

Evolução e Desafios Futuros do Ciberespaço

Arnaut Moreira

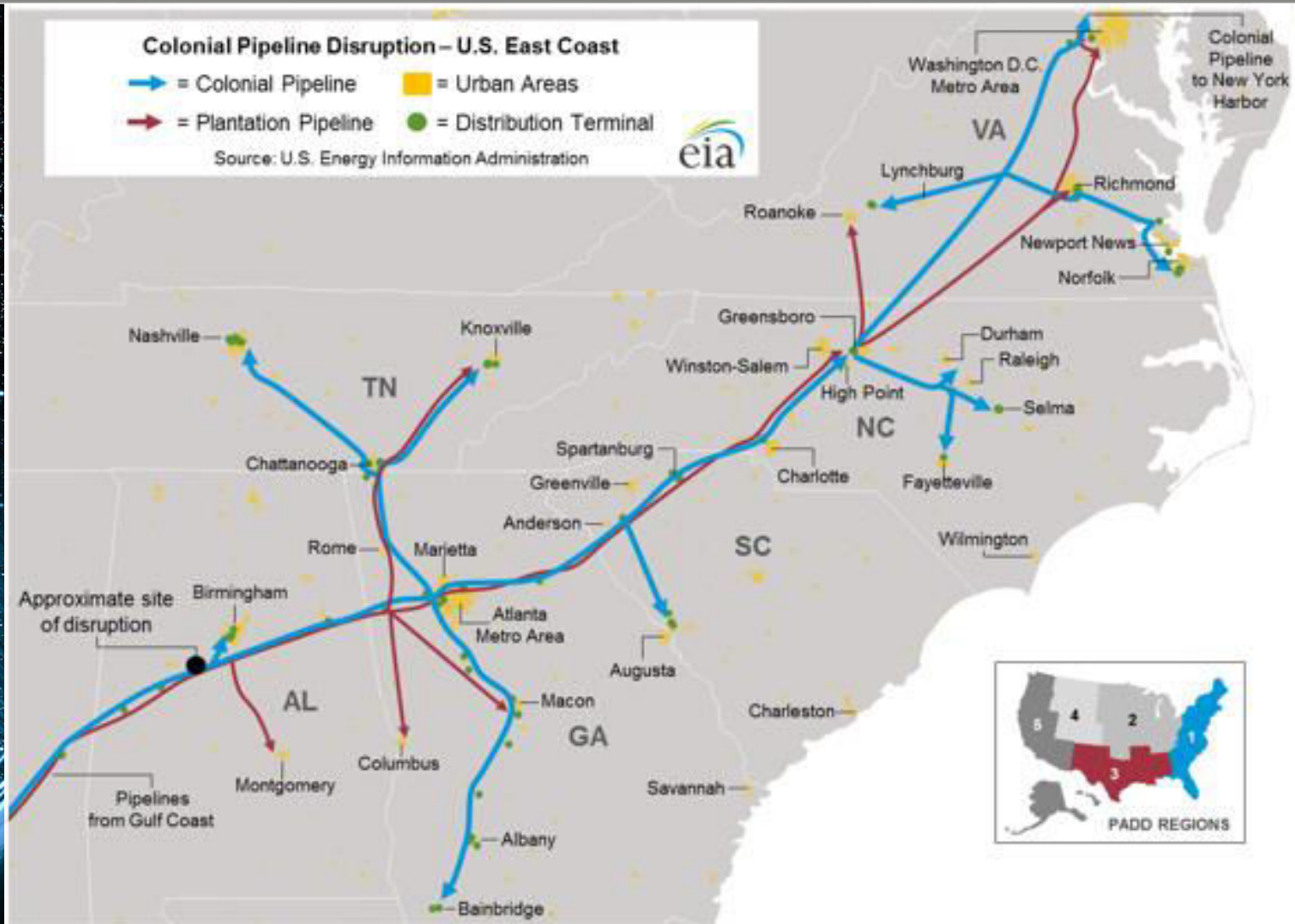
Agenda

1. **Tudo Conectado, todos em Risco**
2. **Da Arpanet à Internet das Coisas**
3. **Os actores do Ciberespaço**
4. **Desafios futuros**

Agenda

- 1. Tudo Conectado, todos em Risco**
2. Da Arpanet à Internet das Coisas
3. Os actores do Ciberespaço
4. Desafios futuros

Colonial Pipeline: Quase 9 000 Km oleodutos

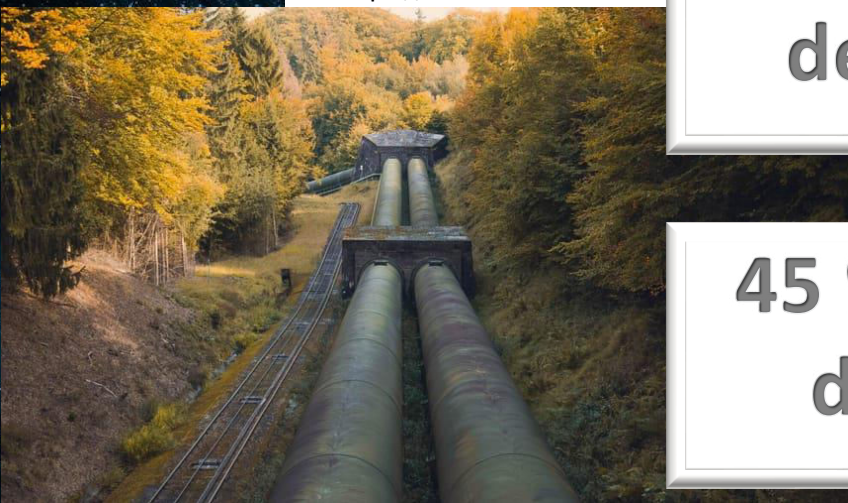


Estende-se desde o Golfo do México ao Porto de Nova Iorque

Importância de uma infraestrutura crítica



Liga 29 Refinarias a 267 terminais de distribuição



Gasolina, diesel, combustível de aquecimento e de aviação

45 % de todo o abastecimento de gasolina da Costa Leste



<https://www.canarymedia.com>

Mas no dia 7 de Maio de 2021 ...



<https://www.bbc.com/news/technology-57063636>

Exemplo de mensagem que aparece no monitor de um sistema afectado pelo Ramsonware DarkSide



FBI

FEDERAL BUREAU
OF INVESTIGATION

May 10, 2021

FBI Statement on Compromise of Colonial Pipeline Networks

The FBI confirms that the **Darkside ransomware** is responsible for the compromise of the Colonial Pipeline networks. We continue to work with the company and our government partners on the investigation.

DarkSide: Um novo tipo de serviço

DarkSide é um grupo de **Ransomware-as-a-Service (RaaS)** que disponibiliza a sua aplicação de malware aos seus clientes criminosos. Já disponível na versão 2.

O grupo cobra 25% para os regates abaixo de \$500,000 e 10% acima de \$5 milhões (info publicada nos seus posts).

Dupla estratégia: Obter dinheiro das companhias afectadas, mas também vender informações à concorrência antes de serem tornadas públicas.

A 13 de Maio a Bloomberg anunciou que a Colonial Pipelines pagou um resgate de 5 milhões de dólares para obter a chave de descriptação.

DarkSide: Guia dos passos a seguir

sophos_READ[REDACTED].TXT - Notepad

File Edit Format View Help

----- [Welcome to DarkSide] ----->

What happend?

Your computers and servers are encrypted, backups are deleted. We use strong encryption algorithms, so you cannot decrypt your data. But you can restore everything by purchasing a special program from us - universal decryptor. This program will restore all your network. Follow our instructions below and you will recover all your data.

Data leak

First of all we have uploaded n

These files include:

- Accounting
- Research & Development

Your personal leak page: [http://darkside\[REDACTED\]](http://darkside[REDACTED])

On the page you will find examples of files that have been stolen.

The data is preloaded and will be automatically published if you do not pay.

After publication, your data will be available for at least 6 months on our tor cdn servers.

We are ready:

- To provide you the evidence of stolen data
- To delete all the stolen data.

What guarantees?

We value our reputation. If we do not do our work and liabilities, nobody will pay us. This is not in our interests.

All our decryption software is perfectly tested and will decrypt your data. We will also provide support in case of problems.

We guarantee to decrypt one file for free. Go to the site and contact us.

How to get access on website?

Using a TOR browser:

- 1) Download and install TOR browser from this site: <https://torproject.org/>
- 2) Open our website: [http://darkside\[REDACTED\]](http://darkside[REDACTED])

When you open our website, put the following data in the input form:

Key:

**Your computers and servers are encrypted,
backups are deleted ... Follow the instructions below ...**

We value our reputation...

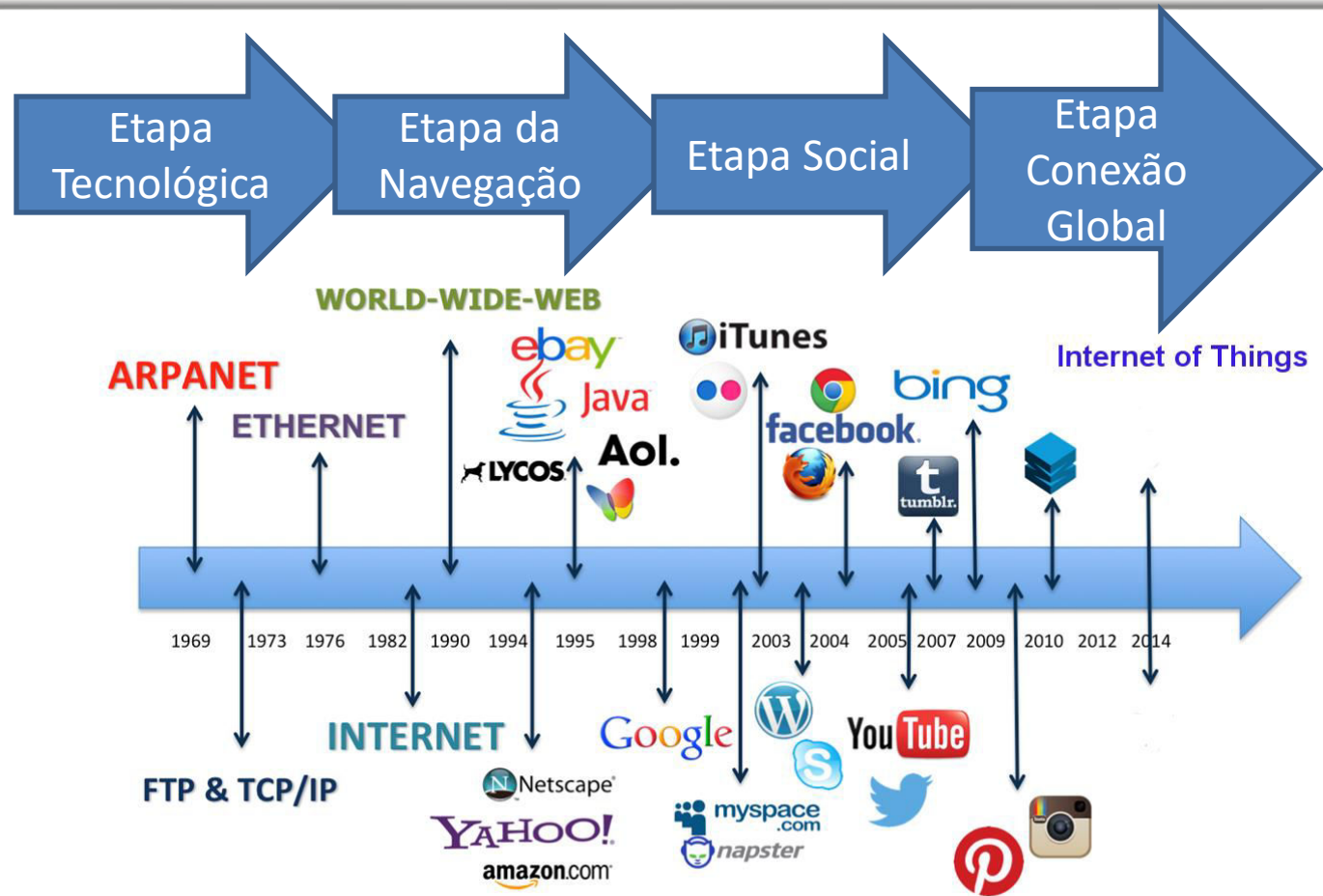


Using a TOR browser...

Agenda

1. Tudo Conectado, todos em Risco
2. Da Arpanet à Internet das Coisas
3. Os actores do Ciberespaço
4. Desafios futuros

A evolução da Internet em 4 etapas



Um Planeta (quase) todo Digital

JAN
2021

DIGITAL AROUND THE WORLD

ESSENTIAL HEADLINES FOR MOBILE, INTERNET, AND SOCIAL MEDIA USE

INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** WITH PREVIOUS REPORTS

TOTAL
POPULATION



7.83
BILLION

URBANISATION:

56.4%

UNIQUE MOBILE
PHONE USERS



5.22
BILLION

vs. POPULATION:

66.6%

INTERNET
USERS*



4.66
BILLION

vs. POPULATION:

59.5%

ACTIVE SOCIAL
MEDIA USERS*



4.20
BILLION

vs. POPULATION:

53.6%

16

SOURCES: THE U.N.; LOCAL GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; GWI; EUROSTAT; CNNIC; APJII; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; COMPANY EARNINGS REPORTS; MEDIASCOPE. ***ADVISORIES:** INTERNET USER NUMBERS NO LONGER INCLUDE DATA SOURCED FROM SOCIAL MEDIA PLATFORMS, SO VALUES ARE **NOT COMPARABLE** TO DATA PUBLISHED IN PREVIOUS REPORTS. SOCIAL MEDIA USER NUMBERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **♦ COMPARABILITY ADVISORY:** SOURCE AND BASE CHANGES.

we
are
social

 **Hootsuite®**

<https://www.slideshare.net/kepios/global-digital-statbites-001>

Mobile Phones lideram o acesso

JAN
2021

SHARE OF WEB TRAFFIC BY DEVICE

EACH DEVICE'S SHARE OF TOTAL WEB PAGES SERVED TO WEB BROWSERS

⚠ THE FIGURES ON THIS CHART ARE BASED ON TRAFFIC TO WEB BROWSERS ONLY, AND DO NOT INCLUDE DATA FOR OTHER CONNECTED ACTIVITIES (E.G. USE OF NATIVE MOBILE APPS)

MOBILE
PHONES



55.7%

DEC 2020 vs. DEC 2019:

+4.6%

+244 BPS

LAPTOPS &
DESKTOPS



41.4%

DEC 2020 vs. DEC 2019:

-5.8%

-253 BPS

TABLET
COMPUTERS



2.8%

DEC 2020 vs. DEC 2019:

+3.3%

+9 BPS

OTHER
DEVICES



0.07%

DEC 2020 vs. DEC 2019:

[UNCHANGED]

55

SOURCE: STATCOUNTER (ACCESSED JAN 2021). FIGURES REPRESENT EACH DEVICE'S SHARE OF WEB PAGES SERVED TO WEB BROWSERS ONLY. NOTES: FIGURES FOR DEVICE SHARE ARE FOR DECEMBER 2020. ANNUAL CHANGE FIGURES COMPARE MONTHLY SHARE VALUES FOR DECEMBER 2020 TO DECEMBER 2019. PERCENTAGE CHANGE VALUES REPRESENT RELATIVE CHANGE (E.G. AN INCREASE OF 2.0% FROM A STARTING VALUE OF 50% WOULD EQUAL 52%, NOT 70%). "BPS" VALUES REPRESENT BASIS POINTS, AND INDICATE THE ABSOLUTE CHANGE IN SHARE VALUE.

we
are
social

Hootsuite

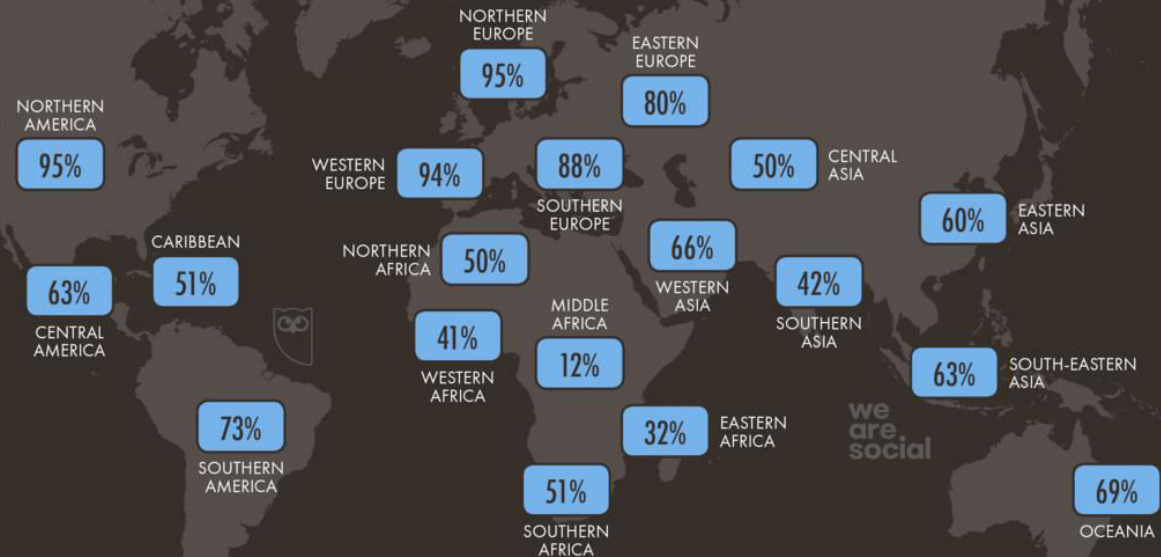
<https://www.slideshare.net/kepios/global-digital-statbites-001>

Desigualdades no acesso à Internet

JAN
2019

INTERNET PENETRATION BY REGION

INTERNET USE BY REGION, COMPARING THE NUMBER OF INTERNET USERS TO TOTAL POPULATION (REGARDLESS OF AGE)



33

SOURCES: INTERNETWORLDSTATS; ITU; WORLD BANK; CIA WORLD FACTBOOK; EUROSTAT; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; MIDEASTMEDIA.ORG; REPORTS IN REPUTABLE MEDIA; SOCIAL MEDIA PLATFORM USER NUMBERS. **NOTE:** PENETRATION FIGURES ARE BASED ON TOTAL POPULATION, REGARDLESS OF AGE. REGIONS AS DEFINED BY THE UNITED NATIONS GEOScheme.

 **Hootsuite™** 

Von Neumann (1903-1957)



Projecto Manhattan
Modelação Matemática



Arnaut Moreira

thing. We can add a certain amount of automaton $A + B$. The automaton C operating them alternately according to the control C will first cause B to make two copies of itself. Then C will next cause A to construct X at the rate $\phi(X)$. Finally, the control C will tie X together and cut them loose from the end the entity $X + \phi(X)$ has been

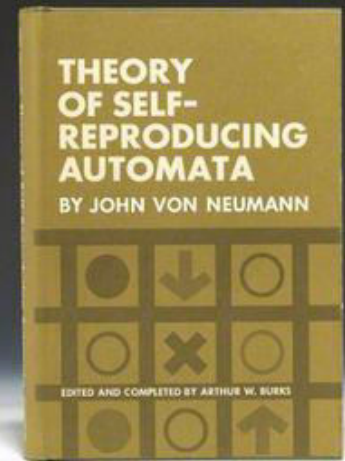
$+ B + C$) for X . The automaton C will produce $(A + B + C) + \phi(A + B + C)$ if production has taken place.

We are given the universal constructor C and a description of itself, $\phi(A + B + C)$. The production starts with $(A + B + C) + \phi(A + B + C)$. C directs B to copy the description twice; C produces $\phi(A + B + C) + \phi(A + B + C)$.

Then C directs A to produce the automaton $A + B + C$ from one copy of the description; the result is $(A + B + C) + (A + B + C) + \phi(A + B + C)$. Finally, C ties the new automaton and its description together and cuts them loose. The final result consists of the two automata $(A + B + C)$ and $(A + B + C) + \phi(A + B + C)$. If B were to copy the description thrice, the process would start with one copy of $(A + B + C) + \phi(A + B + C)$ and terminate with two copies of this automaton. In this way, the universal constructor reproduces itself.]

This is not a vicious circle. It is quite true that I argued with a variable X first, describing what C is supposed to do, and then put something which involved C for X . But I defined A and B exactly, before I ever mentioned this particular X , and I defined C in terms which apply to any X . Therefore, in defining A , B , and C , I did not make use of what X is to be, and I am entitled later on to use an X which refers explicitly to A , B , and C . The process is not circular.

The general constructive automaton A has a certain creative ability, the ability to go from a description of an object to the object. Like-



1949

“In this way, the
universal constructor
reproduces itself

Está criado o modelo
teórico para a
construção de vírus

A era dos Ataques Cibernéticos

2007

Serviços Governamentais da Estónia são bloqueados por uma ataque DDoS quando decidem retirar memorial soviético

2010

Malware Stuxnet ataca centrifugadoras do Irão
(Um ataque digital que tem efeitos destrutivos físicos)

2014

Sony Pictures Entertainment atacada (Coreia N?)
(Um ataque digital sobre o mundo empresarial)


2014

Nato confirma que um ciberataque permite invocar Artº 5
(O Ciberespaço passa a ser um domínio operacional)

Agenda

1. Tudo Conectado, todos em Risco
2. Da Arpanet à Internet das Coisas
3. Os actores do Ciberespaço
4. Desafios futuros

3. Actores do Ciberespaço

- 
- a. Os internautas
 - b. As empresas
 - c. As instituições
 - d. Os serviços de informações
 - e. As forças armadas
 - f. Os activismos
 - g. Os hackers
 - h. O crime organizado
 - i. As forças geoestratégicas

a. Os internautas



A paixão pelo Ciberespaço tem todas as características de um vício

<http://qz.com/553044/india-may-soon-have-more-internet-users-than-the-us/>

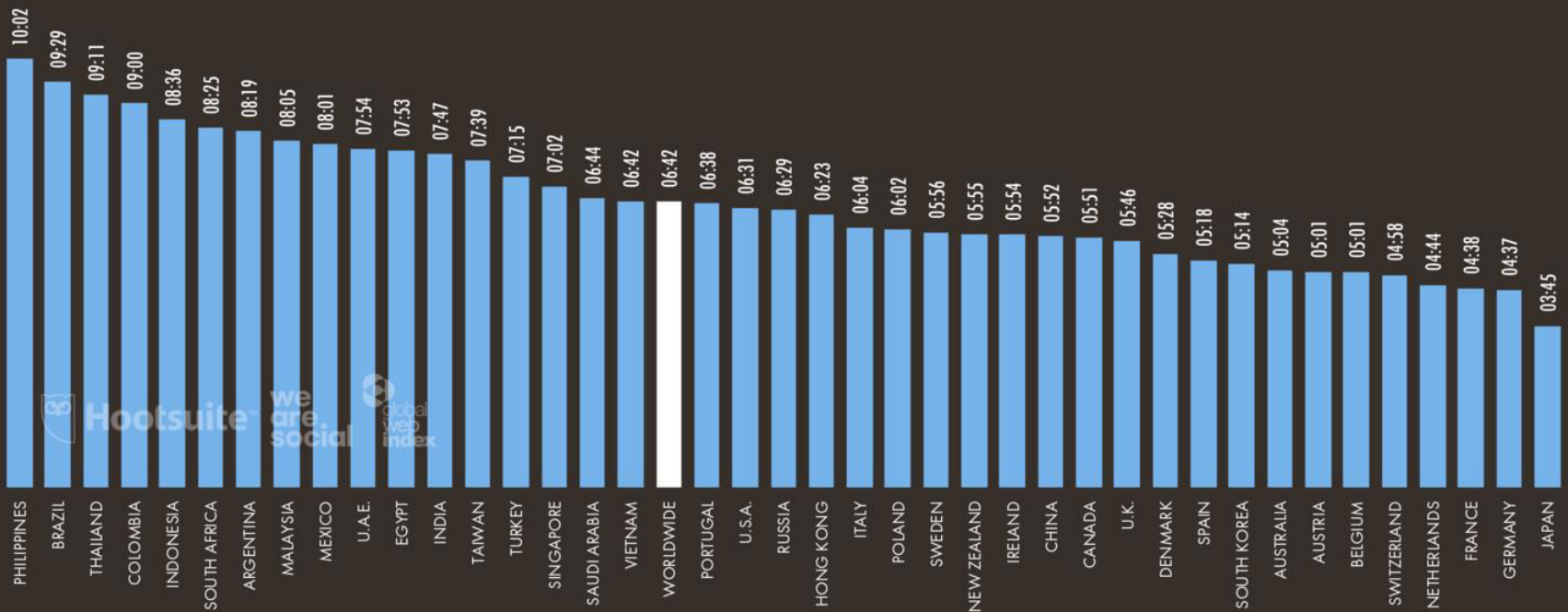
Constitui-se portanto como uma vulnerabilidade que pode ser explorada

Média diária de um utilizador: 6H30m na Internet

JAN
2019

TIME PER DAY SPENT USING THE INTERNET

AVERAGE AMOUNT OF TIME PER DAY SPENT USING THE INTERNET VIA ANY DEVICE, IN HOURS AND MINUTES [SURVEY BASED]



40

SOURCE: GLOBALWEBINDEX (Q2 & Q3 2018). FIGURES REPRESENT THE FINDINGS OF A BROAD SURVEY OF INTERNET USERS AGED 16-64.

A primazia das Paixões

**JAN
2019**

TOP FACEBOOK PAGES

BASED ON FACEBOOK PAGES WITH THE GREATEST NUMBER OF PAGE LIKES

#	PAGE	CATEGORY	'FANS'
01	FACEBOOK	PRODUCT / SERVICE	213,439,863
02	SAMSUNG	PRODUCT / SERVICE	159,534,892
03	CRISTIANO RONALDO	ATHLETE	122,582,580
04	REAL MADRID C.F.	SPORTS TEAM	109,425,674
05	COCA-COLA	PRODUCT / SERVICE	107,533,356
06	FC BARCELONA	SPORTS TEAM	102,658,087
07	SHAKIRA	MUSICIAN	101,753,296
08	VIN DIESEL	ACTOR	98,551,962
09	TASTY	COOKING	96,194,554
10	LEO MESSI	ATHLETE	89,883,368

#	PAGE	CATEGORY	'FANS'
11	EMINEM	MUSICIAN	88,014,532
12	YOUTUBE	PRODUCT / SERVICE	83,526,380
13	MR BEAN	TV SHOW	82,641,600
14	RIHANNA	MUSICIAN	79,887,748
15	MCDONALD'S	PRODUCT / SERVICE	78,946,824
16	JUSTIN BIEBER	MUSICIAN	77,511,620
17	WILL SMITH	ACTOR	77,312,018
18	CGTN	MEDIA	73,688,844
19	MANCHESTER UNITED	SPORTS TEAM	73,295,917
20	HARRY POTTER	MOVIE FRANCHISE	72,930,986

105

SOURCE: BASED ON DATA FROM FACEBOOK (JANUARY 2019).

b. As empresas

Procuram visibilidade, negócio

Alteração profunda no paradigma dos sectores críticos:

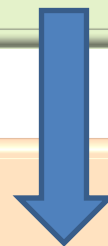
VISÃO TRADICIONAL

Empresas públicas
e
Monopólio de mercado



VISÃO LIBERAL

Empresas privadas
e
Concorrência de mercado



Tudo se altera:

- A cibersegurança passa a ter valor de mercado.
- Os clientes mudarão de fornecedor se entenderem que os seus dados não estão suficientemente protegidos.
- Propensão para ocultar ataques.

c. As instituições

Constituem a presença do Estado no Ciberespaço
Órgãos de Soberania, Ministérios, Institutos, Justiça, etc

Informar o cidadão sobre a actividade do Estado;
Disponibilizar serviços online

- Alvos especialmente apetecíveis
- Possuem muita informação sobre os cidadãos
- Quando falham é o Estado que falha

Possuem elevado valor simbólico !!!

d. Os serviços de informações

Internet é Open Source com baixo custo
Pesquisa com relativa discrição



<http://venturebeat.com/2015/10/06/ia-map-shows-human-intelligence-tech-is-surgin/>

- Qual o grau de confiança da fonte?
- Qual o grau de verosimilhança da informação?

O que é verdadeiramente perigoso está criptado
ou escondido na DarkWeb

e. As Forças Armadas

Concebidas para actuar quando tudo o resto falha

A GUERRA CONVENCIONAL



A GUERRA SUBVERSIVA E ANTI-SUBVERSIVA



A GUERRA HÍBRIDA



A CIBERGUERRA



e. As Forças Armadas (2)



US military steps up cyberwarfare effort

March 12, 2019 10:44am GMT

The U.S. military is shifting the focus of its cyberwarfare forces. U.S. Air Force

Email

Twitter

Facebook

LinkedIn

Print

47

183

The U.S. military has the capability, the willingness and, perhaps for the first time, the official permission to preemptively engage in active cyberwarfare against foreign targets. The first known action happened as the 2018 midterm elections approached: [U.S. Cyber Command](#), the part of the military that oversees cyber operations, [waged a covert campaign](#) to deter [Russian interference](#) in the democratic process.

Authors



Benjamin Jensen

Associate Professor of International Relations, Marine Corps University; Scholar-in-Residence, American University School of International Service



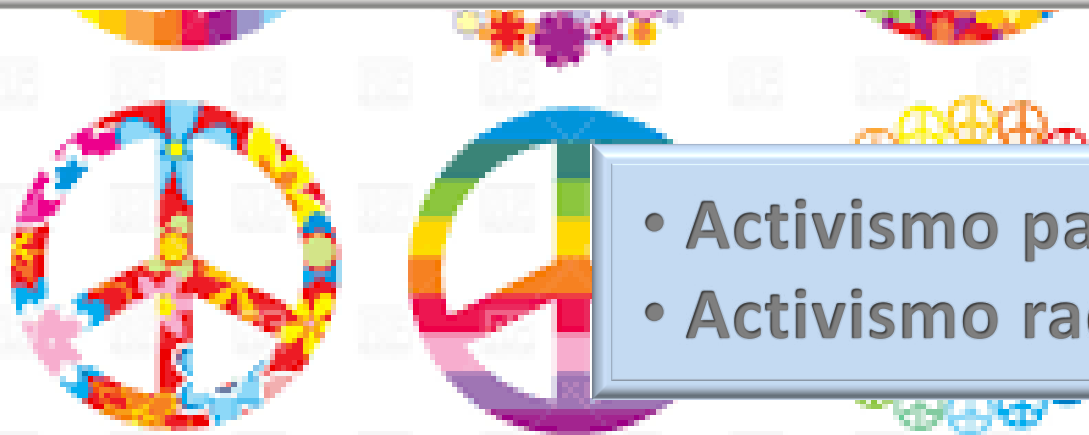
Benjamin Jensen

US Cyber Command foi criado em Fort Meade no Maryland em 2009. Em 4 de Maio de 2018 passou a ser um dos 11 Combatant Commands

f. Os activismos



Promover causas, contestar, mobilizar opiniões



- Activismo pacífico
- Activismo radical

g. Os hackers

Buscam :

- Adrenalina pelo desafio
- Notoriedade

George Hotz

Aos 17 anos
desbloqueou o primeiro
iPhone

Aos 20 anos
desbloqueou a consola
Playstation 3 da SONY

SONY colocou George
Hotz em Tribunal

Aos 24 anos entrou na root
do Samsung Galaxy S5

2014

Contratado pela Google

2011

Contratado pelo Facebook



h. O crime organizado

Principal Motivação: Dinheiro



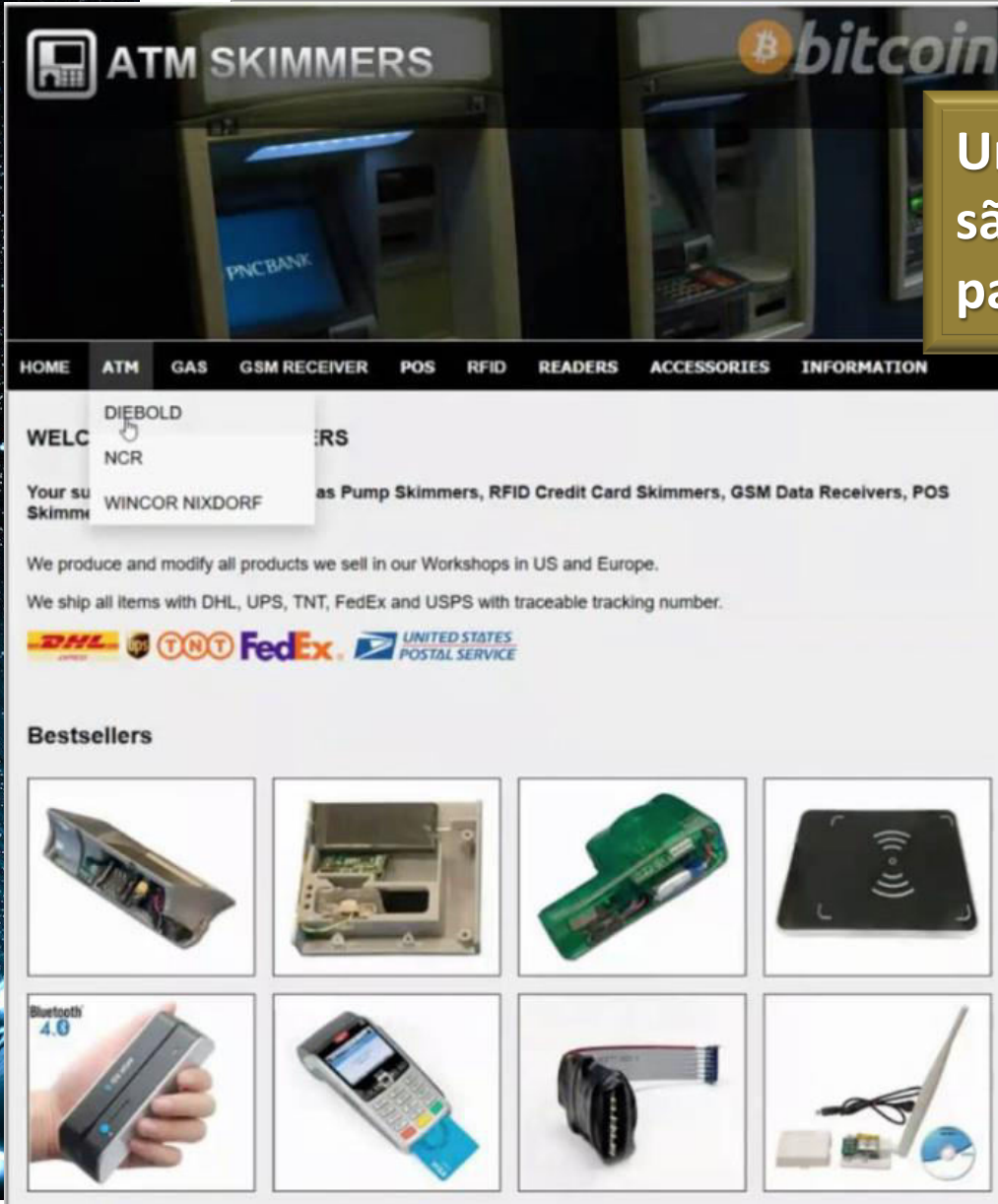
Só 4% da Internet está visível ao público através dos nossos browsers

Actuam em todas as áreas da Internet

96% of content on the Web (estimated)

Especialistas no acesso à Dark Web

h. O crime organizado na Dark Web



The screenshot shows a website with a dark theme. At the top, there's a banner with 'ATM SKIMMERS' and a Bitcoin logo. Below the banner is a navigation menu with links: HOME, ATM, GAS, GSM RECEIVER, POS, RFID, READERS, ACCESSORIES, INFORMATION. A dropdown menu is open under 'ATM', showing options like DIEBOLD, NCR, and WINCOR NIXDORF. The main content area features a welcome message, shipping information (DHL, UPS, TNT, FedEx, USPS), and a 'Bestsellers' section displaying various electronic devices like skimmers, receivers, and a Bluetooth 4.0 device.

Um dos grandes sucessos são os leitores de código para os nossos cartões ...

... mas também o New York Times para países que fazem censura ou bloqueio

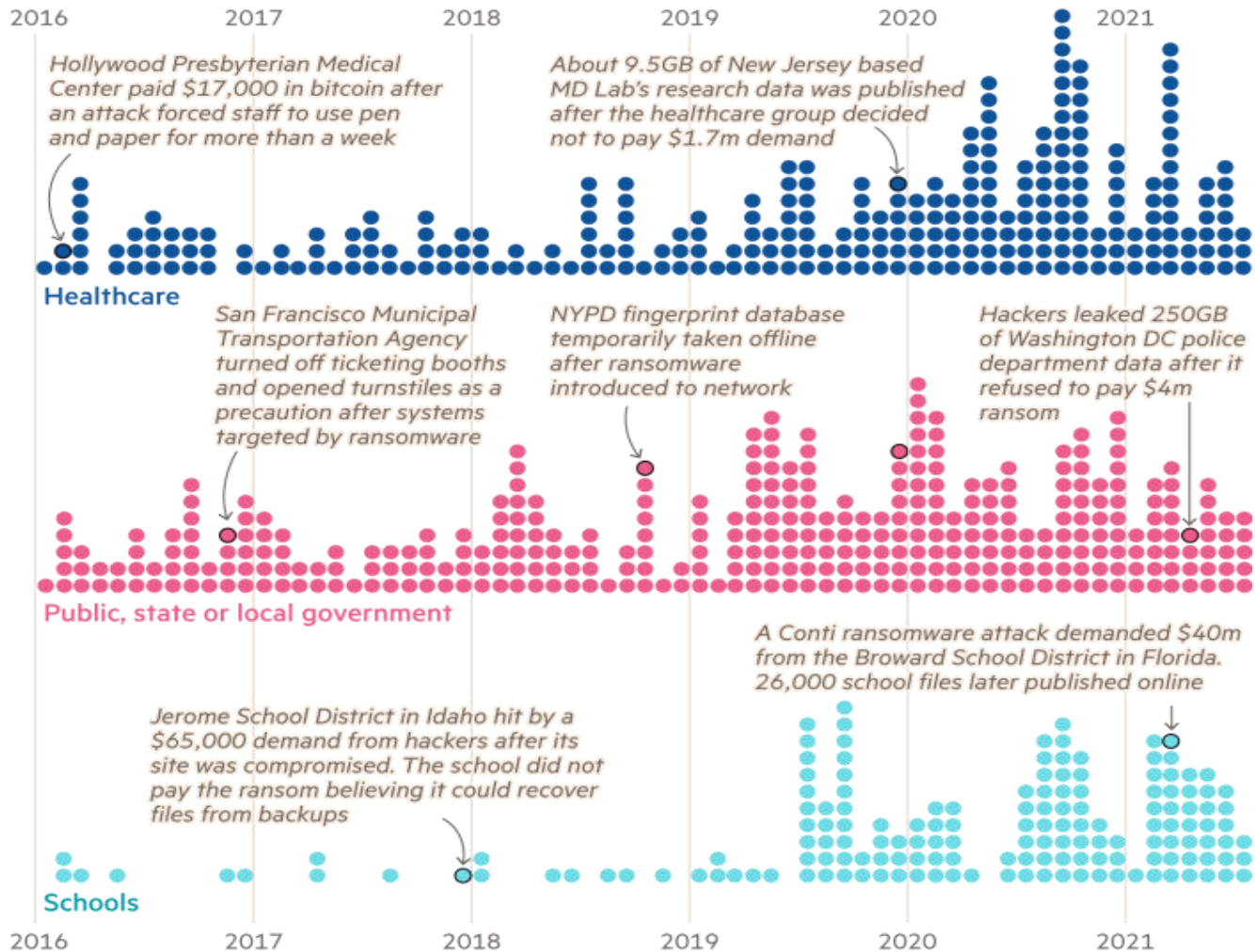


The screenshot shows the front page of the New York Times website. The date is Wednesday, October 3, 2018. The main headline is 'Your Wednesday Briefing: Here's what you need to know to start your day.' Other headlines include 'Listen to "The Daily"' and 'In the "Watching" Newsletter'. A large image of a man's face is visible in the lower part of the page.

h. A moda do Ramsonware

Rising ransomware reports

Publicly reported ransomware attacks on US **healthcare**, **public, state or local government** and **schools**, by month



Based on open sources. Ransomware attacks are not always publicly reported and data should not be viewed as exhaustive
Source: Recorded Future
© FT

i. As forças geoestratégicas (1)



Porque é que os actores geoestratégicos se iriam manter fora do Ciberespaço?

Em Julho 2016, WikiLeaks divulgou 20 000 emails obtidos da rede do DNC

**1Jan2017:
35 Russian diplomats
expelled by Obama over
hacking leave US**



<http://www.bbc.com/news/world-us-canada-38484735>

Primeira vez que questões do Ciberespaço merecem uma resposta diplomática desta gravidade

i. As forças geoestratégicas (2)

IDF: Hamas hacked soldiers' phones by posing as pretty girls

In 'catfishing' attack, dozens of servicemen duped by fake accounts as terrorist group tries to extract intel from social media, smartphones

BY JUDAH ARI GROSS | January 11, 2017, 5:55 pm |

Tweet

G+

2

Email

THE TIMES OF ISRAEL
11Jan2017



A Forças de Defesa de Israel revelaram que o HAMAS criou falsos perfis nas Redes Sociais, para interagir com soldados israelitas e obter informação sensível.

Agenda

1. Tudo Conectado, todos em Risco
2. Da Arpanet à Internet das Coisas
3. Os actores do Ciberespaço
4. **Desafios futuros**

5 G: Mais dispositivos conectados



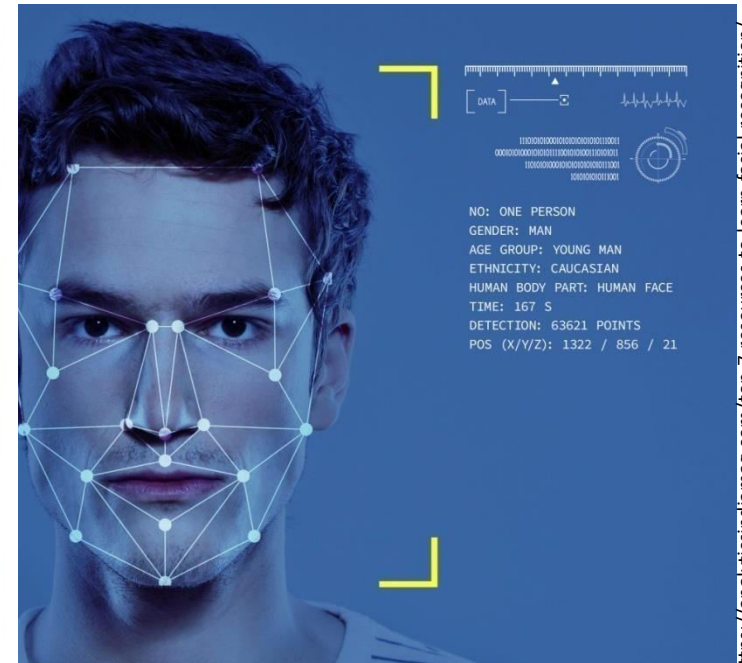
- 4G accommodate a few thousand IoT devices per square mile,
- 5G will provide connectivity for millions of devices per square mile.
- 4G networks have latency rates between 50-100 milliseconds,
- 5G would reduce that to just 1-4 milliseconds, a crucial difference when it comes to systems that need instantaneous reaction, such as autonomous vehicles and remote surgery.

Quem controla o fabricante?

Banned Chinese Security Cameras Are Almost Impossible to Remove



Source: Bloomberg



Several years ago the Department of Homeland Security tried to force all federal agencies to secure their networks by tracking every connected device. As of December 2018, only 35 percent of required agencies had fully complied with this mandate ... As a result, **most U.S. federal agencies still don't know how many or what type of devices are connected to their networks (18Jul2019)**

Segurança e Tecnologia vs. Liberdade



<https://techcrunch.com/2019/05/03/china-smart-city-exposed/>

« Todo aquele que estiver disposto a abdicar da sua Liberdade em nome de Segurança, não merece nem terá nenhuma das duas »

Benjamin Franklin

Esta Conferência já está na Web

1º Passo – Pesquisar no Google o Blogue “Quinta dos Arnaut”



Quinta dos Arnaut

Pesquisa Google

Sinto-me com sorte

2º Passo – Entrar em “Geopolítica”

Quinta dos Arnaut

Uma quinta sobre a montanha

[Blog](#)

[Arboreto](#)

[Fauna](#)

[Contacto](#)

[Documentos](#)

[Geopolítica](#)

3º Passo – Procurar nas
“Conferências”

Conferências

2019_04_10 Universidade Nova: Uma Geopolítica Africana

[Geopolítica de África v5](#)

2019_04_03 Universidade Autónoma: O Crime Organizado Transnacional

Evolução e Desafios Futuros do Ciberespaço

Arnaut Moreira

jfa1959@hotmail.com

