



Comissão Parlamentar Mista de Inquérito “Fake News”

Audiência Pública

Requerimento nº 161/2019 (Convite)

Prof. Thiago Tavares
Presidente da SaferNet Brasil

Brasília, 29 de outubro de 2019

Roteiro

1) Resumo sobre nossa atuação Institucional

2) Eixos da CPMI

a) Fake News, democracia e eleições

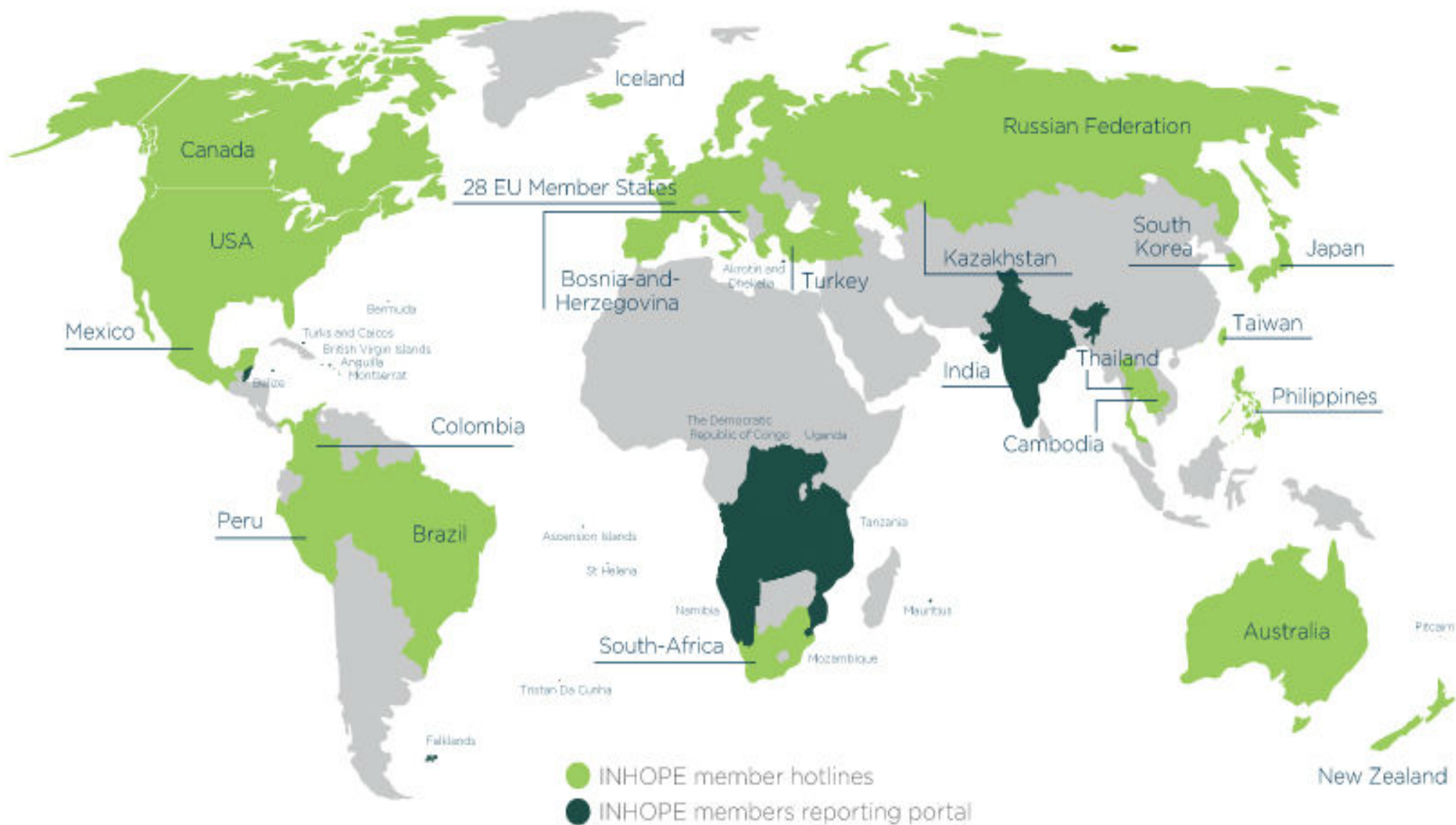
b) Proteção de dados pessoais

c) Cyberbullying e os ataques à dignidade humana

3) Conclusão



Safer
net





hotline

www.denuncie.org.br

SELECIONE ABAIXO O TEMA A SER TRATADO

- **pornografia infantil**
- **racismo**
- **apologia e incitação a crimes contra a vida**
- **xenofobia**
- **neo nazismo**
- **maus tratos contra animais**
- **intolerância religiosa**
- **homofobia**
- **tráfico de pessoas**
- **violência ou discriminação contra mulheres**

URL do site

Comentário

Denunciar

SELECIONE O TEMA AO LADO

Selecione o tema ao lado

O QUE É O HOTLINE?

A SaferNet Brasil oferece um serviço de recebimento de denúncias anônimas de crimes e violações contra os Direitos Humanos na Internet, contando com procedimentos efetivos e transparentes para lidar com as denúncias. Além disso, contamos com suporte governamental, parcerias com a iniciativa privada, autoridades policiais e judiciais, além, é claro, de você usuário da Internet. Caso encontre imagens, vídeos, textos, músicas ou qualquer tipo de material que seja atentatório aos Direitos Humanos, faça a sua denúncia.

ACOMPANHE SUA DENÚNCIA

Protocolo da denúncia:

Compartilhar



3.925.405

DENÚNCIAS ANÔNIMAS

RECEBIDAS DO
CANAL DE
DENÚNCIA



701.224

PÁGINAS (URLS) DISTINTAS

9

IDIOMAS

94.155

HOSTS DIFERENTES

56.416

NÚMEROS IPS DISTINTOS

101

PAÍSES

5

CONTINENTES

246.699

PÁGINAS REMOVIDAS

Denúncias de ódio recebidas pela SaferNet Brasil

COMO LER O GRÁFICO: Aqui você consegue visualizar o total de denúncias, o número de páginas denunciadas e o número de páginas com conteúdo criminoso que foram removidas da internet. Você pode selecionar por tipo de crime, por período e, ao clicar sobre o gráfico, ver o que a mídia noticiou na época para entender o que rolou. Clique e arraste sobre o gráfico para dar zoom.

TOTAL DE DENÚNCIAS

PÁGINAS

REMOÇÕES

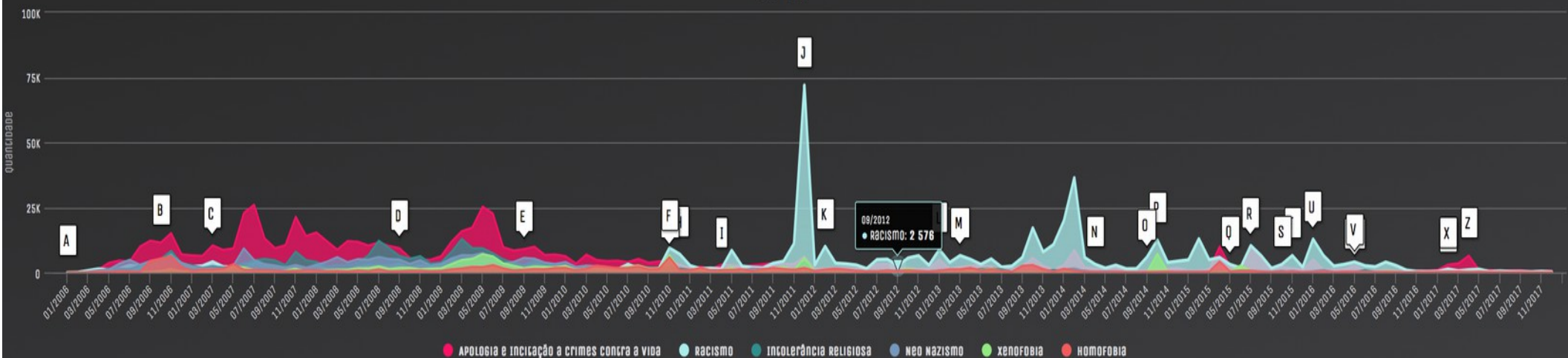
POR DIA

POR MÊS

POR ANO

TOTAL POR MÊS (NÃO-CUMULATIVO)

2006 - 2017



MEMORÁTEZ.COM

A Fundação da SaferNet Brasil



B Manifestações de racismo em cidades de São Paulo



C Denúncias de crimes no Orkut crescem mais de 10 vezes, diz relatório



D Jovens enfrentam ofensas e violência no mundo virtual



E Os neonazistas brasileiros



F SaferNet denuncia mais de mil por racismo na web



G No Twitter, perfil "@HomofobiaSIM" incita violência contra homossexuais



H Denúncias contra homofobia na internet crescem 88%



I Apologia a crimes como o massacre de Realengo (RJ) ganha força na internet



J Perfil no Twitter é denunciado mais de 8 mil vezes por ataques a nordestinos



K PF prende 2 suspeitos de promover racismo e planejar massacre



L Número de denúncias no Facebook cresce 264% em 2012



M Religiões africanas são principal alvo da intolerância religiosa no Brasil



N Vítimas de "nude selfie" e "sexting" na internet dobram no Brasil



O Crimes de ódio em redes sociais disparam no período eleitoral



P Ofensas em redes sociais batem recorde após 2º turno das eleições



Q Aumento no número de casos de racismo na internet preocupa autoridades

R Polícia caça grupos que pregam intolerância no Facebook

S Mulheres são mais de 80% das vítimas do vazamento de imagens íntimas

T Atriz Taís Araújo é alvo de comentários racistas em rede social

U Investigações dizem que existem 300 células de propaganda nazista na web

V Polícia apura estupro coletivo no Rio e identifica autores de posts em redes sociais

W "Fui estuprada": Buscas no Google mostram uso da internet por vítimas em estados brasileiros

X Homem é condenado por incitar discriminação em rede social

2007 / 2018

⊕ TOTAL DE ATENDIMENTO

24.662

PESSOAS ATENDIDAS

27

UNIDADES DA FEDERAÇÃO

6.355

CRIANÇAS E ADOLESCENTES

2.158

JOVENS

1.955

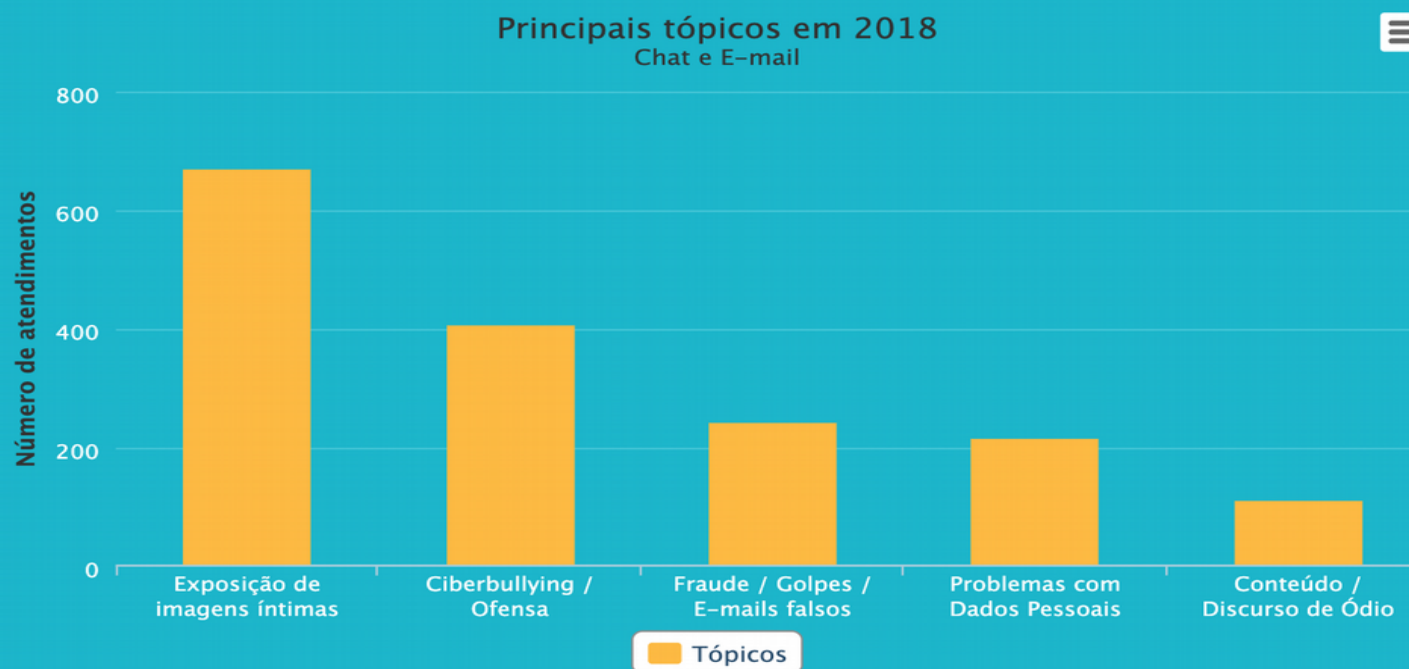
PAIS E EDUCADORES

14.194

OUTROS ADULTOS

1

AS PRINCIPAIS VIOLAÇÕES PARA AS QUAIS OS INTERNAUTAS BRASILEIROS PEDEM AJUDA



Conselho Consultivo sobre Internet e Eleições

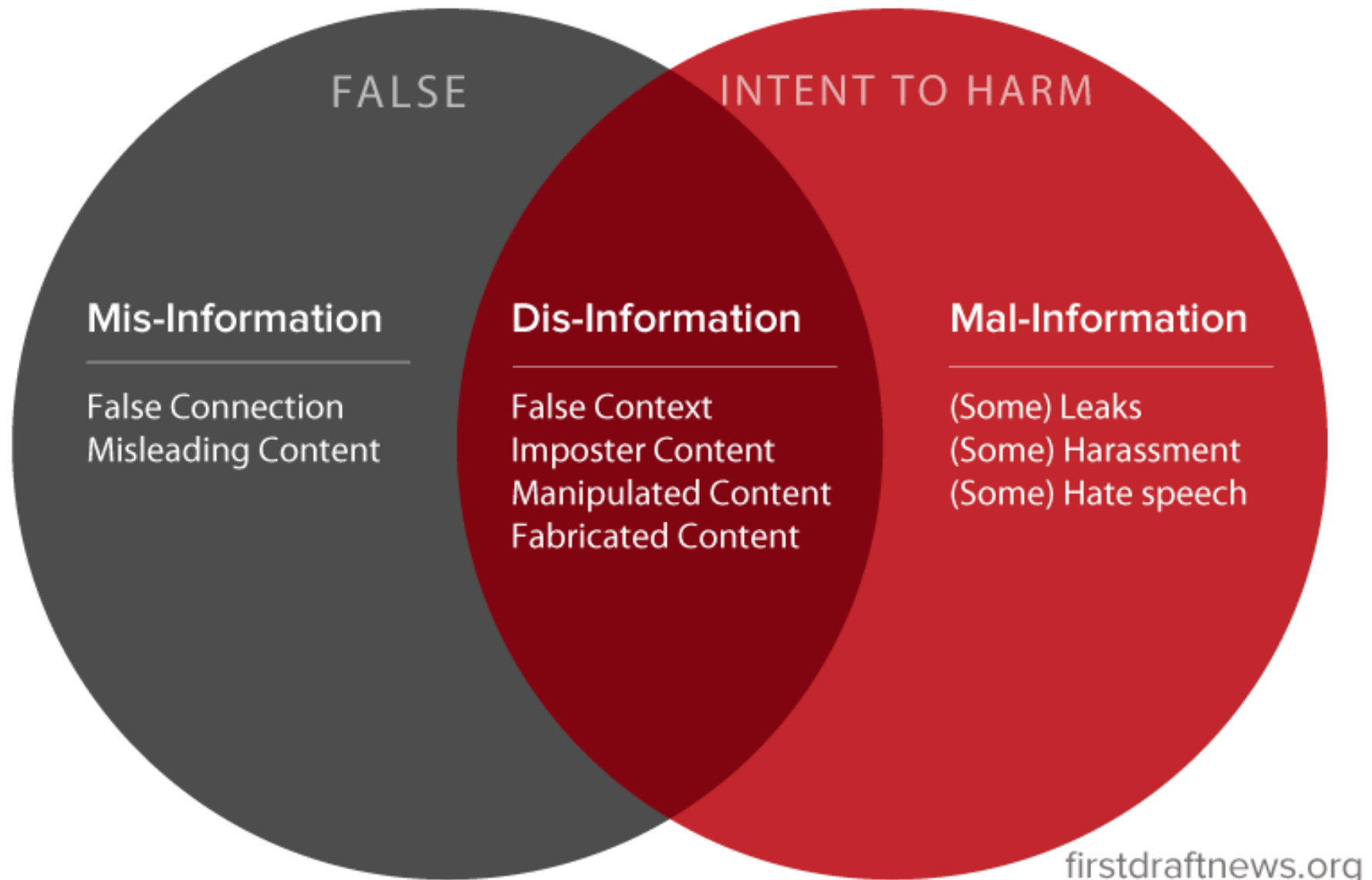
- Participamos ativamente de todas as 10 reuniões convocadas pelo TSE entre dez/2017 e out/2018;
- Apresentamos 2 contribuições por escrito com um total de 22 recomendações ao TSE, WhatsApp e outras empresas;
- Participamos ativamente dos 2 seminários realizados pelo TSE sobre fake news em dez/2017 e jun/2018;



Eixo I) Fake News, democracia e eleições



INFORMATION DISORDER



Majority say fake news has left Americans confused about basic facts

% of U.S. adults who say completely made-up news has caused ___ about the basic facts of current events



Source: Survey conducted Dec. 1-4, 2016.

PEW RESEARCH CENTER

Fake News Is A Real Problem

Facebook engagement of the top five fake election stories*



Total Facebook engagement for top 20 election stories (August-election day)



* Engagement is measured as total number of shares, reactions and comments



Hostile Social Manipulation

Present Realities and Emerging Trends

Michael J. Mazarr, Abigail Casey, Alyssa Demus, Scott W. Harold,
Luke J. Matthews, Nathan Beauchamp-Mustafaga, James Sladden



https://www.rand.org/pubs/research_reports/RR2713.html

CHAPTER ONE

Introduction: Information and Democracy—

A Perilous Relationship 1

The Growing Danger of Social Manipulation 2

Study Design, Methodology, and Scope 5

The Broader Danger: A Corrupted Information Environment 8

CHAPTER TWO

Understanding Social Manipulation: Definitions and Typologies 11

Defining Key Categories 11

The Goals of Social Manipulation 18

The Range of Options: Examples of Hostile Social Manipulation 20

The Past: Understanding the Context for Social Manipulation 23

CHAPTER THREE

Hostile Social Manipulation: Russian Activities 29

Methodology 31

History: Soviet and Russian Approaches to Social Manipulation 33

Doctrine: Russia’s Conceptualization of Social Manipulation 49

Strategies: How Russia Conducts Social Manipulation Today 62

Actions: What Russia Is Doing and How 77

Effectiveness of Russia’s Efforts 92

Conclusions 103

CHAPTER FOUR

Hostile Social Manipulation: Chinese Activities 105

History: China’s Approach to Social Manipulation 107

Doctrine: China’s Goals for Foreign Policy and Information Operations 110

“Magic Weapons”: China’s Offensive Approach to Defense 113

Strategies: Who Manages the Media and the Messages? 121

Actions: China’s Information Operations Through Social Media 131

Effectiveness of China’s Efforts 151

Conclusions and Implications for U.S. Policy 162

CHAPTER FIVE

Does Hostile Social Manipulation Work? Measures of Success in Russian Activities in Europe and the United States 167

United States 171

United Kingdom 184

France 194

Germany 206

The Baltic States 210

Poland 215

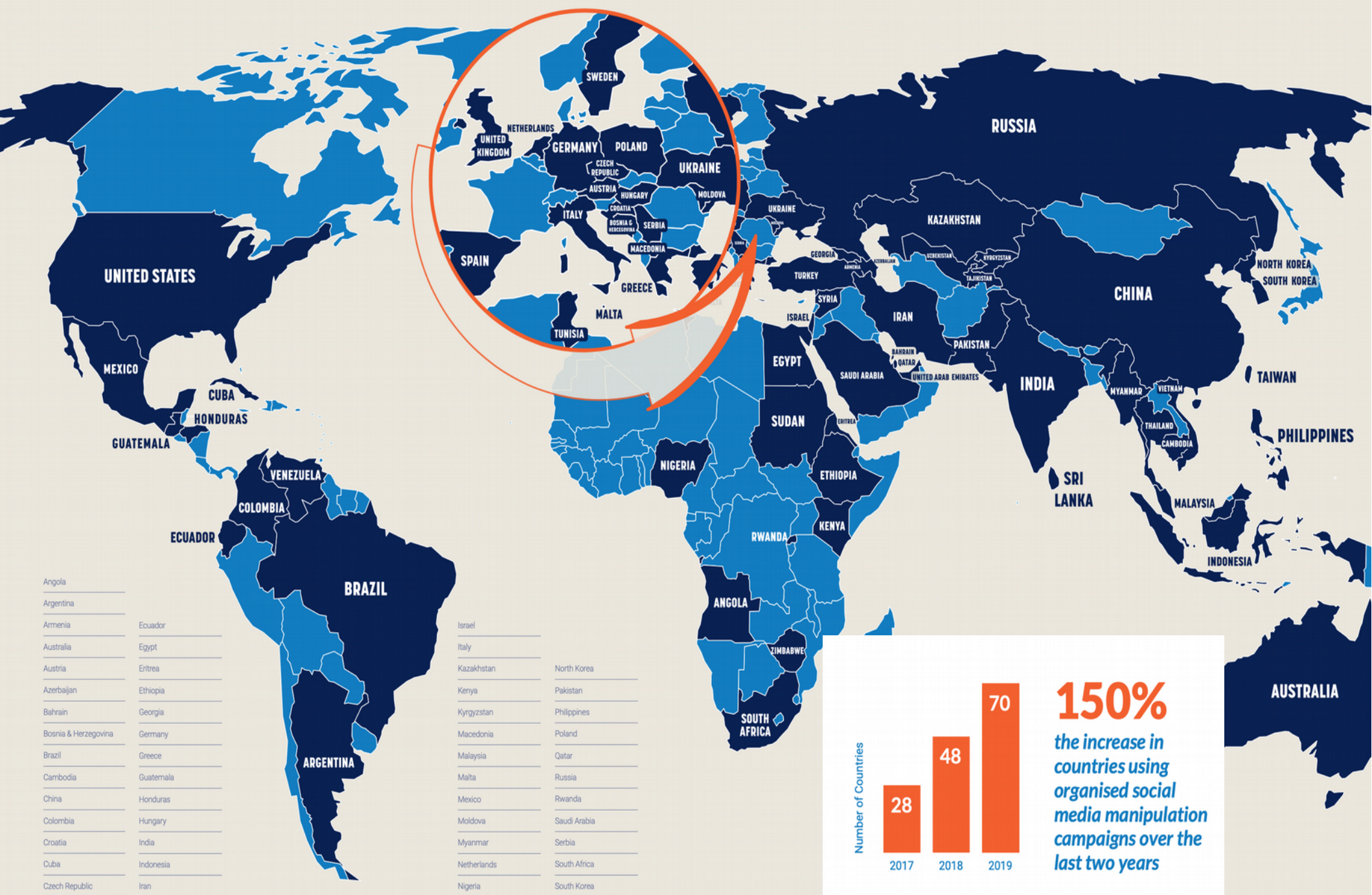
Summary of Outcome Evidence 219

CHAPTER SIX

Hostile Social Manipulation: The Experience to Date—

Conclusions and Implications 225

FIGURE 1 - THE GLOBAL DISINFORMATION ORDER
COUNTRIES TAKING PART IN SOCIAL MEDIA MANIPULATION



<https://www.oii.ox.ac.uk/news/releases/use-of-social-media-to-manipulate-public-opinion-now-a-global-problem-says-new-report/>

FIGURE 2 - COMPUTATIONAL PROPAGANDA AS A TOOL OF INFORMATION CONTROL
AUTHORITARIAN COUNTRIES DEPLOYING COMPUTATIONAL PROPAGANDA



FIGURE 3 - FOREIGN INFLUENCE OPERATIONS ON SOCIAL MEDIA
COUNTRIES ATTRIBUTED BY FACEBOOK AND TWITTER FOR ENGAGING IN FOREIGN INFLUENCE OPERATIONS



Source: Authors' evaluations based on data collected. **Note:** Facebook has also taken down accounts engaged in 'coordinated inauthentic behaviour' that are not explicitly linked to a government or political party. These takedowns include accounts originating from: Egypt, Macedonia, Kosovo, Thailand, and the United Arab Emirates. Additionally, some cyber troop activity identified by Facebook and Twitter is domestically focused, such as in the case of Bangladesh and Honduras, and is therefore not included in this figure on foreign operations.

TABLE 1 - ORGANIZATIONAL FORM AND PREVALENCE OF SOCIAL MEDIA MANIPULATION

Country	Government Agencies	Politicians and Parties	Private Contractors	Civil Society Organizations	Citizens and Influencers
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Bosnia & Herzegovina					
Brazil					
Cambodia					
China					
Colombia					
Croatia					
Cuba					
Czech Republic					
Ecuador					
Egypt					
Eritrea					
Ethiopia					
Georgia					
Germany					
Greece					
Guatemala					
Honduras					
Hungary					
India					
Indonesia					
Iran					
Israel					
Italy					
Kazakhstan					
Kenya					
Kyrgyzstan					
Macedonia					
Malaysia					

Country	Government Agencies	Politicians and Parties	Private Contractors	Civil Society Organizations	Citizens and Influencers
Malta					
Mexico					
Moldova					
Myanmar					
Netherlands					
Nigeria					
North Korea					
Pakistan					
Philippines					
Poland					
Qatar					
Russia					
Rwanda					
Saudi Arabia					
Serbia					
South Africa					
South Korea					
Spain					
Sri Lanka					
Sudan					
Sweden					
Syria					
Taiwan					
Tajikistan					
Thailand					
Tunisia					
Turkey					
Ukraine					
United Arab Emirates					
United Kingdom					
United States					
Uzbekistan					
Venezuela					
Vietnam					
Zimbabwe					

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of political actors using social media influence operations, and the number of examples of those organizations found. For government agencies, political parties, civil society groups, and private contractors, ■ = one organization found, ■■ = two organizations found, ■■■ = three or more organizations found. Since it is difficult to assess the number of individual citizens using these tools, evidence of citizen use is indicated by ■.

Strategies, Tools, and Techniques

Although there is nothing necessarily new about propaganda, the affordances of social networking technologies – algorithms, automation, and big data – change the scale, scope, and precision of how information is transmitted in the digital age.

 **87%**
of countries used
Human accounts

 **80%**
of countries used
Bot accounts

 **11%**
of countries used
Cyborg accounts

 **7%**
of countries used
Hacked or Stolen
accounts

TABLE 2 - FAKE ACCOUNT TYPES

Country	Bots	Human	Cyborg	Hacked or Stolen
Angola				
Argentina				
Armenia				
Australia				
Austria				
Azerbaijan				
Bahrain				
Bosnia & Herzegovina				
Brazil				
Cambodia				
China				
Colombia				
Croatia				
Cuba				
Czech Republic				
Ecuador				
Egypt				
Eritrea				
Ethiopia				
Georgia				
Germany				
Greece				
Guatemala				
Honduras				
Hungary				
India				
Indonesia				
Iran				
Israel				
Italy				
Kazakhstan				
Kenya				
Kyrgyzstan				
Macedonia				
Malaysia				

Country	Bots	Human	Cyborg	Hacked or Stolen
Malta				
Mexico				
Moldova				
Myanmar				
Netherlands				
Nigeria				
North Korea				
Pakistan				
Philippines				
Poland				
Qatar				
Russia				
Rwanda				
Saudi Arabia				
Serbia				
South Africa				
South Korea				
Spain				
Sri Lanka				
Sudan				
Sweden				
Syria				
Taiwan				
Tajikistan				
Thailand				
Tunisia				
Turkey				
Ukraine				
United Arab Emirates				
United Kingdom				
United States				
Uzbekistan				
Venezuela				
Vietnam				
Zimbabwe				



71%

spread pro-government or pro-party propaganda



89%

use computational propaganda to attack political opposition



34%

spread polarising messages designed to drive divisions within society

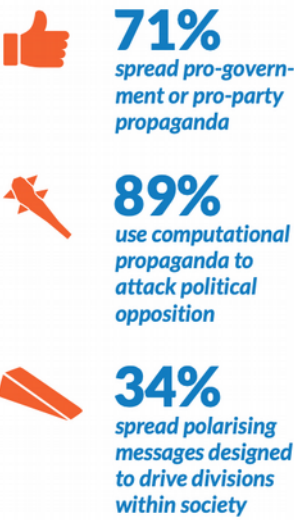
Source: Authors' evaluations based on data collected. Note: This table reports on the types of fake accounts identified between 2010-2019. For fake social media account types: = automated accounts, = human accounts, = cyborg accounts, = Hacked or Stolen accounts, = no evidence found.

TABLE 2 - FAKE ACCOUNT TYPES

Country	Bots	Human	Cyborg	Hacked or Stolen
Angola				
Argentina				
Armenia				
Australia				
Austria				
Azerbaijan				
Bahrain				
Bosnia & Herzegovina				
Brazil				
Cambodia				
China				
Colombia				
Croatia				
Cuba				
Czech Republic				
Ecuador				
Egypt				
Eritrea				
Ethiopia				
Georgia				
Germany				
Greece				
Guatemala				
Honduras				
Hungary				
India				
Indonesia				
Iran				
Israel				
Italy				
Kazakhstan				
Kenya				
Kyrgyzstan				
Macedonia				
Malaysia				

Source: Authors' evaluations based on data collected. Note: This table reports on the types of fake accounts identified between 2010-2019. For fake social media account types: = automated accounts, = human accounts, = cyborg accounts, = Hacked or Stolen accounts, = no evidence found.

Country	Bots	Human	Cyborg	Hacked or Stolen
Malta				
Mexico				
Moldova				
Myanmar				
Netherlands				
Nigeria				
North Korea				
Pakistan				
Philippines				
Poland				
Qatar				
Russia				
Rwanda				
Saudi Arabia				
Serbia				
South Africa				
South Korea				
Spain				
Sri Lanka				
Sudan				
Sweden				
Syria				
Taiwan				
Tajikistan				
Thailand				
Tunisia				
Turkey				
Ukraine				
United Arab Emirates				
United Kingdom				
United States				
Uzbekistan				
Venezuela				
Vietnam				
Zimbabwe				



Messaging and Valence

Cyber troops use a variety of messaging and valence strategies when communicating with users online. Valence describes how attractive or unattractive a message, event, or thing is. For the 2019 report, we have expanded our typology of messaging and valence strategies that cyber troops use when engaging in conversations with users online:

- (1) spreading pro-government or pro-party propaganda;
- (2) attacking the opposition or mounting smear campaigns;
- (3) distracting or diverting conversations or criticism away from important issues;
- (4) driving division and polarization; and
- (5) suppressing participation through personal attacks or harassment.

TABLE 3 - MESSAGING AND VALENCE

Country	Support	Attack Opposition	Distracting	Driving Divisions	Suppressing
Angola					
Argentina					
Armenia					
Australia					
Austria					
Azerbaijan					
Bahrain					
Bosnia & Herzegovina					
Brazil					
Cambodia					
China					
Colombia					
Croatia					
Cuba					
Czech Republic					
Ecuador					
Egypt					
Eritrea					
Ethiopia					
Georgia					
Germany					
Greece					
Guatemala					
Honduras					
Hungary					
India					
Indonesia					
Iran					
Israel					
Italy					
Kazakhstan					
Kenya					
Kyrgyzstan					
Macedonia					
Malaysia					
Malta					
Mexico					
Moldova					
Myanmar					
Netherlands					
Nigeria					
North Korea					
Pakistan					
Philippines					
Poland					
Qatar					
Russia					
Rwanda					
Saudi Arabia					
Serbia					
South Africa					
South Korea					
Spain					
Sri Lanka					
Sudan					
Sweden					
Syria					
Taiwan					
Tajikistan					
Thailand					
Tunisia					
Turkey					
Ukraine					
United Arab Emirates					
United Kingdom					
United States					
Uzbekistan					
Venezuela					
Vietnam					
Zimbabwe					

Source: Authors' evaluations based on data collected. Note: This table reports on the types of messaging and valence strategies of cyber troop activity between 2010-2019. For social media comments: = supporting, = attack opposition, = distracting, = driving division, = suppressing, = no evidence found.

**75%**
of countries used
disinformation
and media
manipulation to mislead users

**68%**
of countries use
state-sponsored
trolling to target
political dissidents,
the opposition or
journalists

**73%**
amplify messages
and content by
flooding hashtags

Communication Strategies

Cyber troops use a variety of communication strategies. We have categorized these activities into four categories:

- (1) the creation of disinformation or manipulated media;
- (2) mass-reporting of content or accounts;
- (3) data-driven strategies;
- (4) trolling, doxing or harassment;
- (5) amplifying content and media online.

The creation of disinformation or manipulated media is the most common communication strategy. In 52 out of the 70 countries we examined, cyber troops actively created content such as memes, videos, fake news websites or manipulated media in order to mislead users. Sometimes, the content created by cyber troops is targeted at specific communities or segments of users. By using online and offline sources of data about users, and paying for advertisements on popular social media platforms, some cyber troops target specific communities with disinformation or manipulated media.

The use of trolling, doxing or harassment is a growing global challenge and threat to fundamental human rights. In 2018, we identified 27 countries that used state-sponsored trolls to attack political opponents or activists via social media. This year, 47 countries have used trolling as part of their digital arsenal. Cyber troops also censor speech and expression through the mass-reporting of content or accounts. Posts by activists, political dissidents or journalists often get reported by a coordinated network of cyber troop accounts in order to game the automated systems social media companies use to take down inappropriate content. Trolling and the takedown of accounts or posts can happen alongside real-world violence, which can have a deep and chilling effect on the expression of fundamental human rights.



Participatory Propaganda – Canada 2017



Participatory Propaganda – Ontario 2018



Participatory Propaganda & Trump 2017



Participatory Propaganda – U.K. 2017

PARTICIPATORY PROPAGANDA IN 7 STEPS

1. Hyper Target Audience Analysis
2. Develop Inflammatory Content
3. Inject Content into Echo Chambers
4. Manipulate Feed Algorithms
5. Mobilize Followers to Action
6. Trending, Stage Scandals, Win Media Coverage
7. Review, Adapt & Repeat (Feedback Loop)

Eixo II) Proteção de dados pessoais



interesting story

Last updated: 1 April 2019



Methodology in Action



BEHAVIOURAL
SCIENCE

+



BIG DATA
ANALYSIS

+



AD
TARGETING

=



TRUMP'S
WIN

Behavioural Science and Big Data Analysis

Club Memberships
Churches Attended
Automotive Data
Shopping Data
Land Registries
Bonus Cards
Magazines read

PERSONAL DATA BOUGHT
FROM DIFFERENT SOURCES



ELECTORAL
ROLLS



ONLINE
DATA

=



BIG FIVE PERSONALITY
PROFILE



STATE LEVEL PROFILING

NAME
AGE
ADDRESS
INTERESTS
PERSONALITY
POLITICAL INCLINATION

INDIVIDUAL LEVEL PROFILING

"We have profiled the personality of every adult in the United States of America—220 million people" - CEO of Cambridge Analytica*

Ad Targeting

Personalised variations in
terms of different:

Headings

Colours Photos
Videos
Messages

"Pretty much every message
that Trump put out was data-
driven" - CEO of Cambridge
Analytica*

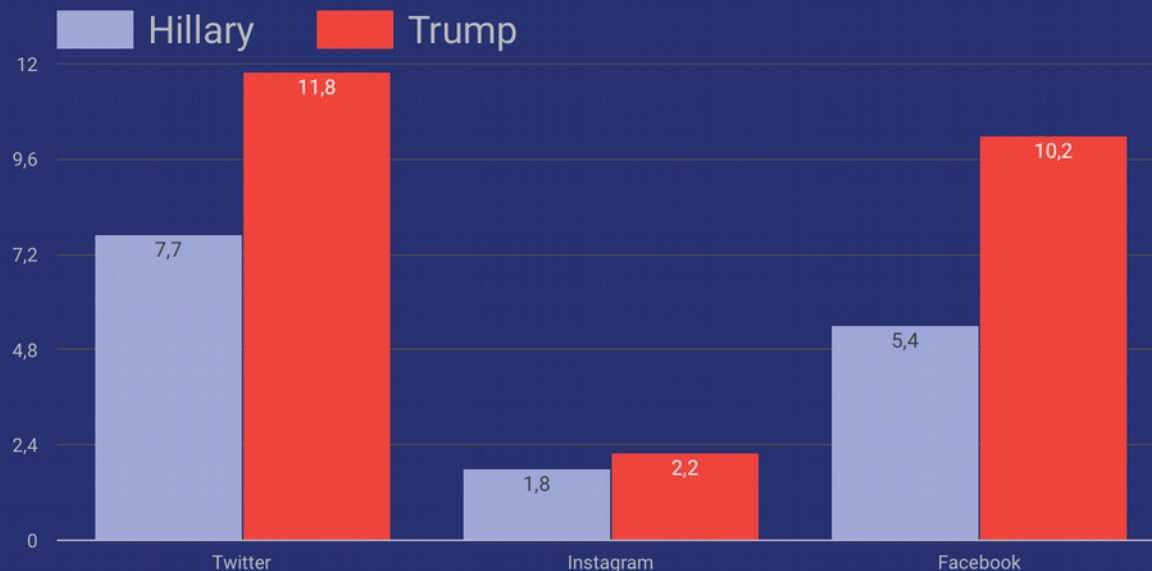
REDWOOD ALGORITHMS - Building Data Science Assets for ALL

*The company hired by Trump for its marketing efforts

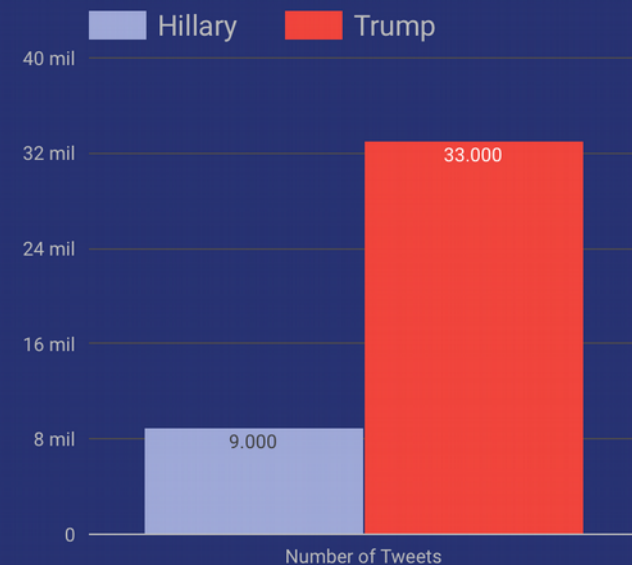
Fonte: <https://www.redwoodalgorithms.com/ra-insights/the-analytics-behind-us-elections-2016>

The differentiating Factor

Trump was ahead of Hillary in Social Media Engagement.



Total number of Followers on different platforms



Total number of Tweets sent during election campaign

REDWOOD ALGORITHMS - Building Data Science Assets for ALL

Total Facebook Engagements for Top 20 Election Stories



ENGAGEMENT REFERS TO THE TOTAL NUMBER OF SHARES, REACTIONS, AND COMMENTS FOR A PIECE OF CONTENT ON FACEBOOK SOURCE: FACEBOOK DATA VIA BUZZSUMO

O que esperar para as
eleições de 2020?

BEHAVIOURAL SCIENCE

- **Demographic**
- **Geographic**
- **Economics**

Influence the world view

- **Psychometrics**
- **Digital Anthropology**

PERSONALITY THAT DRIVES BEHAVIOUR & BEHAVIOUR THAT INFLUENCES HOW SOMEONE **VOTE**.

Most communication companies still segment their audiences by demographics and geographics.

The idea that all women should receive the same message because of their gender, or all African Americans because of their race is getting old fashion and losing effect.

Psychometrics helps the understanding of the voter's personality.

Digital Anthropology helps the understanding of how digital communities appear and behave in the world wide web.

BEHAVIOURAL SCIENCE

VIDEO

OCEAN (BIG 5)

Find among the diverse audiences that interact in the digital environment, where there are those with the potential to act as ambassadors of the government. And where deliveries make more difference.



Behavioural Science

IDEIA BIG DATA

Electorate Traits EXAMPLE



- Is curious about a wide range of topics.
- Is easily bored.
- Is less bound by rules and more playful.
- Language and thinking are more future-oriented.
- Expresses more liberal views.
- Achievement, ambition, success, competence.
- Self-direction, creativity, independent thought.



- Is punctual.
- Tends to go by the rules.
- Is reliable
- Sees life as tasks and goals to accomplish.
- Tradition, family, respect, commitment.
- Achievement, ambition, success, competence.
- Universalism, social justice, welfare of all.



- Is warm and friendly.
- Makes more eye contact.
- Is cheerful
- Takes on responsibility for others
- Readily trusts others.
- Achievement, ambition, success, competence.
- Universalism, social justice, welfare of all.



- Enjoys being helpful.
- Is concerned about others' opinions and reactions.
- Is warm and friendly.
- Tries to maintain harmony in the team.
- Universalism, social justice, welfare of all.
- Tradition, humility, respect, commitment.
- Security, reciprocity, safety, harmony.



- Rationality, keeping emotions subdued.
- Is optimistic and cheerful.
- Speaks with a controlled pace and vocabulary.
- Doesn't show signs of discouragement.
- Recovers quickly from crisis.
- Has a normal amount off eye contact.
- Is slow to anger.

IDEAL METHODOLOGY FOR SOCIAL ENGAGEMENT - WHATSAPP

1

STRATEGY PLANNING FOR SOCIAL ENGAGEMENT

- Scenario analysis
- Strengths, weaknesses, opportunities and threats identification (SWOT)
- Goal setting (S.M.A.R.T.)

2

SCALABLE STRATEGY FOR LEAD GENERATION

- Channels definition for further opt-in inclusion
- Opt-in inclusion guide in digital content

3

DATABASE ORGANIZATION

- Available database (storage organization)
- New data collection
- Data cleansing

4

CLUSTERIZATION AND GAMIFICATION

- Target clusterization
- Group formation / WhatsApp distribution List (Bulk or Organic)

5

ACTIVATION / RELATIONSHIP

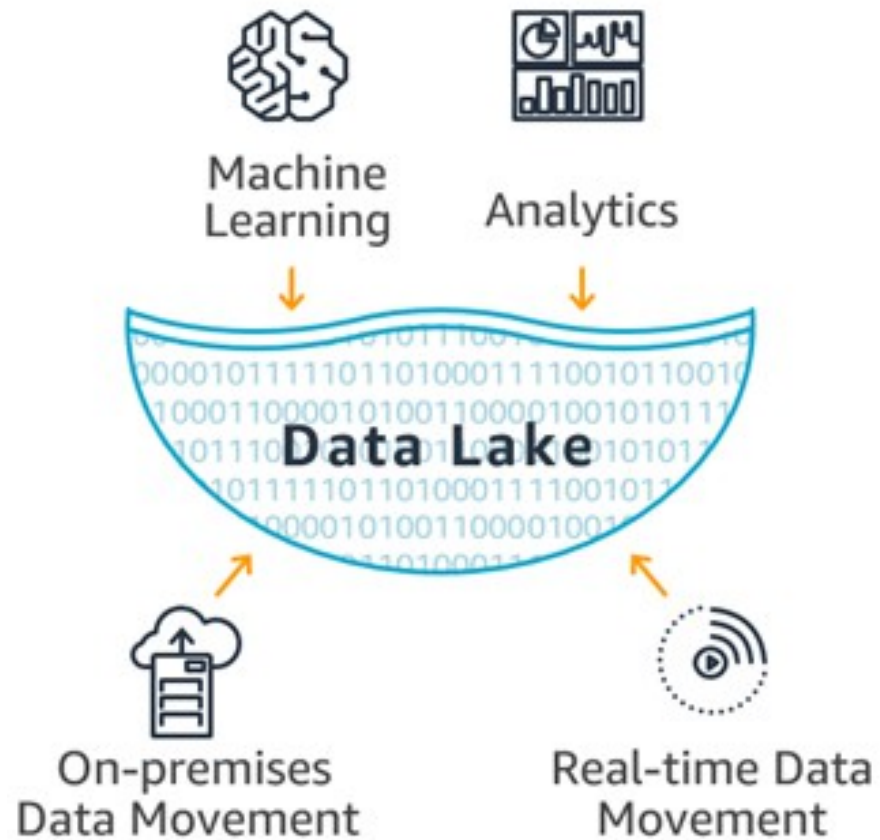
- Segmented content production
- Sending of segmented content
- Relationship

6

MONITORING

- Main guidelines identification
- Dissemination nodes identification
- Participants control and categorization

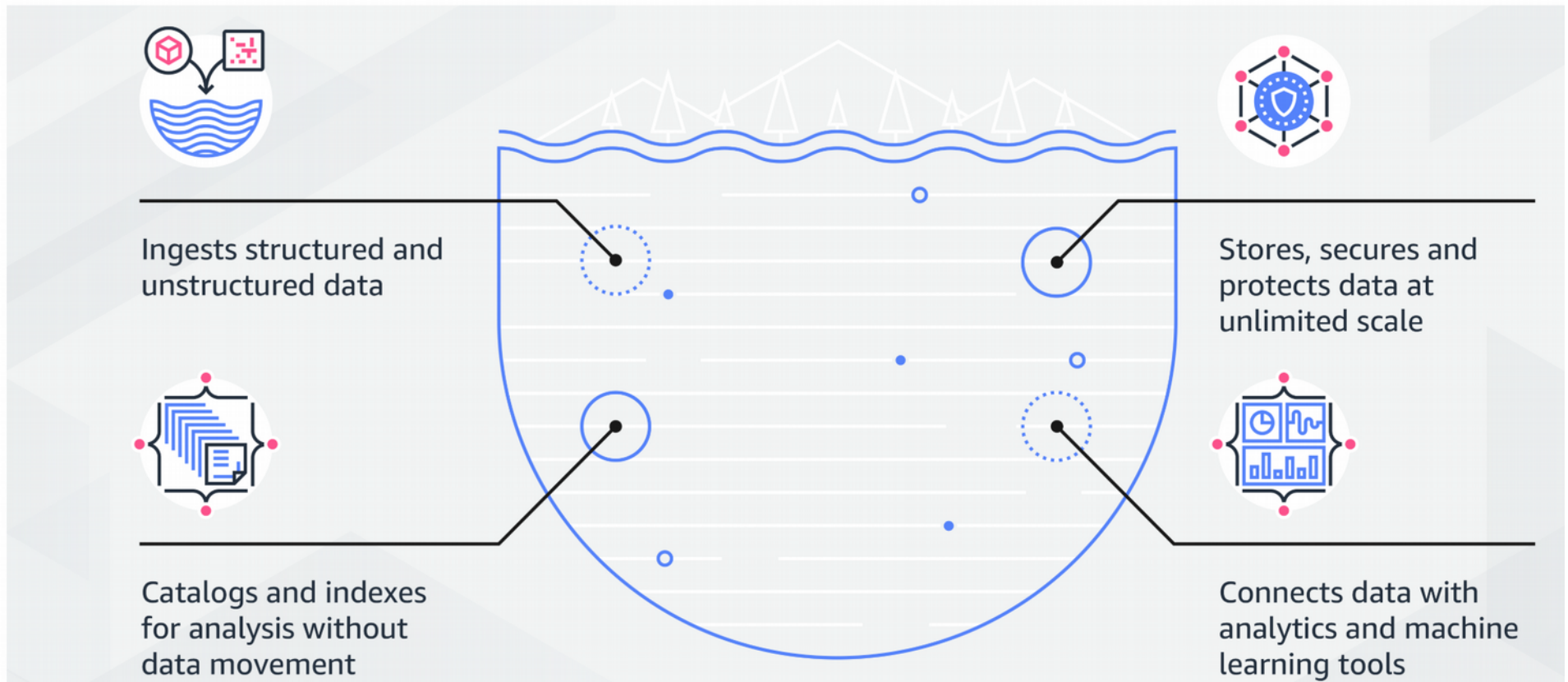
Data Lakes nos municípios



What is a data lake?

A data lake is a centralized repository that allows you to migrate and store all structured and unstructured data at unlimited scale, as well as gain insights through big data analytics and machine learning tools.

Key components of a data lake





TIC PROVEDORES 2017

METODOLOGIA



*Realizada desde 2011
a cada três anos*

População

Empresas provedoras de acesso à Internet no Brasil, que possuem licença concedida pela Anatel para a prestação de Serviços de Comunicação Multimídia (SCM)

Total estimado

6.618 empresas provedoras

Respondentes

2.177 respondentes entre os 3.091 provedores que declararam acessos no SICI (Taxa de Resposta de 70%)

Coleta

Realizada entre setembro de 2017 e maio de 2018 via CATI e questionário Web



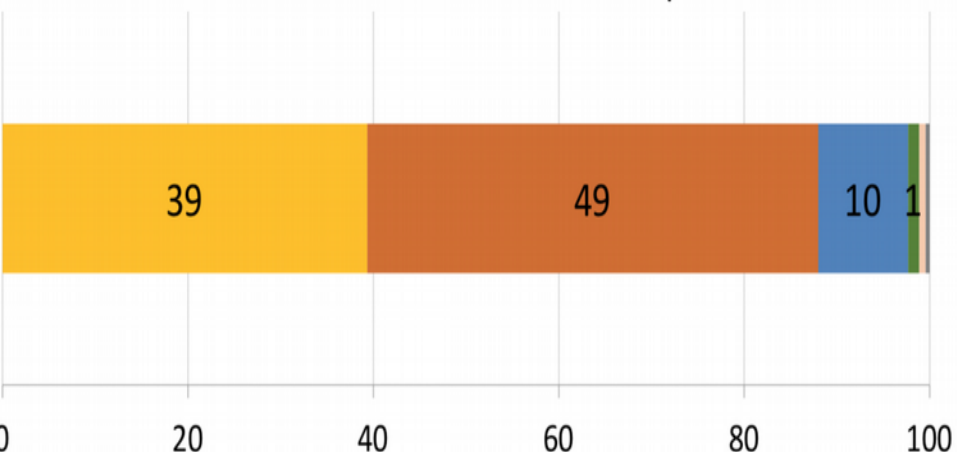


NÚMERO DE PESSOAS OCUPADAS E NÚMERO DE ACESSOS (ANATEL)

% SOBRE O TOTAL DE EMPRESAS PROVEDORAS (2017)

NÚMERO DE PESSOAS OCUPADAS

- De 1 a 9 (micro)
- De 10 a 49 (pequena)
- De 50 a 249 (média)
- De 250 ou mais (grande)
- Não sabe
- Não respondeu

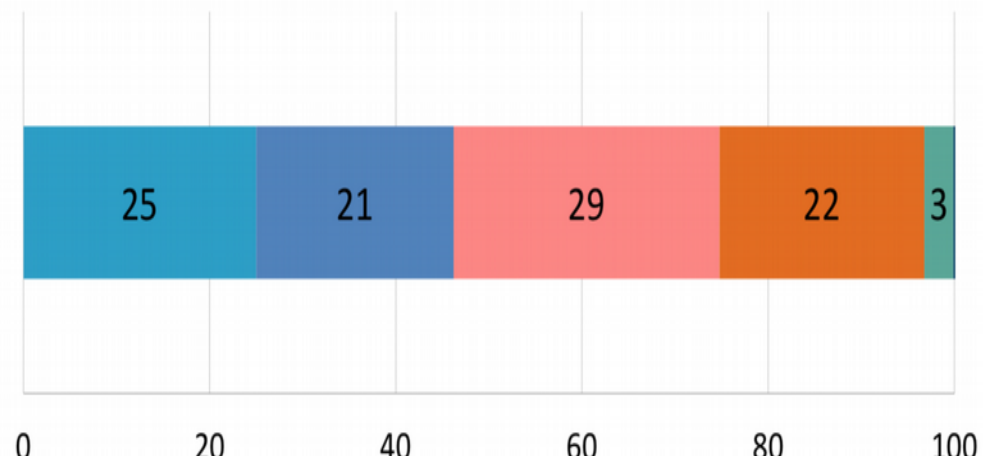


88% das empresas provedoras
são micro ou pequenas empresas
(1 a 49 pessoas ocupadas)



75% das empresas provedoras
reportaram à Anatel até 1.000
acessos

NÚMERO DE ACESSOS

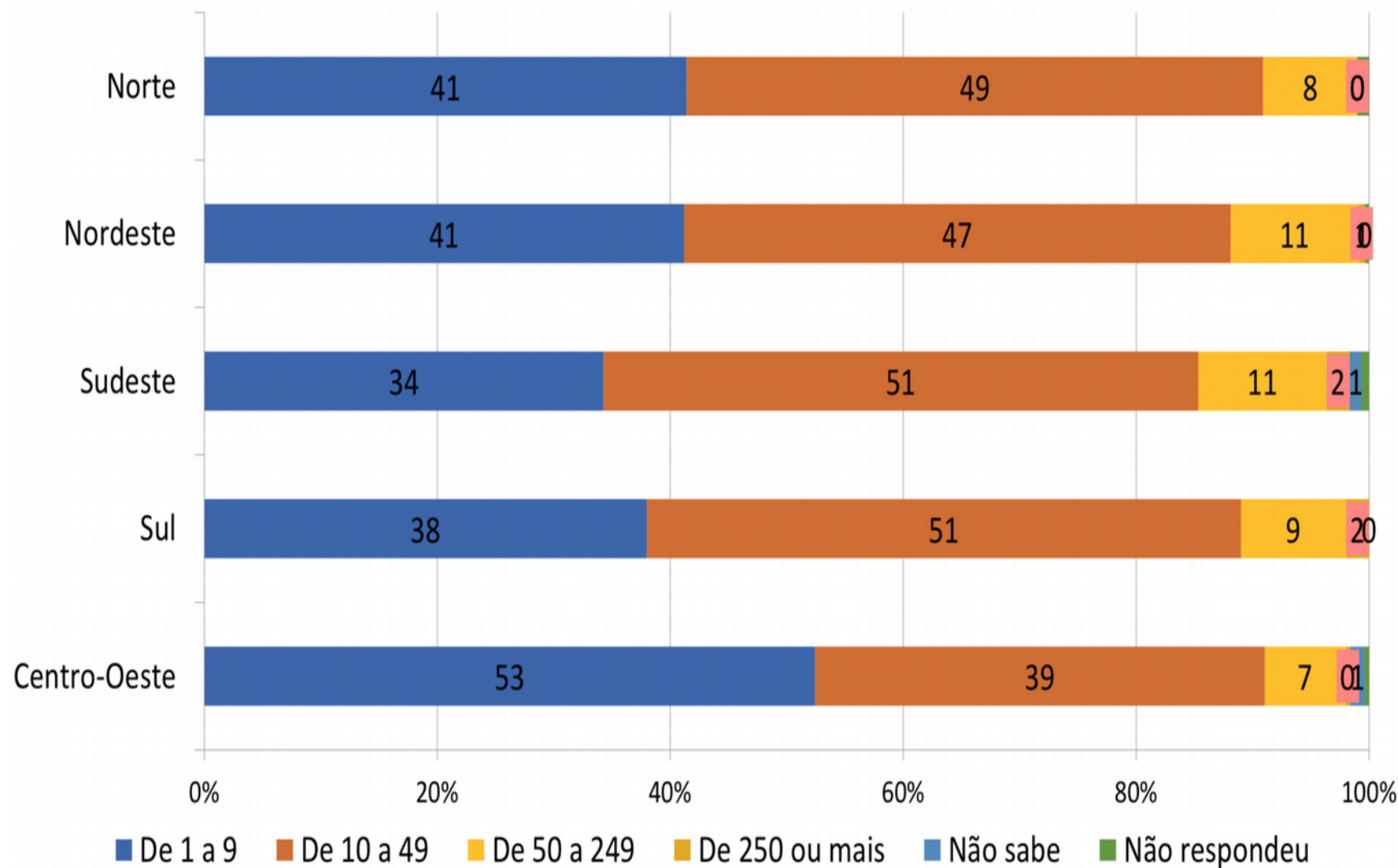


- Menos de 100 acessos
- De 100 a menos de 300 acessos
- De 300 a menos de 1.000 acessos
- De 1.000 a menos de 5.000 acessos
- 5.000 acessos a menos de 45.000 acessos
- Grande provedor (mais de 45.000 acessos)



NÚMERO DE PESSOAS OCUPADAS, POR REGIÃO

% SOBRE O TOTAL DE EMPRESAS PROVEDORAS (2017)



85%
das empresas
provedoras são
optantes do
**Simplex
Nacional**

Eixo III) Cyberbullying e os ataques à dignidade humana

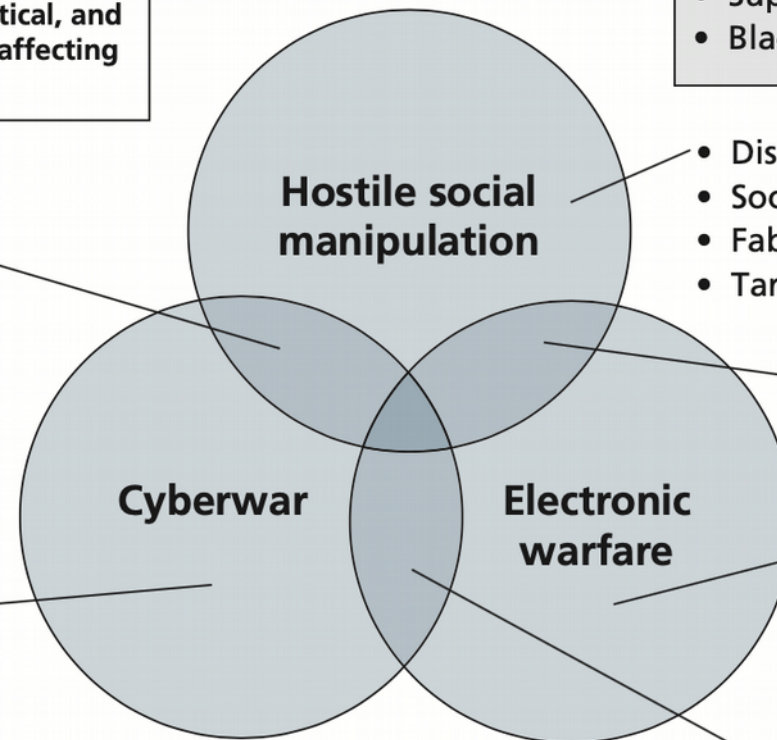
The Boundaries of Social Manipulation

Competition in the information space

Hostile social manipulation is the purposeful, systematic generation and dissemination of information to produce harmful social, political, and economic outcomes in a target country by affecting beliefs, attitudes, and behavior.

- Hacking to gain data for information operations
- Cyberbullying of targeted opponents
- Disruption of automated trading
- Disruption of internet of things

- Malware attacks on power grids
- Distributed denial of service attacks on governments



Classic covert intelligence/ political manipulation

- Recruitment of agents, HUMINT
- Support for political parties, movements
- Blackmailing, discrediting officials

- Disinformation, propaganda
- Social media campaigns
- Fabricated information, images
- Targeted harassment

- Suppression of civilian broadcast systems

- EW jamming, disruption of military systems
- Attacks on civilian information systems

Cyberattacks on military systems

Competitors see these realms as integrated and holistic, do not distinguish among components

NOTE: HUMINT = human intelligence.



DENÚNCIAS RECEBIDAS (TOTAL)

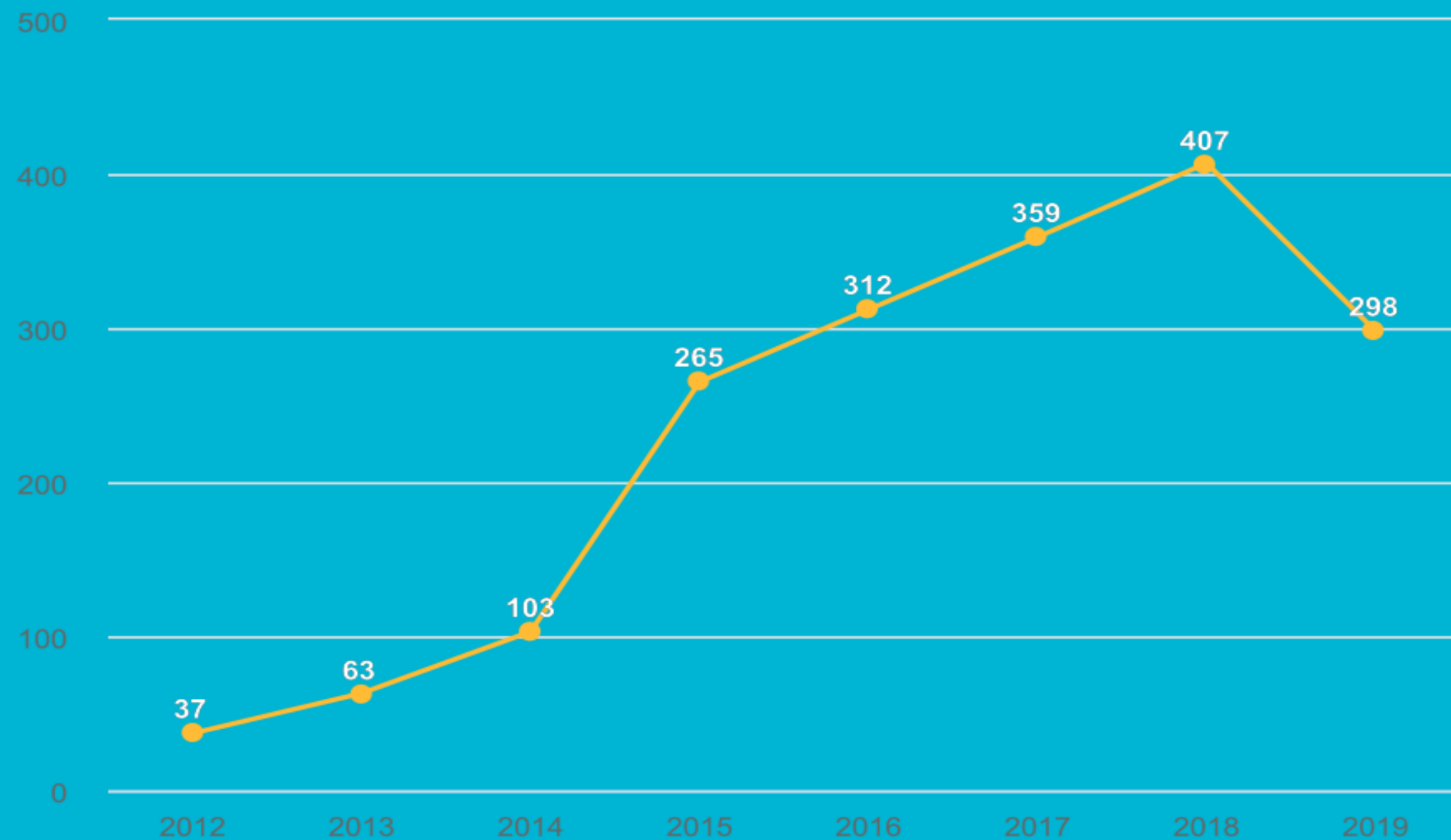
CONTEÚDO DENUNCIADO	Primeiro Turno (16/08 a 07/10)	Segundo Turno (08/10 a 28/10)	TOTAL (1º e 2º turnos)	Variação (1º p/ 2º turno)
Apologia e Incitação a crimes contra a Vida	1.746	11.009	12.755	630,52%
Xenofobia (sobretudo contra nordestinos)	338	8.009	8.347	2369,52%
Violência ou Discriminação contra Mulheres	1.437	1.232	2.669	-14,26%
Racismo	531	1.159	1.690	218,26%
Homofobia/LGBTfobia	422	1.478	1.900	350,23%
Neonazismo	254	1.393	1.647	548,42%
intolerância Religiosa	195	283	478	145,13%
Pornografia Infantil	7.054	2.682	9.736	-61,98%
Tráfico de Pessoas	63	31	94	-50,79%
TOTAL	12.040	27.276	39.316	226,54%

Fonte dos dados: SaferNet Brasil / Central Nacional de Denúncias de Crimes Cibernéticos

Todo o período eleitoral (16/08 a 28/10): 39.316 denúncias de crimes e violações a Direitos Humanos na Web

2007 / 2018

Ciberbullying por Ano





Definição do cyberbullying e exemplos de manifestação. Leis e recursos pedagógicos que ajudam na prevenção e no enfrentamento dos casos.

2.1 - O QUE É CYBERBULLYING? ATORES E SINAIS

2.2 - DADOS SOBRE CYBERBULLYING NO BRASIL

2.3 - ASPECTOS LEGAIS E CONSEQUÊNCIAS JURÍDICAS

2.4 - QUAL O PAPEL DAS ESCOLAS?

2.5 - AÇÕES COM ALUNOS E FAMÍLIAS

2.6 - COMO NOTIFICAR E DENUNCIAR CASOS CONCRETOS?

<http://ead.safernet.org.br/>

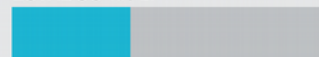
Realização:



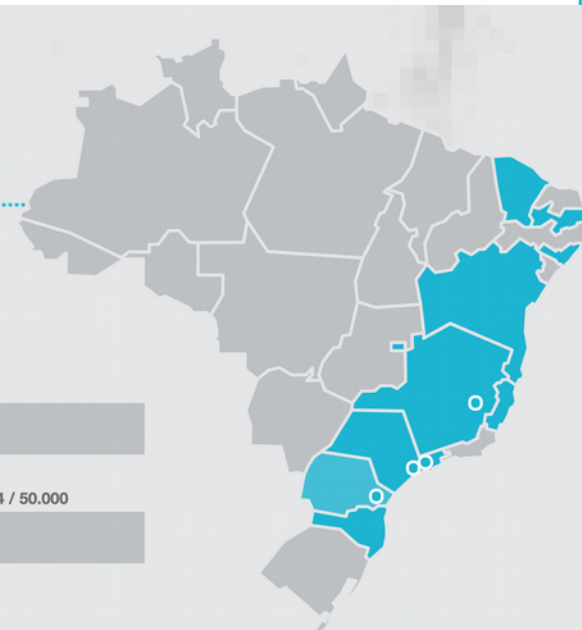
Apoio:



ESTADOS 10 / 27



MATRÍCULAS 21.154 / 50.000





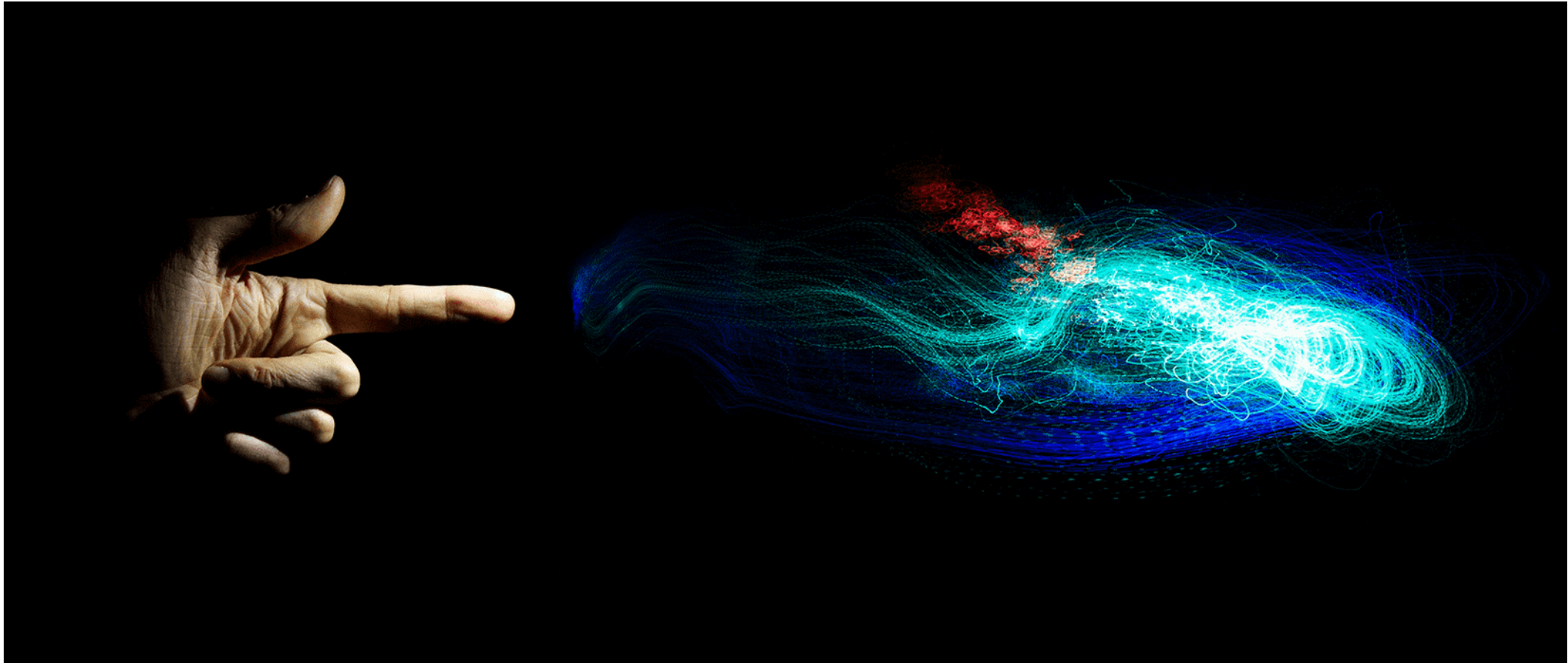


Dando continuidade as ações da Semana de Atenção Especial ao Bullying, ontem, dia 07 de maio, no Teatro Módulo, os alunos e alunas assistiram palestra ministrada por Rodrigo Nejm (psicólogo, diretor de Educação da Safernet e Pesquisador da UFBA). A temática abordada pelo representante da Safernet foi de extrema relevância para toda a comunidade escolar - alunos, professores, equipe técnica, colaboradores - já que englobou a importância do uso seguro e consciente da Internet, o combate ao Cyberbullying e a nossa responsabilidade individual e coletiva em promover ambientes saudáveis, pautados na Empatia e no Respeito Mútuo.

[#ÉdaMinhaConta](#) [#combateabullying](#) [#cyberbullying](#) [#safernet](#) [#ColégioMódulo](#)

Conclusão

Não existe bala de prata!



Foco em estratégias multisetoriais:

- a) detecção, resposta e accountability (curto prazo)
- b) educação para o uso ético, seguro e responsável da Internet (longo prazo)

OBRIGADO!

