostilidades cibernéticas, em tempo real, de forma remota e muito distante do teatro das hostilidades ativas durante um conflito armado.

A quebra dos paradigmas supramencionados, relacionados tanto ao *Jus ad Bellum*, como ao *Jus in bello*, reflete um descompasso entre a velocidade da inovação tecnológica, os decorrentes fenômenos jurídicos e a capacidade do direito se reinventar. Neste caminho, para Simoncini[28], a estrutura normativa que atualmente cerca a TI é multifacetada. Em uma primeira camada surge o nível subjetivo/moral, que, tradicionalmente, não está ao alcance dos juristas, mas não deve ser negligenciado. Uma vez que, em sua estrutura, o ciberespaço é, naturalmente, resiliente à regulamentação clássica, uma maneira eficiente de torná-lo um lugar mais seguro seria por meio da construção de um código moral do ciberespaço. O nível seguinte, intermediário, diz respeito ao conteúdo normativo ético-coletivo, representado por programas de pesquisas, convenções internacionais, legislação da União Europeia, manuais não vinculativos, melhores práticas e diretrizes gerais. A normatização deste nível figura como *soft law*, autorregulação, acordos voluntários ou regulamentos de autoridades privadas. Por fim, há um terceiro nível, público-jurídico, que envolve a regulação jurídica em sentido estrito, e que se materializa nas formas local, nacional, doméstico, constitucional, supranacional e internacional de regulamentos técnicos[29].

Impende a construção de uma base normativa que consiga pacificar a utilização do quinto domínio[30] da guerra, por parte dos Estados. Caso contrário, o domínio cibernético oferecerá uma ótima oportunidade para a perpetração de graves violações do Direito da guerra e do Direito Internacional dos Direitos Humanos (DIDH), inclusive por meio de ações cinéticas, no mundo real, ou ações sub-reptícias, que sorrateiramente enfraquecem as democracias, incomodam as sociedades, quando não criam pânico. Inúmeros são os exemplos de ações realizadas, na Era Contemporânea, com a utilização maliciosa do ciberespaço, independentemente da existência de conflito armado entre as partes envolvidas. As

28 SIMONCINI, A. The Constitutional Dimension of the Internet: Some Research Paths. **EUI Department of Law Research Paper**, Florença, n. 2016/16, 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2781496. Acesso em: 23 jun. 2023.

29 Idem.

30 Os outros quatros são: terra, mar, ar e espaço sideral.

MIOLO_Poder, Tecnologia e Direito - 2.indd 45 26/04/2024 11:12:06

ações cibernéticas que beiram ou passam do limite estabelecido para ser considerado uso da força, segundo o recém-criado Manual de Tallinn 2.0, estão cada vez mais presentes no cotidiano das relações internacionais, solapando a ordem internacional, pela audácia de seus perpetradores.

O quinto capítulo deste livro trará a Realidade, como resultado da convergência entre o Poder, a Tecnologia, o Direito e Disrupção. A Realidade é o produto da utilização do ambiente tecnológico informacional como ferramenta útil no duelo geopolítico entre os Estados. Neste duelo, a primeira vítima é o Direito, que se percebe afogado em um verdadeiro oceano cinzento normativo. Neste capítulo a realidade das operações cibernéticas hodiernas será apresentada por meio da prática. Neste sentido, serão expostos quatro estudos de casos de eventos reais, que ocorreram recentemente, todos envolvendo ações maliciosas de Estados contra outros Estados com a utilização do ciberespaço. O objetivo deste capítulo é apresentar uma aplicação prática sobre o foco principal desta obra, isto é, constatar que a base clássica do Direito Internacional Geral não está apta para responder, com assertividade, a todos os fenômenos decorrentes do uso malicioso do ciberespaço, por parte dos Estados. Desta forma, tentar-se-á provar que em decorrência da existência de zonas cinzentas importantes, Estados estão se aproveitando para, em tempo de paz, buscar vantagens geopolíticas no cenário internacional. O largo uso de operações cibernéticas maliciosas por Estados ou seus *proxies* têm sido capaz de atingir centros de gravidade importantes, que minam e enfraquecem o poder do Estado por meio da realização de ações de efeitos disruptivos indiretos contra às expressões política, econômica e da ciência e tecnologia.

O primeiro caso a ser analisado figura como uma das mais graves operações maliciosas perpetradas por um Estado, contra outro, pelo ciberespaço: o Ataque à Estônia, em 2007. Por conta de ataques cibernéticos em massa, a Estônia teve toda sua estrutura, tanto pública como privada, paralisadas. Tais ataques teriam sido deflagrados em decorrência de uma controvérsia que envolveu a remoção de um memorial de guerra, da era soviética, de uma praça da capital Tallinn. As operações maliciosas afetaram portais do governo, da imprensa e de empresas privadas, causando *blecaute* na Internet estoniana, por várias semanas. O país levou meses para superar as consequências destes ataques, que causaram prejuízos econômicos e humanitários consideráveis, tendo deixado em situação de completa vulnerabilidade a sociedade estoniana, ofendendo os direitos humanos. Estes ataques foram atribuídos à Rússia – que oficialmente negou a acusação – e

MIOLO_Poder, Tecnologia e Direito - 2.indd 46 26/04/2024 11:12:06

tiveram origem em diversos locais, incluindo supostos provedores do governo russo, razão pela qual o episódio é considerado a primeira guerra cibernética, embora não declarada.

No segundo caso a ser abordado será exposto o potencial de letalidade de uma arma cibernética, demonstrando que, em suas consequências finais, a força cibernética, no que tange aos efeitos secundários e terciários, assemelha-se, em resultado, ao que se obtém com o uso da força cinética: no ano de 2010, por meio de uma meticulosa operação de inteligência, um vírus que ficou conhecido como *Stuxnet* foi inserido no sistema cibernético de controle da usina nuclear iraniana de Natanz. O *Stuxnet* tratava-se de um *worm* de computador, projetado especificamente para atacar o sistema operacional SCADA, desenvolvido pela *Siemens* e utilizado para controlar as centrífugas de enriquecimento de urânio iranianas. O vírus foi capaz de reprogramar o sistema de controle da usina e mandar informações erradas para o console de central. O ataque com o *Stuxnet* danificou mais de 1.000 centrifugas e atrasou, significativamente, o programa nuclear iraniano.

O terceiro caso exposto trará os eventos que culminaram na turbação do pleito eleitoral, em 2016, nos Estados Unidos da América (EUA). Por meio de uma sistemática operação de informação, construída com o largo uso de operações cibernéticas maliciosas, que envolveu a intrusão no servidor do Partido Democrata, com posterior divulgação de dados confidenciais. Após o sucesso da intrusão, foi realizada uma minuciosa campanha desestabilizadora, por meio das redes sociais, associada a divulgação de notícias falsas e *trolls*. A interferência na democracia norte-americana teve a contribuição da empresa de mídia Cambridge Analítica, que, com um sofisticado processo de mapeamento das redes sociais e a utilização de um algoritmo superpotente, realizou uma propaganda direcionada que favoreceu o candidato do Partido Republicano. A Rússia foi associada a esta grave "operação negra" de interferência ilícita em um tema que pertence à reserva de domínio da sociedade norte-americana. Este caso será importante para ilustrar a possibilidade de se obter efeitos geopolíticos, com ação sub-reptícia, por meio de uma operação cibernética maliciosa realizada por um Estado nação.

O último caso a ser analisado no capítulo diz respeito ao conflito armado entre Rússia e Ucrânia, iniciado em fevereiro de 2022. O caso aborda um tema de extrema relevância para a questão da responsabilização penal internacional individual por crimes cometidos por civis, que não possuem a prerrogativa de tomarem parte em hostilidades, no

MIOLO_Poder, Tecnologia e Direito - 2.indd 47 26/04/2024 11:12:06

curso dos conflitos armados. O ponto de interesse deste conflito armado, para esta obra se prende ao fato de que ficou publicamente conhecido, quando o Ministro da Defesa Ucraniano, no início do conflito, fez um apelo dramático para que *hackers* de todo mundo se unissem às forças armadas ucranianas, com a finalidade de comporem um "exército digital" contra a Rússia. Tal fato suscitou o debate sobre a legalidade da participação de civis nas hostilidades diretas, ressaltando a importância de serem analisados os conceitos de "*Levée en Masse*" e "participação direta de civis em hostilidades ativas", sob o ponto de vista das operações cibernéticas.

Em 24 de fevereiro de 2022, após o apelo público do Governo da Ucrânia, divulgado pelas redes sociais, milhares de pessoas no mundo todo atenderam ao chamado para a guerra, dentre elas, o grupo de *hackers* conhecido como *Anonymous*, que fez uma declaração de guerra cibernética contra a Rússia. No seu pronunciamento, o grupo alegou que tinha como alvo as estações de TV estatais, os Ministérios do governo e os bancos estatais. Uma série de ataques cibernéticos foram executados pelo grupo, em retaliação aos ciberataques perpetrados pela Rússia a sites e empresas do governo ucraniano.

Para o caso concreto do conflito entre Ucrânia e Rússia o termo "Guerra Cibernética" pode parecer, de uma forma geral, como uma figura de linguagem. Entretanto, especialistas jurídicos internacionais afirmaram, na ocasião, pelos mais diversos meios de mídia, que os voluntários cibernéticos, que se juntaram ao esforço de guerra, para atacar a Rússia no ciberespaço, podem, legalmente falando, terem se tornado combatentes, o que, segundo o Direito Internacional Humanitário, os transformou em alvos legítimos de retaliação, inclusive de ações cinéticas. Eles podem até, involuntariamente, tornarem-se cúmplices de crimes de guerra. Fato é que a utilização da tecnologia da informação como meio de guerra ampliou o escopo territorial dos combates, levando os engajamentos para dentro das residências de civis, em todo o globo. O apelo do governo ucraniano, na tentativa de recrutar seu exército de *hackers*, revela para o mundo um perigoso precedente, que incorpora uma questão de Estado com a privacidade da vida civil e coloca todos na mira de retaliações, inclusive com meios cinéticos, que podem ser executadas pelas partes engajadas no conflito.

Estes e outros casos reais trazidos por este livro possuem um elemento em comum: o uso malicioso da força cibernética, por Estados ou seus *proxies*, com a finalidade de causar efeitos no mundo real,

MIOLO_Poder, Tecnologia e Direito - 2.indd 48 26/04/2024 11:12:06

quer sejam cinéticos ou não. São operações cibernéticas que — apenas na situação do *Stuxnet*, por meio de efeitos secundários e terciários, materializou-se cineticamente — atingem um nível de escala e efeitos compatíveis com o ataque armado cinético. Entretanto, em todos os outros exemplos o que se percebe é a utilização de operações cibernéticas maliciosas, que, apesar de não atingirem o limite do dano físico, são capazes de causar danos imateriais tão ou mais graves do que o dano físico. Tais operações atingem o coração da democracia, como foi a do pleito de 2016, nos EUA, solapando, indubitavelmente, a expressão do poder político norte americano. Ou então geram pânico na sociedade, privando os cidadãos de usufruírem de bens públicos essenciais para subsistência, violando frontalmente direitos humanos, como ocorreu na Estônia. Por último, o caso do Exército de TI da Ucrânia reflete o perigo da participação voluntária de civis em hostilidades cibernéticas durante os conflitos armados, revelando outra grande fragilidade no Direito Internacional posto.

Em relação a escassez de trabalhos acadêmicos sobre a temática trazida pelo presente livro, acredita-se que se omitir em abordar um problema jurídico, que envolve o uso do ciberespaço, e que já é uma realidade incontestável para o Direito, não contribui para o progresso acadêmico, nem para a construção de um entendimento sobre essa complexa temática, em nível nacional. Tal postura reticente da academia não impede que o ciberespaço continue a ser utilizado de forma maliciosa, com a finalidade criminosa. Fatos inegáveis, que estão ocorrendo agora, enquanto este livro é escrito, que estão sendo realizados por pessoas, com o uso do ambiente informacional, são fatos sociais que afetam diretamente a vida dos seres humanos deste planeta, bem como a de suas instituições e, sendo assim, entram no escopo do estudo e na análise por parte do Direito, devendo ser alcançados pelos efeitos da jurisdição, quer seja nacional ou internacional.

Neste sentido, o uso da força cibernética é uma realidade que faz parte do cotidiano do planeta. Seja antes, durante ou depois de um conflito armado, ou até mesmo em tempo de paz, a utilização do ciberespaço como ferramenta bélica pode gerar efeitos nocivos aos seres humanos. Os casos apresentados demonstram que a força cibernética possui o potencial de ser utilizada para gerar efeitos dos mais simples até os mais catastróficos. Com a utilização do ciberespaço pode se obter, desde um simples dano na camada lógica de uma infraestrutura cibernética, até o colapso total do sistema de controle de tráfego aéreo de uma região. Des-

MIOLO_Poder, Tecnologia e Direito - 2.indd 49 26/04/2024 11:12:06

ta forma, é incontestável a necessidade de normatização do ciberespaço, bem como a investigação desta questão, em nível de doutoramento.

Nesse sentido, visando promover a temática no meio acadêmico brasileiro, a obra tem como escopo demonstrar que o Direito Internacional posto não está em condições de alcançar as condutas ilícitas realizadas por Estados e seus *proxies*, com uso da força cibernética, em tempos de paz. Tal vulnerabilidade é decorrente do fato de que tais condutas não atingem o padrão de dano elegível para se caracterizarem como uso da força. Entretanto, como será demonstrado ao longo do livro, por meio de exemplos práticos, tais condutas produzem danos imateriais, atingindo expressões do poder nacional, que podem ser considerados com a mesma gravidade empreendida pelos danos físicos. Neste sentido, pelos exemplos a serem explorados, Estados e seus *proxies* não são responsabilizados por falta de base jurídica que os levem aos tribunais competentes. Com o segundo propósito, a obra também demonstrará que a ausência de base normativa pacífica permite que civis tomem parte de hostilidades, durante os conflitos armados, sem terem tal prerrogativa. Esta questão reforça o fato de que, para alguns fenômenos jurídicos trazidos pela Era da Informação, a adaptação do Direito Internacional posto não alcança a suficiência normativa capaz de responder assertivamente aos referidos fenômenos: nem para alcançar e processar condutas ilícitas de Estados, no curso de operações cibernéticas maliciosas que não cruzam o limite do dano físico; nem para as condutas de civis que participem das hostilidades cibernéticas ativas.

Para tanto, a presente obra, que se pauta em uma tese de doutorado submetida ao Programa de Pós-Graduação em Direito do Centro de Ensino Unificado de Brasília (CEUB), se propõe a: demonstrar que a quebra do paradigma da soberania territorial westfaliana, conceito base para o *Jus ad Bellum*, em decorrência da invasão de soberanias por meio da realização de operações cibernéticas maliciosas, figura como um fator facilitador do cometimento de condutas ilícitas por Estados e seus *proxies*; desvelar as nuances do ciberespaço, sua estrutura e forma de utilização, com destaque para a capacidade sinistra da força cibernética e apresentar o conceito de guerra cibernética sob uma perspectiva técnico-jurídica; expor as principais dificuldades do processo de normatização, decorrentes principalmente das questões de política internacional, que atrasam e, de certa forma, impedem que a consolidação da base normativa esteja apta a alcançar os fenômenos jurídicos revelados pelo uso malicioso do ciberespaço; demonstrar que os conceitos clássicos, para os quais o

MIOLO_Poder, Tecnologia e Direito - 2.indd 50 26/04/2024 11:12:06

instituto do uso da força foi edificado, não se adequam aos novos fenômenos oriundos da Era da Informação; demonstrar que o ciberespaço permite que civis comuns participem das hostilidades cibernéticas ativas, ficando vulneráveis aos ataques diretos e a responsabilização penal pelas condutas realizadas; discorrer sobre as características que permitem com que a força cibernética tenha o potencial de causar disrupção no Direito Internacional posto, revelando assim um tipo de uso de força que ainda não é alcançada pelas regras para o *Jus ad Bellum*, uma vez que o instituto do uso da força existente na Carta da ONU se refere, única e exclusivamente, à força armada de portifólio militar; e apresentar casos concretos com a finalidade de, por meio de análise crítica, enumerar as discrepâncias existentes entre a base vigente do Direito Internacional e ao que se propõe como resposta às condutas maliciosas e crimes cometidos, bem como expor as fraquezas, no Direito Internacional, que dão sustentação à presente obra.

Para atingir os objetivos propostos, o trabalho está organizado da seguinte maneira: o capítulo I abordará a questão relacionada ao "Poder na era do cyber", discorrendo sobre o uso geopolítico do ciberespaço, os reflexos para o enfraquecimento da soberania e o fenômeno da pós-territorialidade; o capítulo II discorrerá sobre a "Tecnologia – O Ciberespaço, sua Força e o novo tipo de Conflito do Século XXI", abordando o despertar da força cibernética, o ciberespaço e a guerra cibernética; o capítulo III abordará o "Direito: o emergente Direito Internacional Cibernético", que demonstrará o difícil processo de construção da base normativa para o ciberespaço, principalmente em função da forte influência da política internacional; o capítulo IV abordará a "Disrupção- O impacto do Ciberespaço nos paradigmas de sustentação do Direito Internacional Aplicado aos Conflitos Armados, trazendo a análise jurídica detalhada sobre os principais paradigmas jurídicos que estão sendo atingidos pelo uso malicioso do ciberespaço; e no capítulo V, finalmente, será apresentada a "Realidade – Estudo de casos sobre Operações Cibernéticas Maliciosas que envolveram Estados, no qual serão analisados casos reais a luz do que preconizam as normas existentes, com a finalidade de expor a fragilidade do Direito posto frente aos novos fenômenos da Era da Informação.

A tese sob a qual a presente obra está pautada foi construída por meio de uma pesquisa aplicada de caráter exploratório e descritivo, que buscou identificar os principais efeitos jurídicos gerados em consequência do uso da força cibernética, sob o prisma dos paradigmas do *Jus ad*

MIOLO_Poder, Tecnologia e Direito - 2.indd 51 26/04/2024 11:12:06

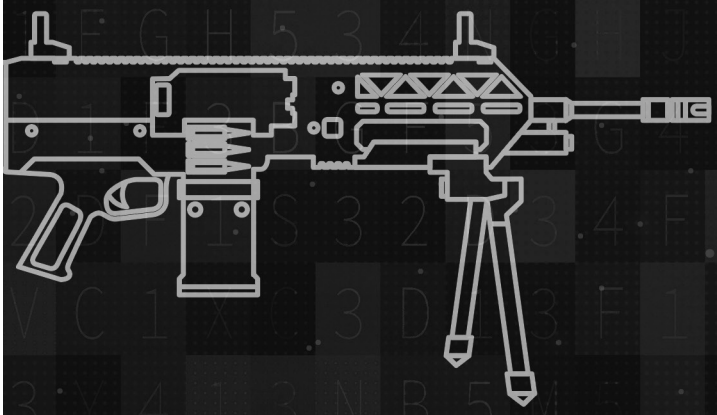
bellum, em situações que não atinjam o limite do dano físico, bem como abordar os aspectos jurídicos do *Jus in bello* decorrentes da participação direta de civis nas hostilidades cibernéticas. Nesse sentido, os resultados foram apresentados de forma qualitativa, a partir da coleta de informações de fontes secundárias, incluindo revisão bibliográfica. Como fontes de pesquisa utilizadas para a busca do referencial teórico, esta obra usufruirá de livros, artigos e sites, relacionados ao tema.

Definido o método, resta elencar os processos metodológicos[31] que foram empregados na elaboração da pesquisa, quais sejam: a) Estudo dogmático-jurídico: este procedimento será utilizado pelo fato de o tema estar vinculado à análise de preceitos de Direito Internacional, envolvendo aí teorias, princípios e doutrinas que buscam explicar a melhor forma de interpretar o assunto; b) Estudo histórico: a análise dos acontecimentos passados é indispensável à compreensão do tema proposto, vez que a essência normativa que regula o conflito armado tem uma forte sustentação no costume internacional; e c) Analítico-sintético: a ser aplicado como incursão analítica nos textos normativos, aplicando-se aos atos e fatos concretos amplamente pesquisados.

31 A formatação da tese de referência para esta obra teve como base os documentos orientativos publicados no site do Instituto CEUB de Pesquisa e Desenvolvimento – ICPD, do Centro Universitário de Brasília – UNICEUB. UNICEUB. Mestrado e Doutorado em Direito. Uniceub, Brasília, 2022. Disponível em: https://www.uniceub.br/pdp/mestrado-e-doutorado/direito/mestrado-e-doutorado-em-direito. Acesso em: 6 dez. 2022.

MIOLO_Poder, Tecnologia e Direito - 2.indd 52 26/04/2024 11:12:06

MIOLO_Poder, Tecnologia e Direito - 2.indd 53 26/04/2024 11:12:06





REFERÊNCIAS

ABBOTT, K.; SNIDAL, D. Hard and Soft Law in International Governance. **International Organization**, [*S. l.*], v. 54, n. 421, 2000. Disponível em: https://www.researchgate.net/publication/4770665_Hard_and_Soft_Law_in_International_Governance. Acesso em: 25 jul. 2023.

ABLON, L.; BOGART, A. **Zero Days, thousands of nights**: the life and times of zeroday vulnerabilities and their exploits. SANTA Monica – CA: Rand Corporation, 2007.

ABRAMS, M; WEISS, J. Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia. Mitre, Austrália, 2008. Disponível em: https://www.mitre.org/news-insights/publication/malicious-control-system-cyber-security-attack-case-study-maroochy-0. Acesso em: 25 jul. 2023.

ACEVES, W.Virtual hatred: how Russia tried to start a race war in the United States (December 19, 2018). **Michigan Journal of Race & Law**, Michigan, v. 24, n. 1, 2019. Disponível em: https://ssrn.com/abstract=3304223. Acesso em: 22 jul. 2020.

ACKERMAN, S.; MACASKILL, E.; ROSS, A. Junaid Hussain: British Hacker for ISIS Believed Killed in US Air Strike. **The Guardian**, New York, 2015. Disponível em: http://www.theguardian.com/world/2015/aug/27/junaid-hussainbritish-hacker-for-isis-believed-killed-in-us-airstrike. Acesso em: 25 jul. 2023.

ADAMS, J. Virtual Defense. **Foreign Affairs**, New York, 2001. Disponível em: https://www.foreignaffairs.com/articles/2001-05-01/virtual-defense. Acesso em: 25 jul. 2023.

AGNEW, J. The Territorial Trap: The Geographical Assumptions of International Relations Theory. **Review of International Political Economy**, v. 1, n. , p. 53-80, 1994. Disponível em: https://doi.org/10.1080/09692299408434268. Acesso em: 25 jul. 2023.

AGO, R. Second Report on State Responsibility—The Origin of International Responsibility. **Yearbook of the International Law Commission**, Europe, v.

MIOLO_Poder, Tecnologia e Direito - 2.indd 873 26/04/2024 11:12:30

II, 1970. Disponível em: https://legal.un.org/ilc/documentation/english/a_cn4_498.pdf. Acesso em: 28 jul. 2023.

AGOSTINHO, S. **A cidade de Deus**. Lisboa: Edição da Fundação Calouste Gulbenkian. 1996.

AKEHURST, M. Custom as a Source of International Law. *In*: ANDRISTYAK, F. **British Contributions to International Law**, 1915-2015 (Set). Holanda: Brill, Nijhoff, v. 47, 1974. Disponível em: https://doi.org/10.1163/9789004386242_025. Acesso em: 25 jul. 2023.

ALBRIGHT, D.; BRANNAN, P.; WALROND, C. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? **Institute for Science and International Security**, Washington, 2010. Disponível em: https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf. Acesso em: 25 jul. 2023.

ALDRICH, G. H. Prospects for United States Ratification of Additional Protocol I to the 1949 Geneva Conventions. **The American Journal of International Law**, Cambridge, v. 85, n. 1, p. 1-20, 1991. Disponível em: https://www.jstor.org/stable/2203556. Acesso em: 25 jul. 2023.

ALEXANDER, K. Attacks on Military Computers Cited, **New York Times**, New York, 2010. Disponível em: https://www.nytimes.com/2010/04/16/world/americas/16military.html. Acesso em: 25 jul. 2023.

ALEXY, R. **Teoria dos Direitos Fundamentais**. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2008.

ALSPACH, K. Ukraine's IT army is doing well, hitting Russia with 'cost and chaos'. **VentureBeat**, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220608145845/https://venturebeat.com/2022/03/04/ukraines-it-army-is-doing-well-hitting-russia-withcost-and-chaos/. Acesso em: 25 jul. 2023.

ALTER, C. U.N. Says Cyber Violence is Equivalent to Physical Violence Against Women, **Time**, Canadá, 2015. Disponível em: https://time.com/4049106/un-cyber-violence-physical-violence/. Acesso em: 25 jul. 2023.

AMBOS, K. Individual Criminal Responsibility for Cyber Aggression. **Journal of Conflict and Security Law**, Northants, v. 21, n. 3, p. 495-504, 2016a. Disponível em: https://doi.org/10.1093/jcsl/krw010. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 874 26/04/2024 11:12:31

AMBOS, K. International Criminal Responsibility in Cyberspace. In: TSAGOURIAS, N.; BUCHAN, R. (eds). **Research Handbook on International Law And Cyberspace and International Law**. Cheltenham: Elgan, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412626. Acesso em: 25 jul. 2023.

AMBOS, K. **Treatise on International Criminal Law**. Oxford: Oxford University Press, 2016b.

ANONYMOUS-UKRAINE, Telegram channel, Ucrânia, 23 March 2022. Disponível em: https://t.me/ciberwars/740 ou https://archive.ph/ShKfQ. Acesso em: 25 jul. 2023.

APPADURAI, A. Soberania sem Territorialidade: notas para uma Geografia pós-nacional. **Novos Estudos - Centro Brasileiro de Análise E Planejamento - CEBRAP**, São Paulo: CEBRAP, n.49, nov.,1997. Disponível em: https://edisciplinas.usp.br/pluginfile.php/236364/mod_resource/content/1/Appadurai-notas_para_uma_geografia.pdf. Acesso em: 25 jul. 2023.

APPLEGATE, S. The Dawn of Kinetic Cyber. *In*: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, 5., 2013, Tallinn. **Proceedings** [**…**]. Taillinn: NATO CCD COE, 2013. Disponível em: https://ccdcoe.org/uploads/2018/10/10_d2r1s4_applegate.pdf. Acesso em: 25 jul. 2023.

APPS, P. Ambiguous Warfare Providing NATO with New Challenges. **Reuters**, [*S. l.*], 2014, Disponível em: http://uk.reuters.com/article/uk-nato-summiti-dUKKBN0GL1KA20140821. Acesso em: 23 jan. 2022.

AREND, A. C. International Law and the Preemptive Use of Military Force. **The Washington Quarterly**, Whasington, v. 26, n. 2, p. 89-103, 2003. Disponível em: https://ciaotest.cc.columbia.edu/olj/twq/spr2003/twq_spr2003a.pdf. Disponível em: 12 jun. 2023

ARQUILLA, J. Twenty Years of Cyberwar. **Journal of Military Ethics**, [*S.l.*], v. 12, n. 1, 2013, p. 80-87. Disponível em: https://doi.org/10.1080/15027570.2013.782632. Acesso em: 25 jul. 2023.

ASHRAF, Cameran. Defining cyberwar: towards a definitional framework. **Defense & Security Analysis**, Londres, v. 37, n. 3, 2021, p. 274-294, Disponível em: https://www.tandfonline.com/doi/full/10.1080/14751798.2021.1959141. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 875 26/04/2024 11:12:31

ASQUITH, P. M.; MORGAN, P. L. Representing a Human-Centric Cyberspace. *AHFE*, 2020. Disponível em: https://orca.cardiff.ac.uk/id/eprint/130447/1/Asquith.Representing.pdf. Acesso em: 25 jul. 2023.

ASSANTE, M. Confirmation of a Coordinated Attack on the Ukrainian Power Grid. **SANS Industrial Control Systems Security Blog**, North Bethesda, 2016. Disponível em: https://www.sans.org/blog/confirmation-of-acoordinated-attack-on-the-ukrainian-power-grid/. Acesso em: 25 jul. 2023.

ATIYAH, P; SUMMERS, R. **Form and Substance in Anglo-American Law.** Oxford: Oxford: Claredon Press, 1991.

AUSTIN, J. **The Province of Jurisprudence Determined**. London: Lawbook Exchange, 1954, p. 134-42.

AUSTRALIAN GOVERNMENT. **Australia's Cyber Security Strategy**: Enabling innovation, growth & prosperity. Austrália: Australia's Cyber Security Strategy, 2009. Disponível em: https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf. Acesso em: 25 jul. 2023.

AZZOPARDI, M. The Tallinn Manual on the International Law Applicable to Cyber Warfare: a brief Introduction on Its Treatment of Jus Ad Bellum Norms. **ELSA Malta Law Review**, Malta, v. 3, 2013. Disponível em: Acesso em: 25 jul. 2023.

BAEZNER, M. **Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions**. ETH: Zurich, 2019.

BAJAK, F. Ukraine digital army brews cyberattacks, intel and infowar. **Voice of America**, Ukraine, 2022. Disponível em: https://web.archive.org/web/20220608141931/https://apnews.com/article/russiaukraine-technology-europe-hacking-f2c4960e48b8022a567780f3602b54e2. Acesso em: 25 jul. 2023.

BAKER, G. Schoolboy hacks into city's tram system. The Telegraph, New York, 2008. Disponível em: https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html. Acesso em: 22 jul. 2023.

BANKS, William, Developing Norms for Cyber Conflict (February 22, 2016). Disponível em: https://ssrn.com/abstract=2736456 or http://dx.doi.org/10.2139/ssrn.2736456. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 876 26/04/2024 11:12:31

BARKHAM, J. Information Warfare and International Law on the Use of Force. **University Journal of International Law and Politics**, New York, v. 34, n. 57, p. 57. 113, 2001. Disponível em: https://universityofleeds.github.io/philtaylorpapers/pmt/exhibits/523/barkham.pdf. Acesso em: 25 jul. 2023.

BARKIN, M. **Law Without Sanctions**. New Haven: Yale University Press, 1967.

BARLOW, J. P. A Declaration of the Independence of Cyberspace. **Electronic Frontier Found**, San Francisco, 1996. Disponível em: http://www.eff.org/cyberspace-independence. Acesso em: 25 jul. 2023.

BARROSO, L. R. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009.

BARROSO, L. R. O Constitucionalismo Democrático ou Neoconstitucionalismo como ideologia vitoriosa do século XX. **Revista Publicum**, Rio de Janeiro, v. 4, ed. comemorativa, 2018, p. 14-36. Disponível em: http://www.e-publicacoes.uerj.br/index.php/publicum. Acesso em: 25 jul. 2023.

BARROSO, L. R. Revolução tecnológica, crise da democracia e mudança climática: limites do direito num mundo em transformação. **Revista Estudos Institucionais**, Rio de Janeiro, v. 5, n. 3, 2019. Disponível em: https://doi.org/10.21783/rei.v5i3.429. Acesso em: 25 jul. 2023.

BASS, W. A Surpise Out of Zion? *In*: **A Surprise Out of Zion?:** Case Studies in Israel's Decisions on Whether to Alert the United States to Preemptive and Preventive Strikes, from Suez to the Syrian Nuclear Reactor (pp. 45–60).Santa Monica: Rand Corporation, 2015. Disponível em: https://www.jstor.org/stable/10.7249/j.ctt19w73b6.10. Acesso em: 12 fev. 2022.

BASSO, D. French army hails Ukraine's cyber defence 'revolution'. **Euractivi**, Brussels, 2023. Disponível em: https://www.euractiv.com/section/politics/news/french-army-hails-ukraines-cyber-defence-revolution/. Acesso em: 25 jul.2023.

BASTOS JUNIOR, L. M. P. Territorialidade, soberania e constituição: as bases institucionais do modelo de estado territorial soberano. **Novos Estudos Jurídicos**, Itajaí, v. 19, n. 1, p. 181-200, 2014. Disponível em: https://doi.org/10.14210/nej.v19n1.p181-200. Acesso em: 25 jul. 2023.

BBC. China Denounces US Cyber-theft Charges. BBC, [*S.l.*], 2014. Disponível em: http://www.bbc.com/news/world-us-canada-27477601. Acesso em: 25 jul. 2023

MIOLO_Poder, Tecnologia e Direito - 2.indd 877 26/04/2024 11:12:31

BBC. Estonia hit by Moscow cyber war. BBC News, Reino Unido, 2007. Disponível em: http://news.bbc.co.uk/2/hi/europe/6665145.stm. Acesso em: 25 jul. 2023.

BBC. Hollande: Bugging Allegations Threaten EU-US Trade Pact. BBC, [*S.l.*], 2013b. Disponível em: http://www.bbc.com/news/world-us-canada-23125451. Acesso em: 25 jul. 2023

BBC. Merkel Calls Obama about 'US Spying on Her Phone. BBC News, [*S.l*], 2013a. Disponível em: http://www.bbc.com/news/world-us-canada-24647268. Acesso em: 25 jul. 2023.

BBC. Theresa May Accuses Vladimir Putin of Election Meddling, BBC News, [*S.l.*], 2017. Disponível em: https://perma.cc/HJ5P5NAF. Acesso em: 25 jul.2023.

BELLINGER, J. B.; HAYNES, W. J. Carta a Jakob Kellinberger, CICV. U.S. Initial Reactions to CICV Study on Customary International Law, Whashington, 2006. Disponível em: http://2001-2009.state.gov/s/l/rls/82630.htm. Acesso em: 25 jul. 2023.

BENTHAM, J. **Introduction to the Principles of Morals and Legislation**. London: CreateSpace Independent Publishing Platform, 1780.

BERNARDES, G. L.; CHOY, M. A. L. O poder de polícia do Exército brasileiro – uma análise. Publica Direto, [*S.l.*], 2005. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/manaus/direito_e_politica_guilherme_bernardes_e_marco_de_lima_choy.pdf. Acesso em 29 jul. 2023.

BERNSTEIN, S.; BLANKSTEIN, A. Key signals targeted, officials say. **Los Angeles Times**, Los Angeles, California, 2007. Disponível em: https://www.latimes.com/archives/la-xpm-2007-jan-09-me-trafficlights9-story.html. Acesso em: 25 jul. 2023.

BETZ, D. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. **Journal of Strategic Studies**, London, v. 35, n. 5, 2012, p. 689-711, Disponível em: https://doi.org/10.1080/01402390.2012.706970. Acesso em: 25 jul. 2023.

BEYER, J. L. The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland. **Journal of Computer-Mediated Communication**, [*S.l.*], v. 19, n. 2, p. 141–154, 2014. Disponível em: https://doi.org/10.1111/jcc4.12050. Acesso em: 25 jul. 2023.

BIGELOW, B. The topography of cyberspace and its consequences for operations. *In*: INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON), 10.,

MIOLO_Poder, Tecnologia e Direito - 2.indd 878 26/04/2024 11:12:31

2018, Tallinn, Estonia. **Proceedings [...]**, Tallinn, 2018, p. 123-138. Disponível em: https://ieeexplore.ieee.org/document/8405014. Acesso em: 11 jun. 2022.

BIGGERSTAFF, W. C. Ukraine Symposium – photos of the dead. Lieber Institute. **West Point**, New York, 2022. Disponível em: https://lieber.westpoint.edu/photos-of-dead/. Acesso em: 25 jul. 2023.

BIGGERSTAFF, W. C. The status of Ukraine's "IT Army" under the Law of Armed Conflict. **Lieber Institute- West Point**, New York, 2023. Disponível em: https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/. Acesso em: 25 jul. 2023.

BLANK, L. R. International law and cyber threats from non-state actors. **International Law Studies**, England, v. 89, n. 406, 34 p., 2013. Disponível em: https://ssrn.com/abstract=2194180. Acesso em: 25 jul. 2023.

BLANK, S. Web war I: is Europe's first information war a new kind of war? **Taylon & Francis Online Journal**, [*S.l.*], v. 3, n. 2, p. 227-247, 2008. Disponível em: https://doi.org/10.1080/01495930802185312. Acesso em: 25 jul. 2023.

BLACK, J. **Western Warfare, 1775-1882**. Bloomington: Indiana Univ. Press, 2001.

BLINDERMAN, E.; DIN, M. Hidden by sovereign shadows: improving the domestic framework for deterring state-sponsored cybercrime. **Vanderbilt Journal of Transnational Law**, Nashville, v. 50, 2017. Disponível em:

BLOUNT, P. J. Reprogramming the World: Cyberspace and the Geography of Global Legal Order. **E-International Relations Press**, [*S.l.*], 2019. Disponível em: https://www.e-ir.info/publication/reprogramming-the-world-cyberspace-and-the-geography-of-global-order/s. Acesso em: 20 jul. 2023.

BÖCKENFÖRDE, E.-W. Demokratie als Verfassungsprinzip. *In*: ISENSEE, J.; KIRCHHOF, P. **Handbuch des Staatsrechts der Bundesrepublick Deutschland (HStR)**. 3. ed. Heidelberg: Müller, 2004, p. 289, 322.

BOGDANDY, A.; DELLAVALLE, S. Universalism and Particularism as Paradigms of International Law. **Institute For International Law And Justice New York University School of Law**, New York, 2008. Disponível em: https://iilj.org/wp-content/uploads/2016/08/Bogdandy-etal-Universalism-and-Particularism-as-Paradigms-of-International-Law-2008-1.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 879 26/04/2024 11:12:31

BOGDANDY, A. v. Legislação governamental: uma redefinição da legislação e do sistema de governo no âmbito da Lei Básica na perspectiva da dogmática europeia comum. **Jus publicum**, Mohr Siebeck, 2000. Disponível em: https://www.mohr-siebeck.com/uploads/tx_sgpublisher/produkte/leseproben/9783161471711.pdf. Acesso em: 23 jul. 2023.

BORGEN, C. Harold Koh on International Law in Cyberspace. Opinio Juris, [*S.l.*], 2012. Disponível em: http://opiniojuris.org/2012/09/19/harold-koh-on--international-law-in-cyberspace. Acesso em: 25 jul. 2023.

BOTHE, M.; PARTSCH, K. J.; SOLF, W. **New rules for victims of armed conflicts**. Leiden: Martinus Nijhoff Publishers, 1982, 289 p. Disponível em: https://www.corteidh.or.cr/tablas/16299.pdf. Acesso em: 25 jul. 2023.

BOWETT, D. W. **Self-Defence in International Law**. Manchester: **The Lawbook Exchange, Ltd.**, 1958.

BRASIL. **Decreto n. 592, de 6 de julho de 1992**. Promulga o Pacto Internacional sobre Direitos Civis e Políticos, e dá outras providências. Brasília: Independência República, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 11 fev.2023.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília: Presidência da República, 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm. Acesso em: 17 fev. 2023.

BRASIL. **Decreto nº 19.841, de 22 de Outubro de 1945**. Promulga a Carta das Nações Unidas, da qual faz parte integrante o anexo Estatuto da Corte Internacional de Justiça, assinada em São Francisco, a 26 de junho de 1945, por ocasião da Conferência de Organização Internacional das Nações Unidas. Rio de Janeiro:Coleção de Leis do Brasil de 1945, Poder Executivo, 1945.

BRASIL. De**creto nº 24.557, de 3 de julho de 1934**. Promulga o Tratado de Renúncia à Guerra, concluído e assinado em Paris em 27 de agosto de 1928. Rio de Janeiro: Câmara dos Deputados, 1934.

BRASIL. **Decreto nº 4.388 de 25 de setembro de 2002**. Promulga o Estatuto de Roma do Tribunal Penal Internacional. Brasília: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/2002/d4388.htm. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 880 26/04/2024 11:12:31

BRASIL. **Decreto nº 42.121, de 21 de agosto de** 1957.,. Promulga as Convenções concluídas em Genebra, a 12 de agôsto de 1949, destinadas a proteger as vitimas da guerra. Rio de Janeiro: Independência da República, 1957. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D42121.htm. Acesso em: 25 jul. 2023.

BRASIL. **Decreto nº 56.435, de 8 de junho de 1965**. Promulga a Convenção de Viena sôbre Relações Diplomáticas. Coleção de Leis do Brasil de 1965, Poder Executivo, Brasília: Presidência da República, 1965. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/antigos/d56435.htm. Acesso em: 25 jul. 2023.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: 11 fev.2023.

BRASIL. **Decreto nº 7.030, de 14 de dezembro de 2009.** Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos Artigos 25 e 66. Brasília: Presidência da República, 2009. Art. 2 (1) (a). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d7030.htm. Acesso em: 25 jul. 2023.

BRASIL. **Decreto nº 849, de 25 de junho de 1993**. Promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. Brasília: Independência da República, 1993. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0849.htm. Acesso em: 25 jul. 2023.

BRASIL. **Estado-Maior Cionjunto das Forças Armadas**: doutrina militar de defesa cibernética. 1. ed. Brasília: Ministério da Defesa, 2014.

BRASIL. **Fundamentos do Poder Nacional**. Rio de Janeiro: ESG, 2019. 164 p. Disponível em: https://www.gov.br/esg/pt-br/centrais-de-conteudo/publicacoes/fundamentos-do-poder-nacional/FPN2022.pdf. Acesso em: 25 jul. 2023.

BRASIL. **Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2020b.

BRAUN, S. Ukraine's info warriors battling Russian trolls. DW, Berlin, 2022. Disponível em: https://www.dw.com/en/nafo-ukraines-info-warriors-battlin-grussian-trolls/a-63124443. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 881 26/04/2024 11:12:31

BRENNER, J. **America the Vulnerable**: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. New York: Penguin Press, 2011.

BRENNER, S. **Cyber Threats**: The Emerging Fault Lines of The Nation State. Oxford: Oxford Academic, 2009. Disponível em: https://doi.org/10.1093/acprof:oso/9780195385014.001.0001. Acesso em: 25 jul. 2023.

BREWSTER, T. Ukraine Starts Using Facial Recognition To Identify Dead Russians And Tell Their Relatives. **Forbes**, Jersey City, 2022. Disponível em: https://www.forbes.com/sites/thomasbrewster/2022/03/23/ukraine-starts-using-facial-recognition-to-identify-dead-russians-and-tell-their=-relatives/?shf5b58ac28985. Acesso em: 25 jul. 2023.

BRITO, J.; WATKINS, T. Loving the Cyber Bomb - The Dangers of Threat Inflation in Cybersecurity Policy. **Harvard National Security Journal**, Cambridge, v. 3, n. 1, p. 39-84, 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1830625. Acesso em: 25 jul. 2023.

BROAD, W.; MARKOFF, J.; SANGER, D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. **New York Times**, New York, 2011. Disponível em: http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Acesso em: 25 jul. 2023.

BRONK, C.; COLLINS, G.; WALLACH, D. Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In? **Baker Institute for Public Policy**, Houston, 2022. Disponível em: https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months. Acesso em 25 jul. 2023.

BROOKS, R. **Rule of Law in The Gray Zone. Modern War Institute at West Point**. New York, 2018. Disponível em: https://mwi.westpoint.edu/rule-law--gray-zone/. Acesso em: 26 jul.2023.

BROWN, D. A Proposalfor an International Convention to Regulate the Use of *Information* Systems in Armed Conflict. **Harvard International Law Journal**, Harvard, v. 47, n. 1, p. 179-221, 2006. DIsponível em: https://api.semanticscholar.org/CorpusID:140858047. Acesso em: 25 jul. 2023.

BROWN, G.; TULLOS, O. On the Spectrum of Cyberspace Operations. **Small Wars Journal**, Maryland, 2012. Disponível em: www.smallwarsjournal.com/print/13595. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 882 26/04/2024 11:12:31

BROWNLIE, I. **International Law and the Use of Force by States**. Oxford: Oxford Academic. 1963. Disponível em: https://www.corteidh.or.cr/tablas/3945.pdf. Acesso em: 25 jul. 2023.

BRUNKHORST, H. Alguns problemas conceituais e estruturais do cosmopolitismo global. **Revista Brasileira de Ciências Sociais**, São Paulo, v. 26, n. 76, 2011. Disponível em: https://www.scielo.br/pdf/rbcsoc/v26n76/02.pdf. Acesso em: 18 jan. 2023.

BRUNNÉE, J.; MESHEL, T. Teaching an old law new trick: international environmental law lessons for cyberspace governance. **German Yearbook of International Law**, [*S.l.*], v. 58, 2015. Disponível em: https://ssrn.com/abstract=2791558. Acesso em: 17 fev. 2023.

BUCHAN, R. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? **Journal of Conflict and Security Law**, Oxford, v. 17, n. 2, 2012, p. 212-27. Disponível em: https://doi.org/10.1093/jcsl/krs014. Acesso em: 25 jul. 2023.

BUCHAN, R.; TSAGOURIAS, N. Ukranian 'IT Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities? EJIL:Talks. Blog of the European Journal of International Law.Mar. 2022.

BUND, J. Cybersecurity and democracy Hacking, leaking and voting. **European Union Institute for Security Studies**, [*S.l.*], 2016. Disponível em: https://www.iss.europa.eu/content/cybersecurity-and-democracy-hacking-leaking-and-voting. Acesso em: 10 jul. 2023.

CAMPEN, A. D.; DEARTH, D. H.; GOODDEN, R. T. **Cyberwar: Security, Strategy, and Conflict in the Information Age** (AFCEA International Press Fairfax, VA, 1996). Moseley: 'The Nation's Guardians: America's 21st Century Air Force, 1996.

CAPORASO, J. Changes in the Westphalian order: territory, public authority, and sovereignity. *In*: CAPORASO, J. **Continuity and change in the Westphalian order**. Malden, USA; Oxford, UK: Blackwell Publishers, 2000.

CARNEIRO, R. L. A Theory of the Origin of the State. **Science**, Washington, v. 169, n. 3947, p. 733-738, 1970. Disponível em: Acesso em: 25 jul. 2023.

CARTA AZERBAIJÃO - Carta datada de 6 de setembro de 2012 do Charge' d'affaires a.i. da Missão Permanente do Azerbaijão junto às Nações Unidas dirigida ao Secretário-Geral, 7 setembro 2012, UN Doc. A/66/897–S/2012/687, p. 1.

MIOLO_Poder, Tecnologia e Direito - 2.indd 883 26/04/2024 11:12:31

CAVALCANTI FILHO, T. **O problema da segurança no direito**. São Paulo: RT, 1964.

CHAUMETTE, A.-L. International Criminal Responsibility of Individuals in Case of Cyberattacks. **International Criminal Law Review**, [*S.l.*], v. 18, 2018. Disponível em: https://brill.com/view/journals/icla/18/1/article-p1_1.xml. Acesso em: 25 jul. 2023.

CHECKOWAY, S; MCCOY, D. Comprehensive experimental analyses of automotive attack surfaces. *In*: USENIX SECURITY SYMPOSIUM, 20., 2011, San Francisco. **Proceedings [...]**, San Francisco: Usenix, 2011.

CHIK, W. B. Customary Internetional Law: Creating a Body of Customary Law for Cyberspace. **Computer Law and Security Review**, [*S.l.*], v. 26, n. 1, p. 3-22, 2010. Disponível em: https://ink.library.smu.edu.sg/solresearch/842. Acesso em: 25 jul. 2023.

CHINA Military Science. *In*: **China's National Defense in a New Era**. Beijing: Foreign Languages Press, 2019. Disponível em: http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc Acesso em: 25 jul. 2023.

CHOUCRI, N. **Co-Evolution of Cyberspace and International Relations***:* new challenges for the Social Sciences. Montreal, Canada: World Social Science Forum (WSSF), 2013.

CICV - INTERNATIONAL COMMITTEE OF THE RED CROSS. **As Convenções de Genebra de 12 de agosto de 1949**. Geneva: CICV, 1949. Disponível em: https://www.icrc.org/pt/publication/convencoes-de-genebra-de-12-de-agosto-de-1949. Acesso em: 25 jul. 2023.

CICV - INTERNATIONAL COMMITTEE OF THE RED CROSS. **Comentários de 1960 atualizados trazem um olhar renovado sobre a contínua relevância das Convenções de Genebra.** Geneva: CICV,1960. Disponível em: https://www.icrc.org/pt/document/comentarios-atualizados-trazem-um-olhar-renovado-sobre-continua-relevancia-das-convencoes. Acesso em: 25 jul. 2023.

CICV - INTERNATIONAL COMMITTEE OF THE RED CROSS. **Convention (III) relative to the Treatment of Prisoners of War 1949**. Article 4 – Prisioners of war. Geneva: CICV. 2020. Disponível em: https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-4/commentary/2020?activeTab=undefined. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 884 26/04/2024 11:12:31

CICV - INTERNATIONAL COMMITTEE OF THE RED CROSS. **International Humanitarian Law and the Challenges of Contemporary Armed Conflicts – Report**. Geneva, Switzerland: cicv, 2011. Disponível em: https://www.icrc.org / en /doc/ assets/ files/ red-cross-crescent-movement/ 31st-international-conference/ 31-int-conference-ihl- challenges- report- 11- 5-1- 2-en.pdf. Acesso em: 25 jul. 2023.

CICV - INTERNATIONAL COMMITTEE OF THE RED CROSS. **International humanitarian law and the challenges of contemporary armed conflicts**. Geneva: CICV, 2015. Disponível em: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts. Acesso em: 25 jul. 2023.

CICV– INTERNATIONAL COMMITTEE OF THE RED CROSS. **The Use of Force in Armed Conficts: Interplay Between the Conduct of Hostilities and Law Enforcement Paradigms**. Genebra, Suíça; CICV, 2013. Disponível em: 25 jul. 2023.

CLARK, D. Characterizing cyberspace: past, present and future. **Massachusettes Institute of Technology - MIT, CSAIL**, Massachusettes 2010. Disponível em: https://ecir.mit.edu/sites/default/files/documents/%5BClark%5D%20Characterizing%20Cyberspace-%20Past%2C%20Present%20and%20Future.pdf. Acesso em: 29 maio 2023.

CLARKE, R. A. War from Cyberspace. **The National Interest online**, [*S.l.*], 2009. Disponível em: http://www.nspm.rs/nspm-in-english/war-from-cyberspace.html?alphabet=c. Acesso em:25 jul. 2023.

CLARKE, R. A.; KNAKE, R. **Cyber War**: The Next Threat to National Security and What to Do About It. 6. ed., New York: Ecco, 2012.

CLARKE, R. A.; KNAKE, R. K. **Cyber War**: The Next Threat to National Security and What to Do About It. New York: **Ecco Press,** 2010.

CLAUSEWITZ, C. v. **On War**. Harmondsworth: Penguin Books, 1982.

CLAVERIE, B.; *et al*. Cognitive warfare. NATO-STO Collaboration Support Office. **NATO's Strategic Warfare Development Command**, Norfolk, 2023. Disponível em: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/#:~:text=Together%2C%20these%20two%20words%20paint,cognitions%20to%20gain%20an%20advantage. Acesso em: 25 jul.2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 885 26/04/2024 11:12:31

CLOVER, C. Kremlin-Backed Group Behind Estonia Cyber Blitz. **Financial Times**, London, 2009. Disponível em: www.ft.com/techblog. Acesso em: 27 out. 2010.

CLULEY, G. Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces. **Bitdefender**, [*S.l.*], 2022. Disponível em: https://web.archive.org/web/20220608141452/https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/. Acesso em: 25 jul. 2023.

COHEN, J. E. Cyberspace As/And Space. **Georgetown Law Faculty Publications and Other Works**, [*S.l.*], v. 807, 2007. Disponível em: https://scholarship.law.georgetown.edu/facpub/807. Acesso em: 29 jun. 2023.

COLEMAN, V. Cyber Attack Causes Rutgers Internet Service Interruptions. **NJ Advance Media for NJ.com**, New Jersey, 2015. Disponível em:

COMENTÁRIO DO CICV 2020 ao GC III, para. 1013-14. 2020. Disponível em: https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-4/commentary/2020?activeTab=undefined. Acesso em: 23 jun. 2023.

COMENTÁRIO DO CICV 1987 ao PA I, para. 1672. 1987. Disponível em: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-43/commentary/1987?activeTab=undefined. Acesso em 23 jun. 2023.

COMISSÃO PÚBLICA para Examinar o Incidente Marítimo de 31 de maio de 2010. **Prime Minister's Office**, [*S.l.*], janeiro de 2010. Disponível em: http://www.gov.il/en/departments/general/turkel_committee. Acesso em: 30 set. 2013.

COMMON CRITERIA for Information Technology Security Evaluation. SO/IEC 15408-1:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model. Disponível em: https://ccsp.alukos.com/standards/iso-iec-15408-1-2022/. Acesso em: 23 jun. 2023.

CONVENTION IV- respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. **The Hague Academy of International Law**, The Netherlands, **Netherlands,** 1907. Disponível em: https://ihl-databases.icrc.org/assets/treaties/195-IHL-19-EN.pdf. Acesso em: 25 jun. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 886 26/04/2024 11:12:31

CONVENTION V- respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. **The Hague Academy of International Law**, The Netherlands, Netherlands, 1907. Disponível em: https://www.refworld.org/pdfid/3ddca4e14.pdf. Acesso em: 25 jul. 2023.

CORN, G. Unarmed but How Dangerous? Civilian Augmentees, the Law of Armed Conflict, and the Search for a More Effective Test for Permissible Civilian Battlefield Functions. **Journal of National Security Law & Policy**, [*S.l.*], v. 2, n. 257, 2008. Disponível em: https://jnslp.com/wp-content/uploads/2010/08/02_cornJCS111008-PR.pdf. Acesso em: 25 jul. 2023.

CORN, G.; O'CONNOR, P. J. M; TAYLOR, R. Sovereignty in the Age of Cyber. **Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0**, Geneva, v. 111, 2017. Disponível em: https://www.researchgate.net/publication/319230444_Sovereignty_in_the_Age_of_Cyber. Acesso em: 25 jul. 2023.

CORTEN, O. 'Article 52'. *In*: CORTEN, O.; KLEIN, P. (eds). **The Vienna Conventions on the Law of Treaties: A Commentary**. Oxford: Oxford University Press, 2011, p. 1205-1211.

COUTINHO, M. O que são 'trolls' e o que é 'trollagem'? **Techtudo**, São Paulo, 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/06/o-que-sao-trolls-e-o-que-e-trollagem.html. Acesso em: 17 ago. 2020.

COUTO, S. S.; CLEARY, K. The Gravity Threshold of the International Criminal Court. **American University International Law Review**, Whashington, v. 23, p. 850-4, 2008. Disponível em: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1046&context=facsch_lawrev. Acesso em: 17 ago. 2020.

CRAWFORD, E. Armed Ukrainian Citizens: Direct Participation in Hostilities, Levée en Masse, or Something Else? **European Journal of International Law – EJIL**, [*S.l.*],. 2022. Disponível em: https://www.ejiltalk.org/armed-ukrainian-citizens-direct-participation-in-hostilities-levee-en-masse-or-something-else/. Acesso em: 25 jul. 2023.

CRAWFORD, M. Utility hack led to security overhaul. **Computerworld**, [*S.l.*], v. 2006, p. 1–2, 2006. DIsponível em: https://www.computerwoche.de/a/utility-hack-led-to-security-overhaul,572421. Acesso em: 25 jul. 2023.

CREVELD, M. v. **Technology and War**: From 2000 B.C. to the Present. New York: The Free Press, 1989.

MIOLO_Poder, Tecnologia e Direito - 2.indd 887 26/04/2024 11:12:31

CRIMINAL COURT FOR FORMER YUGOSLAVIA (ICTY) - Prosecutor v. Tadić, Case No. IT-94-1-A, Judgment of the Chamber of Appeals, ¶ 400 (Intl'l Crim. Trib. for the Former Yugoslavia 15 July 1999. Disponível em: https://www.icty.org/en/sid/7749. Acesso em: 23 jun. 2023.

CRIMINAL COURT FOR FORMER YUGOSLAVIA (ICTY) -. Prosecutor v. D. Tadić, Appeals Chamber, Decision of 2 October 1995, case IT-94-1-AR72, paras. 70. Disponível em: https://www.refworld.org/cases,ICTY,47fdfb520.html. Acesso em: 20 de jun. 2023.

CRIMINAL COURT FOR FORMER YUGOSLAVIA (ICTY) - Prosecutor v. Kunarac et al., Case No. 96-23, Judgment of February 22, 2001 (Trial Chamber), § 416, confirmed by the Appeals Chamber in its judgment in the same case of June 12, 2002, § 89). Disponível em: https://www.icty.org/en/sid/8018. Acesso em: 22 jun. 2023.

CRIMINAL COURT FOR FORMER YUGOSLAVIA (ICTY) - Prosecutor v. Strugar, Case No. IT-01-42-T, Judgment (Int'l Crim. Trib. for the Former Yugoslavia Jan. 31, 2005). Disponível em: https://www.icty.org/en/sid/8655. Acesso em: 20 jul. 2023.

CRONIN, A. K. Cyber-Mobilization: The New Levée en Masse. **Parameters**, [*S.l.*], v. 36, n. 2, 2006. Disponível em: https://press.armywarcollege.edu/parameters/vol36/iss2/7/. Acesso em: 25 jul. 2023.

CYBER COSSACKS. DDoS Attack. Telegram channel, 2022. Disponível em:

CYBERFIRE Chat. Telegram channel, 18 March 2022. Disponível em: https://t.me/cyberfirechatt/52321 ou https://archive.ph/niCZo. Acesso em: 25 jul. 2023.

CYBERPALYANITSA. Telegram channel, 18 March 2022. Disponível em: https://t.me/CyberPalyanitsa/215 ou https://archive.ph/ZKC. Acesso em: 25 jul. 2023.

CYBERSPACE. Part 1: Developing Rules for Transitioning Custom into Law. *Computer Law and Security Review*, v. 26, n. 1, p. 3-22, 2010. Disponível em: https://ink.library.smu.edu.sg/sol_research/842. Acesso em: 12 jan. 2023.

CZOSSECK, C. State Actors and their Proxies in Cyberspace. *In*: ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Tallinn: International Law, International Relations and Diplomacy; NATO CCD COE Publication, 2013.

MIOLO_Poder, Tecnologia e Direito - 2.indd 888 26/04/2024 11:12:31

DAHRENDORF, R. **Der moderne soziale Konflikt**. Stuttgart: Deutsche Verlags--Anstalt, 1992, 282 f.

DAMROSCH, L. F. Politics Across Borders: Nonintervention and Nonforcible Influence over Domestic Affairs. **The American Journal of International Law**, Cambridge, v. 83, 1989. Disponível em: https://www.jstor.org/stable/2202789. Acesso em: 25 jul. 2023.

DAVIS, J. Hackers Take Down the Most Wired Country in Europe. **Wired Magazine**, New York, 2007. Disponível em: https://www.wired.com/2007/08/ff-estonia/. Acesso em: 25 jul. 2023.

DAVIS, J.; LEWIS, C. Beyond the United Nations Group of governmental experts. **The Cyber Defense Review**, New York, p. 161-168, 2019. Disponível em: https://www.jstor.org/stable/26846126. Acesso em: 1 fev. 2023.

DECLARAÇÃO OFICIAL. Comitê Internacional da Cruz Vermelha de 8 de março de 2001 para as Consultas Globais do Alto Comissariado das Nações Unidas para Refugiados sobre Proteção Internacional. **International Committee of the Red Cross**, Geneva, 2001. Disponível em: https://www.icrc.org/en/doc/resources/documents/statement/57jqwh.htm. Acesso em: 23 jul. 2023.

DEGUZMAN, M. M. Gravity and the Legitimacy of the International Criminal Court. **Fordham International Law Journal**, New York, v. 32, n. 5, 2009. Disponível em: https://core.ac.uk/download/pdf/144226632.pdf. Acesso em: 25 jul. 2023.

DEIBERT, R. **Black Code: Surveillance, Privacy, and the Dark Side of the Internet**. Toronto: Signal, 2013.

DELIBASIS, D. **The Right to National Self-Defense: In Information Warfare Operations**. Canberra: Arena Books Limited, 2007.

DEMCHAK, C. C. Economic and Political Coercion and a Rising Cyber Westphalia. *In:* ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Tallinn: International Law, International Relations and Diplomacy, NATO CCD COE Publication, 2013.

DENARDIS, L. Protocol Politics: The Globalization of Internet Governance (Information Revolution and Global Politics). **The MIT Press**, New York, 2009. Disponível em: https://www.jstor.org/stable/j.ctt9qf9sh. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 889 26/04/2024 11:12:31

DENNIS, M. Application of Human Rights Treaties Extraterritorially During Times of Armed Conflict and Military Occupation. **American Journal of International Law**, Cambridge, v. 99, 2005, pp. 119-141. Disponível em: https://www.jstor.org/stable/25660067. Acesso em: 25 jul. 2023.

DEPARTMENT OF THE NAVY. **The Commander's Handbook on the Law of Naval Operations**. Monterey: Department of Homeland Security, 2007. Disponível em: https://www.ca1.uscourts.gov/sites/ca1/files/citations/MCTP%2011-10B%20%28%20Formerly%20MCWP%205-12.1%29.pdf. Acesso em: 25 jul. 2023.

DIAMOND, J. U.S. Rejects POW Label. **Chigaco Tribune**, Chicago 2002. Disponível em: https://www.chicagotribune.com/ct-xpm-2002-01-28-0201280167-story.html. Acesso em: 25 jul. 2023.

DIAS, T. S. Propaganda and Accountability for International Crimes in the Age of Social Media: revisiting accomplice liability in ` international criminal law. **Opinio Juris**, Oxford, 2018. Disponível em: http://opiniojuris.org/2018/04/04/propaganda-and-accountability-for-international-crimes-in--the-age-of-social-media-revisiting-accomplice-liability-in-international-criminal-law/. Acesso em: 25 jul. 2023.

DILANIAN, K. Iran and the Era of Cyber War. **L.A. Times**, Los Angeles, 2011.

DINNISS, H. H. **Cyber Warfare and the Laws of War** (Cambridge Studies in International and Comparative Law). Cambridge: Cambridge University Press, 2012.

DINNISS, H. H. Cyber Warriors, Patriotic Hackers and the Laws of War. **International Humanitarian Law & The Changing Technology of War**, Leiden, v. 269, 2013. Disponível em: https://brill.com/display/book/edcoll/9789004229495/B9789004229495-s013.xml. Acesso em: 24 jul. 2023.

DINSTEIN, Y. Computer Network Attacks and Self-Defense. **Computer Network Attack And International Law**, Newport, v. 76, p.103-105, 2002. Michael N. Schmitt & Brian T. O'Donnell (eds.). Disponível em: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1397&context=ils. Acesso em: 25 jul. 2023.

DINSTEIN, Y. **The Conduct of Hostilities under the Law of International Armed Conflict**. Cambridge: Cambridge University Press, 2004.

DINSTEIN, Y. **War, aggression, and Self-defense**. 4. ed. Cambridge: CUP, 2005.

MIOLO_Poder, Tecnologia e Direito - 2.indd 890 26/04/2024 11:12:31

DINSTEIN, Y. The Interaction between Customary International Law and Treaties. Brill, Niijhoff, v. 322, 2007. Disponível em: https://referenceworks.brillonline.com/entries/the-hague-academy-collected-courses/*A9789004161016_02 . Acesso em: 22 jul. 2023.

DISBALANCER Ukraine, Telegram chat, 18 March 2022. Disponível em: https://t.me/c/1701910482/50239. Acesso em: 25 jul. 2023.

DOCUMENTOS da Conferência das Nações Unidas sobre Organização Internacional, vol. VI, 1945, p. 559, 720-721, 1945. Disponível em: https://digitallibrary.un.org/record/1300969. Acesso em: 20 jun. 2023.

DOLINGER, J. Ordem pública mundial: ordem pública verdadeiramente internacional no direito internacional privado. **Revista de Informação Legislativa**. Brasília, v. 23, n. 90, 1986. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/181712. Acesso em: 25 jul. 2023.

DÖRMANN, K. The Applicability of the Additional Protocols to Computer Network Attacks: an ICRC viewpoint. BYSTRÖM, K. (ed.). **International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law**. Stockholm- Sweden: Swedish National Defence College, 2004, n. 16, p.17–19. Disponível em: http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/68lg92?opendocument. Acesso em: 25 jul. 2023.

DRAPER, G. I. A. D. The implementation and enforcement of the Geneva Conventions of 1949 and of the two additional protocols of 1979, Recueil des Cours. **The Hague Academy of International Law**, The Netherlands, v. 164, n. III, 1979.

DROEGE, C. Get off My Cloud: cyber warfare, International Humanitarian Law, and the Protection of Civilians, **International Review of The Red Cross**, Genebra, v. 94, n. 886, 2012. Disponível em: https://international-review.icrc.org/sites/default/files/irrc-886-droege.pdf. Acesso em: 25 jul. 2023.

DUVERGER, M. **Os partidos políticos**. Rio de Janeiro: Zahar, 1970.

DYSON, E. **Release 2.0:** a design for living in the digital age. Estados Unidos: Broadway Books, 1997.

ECONOMIST. Estonia and Slovenia. New York, 2005. Disponível em: https://www.economist.com/europe/2005/10/13/when-small-is-beautifully-successful. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 891 26/04/2024 11:12:31

ECTHR, Andronicou and Constantinou v. Cyprus, 9 October 1997, para. 194. ECtHR, Kerimova amd Others v. Russia, 3 May 2011, 1997.

ECTHR, A. S. *et al*. Reino Unido, 7 de julho de 2011. Anexo 3: Declaração escrita de Françoise Hampson; Apêndice 6: Resumo da apresentação de Olga Chernishova.

EFRONY, D.; SHANY, Y. A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice. **American Journal of International Law**, Cambridge, v. 112, n. 4, p. 583-657, 2018. Disponível em: https://doi.org/10.1017/ajil.2018.86. Acesso em: 12 jul. 2023.

EGAN, B. International Law and Stability in Cyberspace. **Berkeley Journal of International Law**, California, v. 31, n. 1, 2017. Disponível em: https://www.law.berkeley.edu/wp-content/uploads/2016/12/BJIL-article-International-Law-and--Stability-in-Cyberspace.pdf. Acesso em: 25 jul. 2023.

EICHENSEHR, K. E. Cyberwar & International Law Step Zero. **Texas International Law Journal**, Texas, v. 50, n. 2 & 3, 2015b, p.357-80. Disponível em: https://texashistory.unt.edu/ark:/67531/metapth838918/. Acesso em: 25 jul. 2023.

EICHENSEHR, K. E. The Cyber-Law of Nations. **Georgetown Law Journal**, New Jersey, v. 103, 2015a. Disponível em SSRN: https://ssrn.com/abstract=2447683. Acesso em: 20 jun. 2023.

ELBE, V. The Evolution of the Concept of the Just War in International Law. **The American Journal of International Law**, London, v. 33, p. 665-688, 1939. Disponível em: https://www.jstor.org/stable/2192879. Acesso em: 25 jul. 2023.

EPPSTEIN, J. **The Catholic Tradition of the Law of Nations**. New Jersey: Lawbook Exchange, Ltd., 1935.

ESCOLA SUPERIOR DE GUERRA. **Manual básico**: elementos fundamentais. v. 1. Rio de Janeiro: Editora ESG, 2015.

ESCOLA SUPERIOR DE GUERRA. **Fundamentos do Poder Nacional**. Rio de Janeiro: Editora ESG, 2019.164 p.

EUA. Posição dos Estados Unidos da América. *Departamento de Estado dos EUA*. Segundo e Terceiro Relatório Periódico dos Estados Unidos da América ao Comitê de Direitos Humanos da ONU sobre o Pacto Internacional so-

MIOLO_Poder, Tecnologia e Direito - 2.indd 892 26/04/2024 11:12:31

bre Direitos Civis e Políticos. Anexo 1. 21 de outubro 2005. Disponível em: https://2009-2017.state.gov/j/drl/rls/55504.htm. Acesso em: 25 jul. 2023.

EUROPA. Convenção sobre o cibercrime. Budapeste: Conselho da Europa, 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 25 jul.2023.

EUROPA. **Livro Verde**: Relativo a um programa europeu de protecção das infraestruturas críticas. Bruxelas: COMISSÃO DAS COMUNIDADES EUROPEIAS ,2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52005DC0576. Acesso em: 25 jul. 2023.

EUROPE. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda). **International Court of Justice**, Paris, 2005, p. 168, 223. Disponível em: https://www.icj-cij.org/case/116. Acesso em: 25 jul. 2023.

EUROPE. Council of Europe. Additional Protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. **European Treaty Series**, n. 189, 2003. Disponível em: https://rm.coe.int/168008160f. Acesso em: 25 jul. 2023.

EUROPE. Council of Europe. **Convention on Cyber Crime**. Budapest: Convention Budapest, 2002.

EUROPE. Council of Europe. **International and multi-stakeholder co-operation on cross-border Internet**: interim report of the Ad-hoc Advisory Group on Cross-border Internet to the Steering Committee on the Media and New Communication Services incorporating analysis of proposals for international and multi-stakeholder co-operation on cross-border Internet. Pennsylvanis: Directorate General of Human Rights and Legal Affairs 2010. Disponível em: http://www.umic.pt/images/stories/publicacoes5/MCSCI%20Interim%20Report.pdf. Acesso em: 10 fev. 2023.

EUROPE. **Resolution RC/Res.6**. The crime of aggression. Adopted at the 13th plenary meeting, on 11 June 2010, by consensus. Rome Statute, 2010. Disponível em: https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf. Acesso em: 25 de jul. 2023.

EUROPEAN COMMISSION. **Joint Communication to the European Parliament and the Council**. Brussels: EU Policy on Cyber Defence. 2022. Dis-

MIOLO_Poder, Tecnologia e Direito - 2.indd 893 26/04/2024 11:12:31

ponível em: https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf. Acesso em: 22 jun. 2023.

EUROPEAN UNION. Charter of fundamental rights of the European Union. **Official Journal of the European Communities**, Bruxelas, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_en.pdf. Acesso em: 20 jul. 2023.

FAIFE, C. In Ukraine, Hacktivists fight back with Data Leaks. **The Verge**, [S.l.], 2022. Disponível em: https://www.theverge.com/2022/3/11/22968049/anonymous-hacks-ukraine-russia-cybercrime-danger. Acesso em: 25 jul. 2023.

FANELLI, R.; CONTI, G. A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict. *In*: CZOSSECK, O.; ZIOLKOWSKI, K. (eds.), INTERNATIONAL CONFERENCE, 4., 2012. Tallinn. **Proceedings [...]**, Taillinn: CCDCOE, 2012, p. 323–4.

FARIVAR, C. A Brief Examination of Media Coverage of Cyberattacks (2007 - Present). In: CZOSSECK, C.; GEERS, K. **The Virtual Battlefield: Perspectives on Cyber Warfare**. Amsterdam: IOS Press Ebooks, v. 3, 2009. Cryptology and Information Security Series pp.1-7. Disponível em: https://ccdcoe.org/uploads/2018/10/13_FARIVAR-Web-War-One.pdf. Acesso em: 25 jul. 2023.

FEDERAL POLITICAL DEPARTMENT BERNE. **Final record of the diplomatic Conference of Geneva of 1949**. Geneva: Diplomatic Conference, 1949. Disponível em: https://www.loc.gov/item/2011525350. Acesso em: 25 jul. 2023.

FEITH, D. J. Law in the Service of Terror - The Strange Case of the Additional Protocol. **Akron Law Review**, [*S.l.*], 1985. Disponível em: https://ideaexchange.uakron.edu/akronlawreview/vol20/iss2/3/. Acesso em: 25 jul. 2023.

FENTON III, H. A. Proportionality and Its Applicability in the Realm of Cyber--Attacks. **Duke Journal of Comparative & International Law**, [*S.l.*], v. 29, 2018. Disponível em: https://scholarship.law.duke.edu/djcil/vol29/iss2/6/. ACesso em: 25 jul. 2023.

FERGUSON, Y. H.; MANSBACH, R. W. **Globalization:** The Return of Borders to a Borderless World? New York: Routledge, 2012.

FERNÁNDEZ-VALMAYOR, J. L. C. Sobre los conceptos de orden público, seguridad ciudadana y seguridad pública. **Revista Vasca de Administración Pública**, La Rioja, n. 27, p. 9-26, 1990.

MIOLO_Poder, Tecnologia e Direito - 2.indd 894 26/04/2024 11:12:31

FERRAJOLI, L. **A Soberania no Mundo Moderno**. São Paulo: Martins Fontes, 2002.

FERREIRA, P. **Teoria geral do Estado**. 2. ed. ampliada e atualizada. São Paulo: José Konfino Editor, 1958, Tomo I.

FILDES, J. Stuxnet Worm 'Targeted High-Value Iranian Assets. BBC News, Reino Unido, 2010. Disponível em: http://www.bbc.co.uk/news/technology-11388018. Acesso em: 25 jul. 2023.

FILOCRE, D'A. Revisita à ordem pública. **Revista de Informação Legislativa** , Brasília, v. 46 n. 184, 2009. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/194953. Acesso em 25 jul. 2023.

FINANCE. Here's how much 59 Tomahawk missiles cost. **9finance - nine**, [*S.l.*], 2017. Disponível em: https://finance.nine.com.au/business-news/how-much-a--tomahawk-missile-costs/6e24be03-7033-4ec1-bf4d-7ec6b003f23d. Acesso em: 13 fev. 2023.

FINLAY, C. J. Just War, Cyber War, and the Concept of Violence. **Philosophy & Technology**, v. 31, p. 357–377, 2018. Disponível em: https://doi.org/10.1007/s13347-017-0299-6. Acesso em: 25 jul. 2023.

FINNEMORE, M. Cybersecurity and the concept of norms. **Carnegie Endowment for International Peace**, Whashington, 2017. Disponível em: https://carnegieendowment.org/2017/11/30/ cybersecurity-and-concept-of-norms--pub-74870. Acesso em: 2 fev. 2023.

FITTON, O. Cyber Operations and Gray Zones: Challenges for NATO. **Connections: The Quarterly Journal**, New York, v. 15, n. 2, p. 109–19, 2016. Disponível em: http://www.jstor.org/stable/26326443. Acesso em: 1 jul. 2023.

FITZGERALD, M. C. Russian Views on Electronic and Information Warfare. *In*: INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM: PARTNERS FOR THE 21ST CENTURY. 3., 1997. EStados Unidos. **Proceedings [...]**, Estados Unidos: National Defense University, 1997.

FOLLATH, E.; STARK, H. The Story of Operation Orchard: How Israel Destroyed Syria's Al Kibar Nuclear Reactor. **Spiegel Online**, [*S.l.*], 2009. Disponível em: http://www.spiegel.de/international/world/0,1518,druck-658663. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 895 26/04/2024 11:12:31

FORBES, I.; HOFFMAN, M. **Political Theory, International Relations, and the Ethics of Intervention**. Londres: Editora Macmillan Press Ltd, 1993.

FORÇA. *In*: CONCEITO.de. Brasil: Conceito de. Disponível em: https://conceito.de/forca. Acesso em: 25 jul. 2023.

FORMAN, S.; BARNES, J. E. Cyber-Combat: Act of War—Pentagon Sets Stage for US to Respond to Computer Sabotage with Military Force. **Wall Street Journal**, New York, v. 30, 2011. Disponível em: https://www.wsj.com/articles/SB10001424052702304563104576355623135782718 Acesso em: 22 jun. 2023.

FORREST, A. **Conscripts and Deserters**: The Army and French Society during the Revolution and Empire. Oxford: Oxford Univ. Press, 1989.

FOSTER, P. Bogus' AP Tweet about Explosion at the White House Wipes Billions off US Markets. **Telegraph.Co.Uk**, London, 2013. Disponível em: https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html. Acesso em: 25 jul. 2023.

FOUCHARD, P. **L'Arbitrage Commercial International**.Paris: Dalloz. 1965, p. 398-400.

FRANÇA. Armed Activities on Territory of Congo (Dem. Rep. Congo v. Uganda): overview of the case. **International court of justice**, n. 116, 2005. Disponível em: http://www.icj-cij.org/docket/files/116/10455.pdf. Acesso em: 25 jul. 2023.

FRANCK, T. M. Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States. **American Journal of International Law**, Cambridge, v. 64, n. 809, 1970. Disponível em: https://www.jstor.org/stable/2198919. Acesso em: 25 jul. 2023.

FRANCK, T. M. **Recourse to Force**: State Action Against Threats and Armed Atracks. Cambridge: Cambridge University Press, 2002.

FRIEDMANN, W. **The Changing Structure of International Law**. Cambridge: Cambridge University Press 1964.

FROWEIN; K.; KRISCH, N. Article 39 UN Charter. *In*: SIMMA, B. (ed.). **The Charter of the United Nations: A Commentary**. Repertory of practice of United Nations Organs, v. I, 2002. Disponível em: https://legal.un.org/repertory/art39.shtml. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 896 26/04/2024 11:12:31

GABLE, K. A. Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. **Vanderbilt Law Review**, [S.l.], v. 57, n. 43, 2021. Disponível em: https://scholarship.law.vanderbilt.edu/vjtl/vol43/iss1/2. Acesso em: 30 maio 2022.

GALLI, C. **Political Spaces and Global War**. Minneapolis. Minnesota: University of Minnesota Press, 2010.

GARDAM, J. **Non-Combatant Immunity as a norm of international humanitarian law**. Leiden: Editora Brill, 1993. Disponível em: https://brill.com/display/title/9312. Acesso em: 25 jul. 2023.

GARDOT, A. Jean Bodin. Sa Place Parmi les Fondateurs du Droit International. V. 50. , *In*: BRILL, **Collected Courses of the Hague Academy of International Law**, 1934. Disponível em: http://dx.doi.org/10.1163/1875-8096_pplrdc_A9789028608726_06. Acesso em: 25 jul. 2023.

GARTZKE, E. Making Sense of Cyberwar. Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School, Camvridge, 2014, p. 41-73. Disponível em: https://www.belfercenter.org/publication/making-sense-cyberwar. Acesso em: 30 jun. 2023.

GARTZKE, E. The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth. International Security. The MIT Press, New York, v. 38, n. 2, p. 41-73, 2013. Disponível em: https://www.jstor.org/stable/24480930. Acesso em: 30 jun. 2023.

GARVEY, M. D. A Philosophical Examination on the Definition of Cyberspace. *In*: CARNOVALE, S.; YENIYURT, S. (Eds.). **Cyber Security and Supply Chain Management**: Risks, Challenges, And Solutions. New Jersey: World Scientific Publishing, 2021, p.1-11. Disponível em: https://www.worldscientific.com/doi/abs/10.1142/9789811233128_0001. Acesso em: 12 jun. 2023.

GEER JUNIOR, D. E. Eisenhower Revisited. **Institute of Electrical and Eletronics Engineers Security & Privacy**, [*S.l.*], n. 4, 2011. Disponível em: https://ieeexplore.ieee.org/document/5968096. Acesso em: 29 jun. 2023.

GEHLBACH, S. Reflections on Putin and the Media. **Post-Soviet Affairs**, Geneva, v. 26, n. 1 2013. Disponível em: https://www.tandfonline.com/journals/rpsa20. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 897 26/04/2024 11:12:31

GEISS, R.; LAHMANN, H. Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention. In: ZIOLKOWSKI, K. (ed). **Peacetime Regime for State Activities in Cyberspace**. Taillinn: Nato CCD COE, 2013.

ĢELZIS, Ģ. Cyber-soldiers. DW, Berlin, 2011. Disponível em: https://www.dw.com/en/estonian-voluntary-cyber-soldiers-integrated-into-national-guard/a-14968102. Acesso em: 25 jul. 2023.

GEORGE, A. L.; SIMONS, W. E. **Coercive Diplomacy**: Definition and Characteristics. The Limits of Coercive Diplomacy, 2. ed. San Francisco: Westview, 1994. Disponível em: https://core.ac.uk/download/pdf/76458223.pdf. Acesso em: 25 jul. 2023.

GEORGIA. UN General. **Assembly Resolution 68/243**. Report to the United Nations Secretary General 5. United Nations, Georgia, 2014. Disponível em: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/07/Georgia.pdf. Acesso em: 25 jul. 2023.

GERASIMOV, V. S. The Value of Science Is in the Foresight: new challenges demand rethinking the forms and methods of carrying out combat operations. **Military review**, Kansas, v. 96, p. 23, 2016. Disponível em: https://www.semanticscholar.org/paper/The-Value-of-Science-Is-in-the-Foresight%3A-New-the-Gerasimov/a132e441825bd5314b7135af33ac643bed422e7e. Acesso em: 25 jul. 2023.

GERMAN FEDERAL MINISTRY OF DEFENSE. German Defense White Paper 2016. Berlin: Federal Ministry of Defense, 2016. Disponível em: https://www.bundeswehr.de/resource/blob/4800140/fe103a80d8576b2cd7a135a5a8a86dde/download-white-paper-2016-data.pdf. Acesso em: 23 jul. 2023.

GERVAIS, M. Cyber Attacks and the Laws of War. **Papers SSRN**, [*S.l.*], 2011. Disponível em: . Acesso em: 25 jul. 2023.

GHAPPOUR, A.Tallinn, Hacking, and Customary International Law. Boston **University School of Law, Public Law Research Paper**, Boston, 2017. Disponível em: https://ssrn.com/abstract=3024380. Acesso em: 22 jun. 2023.

GIBSON, W. **Neuromancer**. New York: Penguin Publishing Group, 1984.

GILES, K. **Handbook of Russion Information Warfare**. Roma: NATO Defense College, 2016. Disponível em: https://www.ndc.nato.int/news/news.php?icode=995. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 898 26/04/2024 11:12:31

GILES, K.; MONAGHAN, A. **Legality in Cyberspace**: An adversary view. Morrisville, Carolina do Norte: Lulu.com, 2014. Disponível em: http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1193. Acesso em: 25 jul. 2023.

GILES, K. Russia's public stance on cyberspace issues. *In*: CZOSSECK, C.; OTTIS, R.; ZIOLKOWSKI K. (Eds.). **4th International Conference on Cyber Conflict**, 2012. Disponível em: https://ccdcoe.org/uploads/2012/01/2_1_Giles_RussiasPublicStanceOnCyber InformationWarfare.pdf. Acesso em: 17 fev. 2023.

GILL, T. D. Non-Intervention in the Cyber Context. *In*: ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Taillinn: International Law, International Relations and Diplomacy, NATO CCD COE Publication, 2013.

GILSINAN, K.; CALAMUR, K. Did Putin Direct Russian Hacking? And Other Big Questions. **The Atlantic**, [*S.l.*], 2017. Disponível em: https://www.theatlantic.com/international/archive/2017/01/russianhackingtrump/510689. Acesso em: 25 jul. 2023.

GIORGI, L. M.; WALKER, M. S. Guerra cognitiva. **Visión Conjunta - Escuela Superior de Guerra Conjunta de las Fuerzas Armadas**, Argentina, año 14, n. 27, pp. 9-17, 2022, p. 9 – tradução nossa. Disponível em: http://www.cefadigital.edu.ar/bitstream/1847939/2316/1/VC27%20Giorgi-Walker.pdf. Acesso em: 25 jul. 2023.

GLOSSARY OF COMMON CYBERSECURITY TERMINOLOGY, NICCS. Disponível em: https://definedterm.com/a/download/document/11128. Acesso em: 25 jul. 2023.

GLUM, J. ISIS Hacker Junaid Hussain Confirmed Dead After US Airstrike on Islamic State in Syria: Pentagon. **International Business Times**, New York, 2015. Disponível em: http://www.ibtimes.com/isis-hacker-junaid-hussain-confirmed-dead-after-us-airstrike-islamic-state-syria-2073451. Acesso em: 25 jul. 2023.

GOLDMAN, B. La protection internationale des droits de J'homme et l'ordre public international dans le fonctionnement de la regle de conflit des Iois. *In*: CASSIN, R. **Amicorum discipulorumque liber**. Paris: A. Pedone,1969. Tomo I, p. 449-466.

GOLDSMITH, J. L. Against Cyberanarchy. **University of Chicago Law Review**, Chigaco, v. 1199, p. 1245-46, 1998.

MIOLO_Poder, Tecnologia e Direito - 2.indd 899 26/04/2024 11:12:31

GOLDSMITH, J. L.; WU, T. **Who Controls the Internet?** Illusions of a Borderless World. Oxford: Oxford UP, 2006.

GOUVEIA, J. B. O uso da força no Direito Internacional Público. **Revista Brasileira de Estudos Políticos**, Belo Horizonte, n. 107, p. 149-200, jul./dez. 2013. Disponível em: https://pos.direito.ufmg.br/rbep/index.php/rbep/article/view/P.0034-7191.2013v107p149/241. Acesso em: 24 jul. 2023.

GPO – Authenticated U. S. Government Information. Patriot uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001. (42 U.S.C. 5195c(e)), § 1016(e), **Congressional Record**, v. 37, 2001. Disponível em: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf. Acesso em: 25 jul. 2023.

GRAD, S. Engineers who hacked into L.A. traffic signal computer, jamming streets, sentenced. **Los Angeles Times**, Los Angeles, California, 2009.

GRANDI, B. Considerazioni sull'uso della forza non armata nei rapporti tra stati. **Comunicazioni e studi**, [*S. l.*], v. 278, p. 279–281. 1992. Disponível em: https://www.studocu.com/it/document/universita-degli-studi-di-milano/uso-della-forza/considerazioni-sull-uso-della-forza-non-armata-nei-rapporti-tra-stati-2/5702181. Acesso em: 25 jul. 2023.

GREATHOUSE, C. B. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? *In*: KREMER, J.-F.; MÜLLER, B. (ed.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?* Berlin: Heidelberg: Springer Berlin Heidelberg, 2014, p. 21-40. Disponível em: https://doi.org/10.1007/978-3-642-37481-4_2. Acesso em: 25 jul. 2023.

GREENBERG, A. The Case for War Crimes Charges Against Russia's Sandworm Hackers. **Wired**, [*S.l.*], 2022. Disponível em: https://www.wired.com/story/cyber-warcrimes-sandworm-russia-ukraine/. Acesso em: 25 jul. 2023.

GREENBERG, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History." **Wired**, 2018. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-codecrashed-the-world/. Acesso em: 25 jul. 2023.

GREENEMEIER, L. Heart-Stopper: Could Hackers Hit Pacemakers, Other Medical Implants? **Scientific American**, Canadá, 2008. Disponível em: https://www.scientificamerican.com/article/heart-stopper-med-device-hack/. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 900 26/04/2024 11:12:31

GROSS, L. The Peace of Westfalia, 1648–1948. **The American Journal of International Law**, Cambridge, v. 42, 1948. Disponível em: https://www.jstor.org/stable/2193560. Acesso em: 25 jul. 2023.

GROSS, Michael Joseph. A Declaration of Cyber-War. **Vanity Fair**, [*S.l.*], v. 53, 2011. Disponível em: https://archive.vanityfair.com/article/2011/4/a-declaration-of-cyber-war. Acesso em: 25 jul. 2023.

GROTIUS, H. **De Jure Belli Ac Pacis Libri Tres**. Tradução: William Whewell. London: John W. Parker, 1987.

GROTIUS, H. **Del Derecho de presa**: del derecho de la guerra y de la paz. Madrid: C de E. C., 1987.

HAATAJA, S. Technology, Violence and Law: Cyber Attacks And Uncertainty In International Law. *In*: EUROPEAN CONFERENCE ON INFORMATION WARFARE, 2013. **Proceedings [...]**, 2013. Disponível em: http://www.academia.edu/6776442/Technology_Violence_and_Law_Cyber_Attacks_and_Uncertainty_in_International_Law. Acesso em: 25 jul. 2023.

HACKER FORCES. Telegram channel, [*S.l.*], 2022. Disponível em: https://t.me/hackencyberarmy/101 ou https://archive.ph/. Acesso em 25 jul. 2023.

HAIZLER, O. The United States Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking. **Cyber, Intelligence, and Security**, Israel, v. 1, no. 1, 2017, p. 31-45. Disponível em: https://www.inss.org.il/publication/united-states-cyber-warfare-history-implications-modern-cyber-operational-structures-policymaking/. Acesso em: 13 jun. 2023.

HALPERIN, D.; *et al*. Security and Privacy for Implantable Medical Devices. **Institute of Electrical and Eletronics Engineers Pervasive Computing**, [*S.l.*], v. 7, n. 1, p. 30-39, 2008. Disponível em: https://ieeexplore.ieee.org/abstract/document/4431854. Acesso em: 18 jul. 2023.

HAMPSON, F. O.; SULMEYER, M. Introduction: Getting beyond Norms: New Approaches to International Cyber Security Challenges. **Centre for International Governance Innovation**, Canada, 2017. Disponível em: https://www.cigionline.org/publications/getting-beyond-norms-new-approaches-international-cyber-security-challenges. Acesso em: 15 jan. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 901 26/04/2024 11:12:31

HARKNETT, R. J.; SMEETS, M. Cyber Campaigns and Strategic Outcomes. **Journal of Strategic Studies**, London, v. 45, n. 4, 2020. Disponível em: https://doi.org/10.1080/01402390.2020.1732354. Acesso em: 25 jul. 2023.

HARMES, M. Cyber Attacks: When to Respond. **International Humanitarian Law/Law of Armed Conflict**, Leiden, 2012. Disponível em: https://ssrn.com/abstract=2312039. Acesso em: 25 jul. 2023.

HARRIS, S. *et al.*, As Russia prepared to invade Ukraine, U.S. struggled to convince Zelensky, allies of threat." **The Washington Post**, Whashington, 2022. Disponível em: https://www.washingtonpost.com/national-security/interactive/2022/ukraine-road-towar/. Acesso em: 25 jul. 2023.

HARWELL, D. Ukraine is scanning faces of dead Russians, then contacting the mothers. **The Washington Post**, Washington, 2022. Disponível em: https://www.washingtonpost.com/technology/2022/04/15/ukraine-facial-recognition-warfare/. Acesso em: 25 jul.2023.

HATHAWAY, O. A; *et al.* The Law of Cyber-Attack. **California Law Review**, California, v. 100, n. 4, p. 817-85, 2012. Disponível em: . Acesso em: 25 jul. 2023.

HAYDEN, M. V. The Future of Things Cyber. **Strategic Studies Quarterly,** Harvard, v. 5, n. 1, 2011, p. 3-7. Disponível em: https://www.jstor.org/stable/26270507. Acesso em: 26 jul. 2023.

HCJ 769/02. Against Torture in Isr. v. Gov't of Israel 62(1) PD 507 (2006) (Isr.). **Pub. Comm**, [S.l.], 2006. Disponível em: http://elyon1.court.gov.il/files_eng/02/690/007/A34/ 02007690.a34.pdf. Acesso em: 25 jul. 2023.

HEALEY, J. The Spectrum of National Responsibility for Cyberattacks. **The Brown Journal of World Affairs**, Providence, v. 18, n. 1, 2011, p. 57-70. Disponível em: https://www.jstor.org/stable/24590776. Acesso em: 12 jul. 2023.

HEGEL, G. W. F. **Grundlinien der Philosophie des Rechts oder Naturrecht und Staatswissenschafl im Grundrisse**. Mit Hegels eigenhändigen Notizen und den mündlichen Zusätzen.. Frankfurt an Main: Suhrkamp Verlag, 1970. v. 7.

HEINEGG, W. H. v. Territorial Sovereignty and Neutrality in Cyberspace. **International Law Studies**, England, v. 89, p. 123-156, 2013. Disponível em: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1027&context=ils. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 902 26/04/2024 11:12:31

HELLER, K. J. Situational Gravity Under the Rome Statute. *In*: STAHN, C.; HERIK, L. v. d. (eds.). **Future Perspectives in International Criminal Justice**. The Hague: T.M.C. Asser Press, 2010.

HENCKAERTS, J. M.; BECK, L. D. **Direito Internacional Humanitário Consuetudinário**. Cambridge: Cambridge University Press, 2005, regras 1-11, 12, 14, 15, 17, 24, Volume I e II: Regras. Disponível em: https://www.icrc.org/sites/default/files/topic/file_plus_list/direito_internacional_humanitario_consuetudinario.pdf. Acesso em: 23 jul. 2023.

HENCKAERTS, J-M.; DOSWALD-BECK, L. **Customary International Humanitarian Law**. Cambridge: Comite International Geneve, 2005. Disponível em: https://www.icrc.org/en/doc/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf. Acesso em: 25 jul. 2023.

HENRY, Etienne. The Falklands/Malvinas War – 1982. *In*: CORTEN, Olivier; RUYS, Tom (eds). **International Law and the Use of Force**: A Case-Based Approach. Oxford: Oxford University Press 2018.

HENZEL, S. F. K.. **Cybersecurity: Perspectives on the Challenges of the Information Revolution**. Power and Security in the Information Age. Investigating the Role of the State in Cyberspace. Burlington: Ashgate, 2007.

HERSH, S. M. The Online Threat. **New Yorker**, New York, 2010, p. 44-48. Disponível em: https://www.newyorker.com/magazine/2010/11/01/the-online-threat. Acesso em: 25 jul. 2023.

HERT, P.; THUMFART, J. The Microsoft Ireland Case and the Cyberspace Sovereignty Trilemma. Post-Territorial Technologies and Companies Question Territorial State Sovereignty and Regulatory State Monopolies. **Brussels Privacy Hub, Working Paper**, Brussels, v. 4, n. 11, 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3228388. Acesso em: 20 fev. 2023.

HERTZ, M.; YAMATO, R. V. As Transformações das Regras Internacionais sobre Violência na Ordem Mundial Contemporânea. **Dados-Revista de Ciências Sociais**, Rio de Janeiro, v. 61, n. 1, 2018, p. 3-45. Disponível em: https://www.scielo.br/j/dados/a/dJ3MjxFB9V5WfPgtVpTGPsf/?format=pdf&lang=pt. Acesso em: 27 jul. 2023.

HILF, M.; REUS, M. Verfassungsfragen lebensmittelrechtlicher Normierung im europäischen und internationalen Recht. **Zeitschrift für das gesamte Lebens-**

MIOLO_Poder, Tecnologia e Direito - 2.indd 903 26/04/2024 11:12:31

mittelrecht, v. 24, n. 3, p. 289-302, 1997. Disponível em: http://www.jura.uni-sb.de/projekte/Bibliothek/text.php?id=321. Acesso em: 25 jul. 2023.

HIPPLER, T. **Citizenship and Discipline**: Popular Arming and Military Service in Revolutionary France and Reform Prussia, 1789-1830. Tese (Ph.D. dissertation)- European University Institute, Florence, 2002.

HM GOVERNMENT. **The Future of the United Kingdom's Nuclear Deterrent**. Reino Unido: Ministry of defense, Foreign and Commonwealth Affairs, 2006. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/272429/6994.pdf. Acesso em: 25 jul. 2023.

HOBBES, T. **Leviatã**. Tradução: João Paulo Monteiro, Maria Beatriz Nizza da Silva e Cláudia Berliner. 1. ed. São Paulo: Martins Fontes, 2003.

HOBBES, T. **Leviathan**. Indianapolis, IN: Hackett, 1994, p. 75–76.

HOISINGTON, M. Cyberwarfare, and the Use of Force Giving Rise to the Right of Self-Defense (2009). **Boston College International and Comparative Law Review**, Boston, v. 32, p. 439, 2009. Disponível em: https://ssrn.com/abstract=1542223. Acesso em: 25 jul. 2023.

HOLLAND, H. B. The Failure of the Rule of Law in Cyberspace? Reorienting the Normative Debate on Borders and Territorial Sovereignty. **John of Marshall Journal Computer & Information Law**, Chicago, v. 1, 2005. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=777505. Acesso em: 16 jan. 2021.

HOLLIS, D. B. Could Deploying Stuxnet be a War Crime? **OpinioJuris Blog**, [*S.l.*], 2011. Disponível em: http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/. Acesso em: 25 jul. 2023.

HOLLIS, D. The Influence of War; The War for Influence. **Temple Journal of International & Comparative Law**, New York, v. 32, p. 36 -39, 2018.

HOLYNSKA, K.; MOORE, P. Understanding Russia's Motivations, and Using Them. Rand Corporation. **The Rand Blog**, [*S.l.*] 2022. Disponível em: https://www.rand.org/blog/2022/08/understanding-russias-motivations-and-using-them.html. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 904 26/04/2024 11:12:31

HOMELAND Defense. Joint Publication - JP 3-27. CreateSpace Independent Publishing Platform, 2013. DIsponível em: https://www.hsdl.org/?view&did=742874. Acesso em: 24 jul. 2023.

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE. **Report on RuSsian Active Measures**. Russia: U.S. House, 2018. Disponível em: https://intelligence.house.gov/uploadedfiles/final_ russia_investigation_report.pdf. Acesso em: 20 jul. 2023.

HUBER, M. **Island of Palmas case**. United Nations, 1928, p. 829-838. Disponível em: https://legal.un.org/riaa/cases/vol_II/829-871.pdf. Acesso em: 20 jun. 2023.

HUGHES, Daniel; COLARIK, Andrew. The Hierarchy of Cyber War Definitions. *In*: PACIFIC ASIA WORKSHOP ON INTELLIGENCE AND SECURITY INFORMATICS. 12., 2017, Spring. **Anais [...]**, Springer, 2017, p. 15-33.

HUMAN RIGHTS CENTER. **Digital Fingerprints**: using electronic evidence to advance prosecutions at the international criminal court. Berkeley: UC Berkeley School of Law, 2014. Disponível em: https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. Acesso em: 25 jul. 2023.

HUNTINGTON, S. P. The Clash of Civilizations? **Foreign Affairs**, New York, 1993, p. 22-49. Disponível em: https://www.foreignaffairs.com/articles/united-states/1993-06-01/clash-civilizations. Acesso em: 25 jul. 2023.

HYMON, S. Engineers, Architects Strike Out on Picket Lines. **Los Angeles Times**, Los Angeles, California, 2006.

IBM - International Business Machines Corporation. O que é a tecnologia Blockchaun. **IBM**, São Paulo, 2023. Disponível em: https://www.ibm.com/br-pt/topics/blockchain. Acesso em: 25 jul. 2023.

ICJ- INTERNATIONAL COURT OF JUSTICE Canal de Corfu (**United Kingdom v. Albania)**, 1949 I.C.J. em 22 may 1947. Disponível em: https://www.icj-cij.org/case/1. Acesso em: 20 jun. 2023.

ICJ- INTERNATIONAL COURT OF JUSTICE. Temple case, 1962 ICJ 6, 23, 31; Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria), 2002 ICJ. 275, para. 57 (Oct. 10), 1962. Disponível em: https://www.icj-cij.org/case/94. Acesso em: 23 jun. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 905 26/04/2024 11:12:31

ICJ- INTERNATIONAL COURT OF JUSTICE. North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), 1969 ICJ. 3, paras. 71, 77 (Feb. 20). Dispeonível em: https://www.icj-cij.org/case/52. Acesso em: 14 jun. 2023.

ICJ- INTERNATIONAL COURT OF JUSTICE. Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ, Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 9 July 2004. Disponível em: https://www.icj-cij.org/case/131. Acesso em: 21 jul. 2023.

ICJ – INTERNATIONAL COURT OF JUSTICE. Advisory Opinion Legality Of The Threat Or Use Of Nuclear Weapons. **ICJ**, Haia, 1995. Disponível em: https://www.icj-cij.org/en/case/95. Acesso em: 10 jun 2023. Disponível em: https://www.icj-cij.org/case/95. Acesso em: 25 jul. 2023.

ICRC - INTERNATIONAL HUMANITARIAN LAW DATABASE. **Project of an International Declaration Concerning the Laws and Customs of War**. Brussels: Martens Nouveau Recueil, art. 9. 4 (ser. 2) 219. 1874. Disponível em: https://ihl-databases.icrc.org/en/ihl-treaties/brussels-decl-1874. Acesso em: 25 jul. 2023.

ICTR. Promotor v. Rutaganda, Caso No. ICTR-96–3, Sentença de 26 de maio de 2003 (Câmara de Apelações), § 570).

ICTY. Promotor v. Kunarac e outros, Caso o. -96-23, Sentença de 22 de fevereiro de 2001 (Câmara de Julgamento), § 416, confirmado pela Câmara de Recursos em seu julgamento no mesmo caso de 12 de junho de 2002, § 89).

ICTY. Prosecutor v. D. Tadić, Appeals Chamber, Decision of 2 October 1995, case IT-94-1-AR72, paras. 70.

ICTY. Prosecutor v. Strugar, Case No. IT-01-42-T, Judgment (Int'l Crim. Trib. for the Former Yugoslavia Jan. 31, 2005).

IHL - INTERNATIONAL HUMANITARIAN LAW DATABASES. Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 29 July 1899. Genevaaa; IHL, 1899. Disponível em: https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-ii-1899. Acesso em: 27 jul. 2023.

INFORMATION OPERATION JOINT PUBLICATION. J-13, 2006. Disponível em: www.dtic.mil/doctrine/jel/newpubs/jp313.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 906 26/04/2024 11:12:31

INFORMATION SECURITY POLICY COUNCIL. **Japan, International Strategy on Cybersecurity**. Japan: Information Security Policy Council, 2013. Disponível em: http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation.pdf. Acesso em: 25 jul. 2023.

INFORMATION SECURITY POLICY COUNCIL. **White Paper 21**. Australian: Australian Department of Defence, 2013. Disponível em: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2013#_Toc427841723. Acesso em: 25 jul. 2023.

INTERNATIONAL COURT OF JUSTICE. **Application of the Convention on the Prevention and Punishment of the Crime of Genocide** (Bosn. & Herz. v. Serb. and Montenegro). United Kingdom: International Court of Justice, 2007. Disponível em: https://www.icj-cij.org/case/91. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Asylum Case** (Colom. v. Peru). United Kingdom: International Court of Justice, 1950. Disponível em: https://www.icj-cij.org/case/7. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Case Concerning Right of Passage Over Indian Territory** (Port. v. India). United Kingdom: International Court of Justice, 1960. Disponível em: https://www.icj-cij.org/case/32#:~:text=The%20Court%20found%20that%20Portugal,the%20existence%20of%20that%20right. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Continental Shelf case** (Libya v. Malta). United Kingdom: International Court of Justice, 1985. Disponível em: https://www.icj-cij.org/case/68. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Corfu Channel** (United Kingdom of Great Britain and Northern Ireland v. Albania) (Merits), separate opinion by Judge Alvarez. United Kingdom: International Court of Justice,1949. Disponível em: https://www.icj-cij.org/case/1. Acesso em: 23 jun. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Land and Maritime Boundary between Cameroon and Nigeria** (Cameroon v. Nigeria), 2002. United Kingdom: International Court of Justice, 2002. Disponível em: https://www.icj-cij.org/case/94. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Legality of the Threat or Use of nuclear weapons, advisory opinion**. United Kingdom: International Court of Justice, 1995. Disponível em: https://www.icj-cij.org/case/95. Acesso em: 23 jun. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 907 26/04/2024 11:12:31

ICJ - INTERNATIONAL COURT OF JUSTICE. **Legality of the Threat or Use of nuclear weapons, advisory opinion**. United Kingdom: International Court of Justice, 1996, § 40. Disponível em: https://www.icj-cij.org/case/95. Acesso em: 23 jun. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Military and Paramilitary Activities in and against Nicaragua** (Nicaragua v. United States of America), merits. United Kingdom: International Court of Justice, 1986. Disponível em: https://www.icj-cij.org/case/70/judgments. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **North Sea Continental Shelf** (Ger. v. Den.; Ger. v. Neth.). United Kingdom: International Court of Justice, 1969. Disponível em: https://www.icj-cij.org/case/52. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. **Recueil CIJ** (1969). United Kingdom: International Court of Justice, 1969. Disponível em: https://www.icj-cij.org/public/files/case-related/52/052-19690220-JUD-01-00-EN.pdf. Acesso em: 25 jul. 2023.

ICJ - INTERNATIONAL COURT OF JUSTICE. S.S. **Lotus** (Fr. v. Turk.), Julgamento, 1927. United Kingdom: International Court of Justice, 1927. Disponível em: https://law.justia.com/cases/foreign/international/1927-pcij-series-a-no-10.html. Acesso em: 25 jul. 2023.

INTERNATIONAL CRIMINAL COURT. DCR- Situation in the DRC, Judgment on the Prosecutor's Appeal against the Decision of Pre-Trial Chamber I entitled 'Decision on the Prosecutor's Application for Warrants of Arrest, Article 58'. Haia, 2006. Disponível em: https://www.legal-tools.org/doc/8c20eb/. Acesso em: 25 jul. 2023.

INTERNATIONAL CRIMINAL COURT. **Policy Paper on Case Selection and Prioritisation**. Haia: OTP, 2016. Disponível em: https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf. Acesso em: 25 jul. 2023.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. **The Military Balance 2010**. Abingdon: Routledge, 2010. Disponível em: http://www.iiss.org/publications/military-balance/the-military-balance-2010/military-balance--2010-press-statement/. Acesso em: 25 jul. 2023.

INTERNATIONAL LAW ASSOCIATION. Final Report of the Committee on the Formation of Customary (General) International Law, Statement of Principles Applicable to the Formation of General Customary International Law. In-

MIOLO_Poder, Tecnologia e Direito - 2.indd 908 26/04/2024 11:12:31

ternational Law Association, 2000. Disponível em: https://legal.un.org/ilc/documentation/english/a_cn4_663.pdf. Acesso em: 5 abr. 2023.

INTERNATIONAL TELECOMMUNICATION REGULATIONS. The International Telecommunication Regulations, as well as the Radio Regulations, are a legal instrument of the ITU (art. 4(3)). Constituition of the International Telecommunication. International Telecommunication, [*S.l.*], 1988.

INTERNATIONAL TELECOMMUNICATION UNION. C**onstitution and convention of the international telecommunication union**. Geneva: International Telecommunication Union, v. 1825, 1992, 1825. DIsponível em: https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800b0730&clang=_en. Acesso em: 27 jul. 2023.

IT ARMY OF UKRAINE, Telegram channel, 26 February 2022. Disponível em: https://t.me/itarmyofukraine2022/1 ou https://archive.ph/SMt31. Acesso em: 25 jul.2023.

IT ARMY OF UKRAINE, Telegram channel, 7 May 2022. Disponível em: https://t.me/itarmyofukraine2022/331 ou https://archive.ph/. Acesso em: 25 jul. 2023.

JACEWICZ, A. The Concept of Force in the United Nations Charter. **Polish Yearbook of International Law**, Varsóvia, v. 9, p. 137-141. 1977. Disponível em: https://legal.un.org/ilc/publications/yearbooks/english/ilc_1986_v2_p1.pdf. Acesso em: 25 JUL. 2023.

JANOFSKY, A. This Ukrainian cyber firm is offering hackers bounties for taking down Russian sites. The Record, [*S.l.*], 2022. Disponível em: https://therecord.media/this-ukrainian-cyber-firm-is-offering-hackers-bounties-for-taking-down-russian-sites. Acesso em: 25 jul. 2023.

JELLINEK, G. **Teoria general del Estado**. 2. ed. Tradução: Fernando de Los Rios. Buenos Aires: Albatros, 1970.

JENKS, C. W. **The Common Law of Mankind**. Nova Iorque: Columbia Law Review, 1958.

JENNINGS, R.; WATTS, A. **Oppenheim's International Law**. London: Longman,1996.

MIOLO_Poder, Tecnologia e Direito - 2.indd 909 26/04/2024 11:12:31

JENSEN, E. T. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defence. **Stanford Journal of International Law**, Stanford, v. 38, 2002. Disponível em: https://digitalcommons.law.byu.edu/faculty_scholarship/212/. Acesso em: 25 JUL. 2023.

JENSEN, E. T. Cyber sovereignty: the way ahead. **Texas International Law Journal**, Texas, v. 50, n. 275, 2015. Disponível em: https://ssrn.com/abstract=2466904. Acesso em: 10 jan. 2023.

JENSEN, E. T. The Tallinn Manual 2.0: Highlights and Insights. **Georgetown Journal of International Law**, Georgetown, v. 48, n. 735, 2017. Disponível em: https://ssrn.com/abstract=2932110. Acesso em: 25 jul. 2023.

JOHNSON, D. R.; POST, D. G. Law and Borders - the Rise of Law in Cyberspace. **Stanford Law Review**, Stanfod, v. 48, p. 1367, 1996, Disponível em: https://ssrn.com/abstract=535. Acesso em: 17 jul. 2023.

JOLLEY, J. D., Article 2(4) and Cyber Warfare: How Do Old Rules Control the Brave New World? **International Law Research**, [*S.l.*], v. 2, n. 1, 2013. Disponível em: https://www.ccsenet.org/journal/index.php/ilr/article/view/28683. Acesso em: 23 jun. 2023.

JOQUE, J. **Deconstruction Machines**: Writing in the Age of Cyberwar. Minneapolis: University of Minnesota Press, 2018.

JOSHI, S. Battlefield Lessons- Special Report. **The Economist**, New York, 2023. Disponível em: https://www.economist.com/special-report/2023/07/03/technology-is-deepening-civilian-involvement-in-war. Acesso em: 25 jul. 2023.

JOYNER, C. C.; LOTRIONTE, C. Information Warfare as International Coercion: Elements of a Legal Framework. **European Journal of International Law**, [S.l.], v. 12, n. 5, p. 825–865, 2001. Disponível em: https://doi.org/10.1093/ejil/12.5.825. Acesso em: 17 fev. 2023.

JUPILLAT, N. Armed Attacks in Cyberspace: the unseen threat to peace and security that redefines the law of state responsibility. **University of Detroit Mercy Law Review**, Detroit, v. 92, n. 2, 2015. Disponível em: . Acesso em: 25 jul. 2023.

KAN, M. Pentagon Impressed by Starlink's Fast Signal-Jamming Workaround in Ukraine. **PCMag**, New York, 2022. Disponível em: https://www.pcmag.com/

MIOLO_Poder, Tecnologia e Direito - 2.indd 910 26/04/2024 11:12:31

news/pentagon-impressed-by-starlinks-fast-signaljamming-workaround-in--ukraine. Acesso em: 25 jul. 2023.

KANUCK, S. Sovereign discourse on cyber conflict under international law. **Texas Law Review**, Texas, v. 88, p. 1571-1597, 2010. Disponível em: https://www.law.upenn.edu/institutes/ cerl/conferences/cyberwar/papers/reading/Kanuck.pdf. Acesso em: 17 fev. 2023.

KASPERSKY LAB. Stuxnet Manifests the Beginning of the New Age of Cyber--Warfare. Kaspersky, London, 2010. Disponível: https://www.kaspersky.com/about/press-releases/2010_kaspersky-lab-provides-its-insights-on-stuxnet--worm. Acesso em: 25 jul. 2023.

KASTENBERG, J. Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law. **Air Force Law Review, Rochester**, n. 64, 2009. Disponível em: https://ssrn.com/abstract=3100520. Acesso em: 25 jul. 2023.

KEARNEY, A. T. Measuring Globalization: Economic Reversals, Forward Momentum. **Foreign Policy**, Congers, n. 141, 2004, p. 54-69. Disponível em: https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=191143. Acesso em: 25 JUL. 2023.

KEEGAN, J. **A History of Warfare**. New York: First Vintage Books, 1994.

KELLER, P. Cyberpower: Die Strategische Dimension. *In*: ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Tallinn: International Law, International Relations and Diplomacy; NATO CCD COE Publication, 2012.

KELLOGG-BRIAND Pac t 1928. Pasris, 1928. Disponível em: https://loveman.sdsu.edu/docs/1928KelloggBriand.pdf. Acesso em 25 jul. 2023.

KELSEN, H. **Das Problem der Souveränität**. Kelsen General Theory of Law and State, Harvard UP: Cambridge, 1949.

KELSEN, H. **Das Problem der Souveränität**. Mohr Siebeck: Tübingen, 1928.

KELSEN, H. **General Theory of Law and State**. Harvard UP: Cambridge, 1949.

KELSEN, H. **Teoria pura do direito**. Tradução: João Baptista Machado. 6. ed. São Paulo: Martins Fontes, 1998.

MIOLO_Poder, Tecnologia e Direito - 2.indd 911 26/04/2024 11:12:31

KELSEN, H. The Principle of Sovereign Equality of States as a Basis for International Organization. **Yale Law Journal**, New Haven, v. 53, n. 2, 1944. Disponível em: https://www.jstor.org/stable/792798?seq=1. Acesso em: 28 fev. 2023.

KELSEN, H. **The problem of sovereignty**. Mohr Siebeck: Tübingen, 1928.

KERSCHISCHNIG, G. **Cyberthreats and International Law**. The Hague: Eleven International Publishing, 2012.

KESAN, J. P; HAYES, C. M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. **Harvard Journal of Law and Technology**, Harvard, v. 25, n. 429, 2012. Disponível em: https://ssrn.com/abstract=1805163. Acesso em: 25 jul. 2023.

KIBERBULL. Telegram chat, 14 March 2022. Disponível em: https://t.me/c/1549333360/346. Acesso em 25 jul. 2023.

KILOVATY, I. Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare. **American University National Security Law Brief**, Whashington, v. 5, n. 91, 2014. Disponível em: https://ssrn.com/abstract=2695642. Acesso em: 25 jul. 2023.

KILOVATY, I. Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under Humanitarian Law. **Michigan Telecommunications nad Technology Law Review**, Michigan, v. 23, n. 1, 2016. Disponível em: https://repository.law.umich.edu/mttlr/vol23/iss1/3. Acesso em 22 set. 2023.

KILOVATY, I.The international law of cyber intervention. *In*: TSAGOURIAS, N.; BUCHAN, R. **Research handbook on international law and cyberspace**. Massachusetts: Edward Elgar Publishing Limited, 2019, p. 97-112.

KINETZ, E. 'Kill Everyone': Russian Violence in Ukraine Was Strategic. **Associated Press and Frontline**, New York. 26 out. 2022. Disponível em: https://www.pbs.org/wgbh/frontline/article/russian-general-troops-killed-civilians-ukraine/. Acesso em: 25 jul. 2023.

KJELGAARD, J. M.; MELGAARD, U. Denmark's Position Paper on the Application of International Law in Cyberspace. **Nordic Journal of International Law**, Nijhoff, 2023. Disponível em: file:///C:/Users/alexa/Downloads/nord-article-10.1163-15718107-20230001.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 912 26/04/2024 11:12:31

KLIMBURG, A. Mobilising Cyber Power. **Survival**, Berlin, v. 53, n. 1, 2011, p. 41-60. Disponível em: https://www.researchgate.net/publication/260386421_Mobilising_Cyber_Power. Acesso em: 3 jul. 2023.

KMU.gov.ua. Мінцифри бореться з ворогом на цифровому фронті. KMU, San Francisco, 2022. Disponível em: https://web.archive.org/web/20220310141242/ ou https://www.kmu.gov.ua/news/mincifriboretsya-z-vorogom-na-cifrovomu--fronti. Acesso em: 25 jul. 2023.

KORNS, S. W.; KASTENBERG, J. E. Georgia's Cyber Left Hook. **Parameters**, Houston, v. 38, n. 4, p. 60-76, 2008. Disponível em: https://apps.dtic.mil/sti/tr/pdf/ADA636632.pdf. Acesso em: 3 jul. 2023.

KOSCHER, K. *et al.* Experimental Security Analysis of a Modern Automobile. **Institute of Electrical and Eletronics Engineers Symposium on Security and Privacy**, Oakland-CA, p. 447-462, 2010. Disponível e;: https://ieeexplore.ieee.org/document/5504804. Acesso em: 3 jul. 2023.

KOWALSKI, M. Metamorfoses da restrição do uso da força. **Anuario Janus**, Lisboa, 2014. Disponível em: http://hdl.handle.net/11144/2876. Acesso em: 18 jun. 2023.

KRASIKOV, D. V.; LIPKINA, N. N. Sovereignty in Cyberspace: A Scholarly and Practical Discussion. EUROPEAN-ASIAN LAW CONGRESS. 14., 2020. Paris. **Proceedings […]**, Paris, 2020. Tema: The Value of Law. Disponível em: https://www.atlantis-press.com/proceedings/eac-law-20/125947738. Acesso em: 25 jul. 2023.

KRASNER, S. D. Westphalia and all That. *In:* GOLDSTEIN, J.; KEOHANE, R.(eds). **Ideas and Foreign Policy: Beliefs, Institutions, and Political Change**. Ithaca, N.Y.: Cornell Univ. Press, 1993.

KRASNOWSKI, M. 2 men accused of hacking into traffic system. **The San Diego UnionTribune**, San Diego, CA, 21 jan. 2007.

KREKEL, B. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation Prepared for US Economic and Security Review Commission –China. **Northrop Grumman Corp**, [*S.l.*], 2009, p. 33. Disponível em: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf. Acesso em: 25 jul. 2023.

KRIPPENDORFF, K. The Growth of Cyberspace and the Rise of a Design Culture. *In*: WORKSHOP ON SOCIAL THEORY AND SOCIAL COMPUTING.

MIOLO_Poder, Tecnologia e Direito - 2.indd 913 26/04/2024 11:12:32

2010. Honolulu. Proceedings […], University of Hawaii, Honolulu, Hi, 2010. Disponível em: https://manoa.hawaii.edu/ccpv/workshops/KlausKrippendorff.pdf. Acesso em: 26 jul. 2023.

KUEHL, D. T. From Cyberspace to Cyberpower: Defining the Problem. p. 26-28. *In*: KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. **Cyberpower and National Security**. Nebraska: University of Nebraska Press, Potomac Books, 2009.

KUHN, T. S. **The structure of scientific revolutions**. Chicago: University of Chicago Press, 1970.

KUNZ, J. L. The nature of customary international law. **American Journal of International Law**, Cambridge, v. 47, 1953. Disponível em: https://www.jstor.org/stable/2194914. Acesso em: 14 jan. 2023.

KUROWSKA, X. The Politics of Cyber Norms: Beyond Norm Construction towards Strategic Narrative Contestation. **EU Cyber Direct: Research in Focus**, [*S.l.*], 2019, p. 18. Disponível em: https://research.aber.ac.uk/en/publications/the-politics-of-cyber-norms-beyond-norm-construction-towards-stra. Acesso em 26 fev. 2023.

LABOTT, E. We Are the First in the World to Introduce This New Warfare: Ukraine's Digital Battle Against Russia. **Politico**, [*S.l.*], 2022. Disponível em: https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880. Acesso em: 25 jul. 2023.

LACHOW, I.; RICHARDSON, C. Terrorist Use of the Internet: The Real Story. **National Defense, University of Washington DC**, Washington, 2007. Disponível em: https://apps.dtic.mil/sti/citations/ADA518156. Acesso em: 25 jul. 2023.

LAFRANIERE, S.; ANSFIELD, J. Cyberspying Fears Help Fuel China's Drive to Curb Internet. **New York Times**, New York, 2010. DIsponível em: https://www.mercurynews.com/2010/02/11/cyberspying-fears-help-fuel-chinas-drive-to-curb-internet/. Acesso em: 25 jul. 2023.

LANDLER, M.; MARKOFF, J. Digital Fears Emerge After Data Siege in Estonia. **The New York Times**, New York, 2007. Disponível em: 25 jul. 2023.

LANDLER, M.; MARKOFF, J. In Estonia, what may be the first war in cyberspace. **New York Times**, New York, 2007. Disponível em: https://www.nytimes.

MIOLO_Poder, Tecnologia e Direito - 2.indd 914 26/04/2024 11:12:32

com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html. Acesso em: 24 jul. 2023.

LANGNER, R. Stuxnet's Secret Twin. **Foreign Policy** (blog), Washington, 2013. Disponível em: https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/. Acesso em: 25 jul. 2023.

LANGNER, R. To kill a centrifuge- A technical analysis of what Stuxnet's creators tried to Achieve. **The Langner Group Arlington**, Hamburg, 2013. Disponível em: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf. Acesso em: 25 jul. 2023.

LAZZARINI, Á. Limites do Poder de Polícia. **Revista de Direito Administrativo**, Rio de Janeiro, n. 198, p. 69-83, 1994.

LEE, E. A. Cyber Physical Systems: Design Challenges. *In*: INTERNATIONAL SYMPOSIUM ON OBJECT AND COMPONENT-ORIENTED REAL-TIME DISTRIBUTED COMPUTING (ISORC), 11. 2008, Orlando. **Proceedings [...]**. Orlando: IEEE, 2008. Disponível em: https://ieeexplore.ieee.org/document/4519604. Acesso em: 25 jul. 2023.

LEINER, B. M. *et al*. A Brief History of the Internet. **The Internet Society**, Geneva, 2012. Disponível em: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet. Acesso em: 13 jun. 2023.

LESSIG, L. **Code 2.0**. Amazon: Createspace, 2006. (Basic Books).

LEVY, P. **A emergência do ciberespaço e as mutações culturais**. Tradução: Suely Rolnik. Porto Alegre: Festival Usina de Arte e Cultura, 1998. Disponível em: http://www.sescsp.org.br/sesc/conferencias/subindex.cfm?Referencia=168&ID=35&ParamEnd=9. Acesso em: 15 mai. 2023.

LEWIS, B.; MAYER-SCHONBERGER, V. Protecting Our Future - Shaping Public-Private Cooperation to Secure Critical Information Infrastructures. **Report of a Roundtable of Experts and Policy Make**rs, [*S.l.*], v. 5, 2006. Disponível em: http://www.vmsweb.net/attachments/pdf/Protecting-Report.pdf. Acesso em: 25 jul. 2023.

LEWIS, J. A. The Cyber War Has Not Begun. **Center for Strategic and International Studies**, Canada, 2010. Disponível em: http://scholar.google. com/scholar?hl=en&btnG=Search&q=intitle: The+Cyber+War+Has+Not+Begun#0. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 915 26/04/2024 11:12:32

LEYDEN, J. Israel suspected of 'hacking' Syrian air defenses. Enterprise, [*S.l.*], , 2007. Disponível em: https://www.theregister.com/2007/10/04/radar_hack_raid/. Acesso em: 25 jul. 2023.

LEYDEN, J. Polish teen derails tram after hacking train network. **The Register**, [*S.l.*], 2008. Disponível em: https://www.theregister.com/2008/01/11/tram_hack/. Acesso em: 25 jul. 2023.

LEYDEN, J. Israel suspected of 'hacking' Syrian air defenses. Enterprise, [S.l.], 2007. Disponível em: https://www.theregister.com/2007/10/04/radar_hack_raid/. Acesso em: 25 jul. 2023.

LI, S. When Does Internet Denial Trigger the Right of Armed Self-Defense? **Yale Journal of International Law**, [*S.l.*], v. 38, n. 1, 2013. Disponível em: https://ssrn.com/abstract=2226793. Acesso em: 25 jul. 2023.

LIBICKI, M. C. **Cyberdeterrence and Cyberwar**. Santa Monica: Rand Corporation, 2009.

LIBICKI, Martin C. Cyberspace Is Not a Warfighting Domain. **I/S: A Journal of Law and Policy for the Information Society**, Ohio, v. 8, 2012. Disponível em: https://kb.osu.edu/bitstream/handle/1811/73111/1/ISJLP_V8N2_321.pdf. Acesso em: 24 jul. 2023.

LIFF, Adam P. Cyberwar: A New 'Absolute Weapon? The Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, London, v. 35, n. 3, 2012, p.401-428.

LINAKI, E. Cyber warfare and international humanitarian law: A matter of applicability. **Humanitäres Völkerrecht - Informationsschriften**, Stuttgart, v. 27, n. 4, 2014, p.169-176. Disponível em: https://www.academia.edu/33552299/Cyberwarfare_and_International_Humanitarian_Law. Acesso em: 16 jul. 2023.

LINDSAY, J. R. Restrained by Design: The Political Economy of Cybersecurity. **Digital Policy, Regulation and Governance**, England, v. 19, n. 6, 2017, p. 493-514. Disponível em: https://doi.org/10.1108/DPRG-05-2017-0023. Acesso em: 16 jul. 2023.

LINDSAY, J. R. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, London, v. 22, n. 3, 2013, p.365-404. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122. Acesso em: 24 jul. 2022.

MIOLO_Poder, Tecnologia e Direito - 2.indd 916 26/04/2024 11:12:32

LITFIN, K. T. Sovereignty in world ecopolitics. **Mershon International Studies Review, The International Studies Association**, Oxford, v. 41, n. 2, p. 167-204, nov. 1997. Disponível em: https://www.jstor.org/stable/222667. Acesso em: 24 jul. 2023.

LOBATO, L. C.; KENKEL, K. M. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, Brasília, v. 58, n. 2, p. 23-43, 2015. Disponível em: https://doi.org/10.1590/0034-7329201500202 . Acesso em: 22 jul. 2023.

LONAS, L. Ukraine has used facial recognition tech to notify hundreds of Russian families of dead soldiers: report. **The Hill**, Washington, 2022. Disponível em: https://thehill.com/policy/international/3269911-ukraine-has-used-facial-recognition-tech-to-notify-hundreds-of-russian-families-of-dead-soldiers-report/. Acesso em: 25 jul. 2023.

LONGOBARDO, M. Everything is Relative, Even Gravity. **Journal of International Criminal Justice**, Oxford, v. 4, p. 1022-1023, 2016. Disponível em: https://academic.oup.com/jicj/article-abstract/14/4/1011/2236015. Acesso em: 25 jul. 2023.

LOPES, D. B.; SALIBA, A. T. A Doutrina da Responsabilidade de Proteger (RwP). **Guia de fontes em ajuda humanitária** – MSF, [*S.l.*], 2016. Disponível em: https://guiadefontes.msf.org.br/doutrina-da-responsabilidade-ao-proteger-rwp/. Acesso em: 15 jun. 2023.

LOPES, J. D. R. As funções do Estado, o princípio da legalidade e a separação de poderes no Estado Democrático de Direito. **Revista Jus Navigandi**, Teresina, ano 18, n. 3689, 2013. Disponível em: https://jus.com.br/artigos/25053. Acesso em: 1 mar. 2020.

LOTRIONTE, C.; TIKK, E. (Co-chairs). Applicability of international law to cyberspace & Characterization of cyber incidents. **Cyber Norms Workshop 2.0**, [*S.l.*], 2012. Disponível em: https://citizenlab.ca/cybernorms2012/panel3 summary.pdf. Acesso em: 12 fev. 2023.

LUBELL, N. Challenges in Applying Human Rights Law to Armed Conflict. **International Review of the Red Cross**, Genebra, v. 87, n. 860, p. 745-746, 2005. Disponível em: https://www.icrc.org/en/doc/assets/files/other/irrc_860_lubell.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 917 26/04/2024 11:12:32

LUCAS, G. R. Emerging Norms for Cyberwarfare. **Binary Bullets: The Ethics of Cyberwarfare**, New York, 2016; Oxford Academic, 2015. p. 13-33. Disponível: https://doi.org/10.1093/acprof:oso/9780190221072.003.0002. Acesso em: 25 jul. 2023.

LYNN, W. J. Defending a New Domain: The Pentagon's Cyberstrategy. **Foreign Affairs**, New York, 2010, p.97-108. Disponível em: https://www.jstor.org/stable/20788647. Acesso em: 25 jul. 2023.

MACAK, K. Civilianization of Digital Operations: A Risky Trend. **Lawfare**, [*S.l.*], 2023. Disponível em: https://www.lawfaremedia.org/article/civilianization-digital-operations-risky-trend. Acesso em: 25 jul. 2023.

MACCORMICK, N. **Questioning sovereignty**: law, state, and practical reason. Oxford: Oxford University Press, 1999.

MACHADO, J. B. **Introdução do Direito e ao Discurso Legitimador**. Coimbra: Almedina, 1989.

MAKOVSKY, D. The Silent Strike: How Israel Bombed a Syrian Nuclear Installation and Kept It Secret. **The New Yorker**, New York, 2012. Disponível em: https://www.washingtoninstitute.org/policy-analysis/silent-strike-how-israel-bombed-syrian-nuclear-installation-and-kept-it-secret. Acesso em: 25 jul. 2023.

MALAN, P. Uma perspectiva geral. *In*: BACHA, E.; *et al*. **130 Anos**: Em Busca Da República. Rio de Janeiro: Intrínseca. 2019.

MANJIKIAN, M. M. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. **International Studies Quarterly**, New York, v. 54, n. 2, 2010, p. 381-401. Disponível em: https://www.jstor.org/stable/40664172. Acesso em: 25 jul. 2023.

MARGULIES, Peter. Sovereignty and cyber-attacks: technology's challenge to the law of state responsibility. **Melbourne Journal of International Law**, [*S.l.*], v. 14, p. 496, 2013. Disponível em: https://ssrn.com/abstract= 2557517. Acesso em: 12 fev. 2023.

MATHESON, M. J. **The United States position on the relation of customary international law to the 1977 protocols additional to the 1949 Geneva Conventions**. Abingdon: Routledge, 1987. Disponível em: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315086767-8/united-states-position-relation-

MIOLO_Poder, Tecnologia e Direito - 2.indd 918 26/04/2024 11:12:32

-customary-international-law-1977-protocols-additional-1949-geneva-conventions-michael-matheson. Acesso em: 25 jul. 2023.

MATROSOV, A.; *et al*. Stuxnet under the microscope. **Institute of Electrical and Eletronics Engineers Computer Society**, [*S,l.*], 2011. Disponível em: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf. Acesso em: 25 jul. 2023.

MAURY, J. **L'Eviction de la Loi Normalement Competente**: L'Ordre Public International et la Fraude ti la Loi. Valladolid: Casa Marin éd., 1952.

MCAFEE Report. **Unsecured Economies**: Protecting Vital Information. Santa Clara – CA: MCAFEE, 2009. Disponível em: https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf. Acesso em: 25 jul. 2023.

MCDERMOTT, R. Some Emotional Considerations in Cyber Conflict. **Journal of Cyber Policy**, London, v. 4, no. 3, p. 309-25, 2019. Disponível em: https://doi.org/10.1080/23738871.2019.1701692. Acesso em: 25 jul. 2023.

MCDOUGAL, M. S. The Emerging Customary Law of Space. **Northwestern University Law Review**, Chicago, v. 58, p. 618-642, 1963-1964. Disponível em: http://hdl.handle.net/20.500.13051/1941. Acesso em: 25 jul. 2023.

MCDOUGAL, M. S.; LASSWELL, H. D.; CHEN, L.-c. **Human rights and world public order**: human rights in comprehensive context. Oxford: Oxford editor, 1977.

MEDEIROS, B. P.; GOLDONI, L. R. F. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, Rio de Janeiro, v. 42, n. 1, p. 31-54, 2020. Disponível em: https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?lang=en. Acesso em: 27 jul. 2023.

MEIRELES, G. F.; VASCONCELOS, R. B. A validade da norma no direito internacional: breves apontamentos. *In*: CONPEDI / UNICURITIBA. (Org.). 1. ed., 2013. Florianópolis. **Anais [...]**, Florianópolis: FUNJAB, 2013, v. 1. Tema: Direito internacional. p. 24-47. Disponível em: http://www.publicadireito.com.br/publicacao/unicuritiba/livro.php?gt=53. Acesso em: 27 fev. 2023.

MELKOZEROVA, V. Russian claims of revenge attack on Ukraine debunked. **Politico**, [*S.l.*], 2023. Disponível em: https://www.politico.eu/article/russian--claims-of-revengeattack-on-ukraine-kramatorsk-debunked-war/. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 919 26/04/2024 11:12:32

MELLO, C. D. A. **Curso de direito internacional público**. Rio de Janeiro: Renovar, 1992, v. II.

MELZER, N. Cyber Operations and Jus in Bello. **Disarmament Forum**, New York, n. 4, 2011. Disponível em: http://www.unidir.org/pdf/articles/pdf-art3164.pdf. Acesso em: 25 jul. 2023.

MELZER, N. **Int'l Comm**. Of The Red Cross, Interpretive Guidance On The Notion Of Direct Participation In Hostilities Under International Humanitarian Law. Geneva: International Committee of the Red Cross, 2009. Disponível em: https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf. Acesso em: 25 jul. 2023.

MELZER, N.; KUSTER, E. **International humanitarian law a comprehensive introduction**. Geneva, Switzerland: International Committee of the Red Cross. 2019. Disponível em: https://www.icrc.org/en/publication/4231-international-humanitarian-law-comprehensive-introduction. Acesso em: 2023.

MESERVE, J. US Sources: Staged cyber attack reveals vulnerability in power grid. **Cable News Network**, [*S.l.*], 2007. Disponível em: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html. Acesso em: 30 out. 2012.

MEYROWITZ, H. Le droit de la guerre et les droits de l'homme. **Revue de droit public et de la science politique en France et à l'étranger**, Paris, v. 88, 1972.

MICHAEL, J. B; WINGFIELD, T. C.; WIJESEKERA, D. Measured Responses to Cyber Attacks Using Schmitt Analysis. Proc. **Twenty-seventh Annual Int. Computer Software and Applications Conf. - IEEE**, Dallas, 2003. Disponível em: https://ieeexplore.ieee.org/document/1245406. Acesso em: 25 jul. 2023.

MILITARY AND PARAMILITARY ACTIVITIES. Case concerning the military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America). International Court of Justice, Haia, 1986. Disponível em: https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf. Acesso em: 21 jul. 2023.

MILLETT, A.; MURRAY, W. **Military Innovation in the Interwar Period**. New York: Cambridge University Press, 1996.

MILLS, I. Emergent International Humanitarian Law in the Context of Cyber Warfare. **Journal of Film and Media Studies**, Michigan, v. 2, n. 1, 2017. Dis-

MIOLO_Poder, Tecnologia e Direito - 2.indd 920 26/04/2024 11:12:32

ponível em: https://www.academia.edu/35170204/Emergent_International_Humanitarian_Law_in_the_Context_of_Cyber_Warfare. Acesso em: 25 jul. 2023.

MILONE, M. Hacktivism: Securing the National Infrastructure. **Knowledge, Technology & Policy**, Michigan, v. 16, n. 1, 2003, p.75-103. Disponível em: https://www.jstor.org/stable/40688127. Acesso em: 25 jul. 2023.

MINDUS, P. Updating Democracy Studies: Outline of a Research Program (August 18, 2011). Law, Technology and Society. WORLD CONGRESS OF IVR SPECIAL WORKSHOP, 25., 2011. Frankfurt. **Proceedings [...]**. Frankfurt: Goethe University, 2011. Tema: Legitimacy 2.0: E-democracy and Public Opinion in the Digital Age. Disponível em: https://ssrn.com/abstract=1970966 or http://dx.doi.org/10.2139/ssrn.1970966. Acesso em 01 jul. 2023.

MINISTRY OF DIGITAL TRANSFORMATION. Telegram Channel, 26 February 2022. Disponível em: https://t.me/mintsyfra/2609 ou https://archive.ph/7UYkx. Acesso em 25 jul. 2023.

MITZEN, J. Ontological Security in World Politics: State Identity and the Security Dilemma. **European Journal of International Relations**, California, v. 12, n. 3, p. 341-370, 2006. Disponível em: https://doi.org/10.1177/1354066106067346. Acesso em: 25 jul. 2023.

MORAES, A. **Direito Constitucional**. 3 ed. São Paulo: Atlas, 2015.

MOREIRA NETO, D. F. Revisão doutrinária dos conceitos de ordem pública e segurança pública. **Revista de Informação Legislativa**, Brasília, ano 25, n. 97, p. 133-154, 1988.

MOROZOV, E. An Army of Ones and Zeroes: how i became a soldier in the Georgia-Russia cyberwar. **Slate**, New York, 2008. Disponível em: http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html. Acesso em: 25 jul. 2023.

MOROZOV, E. Battling the Cyber Warmongers. **Wall Street Journal**, New York, 2010, sec. Life and Style. Disponível em: https://www.wsj.com/articles/SB10001424052748704370704575228653351323986. Acesso em: 25 jul. 2023.

MOROZOV, Evgeny. NATO Hammers Out Strategy for Cyberattack. **The Fog of Cyberwar, Newsweek**, New York, 2009. Disponível em: http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 921 26/04/2024 11:12:32

MOSELEY, T. M. **The Nation's Guardians:** America's 21st Century Air Force. Washington: Department of the Air Force Washington Dc, 2007. Disponível em: https://apps.dtic.mil/sti/citations/ADA477488. Acesso em: 25 jul. 2023.

MOSLER, H. The International Society as a Legal Community. V. 140. *In*: BRILL. **Collected Courses of the Hague Academy of International Law**. 1974. Disponível em: http://dx.doi.org/10.1163/1875-8096_pplrdc_A9789028604162_01. Acesso em: 18 jul. 2023

MOWTHORPE, M. The Revolution in Military Affairs (RMA): the United States, Russian and Chinese Views. **The Journal of Social, Political, and Economic Studies**, Washington, v. 30, n. 2, 2005. Disponível em: https://www.proquest.com/docview/216801962. Acesso em: 25 jul. 2023.

MOYNIHAN, H. The Application of International Law to Cyberspace: Sovereignty and Non intervention. **Chatham House**, London, 2019. Disponível em: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks. Acesso em: 25 jul. 2023.

MUNK CENTRE FOR INTERNATIONAL STUDIES. **Tracking GhostNet:** Investigating a Cyber Espionage Network. Toronto: Information Warfare Monitor, 2009. Disponível em: https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5f-e7708d543651/download_file?file_format=application%2Fpdf&safe_filename=Gh0stNet.pdf&type_of_work=Report. Acesso em: 16 jul. 2023.

NAÇÕES UNIDAS. **Código de conduta para os funcionários responsáveis pela aplicação da lei**. Adotado pela Assembléia Geral das Nações Unidas, no dia 17 de Dezembro de 1979, através da Resolução nº 34/169. Nações Unidas, 1979. Disponível em: https://www.mpma.mp.br/arquivos/COCOM/arquivos/centros_de_apoio/cao_direitos_humanos/direitos_humanos/trabalho_e_emprego/codConduta.htm. Acesso em: 25 jul. 2023.

NAGL, J. A. *et al*. **The US Army**/Marine Corps Counterinsurgency Field Manual. Washington: Department of the army, 2008. Disponível em: https://www.marines.mil/Portals/1/MCWP%203-33.5_Part1.pdf. Acesso em: 25 jul. 2023

NAKASHIMA, E.; KREBS, B. Obama Says He Will Name National Cybersecurity Advisor. Washington, 2009.

NATIONAL MILITARY. Strategy for Cyberspace Operations. Chairman of The Joint Chiefs Of Staff. Whashingotn, 2006. Disponível em: https://www.hsdl.org/?view&did=35693. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 922 26/04/2024 11:12:32

NATIONAL RESEARCH COUNCIL. **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**. Washington, DC: The National Academies Press, 2009. Disponível em: https://doi.org/10.17226/12651. Acesso em: 25 jul. 2023.

NATO TREATY. Washington D.C. - 4 April 1949. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf. Acesso em: 23 jun. 2023.

NATO. Wales Summit Declaration. Otan, 2014. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm. Acesso em: 25 jul. 2023.

NATO. Cyber Defence. Nato Otan, [*S.l.*], 2016. Disponível em: https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en. Acesso em 21 jul. 2023.

NATO STANDARDIZATION OFFICE. A**AP-06, NATO Glossary of Terms and Definitions**. Brussels: NATO Standardization Office, 2021. Disponível em: https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_name=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600. Acesso em: 22 Jul. 2023.

NAZARIO, J. Politically Motivated Denial of Service Attacks. *In*: CZOSSECK, C.; GEERS, K. **The Virtual Battlefield: Perspectives on Cyber Warfare**, Amsterdam: IOS Press. v. 3, 2009, p. 163-181. [IOS Press Ebook]. Disponível em: https://ccdcoe.org/uploads/2018/10/12_NAZARIO-Politically-Motivated-DDoS.pdf. Acesso em: 25 jul. 2023.

NEUMANN, J. V. Theory of Self-Reproducing Automata. Illinois: University of Illinois Press, 1966.

NIBOYET, J.-P. Le Role de la Justice Internationale en Droit International Prive. *In*: Collected Courses of the Hague Academy of International Law. **Recueil des Cours**, n° 40, 1932. Disponível em: http://dx.doi.org/10.1163/1875-8096_pplr-dc_A9789028607729_03. Acesso em: 25 jul. 2023.

NICCS. Glossary of common cybersecurity terminology, NICCS, 2015. Disponível em: https://definedterm.com/a/download/document/11128. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 923 26/04/2024 11:12:32

NORTH, D. **Structure and Change in Economic History**. New York: W.W. Norton, 1981.

NSA BLOG. Israeli Attack on Iraq's Osirak 1981: Setback or Impetus for Nuclear Weapons? **National Security Archive**, Washington, 2021. Disponível em: https://nsarchive.gwu.edu/briefing-book/iraq-nuclear-vault/2021-06-07/osirak--israels-strike-iraqs-nuclear-reactor-40-years-later. Acesso em: 25 jul. 2023.

NSPD 16. Guidelines for Offensive Cyber-War Fare. **(C) DOD**, 2002. Disponível em: www.informationwarfare.info. Acesso em: 25 jul. 2023.

NUNES, M. Distributed Terror and the Ordering of Networked Social Space. **Media/ Culture Journal**, [*S.l.*], v. 7, no. 6, 2005, p.1-3. Disponível em: https://core.ac.uk/download/pdf/345085699.pdf. Acesso em: 12 jun. 2023.

NYE JUNIOR, J. S. Deterrence and Dissuasion in Cyberspace. **International Security**, Washington, v. 41, n. 3, 2017, p. 44-71. DIsponível em: https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf. Acesso em: 25 jul. 2023.

NYE JUNIOR, J. S. Nuclear Lessons for Cyber Security? *Strategic* Studies Quarterly. Harvard Library: **Office Scholarly Communication**; v. 5, 4, p.18-38, 2011. Disponível em: http://nrs.harvard.edu/urn-3:HUL.InstRepos:8052146. Acesso em: 17 jul. 2023.

NYE JUNIOR, J. S. Cyber Power. **Belfer Center for Science and International Affairs Harvard Kennedy School**, Cambridge, MA, 2010.Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf. Acesso em: 27 jul. 2023.

O'BRIEN, M. Prosecutorial Discretion as an Obstacle to Prosecution of United Nations Peacekeepers by the International Criminal Court. **Journal of International Criminal Justice**, Oxford, v. 10, n. 3, p. 525–545, 2012. DIsponível em: https://doi.org/10.1093/jicj/mqs040. Acesso em: 25 jul. 2023.

OHLIN, J. D.; GOVERN, K.; FINKELSTEIN, C. (eds). **Cyber War**: Law and Ethics for Virtual Conflicts. Oxford: Oxford University Press, 2015. Disponível em: https://doi.org/10.1093/acprof:oso/9780198717492.001.0001. Acesso em:25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 924 26/04/2024 11:12:32

OLIVEIRA, L. P. S. **A convenção sobre diversidade biológica e o princípio da soberania nacional**. 2006. 176 f. Dissertação (Mestrado em Direito)- Universidade de Brasília, Brasília, 2006.

OLSON, K. Cyberspace as Place and the Limits of Metaphor. **Convergence**, [*S.l.*], v. 11, n. 1, p. 10-18, 2005. Disponível em: https://doi.org/10.1177/135485650501100102. Acesso em: 12 maio 2023.

O'NEILL, P. H. Russia hacked an American satellite company one hour before the Ukraine invasion. **MIT Technology Review**, [*S.l.*], 2022. Disponível em: https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/. Acesso em: 25 jul.2023.

ONU - ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Carta das Nações Unidas. 1945. Disponível em: http://www.onu.org.br/conheca-a-onu/documentos/. Acesso em 22 de junho de 2023.

ONUF, N. G. Sovereignty: outline of a conceptual history. **Alternatives: Global, Local, Political**, New York, v. 16, n. 4, p. 425-446, 1991. Disponível em: https://www.jstor.org/stable/40644726. Acesso em: 25 jul. 2023.

ORCUTT, M. Sizing Up Trump's Cyberwar Strategy. **MIT Technology Review**, [*S.l.*], 2017. Disponível em: https://www.technologyreview.com/s/603898/sizing-up-trumps-cyberwar-strategy/. Acesso em: 25 jul. 2023.

OTP - OFFICE OF THE TRIBUNAL PROSECUTOR. Resposta às Comunicações Recebidas Relativo ao Iraque, 2006. Disponível em: www.icccpi.int/Pages/item.aspx?name=otp-response-iraq-06-02-09. Acesso em: 25 jul. 2023.

OTP TPI- OFFICE OF THE TRIBUNAL PROSECUTOR. Policy Paper on Preliminary Examinations, November 2013. Disponvel em: https://www.icc-cpi.int/sites/default/files/iccdocs/otp/OTP-Policy_Paper_Preliminary_Examinations_2013-ENG.pdf. Acesso em: 13 jul. 2023.

OTTIS, R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Proceedings of the 7th EUROPEAN CONFERENCE ON INFORMATION WARFARE, 7., 2008, Tallin. **Anais [...]**, Tallin – Estonia: Academic Conferences Limited, p. 163-168, 2008. Disponível em: https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. Acesso em: 13 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 925 26/04/2024 11:12:32

OTTIS, R.; LORENTS, P. Cyberspace: Definition and Implications. INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 5., 2010. Dayton. **Anais [...]**, Dayton, OH, US: Reading: Academic Publishing Limited, p 267-270, 2010. Disponível em: https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/. Acesso em: 16 jul. 2023.

OWEN, T. **Disruptive Power***:* The Crisis of the State in the Digital Age. Oxford UP: Oxford 2015.

OWENS, W. A.; DAM, K. W.; LIN, H. S. **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**. Washington: The National Academies Press, 2009.

OWENS, W. A.; *et al.* **Technology, Policy, Law, And Ethics Regarding U.S. Acquisition and Use Of Cyberatack Capabilities**. Whashington: The National Academies Press, 2009.

OXFORD ENGLISH DICTIONARY. 2. ed. Oxford: Clarendon Press, Oxford University Press, 1989.

PADMANABHAN, V. M. Cyber Warriors and the Jus in Bello. **International Law Studies – U.S. Naval War College**, England, v. 89, p .288-298, 2013. Disponível em: https://digital-commons.usnwc.edu/ils/vol89/iss1/10/. Acesso em: 25 jul. 2023.

PARET, P. The Genesis of On War, *In*: HOWARD, M.; PARET, P. (eds.). **Introductory Essay to Carl von Clausewitz, On War**. Princeton, N.J.: Princeton Univ. Press, 1976.

PARKS, W. H. **Air War, and the Law of War**. 1. ed., New York: Routledge, v. 32, 1990.

PARKS, W. H. Part IX of the ICRC "Direct Participation in Hostilities" study: no mandate, no expertise, and legally incorrect. **International Law and Politics**, New York, v. 42, n. 769, 2010. Disponível em: https://nyujilp.org/wp-content/uploads/2012/04/42.3-Parks.pdf. Acesso em: 25 JUL. 2023.

PARTRIDGE, C. "ru-ok" ("Are you - RU - ok?"). Github, [*S.l.*], 2022. disponível em: https://web.archive.org/web/20220608112818/https://github.com/tweedge/ru-ok. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 926 26/04/2024 11:12:32

PASCUCCI, P. Distinction and Proportionality in Cyberwar: virtual problems with a real solution. **Minnesota Journal of International Law**, Minnesota, v. 26, n. 2, p.419-460, 2017. Disponível em: https://core.ac.uk/download/pdf/217210854.pdf. Acesso em: 17 jul. 2023.

PCIJ - PERMANENT INTERNATIONAL COURT OF JUSTICE. Chorzow Factory Case, (ser. A) n. 13, at 28, 1928.

PENA, R. F. A. Era da informação. UOL, Goiânia, 2013. Disponível em: http://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm. Acesso em: 12 fev. 2022.

PERLOFF-GILES, A. **Note: Transnational Cyber Offenses**: Overcoming Jurisdictional Challenges. Yale: Yale University Press, 2018. Disponível em: https://library.au.int/note-transnational-cyber-offenses-overcoming-jurisdictional-challenges. Acesso em: 25 jul. 2023.

PERLROTH, N. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. **New York Times**, New York, 2012. Disponível em: http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudioil-frm-disquiets-us.html?pagewanted=all&_r=0. Acesso em: 25 jul. 2023.

PERSILY, N. **The Internet's Challenge to Democracy**. New York: New York University. 2017, Disponível em: https://www.law.nyu.edu/sites/default/files/Nate%20Persily%20The%20Internets%20Challenge%20to%20Democracy.pdf. Acesso em 25 jul. 2023.

PICTET, J. **Comité International de la Croix Rouge**: Commentaire du plan d'un cours sur le droit international humanitaire. Genebra: CICR, 1976. Disponível em: https://library.icrc.org/library/docs/DOC/icrc-4268-001.pdf. Acesso em: 25 jul. 2023.

PIHELGAS, M. Back-Tracing and Anonymity in Cyberspace. *In:* ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Tallinn: International Law, International Relations and Diplomacy, NATO CCD COE Publication, 2013.

PIPYROS, K.; *et al*. Cyberoperations and international humanitarian law. **Information & Computer Security**, England, v. 24, n. 1 p. 38 -52, 2016. Disponível em: http://dx.doi.org/10.1108/ICS-12-2014-0081. Acesso em: 17 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 927 26/04/2024 11:12:32

PLAWSKI, S. **Etude des principes fondamentaux du Droit International Pènal**. Paris: Librairie Generale de Droit et de Jurisprudence, 1972.

POPKIN, J. D. **Journals: The New Face of News**. Chapter 8 of Darnton and Roche, Revolution in Print. Berkeley: University of California Press in collaboration with the New York Public Library, 1989.

PORCHE, I. R.; SOLLINGER, J. M.; MCKAY, S. *A* **Cyberworm that Knows No Boundaries**. Santa Monica, CA: RAND Corporation, 2011. Disponível em: https://www.rand.org/pubs/occasional_papers/OP342.html. Acesso em: 25 jul. 2023.

POST, D. G. Against Cyberanarchy. **Berkeley Technology Law Journal**, Berkeley, v. 17, p. 1375-76, 2002. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=334581#. Acesso em: 25 jul. 2023.

POULSEN, K. Cyberwar' and Estonia's Panic Attack. **Wired**, [*S.l.*], 2007. Disponível em: http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html. Acesso em: 25 jul. 2023.

PRESSE, F. Rússia veta resolução do Conselho de Segurança da ONU sobre anexações; Brasil e China se abstêm. **Globo, G1**, São Paulo, 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/09/30/russia-veta-resolucao-do-conselho-de-seguranca-da-onu-sobre-anexacoes-brasil-e-china-se-abstem.ghtml. Acesso em: 25 jul. 2023.

PTC- Situation in Darfur, Sudan, Decision on the Confirmation of Charges. **The Prosecutor v. Bahr Idriss Abu Garda**, Sudan, 2010. Disponível em: https://www.icc-cpi.int/court-record/icc-02/05-02/09-243-red. Acesso em: 14 jul. 2023.

PTC- Situation in Kenya, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya. Pre-Trial Chamber II, ICC-01/09-19-Corr. **International Criminal Court (ICC)**, Kenya, 2010.

PTC- Situation in Mali, Judgment and Sentence, Trial Chamber VIII, ICC-01/12-01/15-171, 27 September 2016, para. 77. **International Criminal Court (ICC)**, 2016.

PTC- Situation in the DRC, Decision on the Prosecutor's Application for Warrants of Arrest, Pre-Trial Chamber I, ICC-01/04-01/06-8-Corr. **International Criminal Court (ICC)**, 2006.

MIOLO_Poder, Tecnologia e Direito - 2.indd 928 26/04/2024 11:12:32

PTC- Situation in the Islamic Republic of Afghanistan, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan., Pre-Trial Chamber II, ICC-02/17. **International Criminal Court (ICC)**, 2019.

PTC- Situation in the Republic of Coˆte d'Ivoire, Corrigendum to "Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Republic of Coˆte d'Ivoire", Pre-Trial Chamber III, ICC-02/11-14-Corr. **International Criminal Court (ICC)**, 2011.

PTC- Situation on Registered Vessels of the Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia, Decision on the Request of the Union of the Comoros. **International Criminal Court (ICC)**, 2015. Disponível em: https://www.icc-cpi.int/court-record/icc-01/13-34. Acesso em: 23 jun. 2023..

RAFTER, D. What is a botnet? **Norton site**, [*S.l.*], 2022. Disponível em: http://us.norton.com/botnet/. Acesso em: 25 jul. 2023.

RAMIRO, C. H. L.; HERRERA, L. H. M. Hans Kelsen: filosofia jurídica e democracia. **Revista de informação legislativa**, Brasília, v. 52, n. 205, p. 235-260, jan./mar. 2015. Disponível em: https://www12.senado.leg.br/ril/edicoes/52/205/ril_v52_n205_p235.pdf. Acesso em: 01 fev. 2021.

RANDELZHOFER, A. Article 2(4). *In*: SIMMA, B. *et al.* (eds.). **The Charter of the United Nations**: a commentary. 2. ed. Oxford: OUP, 2002.

RASHID, H. It Army of Ukraine Hit Russian Banking Giant with Crippling DDoS Attack. **Hack Read**, United Kingdon, 2022. Disponível em: https://www.hackread.com/it-army-ofukraine-russia-bank-ddos-attack/. Acesso em: 25 jul. 2023.

RATTRAY, G. An Environmental Approach to Understanding Cyberpower. *In*: KRAMER, F. D.; STARR, S.; WENTZ, L. K. (ed.). **Cyberpower and National Security**. Washington, D.C.: National Defense UP, 2009.

RAUSCHER, K. F.; YASCHENKO, V. (ed.). **The Russia - U.S. Bilateral on Cybersecurity**: Critical Terminology Foundations. Moscow: EastWest Institute and the Information Security Institute of Moscow State University, 2011.

RAVIV, D.; MELMAN, Y. **Spies Against Armageddon:** Inside Israel's Secret Wars. NY: Levant Books, 2012.

MIOLO_Poder, Tecnologia e Direito - 2.indd 929 26/04/2024 11:12:32

REISMAN, W. M.; BAKER, J. E. Regulating Covert Action. Yale: Yale University Press, 1992.

REMUS, T. Cyber-Attacks and International Law of Armed Conflicts: A 'Jus Ad Bellum' Perspective. **Journal of International Commercial Law and Technology**, [*S.l.*], v. 8, n. 3, p. 179-189, 2013. Disponível em: https://ssrn.com/abstract=1946470. Acesso em: 25 jul. 2023.

REPORT ICC- Situação em Embarcações Registradas de Camarões, Grécia e Camboja, Artigo 53°(1) Report, ICC-01/13-6-AnxA, 2014. Disponível em: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2019_00871.PDF. Acesso em: 23 jun. 2023.

REPORT MYANMAR. Report of the Independent International Fact-Finding Commission on Myanmar, UN Doc. (A/HRC/39/64). Human Rights Council, 2018. Disponível em: https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf. Acesso em: 25 jul.2023.

REPORT OF ARBITRAL TRIBUNAL. Guyana v. Suriname maritime delimitation case, award of 17 September 2007. Disponível em: https://legal.un.org/riaa/cases/vol_XXX/1-144.pdf. Acesso em: 23 jul. 2023.

REPUBLIC of Korea, Report to the United Nations Secretary General 1. AmazonaWS, [*S.l.*], 2014. Disponível em: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2014/10/ROK.pdf. Acesso em: 25 jul. 2023.

RESS, G. Interpretation of the Charter. *In*: SIMMA, B. (ed.). **The Charter of the United Nations***:* a Commentary. Oxfrd: Oxford University Pres, 2002.

REUTER, P.; COMBACAU, J. **Institutions et relations internationales**. Paris: PUF, 1980.

REZEK, J. F. **Direito Internacional Público**: curso elementar. 13. ed. São Paulo: Saraiva, 2011.

RHODES, R. **The Making of the Atomic Bomb**. London: Simon & Schuster, 2012.

RICHARDSON, J. C. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. **SSRN**, New York, 2011. Disponível em: https://ssrn.com/abstract=1892888. Acesso em: 25 JUL. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 930 26/04/2024 11:12:32

RID, T. **Cyber War Will Not Take Place**. 4. ed. London: Hurst, 2013.

RID, T. Cyber War Will Not Take Place. **Journal of Strategic Studies**, London, v. 35, no. 1, 2012. Disponível em: https://doi.org/10.1080/01402390.2011.608939. Acesso em: 17 jul. 2023.

RID, T.; BUCHANAN, B. Attributing Cyber Attacks. **Journal of Strategic Studies**, London, v. 38, n. 1-2, 2015, p. 4-37. Disponível em: https://doi.org/10.1080/01402390.2014.977382. Acesso em: 25 JUL. 2023.

ROBERTS, G. The New Rules for Waging War: The Case Against Ratification of Additional Protocol I. **The Michigan Law Review Association**, Michigan, v. 26, n. 3, 1985. Disponível em: https://www.jstor.org/stable/40041627. Acesso em: 25 jul. 2023.

ROBINSON, M.; JONES, K.; JANICKE, H. Cyber Warfare: Issues and Challenges. **Computers & Security**, [*S.l.*], v. 49, p. 70-94, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404814001692. Acesso em: 17 jul. 2023.

RODENHÄUSER, T.; *et al.* Signaling legal protection in a digitalizing world: a new era for the distinctive emblems? **ICRC Humanitarian Law & Policy Blog**, [*S.l.*], 2021. Disponível em: https://blogs.icrc.org/law-and-policy/2021/09/16/legal-protection-digital-emblem/. Acesso em: 25 jul. 2023.

ROGERS, A. Combatant Status. *In*: WILMSHURST, E.; BREAU, S. (eds). **Perspectives on the ICRC Study of Customary International Humanitarian Law**. Geneve: CUP, 2007.

ROGERS, K. Beyonce Faces Police Boycott of Her Concert in Miami, **New York Times**, New York, 2016. Disponível em: https://www.nytimes.com/2016/02/20/arts/music/beyonceconcertboycotted-by-police-group-over-halfti. Acesso em: 25 jul. 2023.

ROLLINS J.; HENNING, A. C. Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations. **Congressional Research Service**, CRS Report for Congress: Prepared for Members and Committees of Congress, 2009. Disponível em: https://obamawhitehouse.archives.gov/files/documents/cyber/Congressional%20Research%20Service%20%20CNCI%20%20Legal%20Authorities%20and%20Policy%20Considerations%20%28March%202009%29.pdf. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 931 26/04/2024 11:12:32

ROMANDASH, A. Ukraine's IT Army: Digital Resistance to Russian Propaganda. *In*: O'Brien, J. **Peace Policy:** Solutions to Violent Conflict, May 2023. Notre Dame: Kroc Institute for International Peace Studies, 2023. Disponível em: https://doi.org/10.7274/qr46qz24c90. Acesso em: 23 jul. 2023.

ROMM, T. "Pro-Beyoncé" vs. "Anti-Beyoncé:" 3,500 Facebook Ads Show the Scale of Russian Manipulation, POST, Wash. May 10, 2018; Olivia Solon & Julia Carrie, #BlueLivesMatter and Beyoncé: Russian Facebook Ads Hit Hot-Button US Issues. **The Guardian**, New York, 2018. Disponível em: https://www.theguardian.com/usnews/2018/may/10/russia-facebook-ads-us-elections-congress. Acesso em: 25 jul. 2023.

RORTY, R. **Objetivismo, relativismo e verdade**. Rio de Janeiro: Dumará, 2002.

ROSCINI, M. **Cyber operations and the use of force in international law**. Oxford: Oxford University Press, 2014.

ROSCINI, M. Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations. **Texas International Law Journal**, Texas, v. 50, 2015. DIsponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2611753. Acesso em: 24 jul. 2023.

ROSCINI, M. Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes. **Criminal Law Forum**, v. 30, 2019, p. 247-272. Disponível em: http://dx.doi.org/10.2139/ssrn.3435439. Acesso em: 25 jul. 2023.

ROSCINI, M. Worldwide Warfare—Jus ad bellum and the Use of Cyber Force. **Max Planck Yearbook of United Nations Law**, Boston, v. 14, p. 85-130, 2010. Disponível em: https://ssrn.com/abstract=1683370. Acesso em: 24 jul. 2023.

ROSENFIELD, D. K. Rethinking Cyber War. **A Journal of Politics and Society**, Columbia, v. 21, n. 1, p.77-90, 2009. Disponível em: https://doi.org/10.1080/08913810902812156. Acesso em: 25 JUL. 2023.

ROSENSTOCK, R. The Declaration on Principles of International Law Concerning Friendly Relations. **The American Journal of International Law**, Cambridge, v. 65, n. 5, 1971. Disponível em: https://www.jstor.org/stable/2199354. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 932 26/04/2024 11:12:32

ROUSSEFF, D. Statement by brazilian president H. E. Dilma Rousseff on September 24, 2013 at the Opening of the General Debate of the 68th session of the United Nations General Assembly. Translated reprint at 2. 2013. Diponível em: http://gadebate.un.org/sites/default/fles/gastatements/68/BR_en.pdf. Acesso em: 25 jul. 2023.

RUSSIA FEDERATION. **Appendix:** Developments in the field of information and telecommunications in the context of international security Russian Federation. draft resolution, 3. New York: United Nations, 1998. Disponível em: https://digitallibrary.un.org/record/263069. Acesso em: 25 jul. 2023.

RUSSIA FEDERATION. Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. Annex: Letter dated 23 September 1998 from the Minister for Foreign Affairs of the Russian Federation addressed to the Secretary General, 2. New York: United Nations, 1998. Disponível em: https://digitallibrary.un.org/record/261158. Acesso em: 25 jul. 2023.

RUTH, I.; PANOS, L. Identifying Data And Information Streams in Cyberspace: A Multi-Dimensional Perspective. **ArXiv**, [*S.l.*], 2019. Disponível em: https://arxiv.org/abs/1906.03757. Acesso em: 18 jun. 2023.

RUYS, T. The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)? **American Journal of International Law**, Cambridge, v. 108, 2014, p. 159-210. Disponível em: https://doi.org/10.5305/amerjintelaw.108.2.0159. Acesso em: 17 jul. 2023.

RYABOSHTAN, I. Мстислав Банік, Мінцифри: Західні компанії не мають ставати спонсорами російського вторгнення та загибелі українців," Media Sapens, [*S.l.*], 2022. Disponível em: https://web.archive.org/web/20220608112712/ ou https://ms.detector.media/internet/post/29223/2022-03-23-mstyslav-banik-mintsyfry-zakhidni-kompaniine-mayut-stavaty-sponsoramy-rosiyskogo-vtorgnennya-ta-zagybeliukraintsiv/ ou https://ms.detector.media/internet/post/29223/2022-03-23-mstyslav-banik-mintsyfry-zakhidni-kompaniine-mayut-stavaty-sponsoramy-rosiyskogo-vtorgnennya-ta-zagybeliukraintsiv/. Acesso em: 25 jul. 2023.

SABADELLO, M. The Role of New Media for the Democratization Processes in the Arab World. Dokumen, [*S.l.*], 2011. Disponível em: https://dokumen.tips/documents/the-role-of-new-media-for-the-democratization-processes-in-the--2015-11-13-the.html?page=10. Acesso em 27 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 933 26/04/2024 11:12:32

SALDAN, E. **Os desafios jurídicos da guerra no espaço cibernético**. 2012. 118 f. Dissertação (Mestrado em Direito Constitucional)- Instituto Brasiliense de Direito Público, Brasília, 2012.

SANDER, B. Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections. **Chinese Journal of International Law**, Oxford, v. 18, n. 1, p. 1-56, 2019. Disponível em: https://ssrn.com/abstract=3341681. Acesso em: 22 set. 2020.

SANDHOLTZ, W.; WHYTOCK, C. A. The Politics of International Law. Research handbook on the politics of international law. **UC Irvine School of Law Research**, Irvine, 2018. Disponível em: https://ssrn.com/abstract=3141357. Acesso em: 25 jul. 2023.

SANDOZ, Y. *et al (*eds). Commentary on the additional protocols of 8 june 1977 to the geneva conventions of 12 august 1949. **International Committee of the red Cross**, Geneva, 1987. Disponível em: https://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_ Protocols.pdf. Acesso em: 25 jul 2023.

SANGER, D. E. **The Perfect Weapon***:* War, Sabotage, and Fear in the Cyber Age. Reprint edition. New York: Broadway Books, 2019.

SANGER, D.; MARKOFF, J. Obama Outlines Coordinated Cyber-Security Plan. **New York Times**, New York, 2009. Disponível em:

SANTOS, S. O Uso da Força no Direito Internacional e os desafios ao paradigma onusiano. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 61, pp. 533 - 568, jul./dez. 2012. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/P.0304-2340.2012v61p533/237. Acesso em: 15 jun. 2023.

SASSÒLI, M. **International Humanitarian Law Rules, Controversies, and Solutions to Problems Arising in Warfare**. Massachusetts: Edward Elgar Publishing Limited, 2019.

SAUTER, M.; ZUCKERMAN, E. **The Coming Swarm:** DDOS Actions, Hacktivism, and Civil Disobedience on the Internet. New York: Bloomsbury Academic, 2014.

SAXON, D. Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions. **Journal**

MIOLO_Poder, Tecnologia e Direito - 2.indd 934 26/04/2024 11:12:32

of Conflict and Security Law, Oxford, v. 21, n. 3, 2016. Disponóvel em: https://doi.org/10.1093/jcsl/krw018. Acesso em: 24 jul. 2023.

SCHABAS, W. A. Enforcing International Humanitarian Law: Catching the Accomplices. **International Committee of the Red Cross**, Geneva, v. 83, n. 842, p. 442–43, 2001. Disponível em: https://www.icrc.org/en/doc/assets/files/other/439-460_schabas.pdf. Acesso em: 25 jul. 2023.

SCHABAS, W. A. Prosecutorial Discretion v. Judicial Activism at the International Criminal Court. **Journal of International Criminal Justice**, Oxford, v. 6, n. 4, 2008. Disponível em: https://doi.org/10.1093/jicj/mqn045. Acesso em: 14 jul. 2023.

SCHABAS, W. A.; ZEIDY, M. M. El, 'Article 17'. *In*: TRIFFTERER, O.; AMBOS, K. (eds.). **The Statute of the International Criminal Court**: a Commentary. 3. ed., München/Oxford/ Baded-Baden: C.H. Beck-Hart-Nomos, 2016.

SCHABAS, W.A. **An Introduction to the International Criminal Court**. 5. ed., Cambridge: Cambridge University Press, 2017.

SCHACHTER, O. The Right of States To Use Armed Force. **Michigan Law Review**, Michigan, v. 82. p.1620-1624, 1984. Disponível em: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=3592&context=mlr. Acesso em: 24 jul. 2023.

SCHECTMAN, J.; BING, C. Exclusive Ukraine calls on hacker underground to defend against Russia. Reuters, [*S.l.*], 2022. Disponível em: https://web.archive.org/web/20220608141232/https://www.reuters.com/world/exclusive-ukraine--calls-hacker-underground-defendagainst-russia-2022-02-24/. Acesso em: 25 jul. 2023.

SCHEIER, F. Retrieved from Geneva Centre for the Democratic Control of Armed Forces (DCAF). **Cyberwarfare**, Geneva, n. 7, 2015. Disponível em: https://www.dcaf.ch/cyberwarfare. Acesso em: 15 jun. 2023.

SCHIER, A. C. R.; MELO, J. A. M. H. O direito à participação popular como expressão do Estado Social e Democrático de Direito. **A&C – Revista de Direito Administrativo & Constitucional**, Belo Horizonte, ano 17, n. 69, p. 127- 147, jul./set. 2017. Dosponível em: https://www.10.21056/aec.v17i69.825. Acesso em: 15 jun. 2023.

SCHMITT, M. N. (ed.). **Tallinn Manual on the International Law Applicable to Cyber Warfare**. Cambridge ; New York: Cambridge University Press, 2013.

MIOLO_Poder, Tecnologia e Direito - 2.indd 935 26/04/2024 11:12:32

SCHMITT, M. N. "Attack" as a Term of Art in International Law: the cyber operations context. *In*: OTTIS, R.; ZIOLKOWSKI, K. (Eds.) INTERNATIONAL CONFERENCE ON CYBER CONFLICT. 4., 2012. Taillinn. **Proceedings [...]**, Taillinn: Nato CCD COE, 2012. Disponível em: http://www.ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf. Acesso em: 25 jul. 2023.

SCHMITT, M. N. "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law. **Chicago Journal of International Law**, Chicago, v. 19, n. 1, 2018. Disponível em: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1736&context=cjil. Acesso em: 25 jul. 2023.

SCHMITT, M. N. Computer network attack and the use of force in international law: thoughts on a normative framework**Columbia Journal of Transnational Law**, New York, v. 37, n. 7, 1999. Disponível em: https://ssrn.com/abstract=1603800. Acesso em: 17 fev. 2023.

SCHMITT, M. N. Deconstructing Direct Participation in Hostilities: The Constitutive Elements. **International Law and Politics**, New York, v. 42, n.697, 2010. Disponível em: https://nyujilp.org/wp-content/uploads/2012/04/42.3-Schmitt.pdf. Acesso em: 25 jul. 2023.

SCHMITT, M. N. Grey Zones in the International Law of Cyberspace. **The Yale Journal of International Law**, Yale, v. 42, p. 1-21, 2017a. Disponível em: https://www.yjil.yale.edu/grey-zones-in-the-international-law-of-cyberspace/. Acesso em: 13 fev. 2023.

SCHMITT, M. N. **Tallinn Manual 2.0 on the international law applicable to cyber operations**. Cambridge: Cambridge University Press, 2017b. Disponível em: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf. Acesso em: 25 fev. 2023.

SCHMITT, M. N. The Law of Cyber Warfare: Quo Vadis? **Stanford Law & Policy Review**, Stanford, v. 25, p.269-299, 2014a. Disponível em: https://ssrn.com/abstract=2320755. Acesso em: 25 jul. 2023.

SCHMITT, M. N. The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision. **Israel Law Review**, New York, v. 48, p.81-109, 2015a. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2557989. Acesso em: 25 JUL. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 936 26/04/2024 11:12:32

SCHMITT, M. N. The State of Humanitarian Law in Cyber Conflict. **Just Security**, New York, 2015b. Disponível em: https://www.justsecurity.org/18891/state--humanitarian-lawcyber-conf. Acesso em: 25 JUL. 2023.

SCHMITT, M. N. Wired Warfare: Computer Network Attack and Jus in Bello. **International Review of the Red Cross**, Genebra, v. 84, n. 846, 2002, p. 377. Disponível em: https://www.icrc.org/en/doc/assets/files/other/365_400_schmitt.pdf. Acesso em: 25 jul. 2023.

SCHMITT, M. N. Cyber Operations and the Jus in Bello: Key Issues (March 2, 2011). **Naval War College International Law Studies**, [*S.l.*], 2011. Disponível em: https://ssrn.com/abstract=1801176. Acesso em 27 jul. 2023.

SCHMITT, M. N..; VIHUL, Liis. Proxy Wars in Cyber Space: The Evolving International Law of Attribution. I(II) **Fletcher Security Review**, [*S.l.*], p. 55-73, 2014b. Disponível em: . Acesso em: 25 JUL. 2023.

SCHMITT, M. N.; VIHUL, L. Sovereignty in Cyberspace: Lex Lata Vel Non?111 **American Journal of International Law Unbound**, Cambridge, v. 213, 2017c. Disponível em: https://ssrn.com/abstract=3024405. Acesso em: 13 fev. 2023.

SCHMITT, M. N.; VIHUL, L. **The nature of international law cyber norms**. Tallinn: Tallinn Paper, n. 5, 2014c. Disponível em: https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf. Acesso em: 25 jul. 2023.

SCHULTZ, T. Private Legal Systems: what cyberspace might teach legal theorists. **Yale Journal of Law & Technology**, Yale, v. 10, 2008. Disponível em: https://digitalcommons.law.yale.edu/yjolt/vol10/iss1/5. Acesso em: 14 fev. 2023.

SCHWARZENBERGER, G. Power politics. London: Stevens and Sons Ltd. 1964. xxi and 590 and (index) 24 pp. 70s. net. (1964). **Journal of African Law**, Cambridge, v. 8, n. 2, p. 150-150. Disponível em: https://www.jstor.org/stable/1090950. Acesso em: 25 jul 2023.

SCO - SHANGHAI COOPERATION ORGANIZATION. Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security. **Plenary Meeting**, Shanghai, 2008. Disponível em: https://cis-legislation.com/document.fwx?rgn=28340. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 937 26/04/2024 11:12:32

SCOTT, A. N. Can Cyberterrorists Actually Kill People? **Sans Institute Infosec Reading Room**, [*S.l.*], 2002. Disponível em: https://www.sans.org/reading-room/whitepapers/warfare/cyberterrorists-kill-people-820. Acesso em: 25 jul. 2023.

SCOTT, M. How Ukraine used Russia's digital playbook against the Kremlin. **Politico**, [*S.l.*], 2022. Disponível em: https://www.politico.eu/article/ukraine-russia-digitalplaybook-war/. Acesso em: 25 jul. 2023.

SEGAL, A. **Chinese Cyber Diplomacy in a New Era of Uncertainty**. Washington, DC: Hoover Institution, 2017. Disponível em: https://www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty. Acesso em: 22 jul. 2023.

SEYMOUR, M. H. The Online Threat. **New Yorker**, New York, 2010. Disponível em: https://www.newyorker.com/magazine/2010/11/01/the-online-threat. Acesso em: 17 jul. 2023.

SHACKELFORD, S. J. From nuclear war to net war: analogizing cyber attacks in International Law. **Berkley Journal of International Law**, Berkley, v. 25, n. 3, 2009. Disponível em: https://ssrn.com/abstract=1396375. Acesso em: 25 jul 2023.

SHACKELFORD, S. J.; ANDRES, R. B., State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. **Georgetown Journal of International Law**, Georgetown, v. 42, 2011. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/geojintl42&div=35&id=&page=. Acesso em: 17 jul. 2023.

SHAKARIAN, P.; SHAKARIAN, J.; RUEF, A. **Introduction to cyber-warfare**: A multidisciplinary approach. Oxford: Syngress, 2013.

SHANE QUINLAN, J. Bomb Hack? U.S. Cyber Capabilities and the Suppression of Enemy Air Defenses. **Georgetown Security Studies Review**, Georgetown, 2014. Disponível em: http://georgetownsecuritystudiesreview.org/2014/04/07/jam-bomb-hack-new-us-cyber-capabilities-and-the-suppression-of-enemy-air-defenses/. Acesso em: 25 jul. 2023.

SHARP, W. G. Cyberspace and the use of force. **Falls Church**, Berkeley, p.88-91, 1999. Disponível em: https://lawcat.berkeley.edu/record/106826. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 938 26/04/2024 11:12:32

SHAW, M. N. **International law**. 8. ed. Cambridge: Cambridge University Press, 2017.

SHELDON, J. B. Deciphering Cyberpower: Strategic Purpose in Peace and War. **Strategic Studies Quarterly**, Harvard, 2011. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf. Acesso em: 25 jul 2023.

SHELEST, H. Defend. Resist. Repeat: Ukraine's lessons for European defence. **The European Council on Foreign Relations**, London, 2022. Disponível em: https://ecfr.eu/publication/defend-resist-repeat-ukraines-lessons-for-european--defence/. Acesso em: 25 jul. 2023.

SHERMAN, A. Hillary Clinton Claims Donald Trump Invited Russian President Vladimir Putin to Hack Americans. **Politifact**, Flórida, 2016. Disponível em: http://www.politifact.com/truth-o-meter/statements/2016/sep/26/hillaryclinton/hillary-clintonclaims-donald-trump-invited-russia/. Acesso em 25 jul. 2023.

SHORE, J. Don't Underestimate Ukraine's Volunteer Hackers. **Foreign Policy**, Washington, 2022. Disponível em: https://foreignpolicy.com/2022/04/11/russia--cyberwarfare-us-ukraine-volunteer-hackers-it-army/. Acesso em: 25 jul. 2023.

SILVA, A. C. O princípio da segurança jurídica (proteção à confiança) no direito público brasileiro. **Revista Brasileira de Direito Público – RBDP,** Porto Alegre, v. 2, n. 6, p. 7-59, 2004. Disponível em: https://doi.org/10.12660/rda.v237.2004.44376. Acesso em: 25 jul. 2023.

SILVER, D. Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter. **International Law Studies**, England, v. 76, 2002. Disponível em: https://core.ac.uk/download/pdf/236321477.pdf. Acesso em: 25 jul. 2023.

SIMONCINI, A. The Constitutional Dimension of the Internet: Some Research Paths. **EUI Department of Law Research Paper**, Florença, n. 2016/16, 2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2781496. Acesso em: 23 jun. 2023.

SIMONITE, T.; VOLPICELLI, G. M. Ukraine's Digital Ministry is a Formidable War Machine. **Wired**, [*S.l.*], 2022, Disponível em: https://www.wired.com/story/ukraine-digital-ministry-war/. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 939 26/04/2024 11:12:32

SINGER, P. W.; FRIEDMAN, A. **Cybersecurity and cyberwar:** what everyone needs to know. New York: Oxford University Press, 2014.

SLIEDREGT, E. v. Command Responsibility and Cyberattacks. **Journal of Conflict and Security Law**, Oxford, v. 21, n. 3, 2016. Disponível em: https://www.jstor.org/stable/26298213. Acesso em: 23 jul. 2023.

SMITH, R.; BARRY, R. America's Electric Grid Has a Vulnerable Back Door and Russia Walked Through It. **Wall Street Journal**, New York, 2019. Disponível em: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112. Acesso em: 25 jul. 2023.

SMITH, T. Hacker jailed for revenge sewage attacks Job rejection caused a bit of a stink. **The Register**, [*S.l.*], 2001. Disponível em: https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/. Acesso em: 25 jul. 2023.

SOARES, F. S. C. O direito à legítima defesa como exceção da proibição do uso da força no contexto pós-criação da ONU. *In*: CONPEDI - CONSELHO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM DIREITO. (Org.). 22., 2013. São Paulo. **Anais [...],** São Paulo: FUNJAB, 2013. Tema: Sociedade global e seus impactos sobre o estudo e a efetividade do Direito na contemporaneidade, p. 320-349.

SOESANTO, S. **The IT Army of Ukraine Structure, Tasking, and Ecosystem**. ETH Zürich: Cyberdefense Report Center for Security Studies (CSS), 2022. Disponível em: css.ethz.ch/en/publications/risk-and-resilience-reports.html. Acesso em: 25 jul. 2023.

SOFAER, A. D. International Law and the Use of Force. **American Society of International Law Proceedings**, Cambridge, v. 82, p. 420- 422, 1988. Disponível em: https://www.jstor.org/stable/25658436. Acesso em: 25 jul. 2023.

SOHAIL, H. Fault Lines In The Application Of International Humanitarian Law To Cyberwarfare. **Journal of Digital Forensics, Security and Law**, [*S.l.*], v. 17, article 8, 2022. Disponível em: https://commons.erau.edu/jdfsl/vol17/iss1/8. Acesso em: 25 jul. 2023.

SOLCE, N. The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force. **Journal of Science and Technology**, Washington, v. 18, n. 293, 2008. Disponível em: https://www.albanylawscitech.org/article/19149-the-battlefield-of-cyberspace-the-inevitable-new-military-branch-the-cyber-force. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 940 26/04/2024 11:12:32

STAHN, C. A **Critical Introduction fo International Criminal Law**. Cambridge: Cambridge University Press, 2019.

STARR, S. H. Toward a Preliminary Theory of Cyberpower. *In*: KRAMER, F. D.; STARR, S.; WENTZ, L. K. (eds.). **Cyberpower and National Security.** Washington D.C.: National Defense UP, 2009.

STATE OF MICHIGAN EXECUTIVE OFFICE. Michigan cyber disruption response strategy: protecting Michigan's critical infrastructure and systems. Michigan, 2013. Disponível em: https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf. Acesso em: 25 jul. 2023.

STAVRIDIS, J.; WEINSTEIN, D. The Internet of Things Is a Cyberwar Nightmare. **Foreign Policy (blog)**, Congers, 2016. Disponível em: https://foreignpolicy.com/2016/11/03/theinternet-of-things-is-a-cyber-war-nightmare/. Acesso em: 25 jul. 2023.

STEGMILLER, I. The Gravity Threshold under the ICC Statute: Gravity Back and Forth in Lubanga and Ntaganda. **International Criminal Law Review**, [*S.l.*], 2009. Disponível em: https://brill.com/view/journals/icla/9/3/article-p547_4.xml. Acesso em: 13 jul. 2023.

STEGMILLER, I. **The Pre-Investigation Stage of the ICC**: criteria for situation selection. Berlin: Duncker & Humblot, 2011.

STOCKBURGER, P. Z. Known unknowns: State Cyber Operations, Cyber Warfare, and the jus ad bellum. **American University International Law Review**, New York, v. 31, n. 4, 2016. Disponível em: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?referer=https://www.google.com.br/&httpsredir=1&article=1898&context=auilr. Acesso em: 25 fev. 2023.

STOLLEIS, M. **Nationalität und Internationalität**. Rechtsvergleichung im öffentlichen Recht des 19. Jahrhunderts (1998). Mainz: Akademie der Wissenschaften und der Literatur, 1998.

STONE, J. **Conflict Through Consensus**: United Nations Approaches to Aggression. Baltimore, Maryland, EUA: The Johns Hopkins University Press, 1977.

STONE, J. Non Liquet and the Function of Law in the International Community. **British Yearbook of International Law**, London, v. 35, 1959. Disponível

MIOLO_Poder, Tecnologia e Direito - 2.indd 941 26/04/2024 11:12:32

em: https://www.taylorfrancis.com/chapters/edit/10.4324/9781315087795-15/non-liquet-function-law-international-community-1-julius-stone. Acesso em: 25 jul. 2023.

STRATE, L. The Varieties of Cyberspace: Problems in Definition and Delimitation. **Western Journal of Communication**, Western, v. 63, n. 3, p. 382-412, 1999. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/10570319909374648. Acesso em: 24 jul. 2023.

STRATEGIC TECHNOLOGY OFFICE. The National Cyber Range: A National Testbed for Critical Security Research. **White House**. Washington, Disponível em: http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf. Acesso em: 13 dez. 2022.

STRECK, J. **Pulling the Plug on Electronic Town Meetings**: Participatory Democracy and the Reality of Usenet. New York: Routledge, 1998. Disponível em: https://t.me/studentcyberarmy/193 ou https://archive.ph/mfXYH. Acesso em: 25 jul. 2023.

STUDENTCYBERARMY. Telegram channel, 22 March 2022. Disponível em: https://t.me/studentcyberarmy/209 ou https://archive.ph/Dn. Acessso em: 25 jul. 2023.

SUNSTEIN, C. **Going to Extremes: How Like Minds Unite and Divide**. Oxford: OUP, 2009.

TABANSKY, L.; ISRAEL, I. B. **Cybersecurity in Israel, SpringerBriefs in Cybersecurity**. New York:The MIT Press, 2015.

TABAK, S. Ambivalent Enforcement: International Humanitarian Law at Human Rights Tribunals. **Michigan Journal of International Law**, Michigan, v. 37, n. 661, 2016. Disponível em: https://repository.law.umich.edu/mjil/vol37/iss4/3. Acesso em: 25 jun. 2023.

TEDH - TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Al-Saadoon e Mufdhi v. Reino Unido. Council of Europe/European Court of Human Rights, 2009. Disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-1021%22]}. Acesso em: 25 jul. 2023.

TEDH - TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Loizidou v. Turquia. Council of Europe/European Court of Human Rights, 1995. Disponível

MIOLO_Poder, Tecnologia e Direito - 2.indd 942 26/04/2024 11:12:32

em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-57920%22]}. Acesso em: 25 jul. 2023.

TEDH - TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Chipre v. Turquia. Council of Europe/European Court of Human Rights, 2001. Disponível em: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-144151%22]}. Acesso em: 25 jul. 2023.

TEDH. - TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Öcalan v. Turquia. Council of Europe/European Court of Human Rights, 2003. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-69022%22]}. Acesso em: 25 jul. 2023.

TEIXEIRA, A. P. **A guerra assimétrica global**: a batalha do século XXI e a capitulação do direito internacional. 2006. 60 f. Monografia (Especialização em Direito Internacional dos Conflitos Armados) – Faculdade de Direito, Universidade de Brasília, Brasília, 2006.

TEIXEIRA, A. P. Fundamentalismo islâmico: a primazia do Mythos sobre o Logus. **Revista Marítima Brasileira**, Rio de Janeiro, v. 129, n. 02/11. Serviço de Documentação da Marinha, 2011.

TEIXEIRA, A.P. **O combatente ilegal à luz do direito internacional dos conflitos armados**. 2008. 50f. Dissertação (Mestrado em Ciências Navais) – Escola de Guerra Naval, Rio de Janeiro, 2008.

TERRY, J. P. The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints? **Military Law Review**, [*S.l.*], v. 169, n. 169, p. 90-91, 2001. Disponível em: https://www.researchgate.net/publication/296816451_The_lawfulness_of_attacking_computer_networks_in_armed_conflict_and_in_self-defense_in_periods_short_of_armed_conflict_What_are_the_targeting_constraints. Acesso em:25 jul. 2023.

TGSTAT. IT Army of Ukraine – Subscribers number growth. 2022. Disponível em: https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers. Acesso em: 25 jul. 2023.

THE ASTROLOGY PAGE. Was ist die Internet Engineering Task Force (IETF)? - Definition aus techopedia. Blog, 2023. Disponível em: https://theastrologypage.com/internet-engineering-task-force. Acesso em: 23 jul. 2024.

MIOLO_Poder, Tecnologia e Direito - 2.indd 943 26/04/2024 11:12:32

THE ECONOMIST. How a chatbot has turned Ukrainian civilians into digital resistance Fighters. The Economist, [*S.l.*], 2023. Disponível em: https://www.economist.com/the-economist-explains/2023/02/22/how-a-chatbot-has-turned-ukrainian-civilians-into-digital-resistance-fighters. Acesso em: 25 jul. 2023.

THE History of Computer Viruses. **VIRUS Scan Software**, [*S.l.*]. Disponível em: http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml. Acesso em: 25 jul. 2023.

THE ODESSA JOURNAL. Ukraine received two awards in the field of cybersecurity at the CYBERSEC European Cybersecurity Forum. **Odessa-journal**, [*S.l.*], 2022. Disponível em: https://web.archive.org/web/20220608141159/https://odessa-journal.com/ukraine-received-two-awards-in-the-field-of-cybersecurity-at-thecybersec-european-cybersecurity-forum/. Acesso em: 25 jul. 2023.

THE OVAL OFFICE. President Bush Addresses the Nation. **The White House**, Washington, 2003. Disponível em: http://georgewbush-whitehouse.archives.gov/news/releases/2003/03/20030319-17.html. Acesso em: 25 jul. 2023.

THE WHITE HOUSE. **The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets**. Wasgington: The White House, 2003. Disponível em: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. Acesso em: 25 jul. 2023.

THIELMAN, S. Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History. **The Guardian**, New York, 2016. Disponível em: https://www.theguardian.com/technology/2016/dec/14/yahoohack-security-of-one-billion-accounts-breached. Acesso em: 25 jul. 2023.

THORNBURG, E. G. Metaphors Matter: How Images of Battle, Sports, and Sex Shape the Adversary System. **Wisconsin Women's Law Journal**, Madison, WI, v. 10, p. 229, 1995. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1006305#. Acesso em: 25 jul. 2023.

TIKK, E.; KASKA, K.; VIHUL, L. **International Cyber Incidents:** Legal Considerations. Taillinn: NATO CCD COE Publications, 2010. Disponível em: https://ccdcoe.org/publications/books/legalconsiderations.pdf. Acesso em: 25 jul. 2023.

TILLY, C. War Making and State Making as Organized Crime. *In*: EVANS, P.; RUESCHEMEYER, D.; SKOCPOL, T. **Bringing Back the State**. Cambridge: Cambridge University Press, 1985.

MIOLO_Poder, Tecnologia e Direito - 2.indd 944 26/04/2024 11:12:32

TOEPHER, J. **SEAD from the Ground up**: SOF's role in the Suppression of Enemy Air Defenses. Tese (Mestrado) — Naval Postgraduate School Monterey. CA, p.83. 2019. Disponível em: https://apps.dtic.mil/sti/pdfs/AD1080474.pdf. Acesso em:25 jul. 2023.

TOMUSCHAT, C. International law: Ensuring the survival of mankind on the eve of a new century. **Recueil des Cours**, [*S.l.*], v. 281, p.13-438, 2001. Disponível em: https://referenceworks.brillonline.com/entries/the-hague-academy-collected-courses/*A9789041114884_01. Acesso em: 12 jul. 2023.

TRAUTMAN, L. J.; ORMEROD, P. Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things. **University of Miami Law Review**, Miami, v.72, n. 761, 2018. Disponível em: https://ssrn.com/abstract=2982629. Acesso em: 25 jul. 2023.

TRAYNOR, I. Russia accused of unleashing cyberwar to disable Estonia. **The Guardian**, London, 2007b. Disponível em: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia. Acesso em: 25 jul. 2023.

TRAYNOR, I. Web Attackers Used a Million Computers, Says Estonia. **The Guardian**, London, 2007a. Disponível em: https://www.theguardian.com/technology/2007/may/18/news.russia. Acesso em: 25 jul. 2023.

TREATY OF WESTPHALIA. Peace Treaty Between the Holy Roman Emperor and the King of France and Their Respective Allies. **Yale Law School**, Yale, 1648. Disponível em: https://avalon.law.yale.edu/17th_century/westphal.asp. Acesso em: 22 fev. 2021.

TRIBUNAL FEDERAL, Ottawa, Canadá. Anistia Internacional do Canadá e Associação de Liberdades Civis da Colúmbia Britânica v. Chefe do Estado-Maior de Defesa das Forças Canadenses, Ministro da Defesa Nacional e Procurador Geral do Canadá. Ottawa: tribunal de justiça, 2008. Disponível em: https://internationalcrimesdatabase.org/Case/966/Amnesty-International-Canada-v-Canada/. Acesso em: 25 jul. 2023.

TRYON, J. L. The Hague Conferences. **The Yale Law Journal**, Yale, v. 20, n. 6, 1911. Disponível em: https://www.jstor.org/stable/i232085. Acesso em: 25 jul. 2023.

U.S. DEPARTMENT OF STATE. Joint Statement on Advancing Responsible State Behavior in Cyberspace. U.S. Department of State, Canadá, 2019. Disponível em: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 945 26/04/2024 11:12:32

UN GENERAL ASSEMBLY. **Declaration on The Inadmissibility of Intervention and Interference in the Internal Affairs of States**. New York: UN General Assembly, 1981. Disponível em: https://www.refworld.org/docid/3b00f478f.html. Acesso em: 26 ago. 2020.

UNGA Res 2625 (XXV). Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (24 October 1970) UN Doc. A/RES/2625 (XXV). Disponível em: https://digitallibrary.un.org/record/202170. Acesso em: 25 jul. 2023.

UNGA Res 56/19. Developments in the field of information and telecommunications in the context of international security. 2001. UN Doc. A/RES/56/19, 2 [4]. Disponível em: https://undocs.org/A/RES/56/19. Acesso em: 25 jul 2023.

UNGA Res 70/237. Developments in the field of information and telecommunications in the context of international security. n 20, 2-3. Disponível em: https://undocs.org/A/RES/70/237. Acesso em: 25 jul. 2023.

UNGA Res 72-4. Necessity of ending the economic, commercial and financial embargo imposed by the United States of America against Cuba (10 November 2017) UN Doc. A/RES/72/4. Disponível em: https://digitallibrary.un.org/record/1648511. Acesso em: 25 jul. 2023.

UNGA Res. 45/166, 18 de dezembro de 1990, Princípio 9.

UNGA Res. 56/83. Anexo, art. 4 Responsibility of States for internationally wrongful acts (28 de jan. de 2002). Disponível em: https://undocs.org/A/RES/56/83. Acesso em: 25 jul. 2023.

UNGA. Res. 217 (III) A, arts. 12, 19, Universal Declaration of Human Rights (Dec. 10, 1948); International Covenant on Civil and Political Rights arts. 17, 19(2), Dec. 16, 1966, S. EXEC. DOC. E, 95-2 (1978), 999 U.N.T.S. 171.

UNGAR- Resolução 55/63 da Assembleia Geral da ONU, 4 de dezembro de 2000, parágrafo 1 (a).

UNGAR, Resolução 3314 (XXIX). Disponível em: https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/PDF/NR073916.pdf?OpenElement. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 946 26/04/2024 11:12:32

UNGAR. Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, G.A. Res. 2131, 11 1-2.

UNIÃO EUROPEIA. **Convenção Europeia dos Direitos do Homem e Liberdades Fundamentais**. Roma: Conselho da Europa,1950.

UNICEUB. Mestrado e Doutorado em Direito. Uniceub, Brasília, 2022. Disponível em: https://www.uniceub.br/pdp/mestrado-e-doutorado/direito/mestrado-e-doutorado-em-direito. Acesso em: 6 dez. 2022.

UNITED KINGDOM CABINET OFFICE. The Uk Cyber Security Strategy: Protecting and Promoting The Uk In The Digital World. Written Ministerial Statement, 2011. Disponível em: https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf. Acesso em: 25 jul. 2023.

UNITED NATIONS. General commentn. 36 on article 6: right to life. CCPR, [*S.l.*], 2019. Disponível em: https://www.ohchr.org/en/calls-for-input/general-comment-no-36-article-6-right-life#:~:text=It%20lays%20the%20foundation%20for,of%20the%20right%20to%20life. Acesso em: 25 jul. 2023.

UNITED NATIONS CONFERENCE ON THE LAW OF TREATIES: First and Second Sessions, Vienna, 26 March-24 May 1968 and 9 April-22 May 1969 - Documents' (United Nations Secretariat 1971) A/CONF.39/11/Add.2 171–173. Disponível em: https://legal.un.org/diplomaticconferences/1968_lot/. Acesso em: 25 jul. 2023.

UNITED NATIONS HUMAN RIGHTS COUNCIL, 'General Comment No 25' (n 69) para 9. US Department of Defense, The Strategy for Homeland Defense and Civil Support, 2005.

UNITED NATIONS INFORMATION ORGANIZATIONS. **Commission I: General Provisions**. San Francisco: Documents of the United Nations Conference on International Organization, v. VI, 1945. Disponível em: https://digitallibrary.un.org/record/1300969. Acesso em: 25 jul. 2023.

UNITED NATIONS INFORMATION ORGANIZATIONS. **Dumbarton Oaks Proposals, Comments and Proposed Amendments**. San Francisco: Documents of the United Nations Conference on International Organization, v. III, 1945. Disponível em: https://digitallibrary.un.org/record/1300969. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 947 26/04/2024 11:12:32

UNITED NATIONS INTERNATIONAL LAW COMMISSION. Draft Articles on State Responsibility for Internationally Wrongful Acts, art. 1, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. Document A/56/10, GAOR 56th Session, Supp. 10 (2001), reprinted in [2001] Yearbook of the International Law Commission 32, U.N. Document A/CN.4/ SER.A/2001/Add.1 (Part 2), 2001.

UNITED NATIONS. **Convention on the high Seas**. United Nations, Geneva, Treaty Series, v. 450, 1958. Disponível em: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXI-2&chapter=21. Acesso em: 27 jul. 2023.

UNITED NATIONS. **Declaração Universal dos Direitos Humanos**. Paris: Assembleia Geral das Nações Unidas. 1948. Disponível em: https://brasil.un.org/sites/default/files/2020-09/por.pdf. Acesso em: 26 ago. 2020.

UNITED NATIONS. **Documents of the United Nations Conference on International Organization, San Francisco, 1945**. New York: The Library Congress, 1945. Docs. 334, 609 (1945); Doc. 2, 617(e)(4), 3 UNCIO Docs. 251, 253–254 (1945)). Disponível em: https://digitallibrary.un.org/record/1300969. Acesso em: 25 jul. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- Comentário **Geral No. 31/80**: Natureza da Obrigação Legal Geral Imposta aos Estados Partes do Pacto, 26 de maio de 2004, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 10. Disponível em: https://www.ohchr.org/sites/default/files/Documents/HRBodies/CCPR/GCArticle6/GCArticle6_EN.pdf. Acesso em: 20 jul. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Draft General Comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights**, on the Right to Life' (Revised draft prepared by the Rapporteur, 2017) para. 71. Disponível em: https://www.ohchr.org/en/calls-for-input/general-comment-no-36-article-6-right-life. Acesso em: 18 jun. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Lilian Celiberti de Casariego v. Uruguai,** 29 de julho de 1981, UN Doc.CCPR/C/13/D/56/1979, para. 10. Disponível em: https://www.refworld.org/cases,HRC,4028af854.html. Acesso em 20 jun. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Observações Finais: Israel**, 18 de agosto de 1998, UN Doc. CCPR/C/79/Add.93, para. 10 e 11. Disponível: https://www.refworld.org/docid/3ae6b0284.html. Acesso em: 23 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 948 26/04/2024 11:12:32

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Sexagésima terceira sessão**. Registro resumido da 1675ª reunião: Consideração do Relatório Inicial de Israel, 21 de julho de 1998, UN Doc. CCPR/C/SR.1675, parágrafos 21 e 27. Disponível em: https://www.un.org/unispal/document/auto-insert-181927/. Acesso em: 21 jun. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Adendo ao Segundo Relatório Periódico**, Israel, 4 de dezembro de 2001, UN Doc. CCPR/C/ISR/2001/2, par. 8. Disponível em: https://www.un.org/unispal/document/auto-insert-179634/. Acesso em: 20 jun. 2023.

UNITED NATIONS HUMAN RIGHTS COMMITTEE (HRC)- **Burgos v. Uruguai**, 29 de julho de 1981, UN Doc. CCPR/C/13/D/52 /1979, para. 12.3. Disponível em: https://juris.ohchr.org/casedetails/298/en-US. Acesso em: 20 jun. 2023.

UNITED NATIONS. **Implementation of the international covenant on economic, social and cultural rights**: second periodic reports submitted by States parties under articles 16 and 17 of the Covenant. Israel: United Nations, 2001. Disponível em: https://www.un.org/unispal/document/auto-insert-179348/. Acesso em: 25 jul. 2023.

UNITED NATIONS. International Covenant on Civil and Political Rights. *In*: General Assembly resolution 2200A (XXI). Treaty Series 999 (December): 171. 1996. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Acesso em: 25 jul. 2023.

UNITED NATIONS. **Letter dated 20 March 2003 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council**. U.N. Doc. S/2003/351, 2003. Disponível em: https://digitallibrary.un.org/record/490434. Acesso em: 25 jul. 2023.

UNITED NATIONS. Materials On the Responsibility Of States For Internationally Wrongful Acts, U.N. Doc. ST/LEG/SER.B/25 (2012), ¶ 2 of commentary to art. 8.

UNITED NATIONS. Presidential Decision Directive 63, "Critical Infrastructure Protection". 1998, § I. Disponível em: https://irp.fas.org/offdocs/pdd/pdd-63.htm. Acesso em: 25 jul. 2023.

UNITED NATIONS. Prosecutor v. Dragoljub Kunarac Radomir Kovac and Zoran Vukovic. International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the

MIOLO_Poder, Tecnologia e Direito - 2.indd 949 26/04/2024 11:12:32

Territory of the Former Yugoslavia. Netherlands: United nations, 12 de junho de 2002. Disponível em: https://www.icty.org/x/cases/kunarac/tjug/en/kun-tj010222e.pdf. Acesso em: 25 jul. 2023.

UNITED NATION. Report of the group of governmental experts on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security, 15, U.N. Doc. (A/70/174). United Nations, 2015. Disponível em: https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf. Acesso em 22 jun. 2023.

UNITED NATION. Report of the group of governmental experts on Dev. in the Field of Info. & Telecomm. in the Context of Int'l Sec., 65th Sess., 1, U.N. Doc. A/65/201. United Nation, 2010. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement. Acesso em: 23 jun. 2023.

UNITED NATION. REPORT OF THE GROUP OF GOVERNMENTAL EXPERTS on Dev. in the Field of Info. and Telecomm. in the Context of Int'l Security, 19, U.N. Doc. (A/68/98). United Nation, 2013. Disponível em: http://undocs.org/A/68/98. Acesso em: 24 jul. 2023.

UNITED NATIONS. Report of the group of governmental experts on developments in The Field Of Information And Telecommunications In The Context Of International Security: Report of the Secretary-General (A/72/327), United Nations, 2017. Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/257/46/PDF/N1725746.pdf?OpenElement. Acesso em: 24 jul. 2023.

UNITED NATIONS. **Reports of International Arbitral Awards**: Trail Smelter (United States, Canada). 3 v. Utha: united nations, 1941. Disponível em: https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf. Acesso em: 25 jul. 2023.

UNITED NATIONS. **Resolution adopted by the General Assembly** [on the report of the Second Committee (A/58/481/Add.2)]. Netherlands: UN, 2004. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf. Acesso em: 25 jul. 2023.

UNITED NATIONS. **Resolution adopted by the General Assembly [on the report of the Sixth Committee** (A/56/589 and Corr.1)]. A/RES/56/83 of 12. Netherlands: UN, 2001. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F56%2F83&Language=E&DeviceType=Desktop&LangRequested=False. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 950 26/04/2024 11:12:32

UNITED NATIONS. Security Council, 3245th meeting, 27 June 1993, UN Doc. S/PV.3245. 1993.

UNITED NATIONS. The Paquete Habana case. 175 U.S. 686-700, 1900. Disponível em: https://supreme.justia.com/cases/federal/us/175/677/. Acesso em: 25 jul. 2023.

UNITED STATES JOINT FORCE DEVELOPMENT. **Information in Joint Operations**: JP 3-04. United States: Washigton D.C.: Department of Defense, 2022.

UNITED STATES SPECIAL OPERATIONS COMMAND. **The Gray Zone. White paper**. United State, 2015. Disponível em: http://army.com/sites/army.com/files/Gray%20Zones%20- %20USSOCOM%20White%20Paper%209%20Sep%202015.pdf. Acesso em: 23 jan. 2016.

UNITED NATIONS **Security Council. Security Council resolution 138** (1960) [Question relating to the case of Adolf Eichmann]. Geneva: S/RES/138 (1960). Disponível em: https://digitallibrary.un.org/record/112107. Acesso em: 12 jul. 2023.

US ARMY. **Field Manual 3-0, C1**: Operations. Washington, DC, USA: Government, 2017.

US ARMY. **Joint Publication JP 3-27 Homeland Defense 29 July 2013**. Scotts Valey – CA: CreateSpace Independent Publishing Platform, 2013. Disponível em: https://www.amazon.com.br/Joint-Publication-3-27-Homeland-Defense/dp/1492795682. Acesso em 27 jul. 2023.

US DOD- DEPARTMENT OF DEFENSE LAW OF WAR MANUAL. General Counsel of the Department of Defense. Washington, 2016. Disponível em: https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?-ver=2016-12-13-172036-190. Acesso em: 23 jul. 2023.

VALERIANO, B.; MANESS, R. The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype. **Foreign Affairs**, New York, 2012. Disponível em: https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar. Acesso em: 25 jul. 2023.

VANDIVER, J. Breedlove: NATO Must Redefine Responses to Unconventional Threats. **Stars and Stripes**, New Jersey, 2014. Disponível em: http://www.stripes.com/news/breedlovenato-must-redefine-responses-to-unconventional-threats-1.296129. Acesso em: 23 jan. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 951 26/04/2024 11:12:32

VELDE, J. V. The Law of Cyber Interference in Elections. **SSRN**, [*S.l.*], 2017. Disponível em: https://ssrn.com/abstract=3043828 or http://dx.doi.org/10.2139/ssrn.3043828. Acesso em 20 set. 2020.

VENABLES, A. Modelling Cyberspace to Determine Cybersecurity Training Requirements. **Frontiers in Education**, London, v. 6, n. 768037, 2021. Disponível em: https://www.frontiersin.org/articles/10.3389/feduc.2021.768037/full. Acesso em: 08 jun. 2022.

VENTRE, D. (ed). **Cyber Conflict***:* Competing National Perspectives. Hoboken: John Wiley & Sons, 2013.

VESENTINI, J. W. **Novas geopolíticas**. São Paulo: Contexto, 2008.

VICE CHAIRMAN OF THE JOINT CHIEFS OF STAFF. Joint Terminology for Cyberspace Operations. Department of Defence, Whashington, 2010. DIsponível em: https://info.publicintelligence.net/DoD-JointCyberTerms.pdf. Acesso em: 25 jul. 2023.

VIOLENCE. *In*: DICTIONNAIRE de Fracais. França: Larousse, 2023. Disponível em: http://www.larousse.fr/dictionnaires/francais/violence/82071?q=violence#81105. Acesso em: 25 jul. 2023.

VISSCHER, C. **Théories et réalités en droit international public**. Paris: Pedone, 1953.

VOLZ, D. Russian hackers tracked Ukrainian artillery units using Android implant: report. **Reuters**, [*S.l.*], 2016. Disponível em: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-trackedukrainian-artillery-units-using-android-impla. Acesso em: 25 jul. 2023.

WALDOCK, H. The Regulation of the Use of Force by Individual States in International Law. **Collected Courses of the Hague Academy of International Law**, Brill, [*S.l.*], v. 81, 1982. Disponível em: https://referenceworks.brillonline.com/entries/the-hague-academy-collected-courses/*A9789028611825_05. Acesso em: 25 jul. 2023.

WALKER, C. S.; MILMO, D. 'It's the right thing to do': the 300,000 volunteer hackers coming together to fight Russia. **The Guardian**, New York, 2022. Disponível em: https://web.archive.org/web/20220608145557/https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 952 26/04/2024 11:12:32

WARNER, M. Cybersecurity: A Pre-History. **Intelligence and National Security**, New York, v. 27, n. 5, 2012, p.781-99. Disponível em: https://www.researchgate.net/publication/263693956_Cybersecurity_A_Pre-history. Acesso em: 25 jul. 2023.

WATERMAN, S. Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army. **Newsweek**, New York, 2023a. Disponível em: https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814. Acesso em: 25 jul. 2023.

WATERMAN, S. Ukraine's Volunteer Cyber Army Could Be Blueprint for the World: Experts **Newsweek 90**, New York, 2023b. Disponível em: https://www.newsweek.com/ukraine-war-cyber-army-attack-strategy-warfare-1780970. Acesso em: 25 jul. 2023.

WATERMAN, S. Who Cyber Smacked Estonia? **United Press International**, Washington, 2007. Disponível em: http://www.spacewar.com/reports/Who_Cyber_Smacked_Estonia_999.html. Acesso em: 25 jul. 2023.

WATKIN, K. Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance. **International Law and Politics**, New York, v. 42, n. 641, 2010. Disponível em: https://nyujilp.org/wp-content/uploads/2012/04/42.3-Watkin.pdf. Acesso em: 25 jul. 2023.

WATKIN, K. Use of Force during Occupation: Law Enforcement and Conduct of Hostilitys. **International Review of the Red Cross**, Genebra, v. 94, n. 885, p. 295-296, 2012. Disponível em: https://international-review.icrc.org/sites/default/files/irrc-885-watkin.pdf. Acesso em: 25 jul. 2023.

WATTS, S. Low-Intensity Computer Network Attack and Self-Defense. **International Law Studies**, England, 2010. Disponível em: https://ssrn.com/abstract=1685896. Acesso em: 25 jul. 2023.

WATTS, S.; RICHARD, T. T. Baseline territorial sovereignty and cyberspace. **Lewis & Clark Law Review**, Oregon, 2018. Disponível em: https://ssrn.com/abstract=3142272. Acesso em: 13 fev. 2023.

WAXMAN, M. C. Cyber-Attacks and the Use of Force: Back to the Future of Article **Yale Journal of Law**, Yale, v. 36, n. 421, 2011. Disponível em: https://scholarship.law.columbia.edu/faculty_scholarship/1653. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 953 26/04/2024 11:12:32

WAY BACK MACHINE. Centro para o Estudo de Tecnologia e Sociedade, Foco Especial: Guerra Cibernética. 2001. Disponível em: http://web.archive.org/web/20061205020720/tecsoc.org/natsec/focuscyberwar.htm. Acesso em: 25 jul. 2023.

WEBER, M. **Wirtschaft und Gesellschaft**. 5. ed. Baviera: Mohr Siebeck Tübingen, 1972.

WEBER, Max. The Profession and Vocation of Politics. *In*: WEBER, M. **Political Writings**. Cambridge: Cambridge University Press, 1994. pp. 309-369.

WEEDON, J.; NULAND, W.; STAMOS, A. **Information Operations and Facebook**. [*S.l.*]: Facebook, Inc., 2017. Disponível em: https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf. Acesso em: 25 jul. 2023.

WEINER, N. **Cybernetics or Control and Communication in the Animal and the Machine**. Massachusetts: MIT press, 1948.

WEISSBRODT, D. The Role of the Human Rights Committee in Interpreting and Developing Humanitarian Law. **University of Pennsylvania Journal of International Law**, Pennsylvania, v. 31, 2010. Disponível em: https://scholarship.law.upenn.edu/jil/vol31/iss4/3/. Acesso em: 25 jul. 2023.

WHEELER, W. The MQ-9's cost and performance. **Nation Time**, New York, 2012. Disponível em: https://nation.time.com/2012/02/28/2-the-mq-9s-cost-and-performance/. Acesso em: 13 fev. 2021.

WHETHAM, D. Cyber Chevauchees: Cyber War Can Happen. In: ALLHOFF, F.; HENSCHKE, A.; STRAWSER, B. J. **Binary Bullets**: The Ethics of Cyberwarfare. Oxford: Oxford University Press**,** 2016. Disponível em: https://kclpure.kcl.ac.uk/portal/en/publications/cyber-chevauch%C3%A9es-cyber-war-can-happen. Acesso em: 25 jul. 2023.

WHITE HOUSE. United States & United States. **Library of Congress**, Washington, 2017. Disponível em: https://www.loc.gov/item/lcwaN0027881/. Acesso em: 18 maio 2022.

MIOLO_Poder, Tecnologia e Direito - 2.indd 954 26/04/2024 11:12:33

WHITTON, J. B. Aggressive Propaganda, *In*: MARTIN, J. **International Propaganda**: Its legal and diplomatic control. Minisota: University Of Minnesota Press, 1974.

WHYTOCK, C.A. Thinking Beyond the Domestic-International Divide: Toward a Unified Concept of Public Law. **Georgetown Journal of International Law**, Georgetown, v. 36, 2004. Disponível em: https://scholarship.law.uci.edu/faculty_scholarship/714/. Acesso em: 24 jul. 2023.

WIENER, N. **Cybernetics**: Or Control and Communication in the Animal and the Machine. New York: John Wiley, 1948.

WILLETT, M. The Cyber Dimension of the Russia–Ukraine War. **Survival**, Berlin, v. 64, n. 5, p. 7-26, 2022. Disponível em: https://doi.org/10.1080/00396338.2022.2126193. Acesso em: 25 jul. 2023.

WILMHURST, E. Principles of International Law on the Use of Force by States in Self-Defence. **Chatham House International Law**, [*S.l.*], 2005. Disponível em: http://www.chathamhouse.org.uk/files/3278_ilpforce.doc. Acesso em: 25 jul. 2023.

WINNER, L. **The Whale and the Reactor:** A Search for Limits in an Age of High Technology. 1 ed. Chicago: University Of Chicago Press, 1989.

WIPPMAN, D. The Nine Lives ofArticle 2(4), **University of Minnesota Law School**, Minnesota, v. 16, 2007. Disponível em: https://core.ac.uk/download/pdf/217210801.pdf. Acesso em: 25 jul. 2023.

WRIGHT, Q. Subversive Intervention, **The American Journal of International Law**, Cambridge, v. 54, 1960. Disponível em: https://www.jstor.org/stable/2195306. Acesso em: 26 jul. 2023.

YAACOUB, J.-P. A. NOURA, Hassan N. SALMAN, Ola. CHEHAB, Ali. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations, **Internet of Things and Cyber-Physical Systems**, Volume 3, 2023, Pages 280-308.

YURCIK, W. Information Warfare: Legal & Ethical Challenges of the next Global Battleground. ANNUAL ETHICS AND TECHNOLOGY CONFERENCE (ETHICS' 97), 2., 1997. Chicago. **Proceeding [...]**, Chicago: Loyola University Chicago, Chicago, Citeseer, 1997. Disponível em: https://www.researchgate.net/

MIOLO_Poder, Tecnologia e Direito - 2.indd 955 26/04/2024 11:12:33

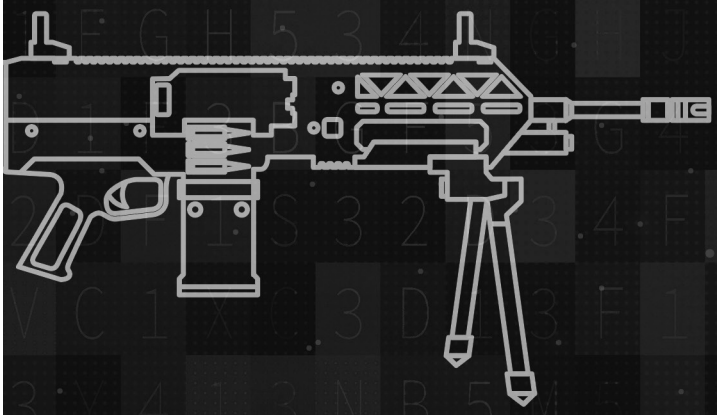
publication/2831747_Information_Warfare_Legal_and_EthicaChallengesofthe-NextGlobalBattleground. Acesso em: 25 jul. 2023.

ZEMANEK, K. Armed attack. **Max Planck Encyclopedia of Public International Law**, Oxford, 2010. Disponível em: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e241. Acesso em: 25 jul.2023.

ZIOLKOWSKI, K. (ed.). **Peacetime regime for state activities in cyberspace**. Tallinn: International Law, International Relations and Diplomacy, NATO CCD COE Publication, 2013. Disponível em: https://ccdcoe.org/library/publications/peacetime-regime-for-state-activities-in-cyberspace/. Acesso em: 25 jul. 2023.

MIOLO_Poder, Tecnologia e Direito - 2.indd 956 26/04/2024 11:12:33

MIOLO_Poder, Tecnologia e Direito - 2.indd 957 26/04/2024 11:12:33





PÓSFACIO

Foi com grande alegria que recebi o pedido do meu querido amigo Alexandre para preparar o posfácio desta obra inovadora e ousada que, após um período de 4 anos de exaustiva pesquisa, ele introduz no cenário acadêmico brasileiro. O autor, ao analisar um ambiente tão desafiador como o ciberespaço, sob o ponto de vista jurídico, em uma conjuntura na qual pouco material de pesquisa existe em nossa academia, sem sombra de dúvida, torna a obra um marco jurídico para professores, pesquisadores, profissionais em geral, pensadores e construtores de política.

Para você que chegou até o final da trilha de análise proposta por Alexandre, que nos coloca no caminho do "Poder – Tecnologia – Direito – Disrupção – Realidade", provavelmente sua percepção sobre a temática foi impactada de forma contundente. As noticiais de mídia, os fatos cotidianos e as rodas de conversa serão vistos de forma diferente, daqui para frente, de uma vez por todas. A obra "*Poder, Tecnologia e Direito: A Força Cibernética e a Disrupção nos Principais Paradigmas de Sustentação do Direito Aplicável aos Conflitos Armados*" coloca o leitor em uma jornada de reflexão, de análise jurídico-científica e de abstração acadêmica peculiar, intrigante e nova em nosso ambiente nacional.

Partindo das nuances do "Poder" planetário, objeto de desejo para Estados e governos, analisado no Capítulo 1, onde encontramos a reflexão sobre os conceitos de soberania, territorialidade e pós-territorialidade, até se atingir a capacidade de se enxergar com lucidez a grave "Realidade" fática de um mundo imerso no emaranhado das operações cibernéticas maliciosas, proposta no Capítulo 5, cuja visão é proporcionada pela análise profunda de importantes casos concretos passados no planeta Terra, Alexandre nos permite uma magnífica viagem na temática que mais afeta a vida das sociedades hodiernamente.

Nesta jornada de reflexão e conhecimento, o leitor tem parada garantida na estação da "Tecnologia", no Capítulo 2, na qual lhe é proposto não apenas uma imersão na composição e estrutura do ambiente cibernético, como também uma visitação ao conceito da "Guerra Cibernética". O Capítulo 3 está localizado na estação do "Direito",

MIOLO_Poder, Tecnologia e Direito - 2.indd 959 26/04/2024 11:12:33

onde se consegue abstrair um pouco do processo de construção deste mais novo ramo da ciência jurídica, bem como das peculiaridades que perpassam a construção da ordem pública internacional. E, na estação da "Disrupção", localizada no capítulo 4, o autor atinge o clímax de sua pesquisa ao focar nas lides do Direito Internacional Aplicado aos Conflitos Armados com o aprofundamento da análise dos paradigmas jurídicos do *Jus ad Bellum* e do *Jus in Bello*, sendo ainda onde se localiza a sustentação da tese pela qual a Força Cibernética possui o potencial para afetar diretamente a percepção jurídica do uso da força pelos Estados, no âmbito das relações internacionais, e como ela também se manifesta com plena capacidade de irromper os padrões conhecidos de emprego da força por Estados contra pessoas. Antes de comprovar sua tese com a apresentação de casos reais que ocorreram no mundo, nestes últimos anos, Alexandre nos traz uma reflexão peculiar sobre o conceito jurídico de "*Leveé em Masse*" e "*Participação Direta de Civis em Hostilidades*", iluminando o viés cibernético proposto pela era da informação e do conhecimento.

Eu não tenho dúvidas de que a obra afetará de forma significativa o ambiente acadêmico brasileiro. Falo isto não apenas pela constatação da presença de uma riquíssima referência bibliográfica, que ocupa nada menos do que 60 páginas da obra, mas também pelo nível de aprofundamento intelectual que o livro impõe e propõe às gerações futuras de pesquisadores que possam se interessar pelo estudo do tema e se animem em seguir pelas trilhas abertas por Alexandre, nas lides acadêmicas brasileiras. Sabe-se que no Brasil, principalmente na academia jurídica, pautada em um nítido viés conservador, as tentativas de inovação não costumam lograr êxito nas suas investidas primárias. Tanto que o próprio Alexandre faz uma rápida referência à dificuldade com a qual se deparou no início de sua pesquisa. Entretanto, como operadora do Direito eu posso assegurar que, independentemente do impacto (positivo ou negativo) que a presente obra possa causar em nosso ambiente acadêmico-jurídico, ela já se desponta como a principal referência de Direito Internacional Cibernético para aqueles que se lançarem na pesquisa desta inovadora e emergente área do Direito.

Ao dileto amigo, dirijo minhas palavras finais de incentivo para que prossiga em sua jornada desbravadora, agradecendo o carinho e a deferência a mim dispensados com a satisfatória oportunidade de dividir minhas rápidas percepções sobre a presente obra. Para aqueles que aqui chegaram, fica a sugestão para que prossigam contribuindo com o apro-

MIOLO_Poder, Tecnologia e Direito - 2.indd 960 26/04/2024 11:12:33

fundamento do estudo do impacto que as tecnologias trazidas pela Era da Informação têm causado no comportamento das sociedades e, consequentemente, no Direito em geral.

Prezado amigo, muita sorte, sucesso e segurança para o prosseguimento da jornada que se abre com a chegada desta brilhante obra ao nosso cenário nacional.

Najla Nassif Palma
Procuradora do Ministério Público Militar

MIOLO_Poder, Tecnologia e Direito - 2.indd 961 26/04/2024 11:12:33

MIOLO_Poder, Tecnologia e Direito - 2.indd 963 26/04/2024 11:12:33



DIALÉTICA
EDITORA

Este livro foi impresso sob demanda, sem estoques. A tecnologia POD (Print on Demand) utiliza os recursos naturais de forma racional e inteligente, contribuindo para a preservação da natureza.

"Rico é aquele que sabe ter o suficiente"
(Lao Tze)