Cibersegurança na Transformação Digital: ameaças, desafios e soluções

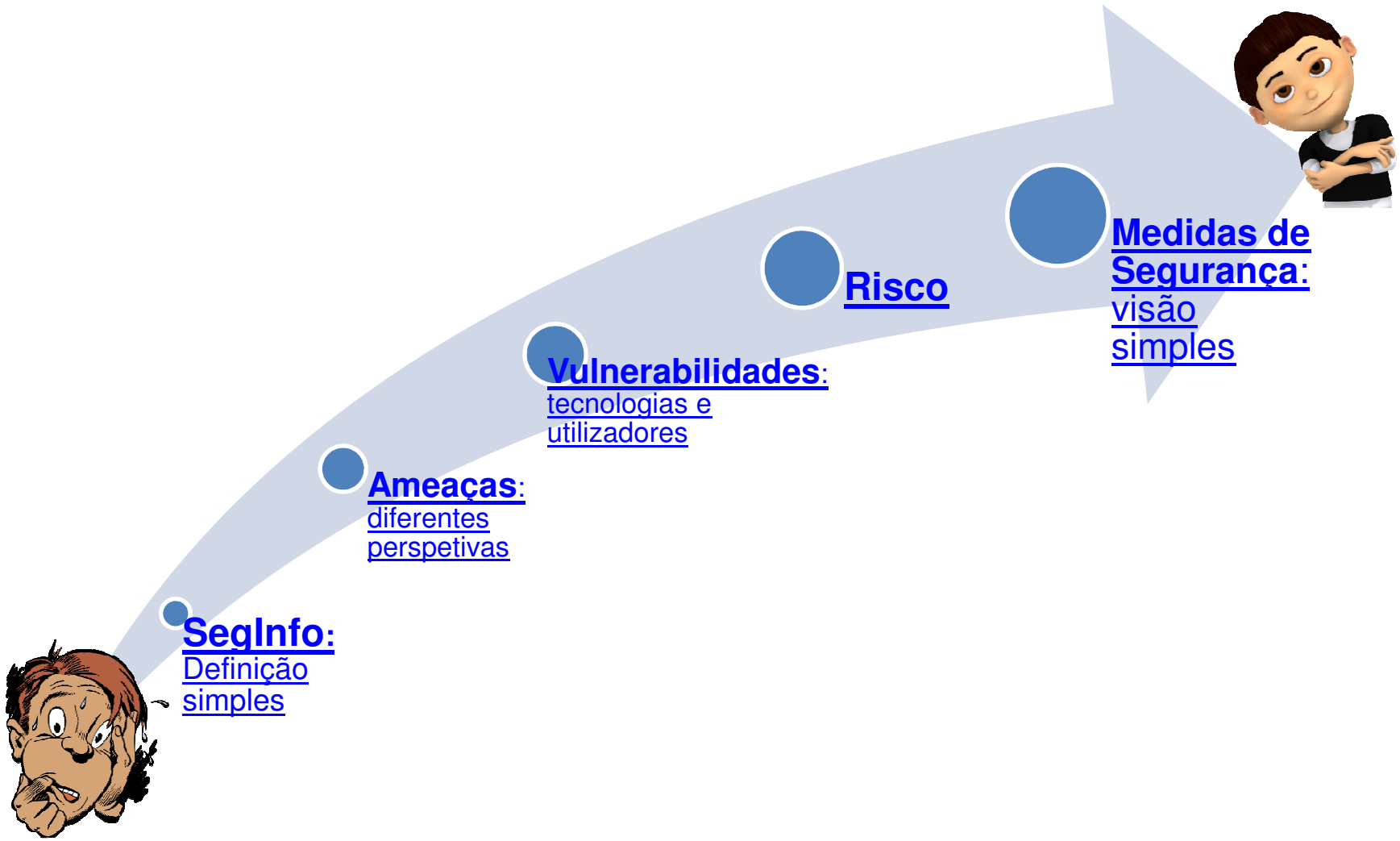
In Webinar "Digitalização de Processos e Cibersegurança", IAPMEI/UM

Henrique Dinis Santos (hsantos@dsi.uminho.pt)
Centro Algoritmi
Universidade do Minho
Algures, no Ciberespaço
2 de junho de 2020

"É uma infelicidade da época que os doidos guiem os cegos"

William Shakespeare

Sumário


SegInfo: Definição simples
Ameaças: diferentes perspetivas
Vulnerabilidades: tecnologias e utilizadores
Risco
Medidas de Segurança: visão simples

Segurança da Informação

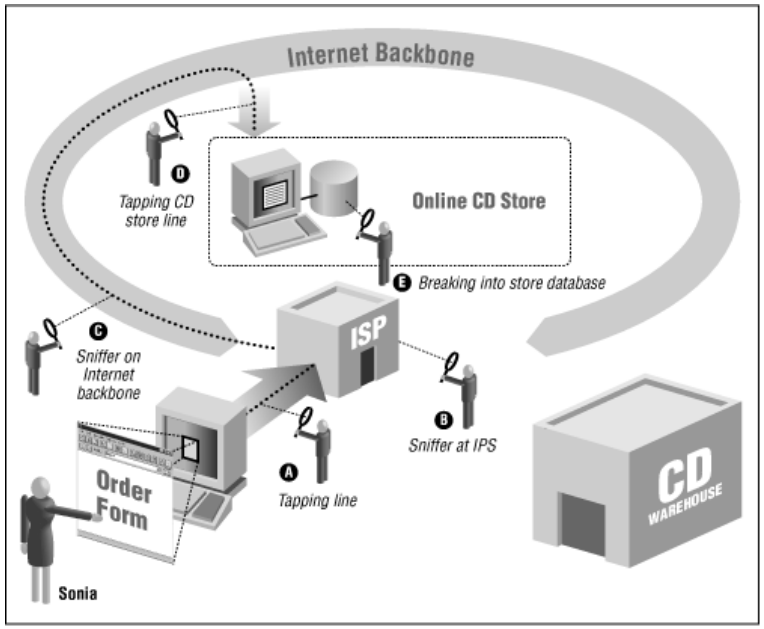
- Proteger a **informação** e os **Sistemas de Informação** do que **não é autorizado** quanto a:
  - Acesso
  - Utilização
  - Divulgação
  - Modificação
  - Destruição
  - Interrupção
  - …

Fonte: http://en.wikipedia.org/wiki/Information_security, 2010

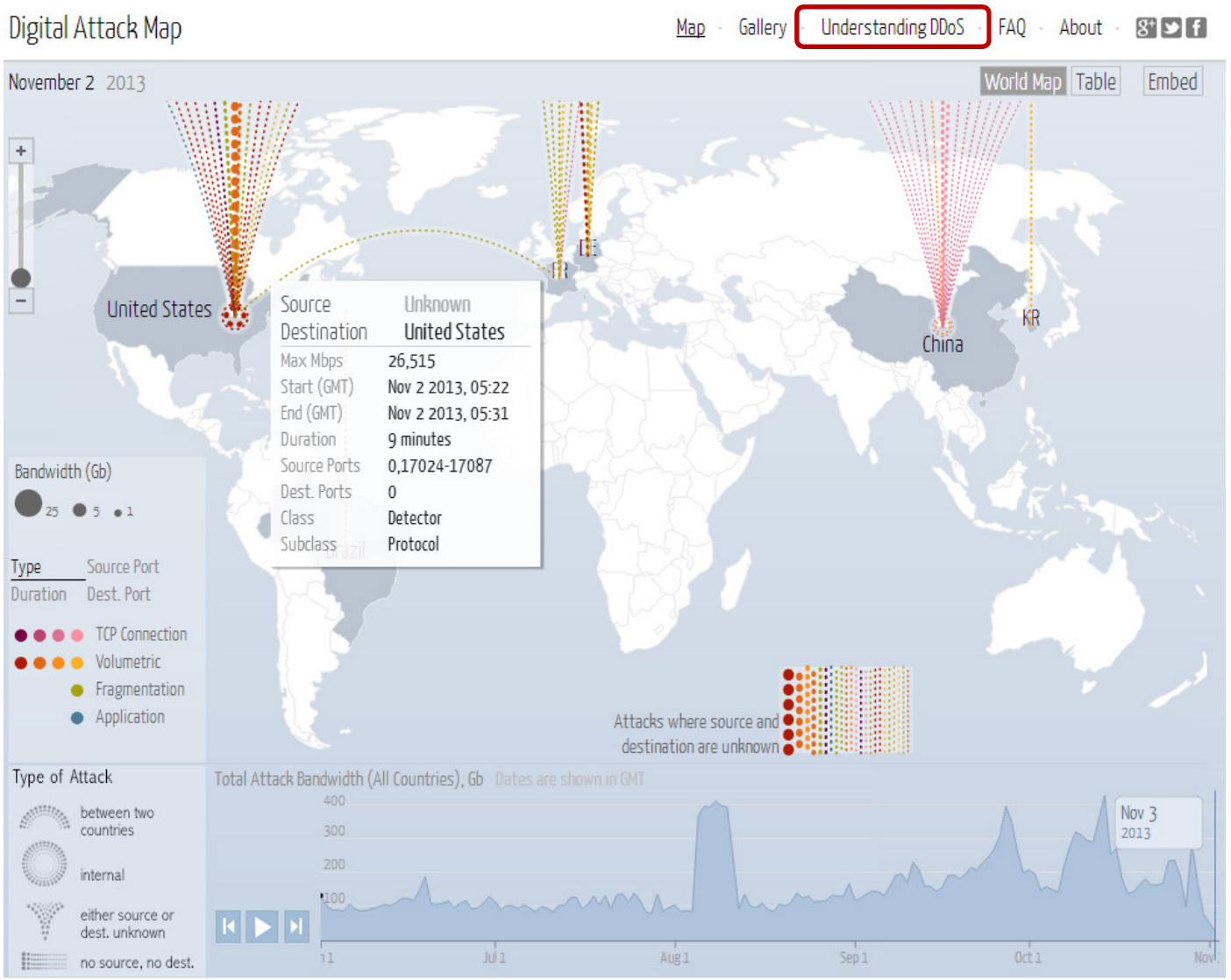
Quais são as ameaças?

- Terrorismo e Crime organizado
- Erros e falhas humanas
- Erros e falhas técnicas
- Atentados contra a Propriedade Intelectual
- **Várias formas de ludibriação**
- Roubo
- **Fraude**
- Degradação da QoS
- **Coação física e psicológica**
- Acidentes naturais
- Violação da privacidade
- …

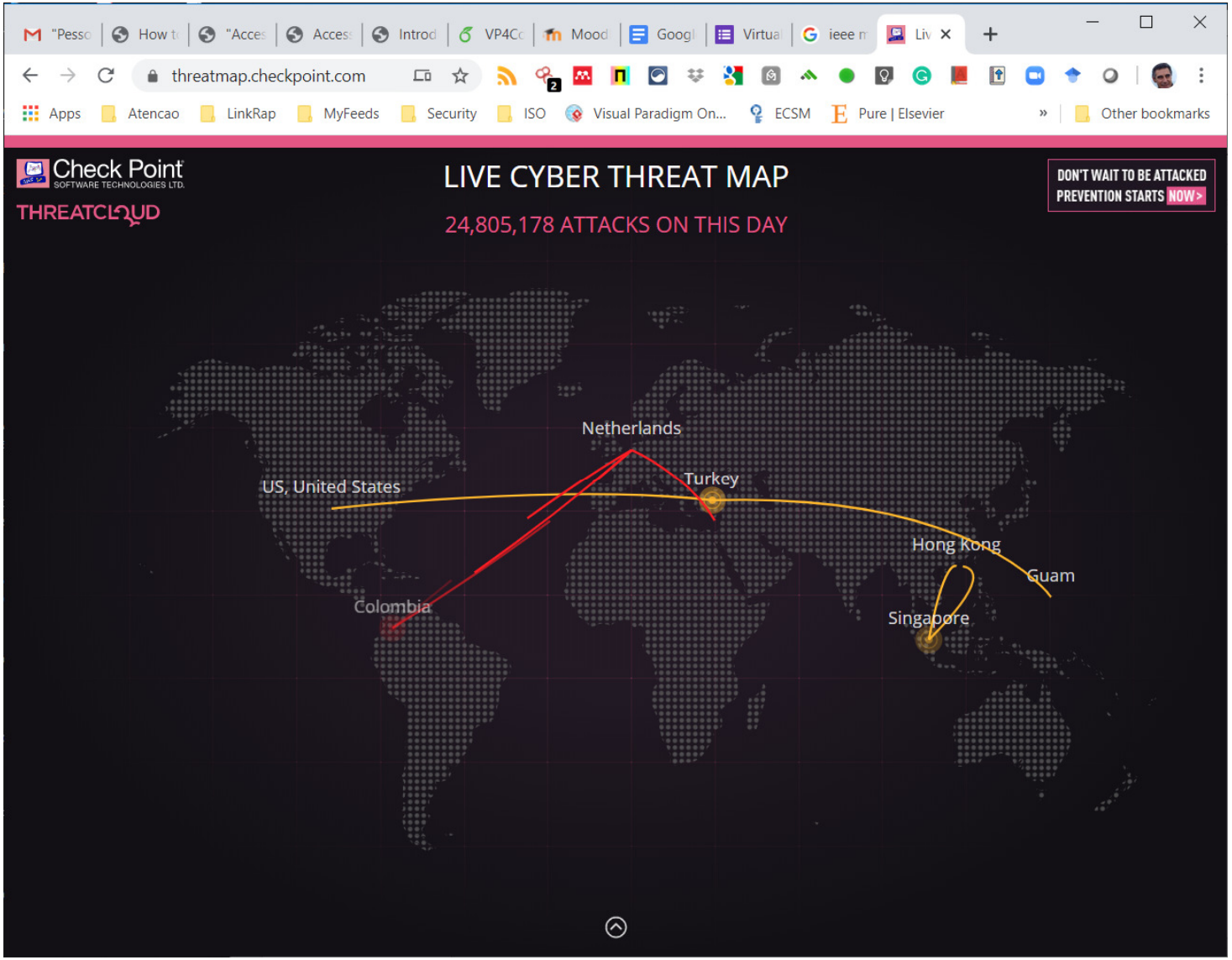
Alteram-se com frequência



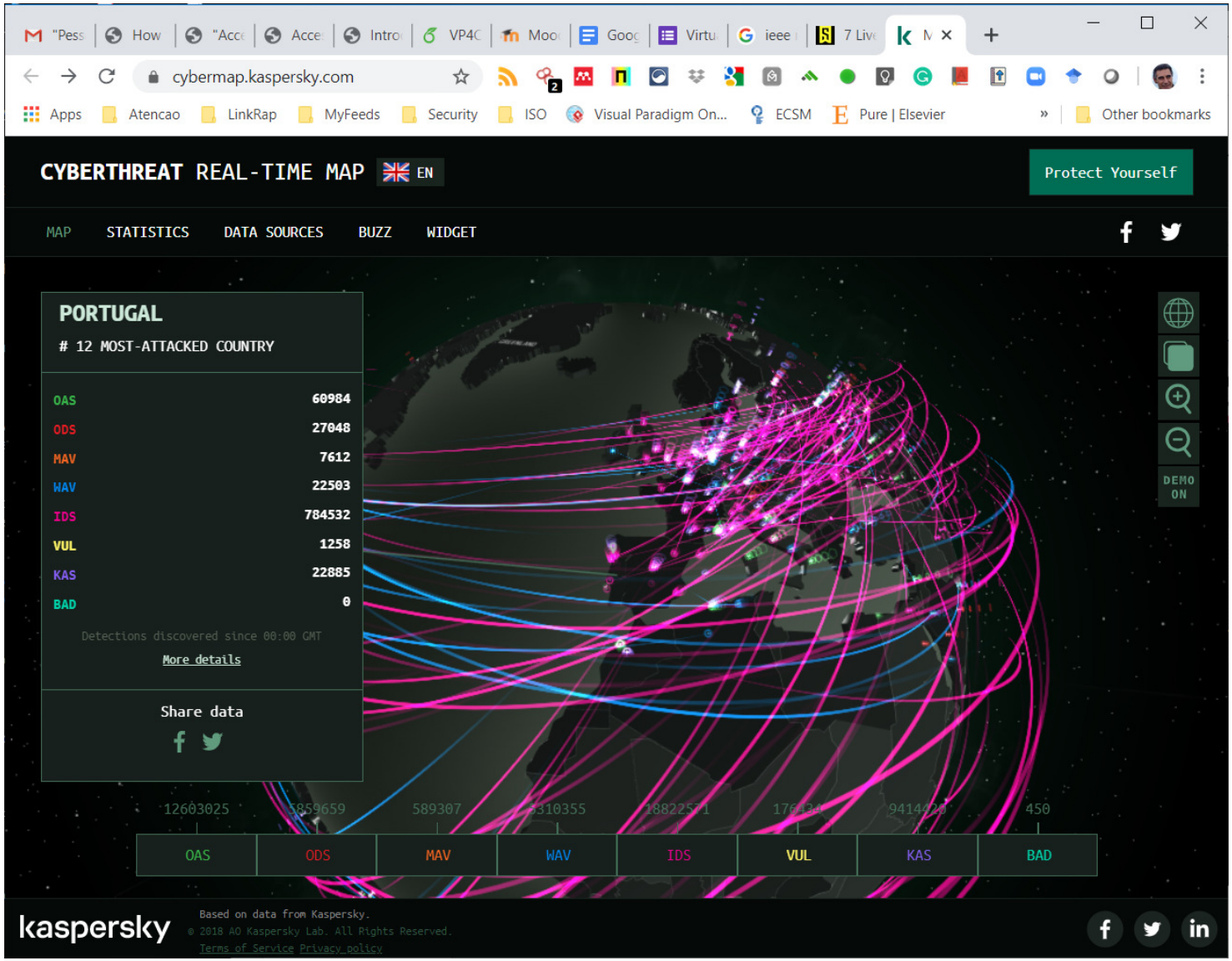
Digital Attack Map



Live Cyber Threat Map

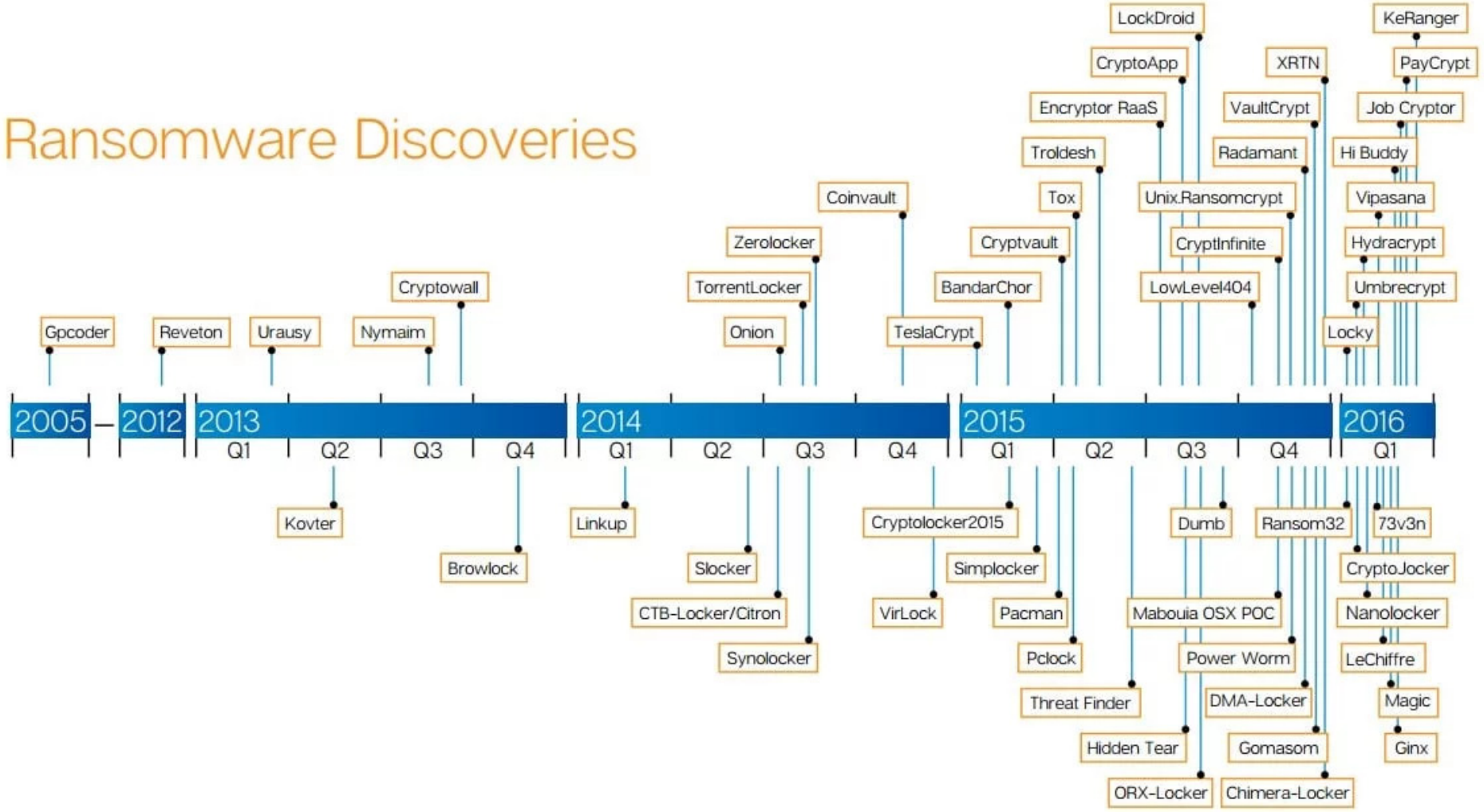


CyberThreat Real-Time Map



Threatbutt Internet Hacking Attack Attribution Map

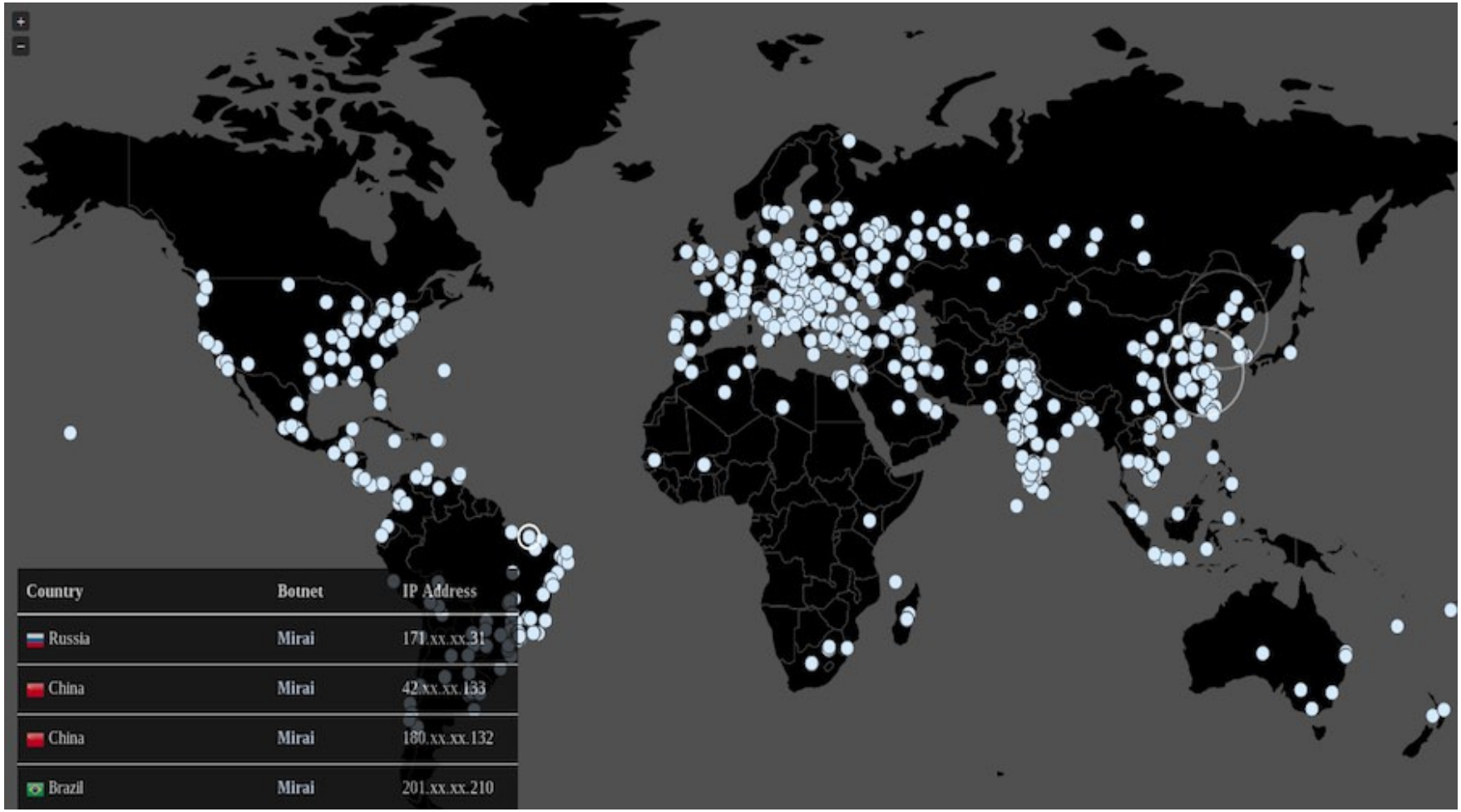
Evolução do *Ransomware*



https://www.complete-it.co.uk/data-recovery/a-brief-history-of-ransomware/

Botnets

Alcance da famosa Botnet Mirai (projeto Atena – H2020)



https://www.atena-h2020.eu/one-biggest-cyber-attacks-iot-ever-witnessed/mirai-botnet-attack/

Ransomware

The ransomware that attacks you from inside a virtual machine

…SophosLabs published details of a sophisticated new ransomware attack that takes the popular tactic of “living off the land” to a new level.
To ensure their **49 kB Ragnar Locker ransomware ran undisturbed**, the crooks behind the attack bought along a 280 MB Windows XP virtual machine to run it in (and a copy of Oracle VirtualBox to run that).
It’s almost funny, but it’s no joke….

Dark Web

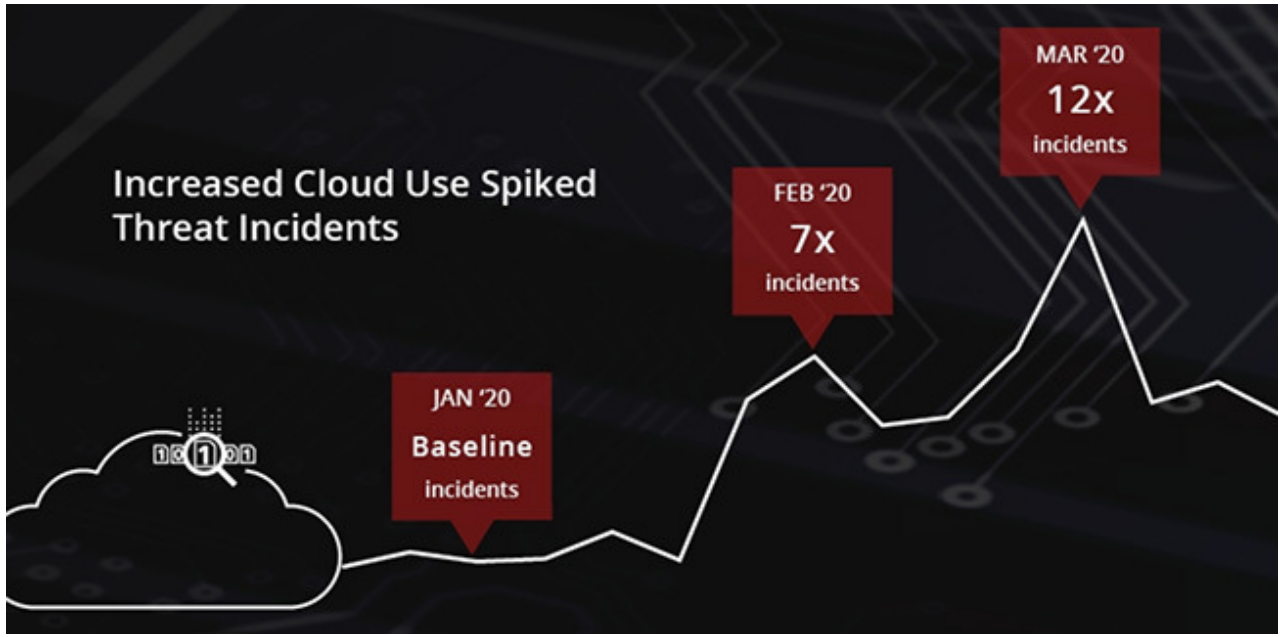
The dark web is flooded with offers to purchase corporate network access

There is a flood of interest in accessing corporate networks on the dark web, according to Positive Technologies.

In Q1 2020, the number of postings advertising access to these networks increased by 69 percent compared to the previous quarter. This may pose a significant risk to corporate infrastructure, especially now that many employees are working remotely.

Ataques baseados na *Cloud*

External attacks on cloud accounts grew 630 percent from January to April
The McAfee report uncovers a correlation between the increased use of cloud services and collaboration tools, such as Cisco WebEx, Zoom, Microsoft Teams and Slack during the COVID-19 pandemic, along with an increase in cyber attacks targeting the cloud.



There are significant and potentially long-lasting trends that include an increase in the use of cloud services, access from unmanaged devices and the rise of cloud-native threats. These trends emphasize the need for new security delivery models in the distributed work-from-home environment of today–and likely the future.

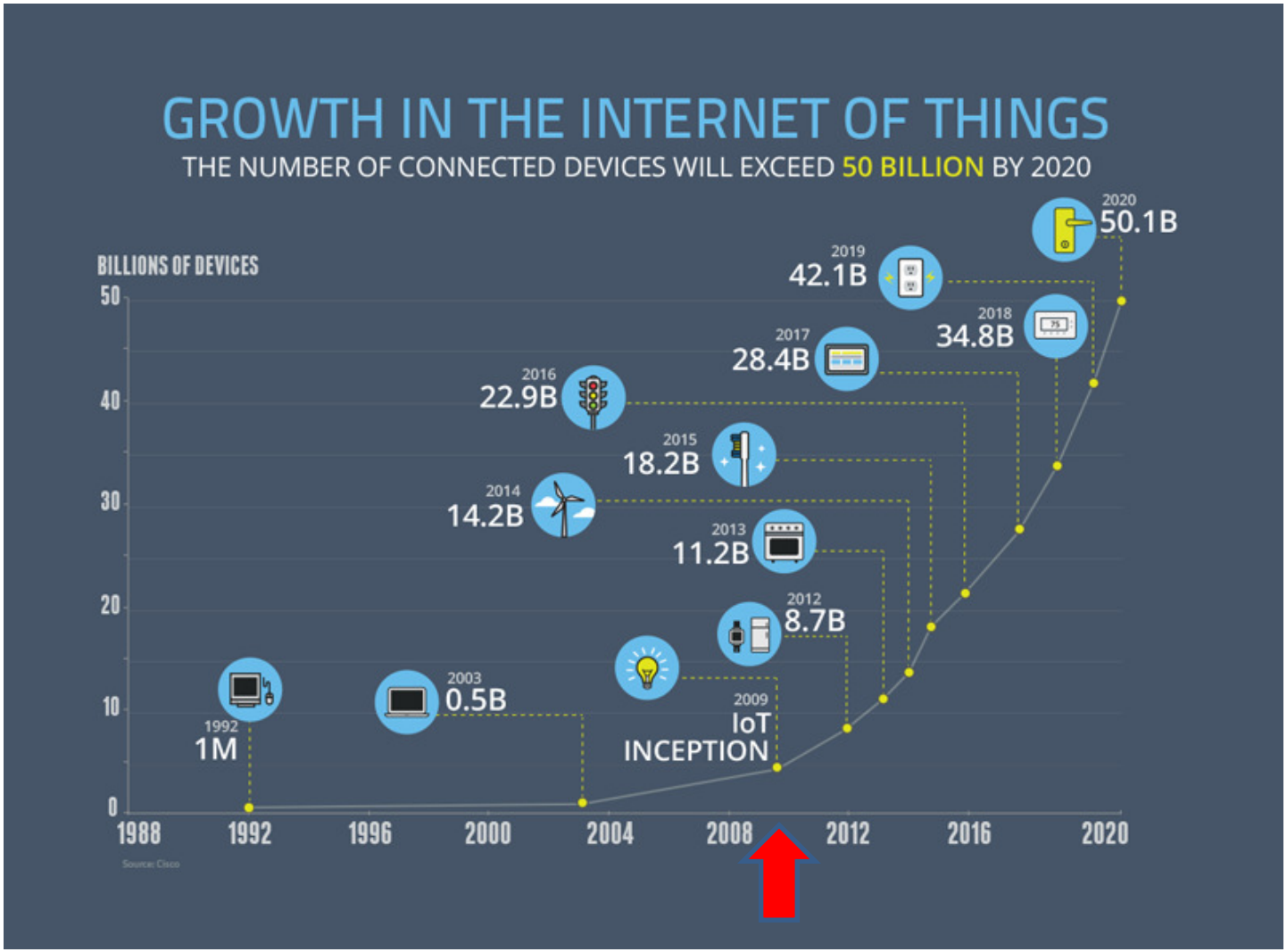
Origem das vulnerabilidades

- Sistemas informáticos, terminais de comunicação e componentes de redes
  - **Complexidade**, **flexibilidade**, grau de autonomia, miniaturização, desmaterialização, ubiquidade, **interconetividade** (…)
  - Requisitos não funcionais incompletos (**o que o sistema não deve fazer?**)

Complexidade?!

≅ 2,1 Mil Milhões de transístores em 1,2cm^2
≅ 50 Milhões de operações por segundo

Internet of Things



Internet of Things

Número máximo (teórico) de endereços **IPv6** (2^{128}):

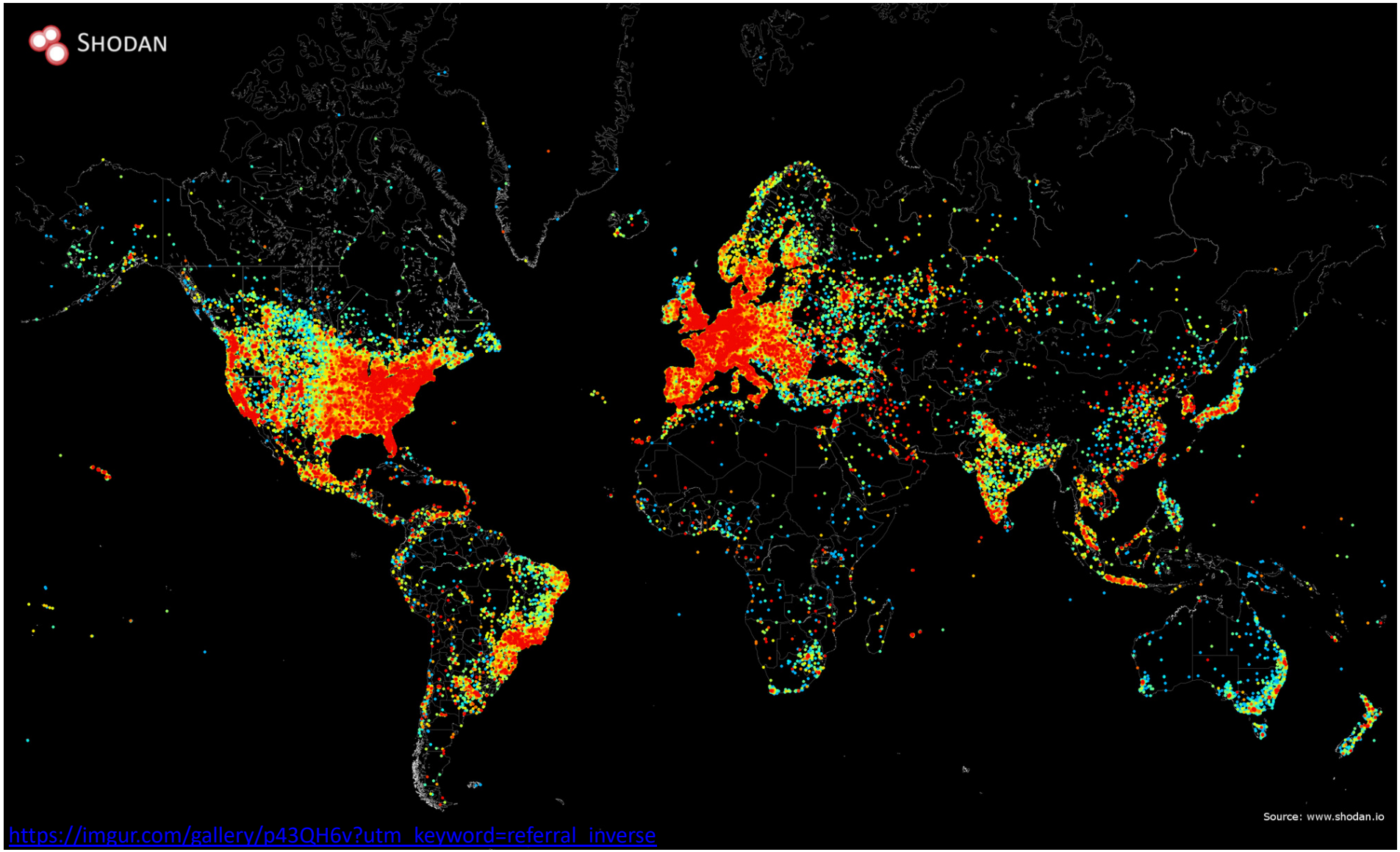
340,282,366,920,938,463,463,374,607,431,768,211,456

(cerca de 4,3 biliões como **IPv4** – cerca de 10 biliões, usando NAT)

Área da superfície da Terra (estimada, em cm^2):

5,100,644,719,000,000,000

Complexidade?!

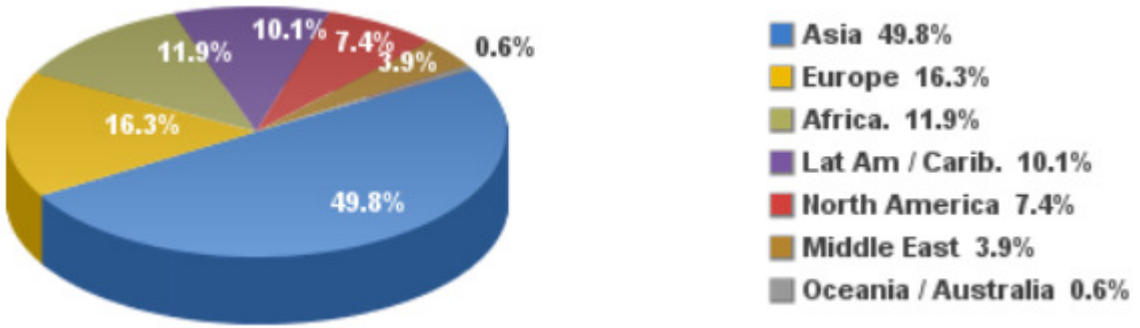


https://imgur.com/gallery/p43QH6v?utm_keyword=referral_inverse

Complexidade das redes

- Estatísticas da Internet

WORLD INTERNET USAGE AND POPULATION STATISTICS 2019 Mid-Year Estimates						
World Regions	Population (2019 Est.)	Population % of World	Internet Users 30 June 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet World %
Africa	1,320,038,716	17.1 %	522,809,480	39.6 %	11,481 %	11.5 %
Asia	4,241,972,790	55.0 %	2,300,469,859	54.2 %	1,913 %	50.7 %
Europe	829,173,007	10.7 %	727,559,682	87.7 %	592 %	16.0 %
Latin America / Caribbean	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	258,356,867	3.3 %	175,502,589	67.9 %	5,243 %	3.9 %
North America	366,496,802	4.7 %	327,568,628	89.4 %	203 %	7.2 %
Oceania / Australia	41,839,201	0.5 %	28,636,278	68.4 %	276 %	0.6 %
WORLD TOTAL	7,716,223,209	100.0 %	4,536,248,808	58.8 %	1,157 %	100.0 %



http://www.internetworldstats.com/stats.htm

Comportamentos inadequados: comparação simples

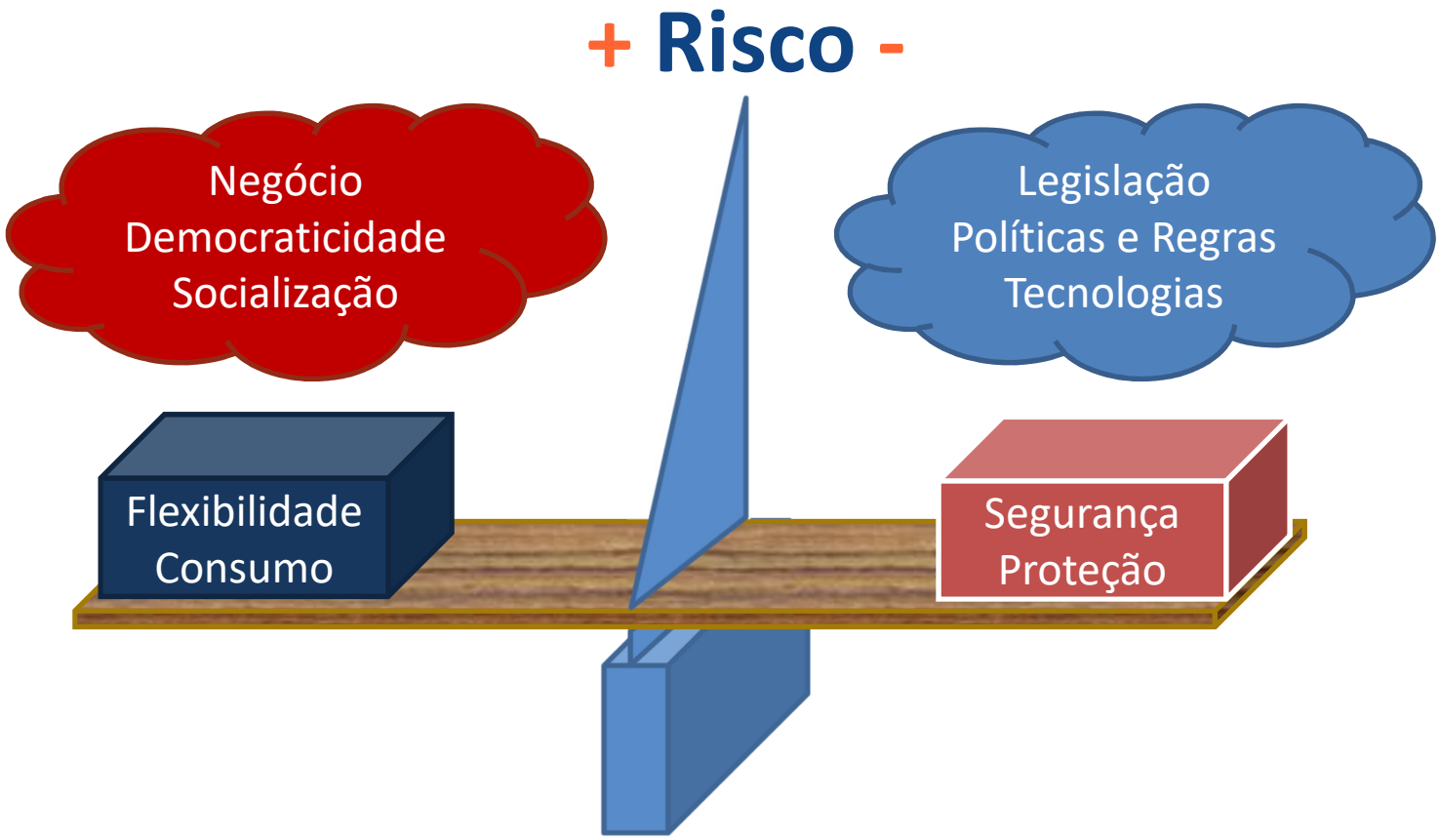
Automóvel/Rede viária

- Complexo
- Acidentes com elevado impacto (imediato)
- Regras bem estabelecidas e aprendizagem regulada
- Condições mínimas para circular
- Tráfego (±) controlado
- Bom condutor
  - Automóvel sempre "afinado"
  - …

Computador/Internet

- Muito mais complexo
- Incidentes passam despercebidos e impacto (imediato) é reduzido
- Recomendações, boas práticas, autoaprendizagem
- Acesso livre
- Sem controlo (muito difícil)
- Bom "Cibernauta"
  - Computador atualizado
  - Comportamento seguro (eu e os **OUTROS**

Introdução à noção de **Risco**



Gestão do Risco

- Risco
  - Quantitativo

    Probabilidade x Valor

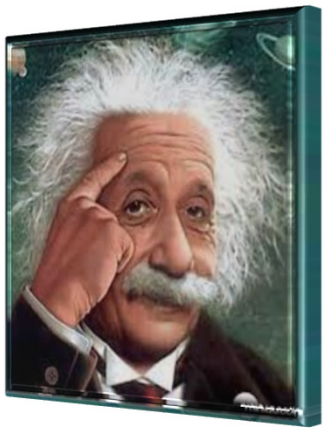
  - Qualitativo

    Alto, Médio, Baixo, …
- Não é o mesmo para todos

Qual o limite aceitável?
"Confiança"

O que condiciona a perceção do risco?

- Características pessoais e estilo de vida (**(des)confiança**)
- Imposições do contexto (social ou laboral – **Políticas** e **Normas**)
- **O conhecimento objetivo do sistema**
  - Valor da informação
  - Vulnerabilidades
  - Ameaças
  - …



Estilo de vida

- O “**Nativo Digital**”
  - Todo aquele que nasceu e cresceu no seio das Tecnologias de Informação e Comunicações (TIC)
  - No contexto da educação é particularmente crítico (Bennett, Maton & Kervin, 2008); a OCDE define-os como “Aprendizes do Novo Milénio”)

- O “**Imigrante Digital**”
  - Todo aquele que nasceu e cresceu numa época anterior, mas que “vive” no seio das TIC

Medidas para a Cibersegurança

- Norma ISO/IEC 27001 (e/ou NIST SP800-39)
- Primeira linha de defesa (preparar)
  - Planeamento e gestão da Infraestrutura, incluindo:
    - Segmentação da rede e DMZ
    - Redes privadas
    - Análise e avaliação de Risco (pode incluir riscos de quebra de privacidade)
    - **Políticas**: **Controlo de Acesso**; utilização de passwords; utilização do e-mail; utilização de equipamento informático; utilização da Internet; backups; administração de sistemas (incluindo auditorias regulares);… (pode incluir política de privacidade)
      Política de Segurança da Informação – quanto mais formalizado, melhor - COMUNICAÇÂO

Medidas para a Cibersegurança

- Segunda linha de defesa (previnir)
  - Filtragem de tráfego (*firewalls)* – procurar reduzir ao mínimo possível o tráfego que entra e sai do perímetro da rede
- Terceira linha de defesa (detetar e responder)
  - Monitorizar o máximo possível, todo o tráfego e a atividade dos Sistemas Informáticos (IDS, HIDS, SIEM)
  - Política e guia de resposta a incidentes (pode incluir acidentes de quebra de privacidade)
  - Integração com equipas de resposta a acidentes (CERT)

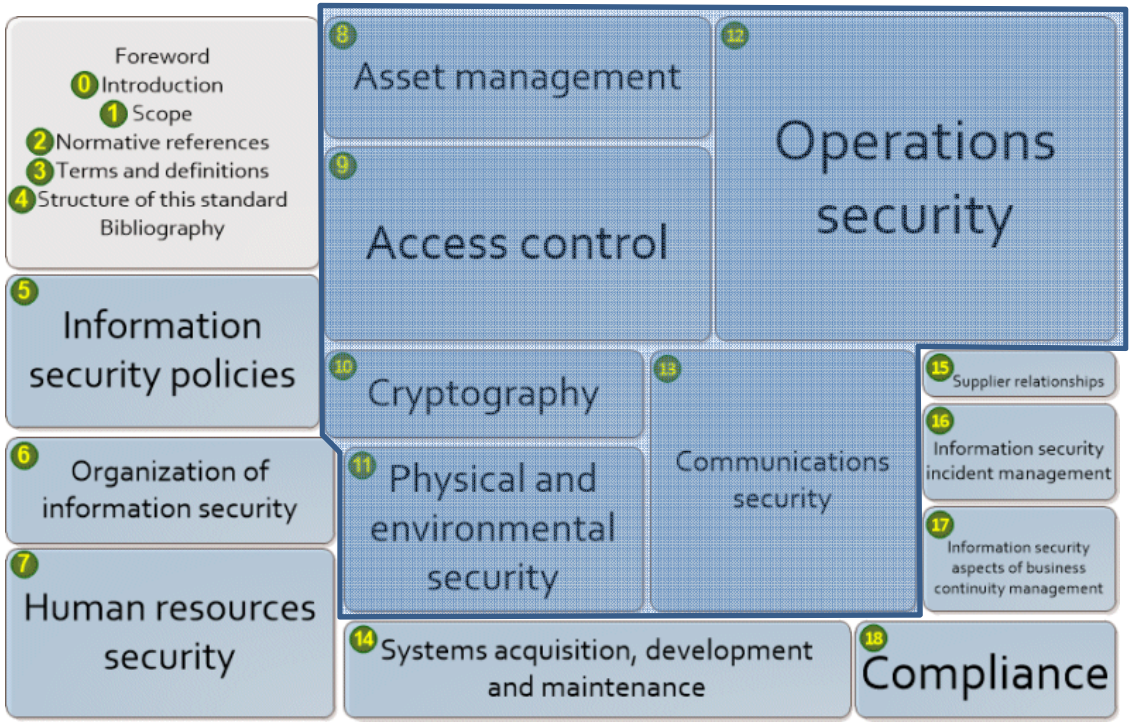
Medidas para a Cibersegurança

- Quarta linha de defesa (previnir)
  - Cifrar informação crítica (em particular, informação privada)
- Linha de defesa sem ordem! (prevenir)
  - Treinar e educar
  - Treinar e educar
  - Treinar e educar
  - Treinar e educar
  - Treinar e educar
  - Treinar e educar
  - …

Medidas para a Cibersegurança

ISO/IEC **27002:2013** (*Code of Practice for InfoSec Management*)

- 14 classes (Cláusulas) – secção 5 a secção 18
- 35 objetivos de controlo
- 114 Controlos de segurança
- Cerca de metade de natureza tecnológica
- Os restantes de natureza organizacional e de gestão



http://www.iso27001security.com/html/27002.html

Recomendações gerais (pessoal)

- Manter o computador sempre atualizado (no mínimo verificar 1/semana)
- Não instalar *plug-ins* ou *addons* nem permitir *pop-ups* e *cookies* no *browser* **sem ter consciência do efeito**
- **Não aceitar anexos** que não sejam aguardados
- **Não facultar a *password*** a ninguém e não usar "123456", ou "password"!!!
- **Manter cópias de segurança de informação mais crítica**
- Exigir que o computador não esteja "no modo administrador"
- **Perguntar, em caso de dúvida e partilhar a informação…**

CENTROALGORITMI

Universidade do Minho

Obrigado pela vossa atenção. Questões?