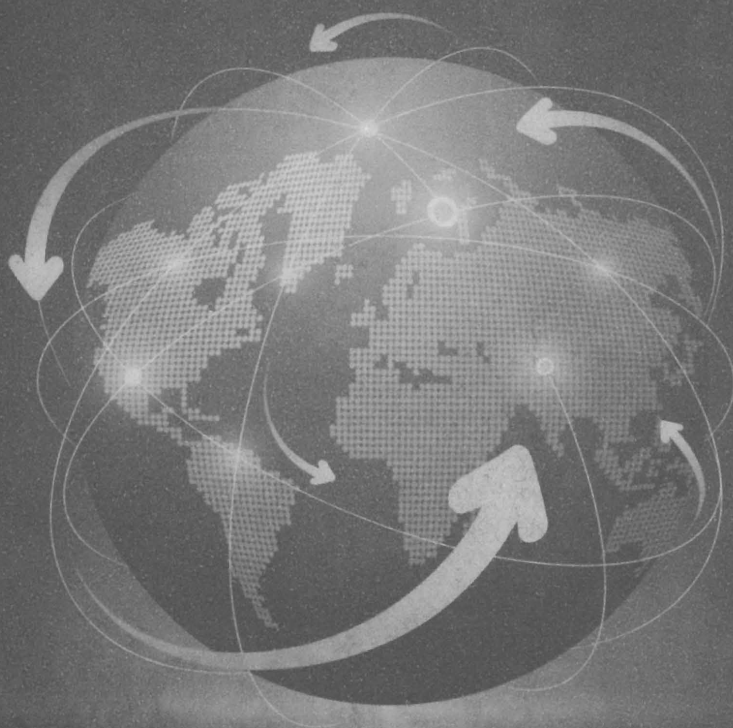


EDUARDO IZYCKI

NATION-STATE CYBER OFFENSIVE CAPABILITIES

an in-depth look into a multipolar dimension



DIALÉTICA
EDITORA

Todos os direitos reservados. Nenhuma parte desta edição pode ser utilizada ou reproduzida – por qualquer meio ou forma, seja mecânica ou eletrônica, fotocópia, gravação etc. – sem a aprovação ou estorada em sistema de banco de dados, sem a expressa autorização da Editora.



DIALÉTICA
EDITORA

 /editoradialetica

 @editoradialetica

www.editoradialetica.com

Copyright © 2022 by Editora Dialética Ltda.
Copyright © 2022 by Eduardo Izycki.

EQUIPE EDITORIAL

Editores-chefes

Prof. Dr. Rafael Alem Mello Ferreira
Prof. Dr. Vitor Amaral Medrado

Designer Responsável

Daniela Malacco

Produtora Editorial

Camila Gabarrão

Controle de Qualidade

Marina Itano

Capa

Ygor Moretti

Diagramação

Gilmar Santos

Preparação de Texto

Lucas Ben
Suzana Itano

Revisão

Responsabilidade do autor

Assistentes Editoriais

Jean Farias
Letícia Machado
Ludmila Vieira

Estagiárias

Georgia Oliveira
Larissa Teixeira
Laís Silva Cordeiro



Dados Internacionais de Catalogação na Publicação (CIP)

- 199n Izycki, Eduardo.
Nation-State Cyber Offensive Capabilities : an in-depth look into a
multipolar dimension / Eduardo Izycki. – São Paulo : Editora
Dialética, 2022.
264 p.
Inclui bibliografia.
ISBN 978-65-252-1472-6
1. Cyber Offensive Capabilities. 2. Cyberspace. 3. Information
Technology. I. Título.

CDD 300:600
CDU 30:62

CONTENTS

1.INTRODUCTION	11
2.CONCEPTUAL FRAMEWORK	15
3.LITERATURE REVIEW	25
4.RESEARCH QUESTIONS	29
5.METHODOLOGY	31
5.1. Technical Reports and Independent Studies	32
5.2. Data Breaches	33
5.3. Report from Exports Controls	34
5.4. Processing the data collected	35
5.5. The Classification and Entity Recognition	36
5.6. Parsing Structured Data	36
5.7. Threat actors and document clustering	38
5.8. Merging the Datasets	39
5.9. Research Limitations	40
6. OVERARCHING RESULTS	41
7. NATION-STATE CYBER OFFENSIVE ACTIONS	49

7.1. Threat Actors	49
7.2. Indigenous Technology or Outsourcing	50
7.3. Target's Geographical Dispersion	52
7.4. Preferred Targeted Sectors	54
7.5. Actions Complexity	57
7.6. Attacks Objectives	60
8. CYBER OFFENSIVE CAPABILITIES ACQUISITION	63
8.1. Multiple Acquisitions	65
8.2. Customers	68
9. DISCUSSION	71
9.1. Diffusion (not equality) of Cyber Offensive Capabilities	71
9.2. Geography Matters	73
9.3. Profiling Nation-State Behavior	76
9.4. Building Cyber Offensive Capabilities	83
9.5. Correlating Cyber Offensive Capabilities and Authoritarianism	85
9.6. Is the best defense a good offense?	89
9.7. Multipolarity in Cyberspace	91
10. CONCLUSIONS	93
11. REFERENCES	99

APPENDIX A - CYBER CAPABILITIES PROVIDERS	111
APPENDIX B - CYBER CAPABILITIES PURCHASES	125
APPENDIX C - COUNTRIES PROFILES	143