Cibersegurança e proteção do espaço digital

Luis Borges Gouveia, Professor Catedrático (UFP)

homepage.ufp.pt/lmbg | lmbg@ufp.edu.pt

Faculdades Integradas Santa Cruz de Curitiba,

25 de Junho de 2018 – Curitiba – Paraná, Brasil

- *Informática, Engenharia, Ciências da Computação, Gestão do Conhecimento*
- *Professor Catedrático*
  Faculdade de Ciência e Tecnologia
  Universidade Fernando Pessoa, Porto, Portugal

Luís Borges Gouveia, lmbg@ufp.edu.pt

As questões associadas com a proteção do espaço digital

Estrutura da apresentação:

- Sociedade da Informação
- Ecosistema digital e enquadramento operacional
- Do risco ao ciber ataque e, deste, à cibersegurança
- A geografia conta
- Conceitos associados com a ciberdefesa e a cibersegurança
- Considerações finais

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sociedade da Informação

*Uma sociedade que predominantemente utiliza o recurso às **tecnologias** da informação e comunicação para a troca de informação em formato **digital** e que suporta a **interação** entre indivíduos com recurso a práticas e métodos em **construção permanente***
(Gouveia e Gaio, 2004)

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sociedade da Informação

Uso intensivo de tecnologias de informação e comunicação

Uso crescente do digital

Organização em rede

Luís Borges Gouveia, lmbg@ufp.edu.pt

Sociedade da Informação

Uso intensivo de tecnologias de informação e comunicação

Uso crescente do digital

Organização em rede

infra-estruturas
& acesso

processos
& formação

de
comando & controlo
para
partilha & regulação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Uma ideia de mundo

Agora…

Sociedade da Informação

1. Uso intensivo de computadores e redes
   (do saber usar ao saber o que fazer com eles…)
2. A informação que conta é digital
   (a informação já não é o que era e vale pouco…)
3. A organização que conta é a rede
   (as hierarquias são uma simplificação num momento,
   logo efémeras e exigentes em tempo e recursos…)

O que significa?

Luís Borges Gouveia, lmbg@ufp.edu.pt

Dois aspetos essenciais

Sustentabilidade

- *Como garanto a minha liberdade ou como o valor gerado cobre o valor* absorvido*
  **(valor: económico, social, político e satisfação)*

Soberania

- *Como garanto a minha identidade** ou como posso ser reconhecido como eu próprio e ser o que quero/posso ser*
  ***(marca: pessoa, empresa, nação)*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Tempo e espaço

- **Tempo**
  24/7 sempre ligado, sempre presente
  MAS disponibilidade inteligente e bem gerida
  AFINAL o tempo humano é limitado
- **Espaço**
  em qualquer lugar, de qualquer forma
  MAS como estar presente?
  AFINAL a experiência é o memorável

Implicações do digital

- Mundo complexo
  - Computadores e redes (tudo ligado)
  - Mais gente com competências à escala global
- Exigidos novos cuidados ou o reforço dos existentes
  - …e alargado a mais pessoas e empresas
  - As instituições são alvo
  - As figuras públicas são alvo
  - No geral, quem pode contribuir (*) é alvo

Vivemos um ecossistema digital

http://stevenvanbelleghem.com/blog/the-essence-of-when-digital-becomes-human

Luís Borges Gouveia, lmbg@ufp.edu.pt

Enquadramento operacional

- Para a tomada de decisão ou ação, é exigida informação
  - *Todos os recursos que assegurem a melhor qualidade da informação, a sua mais fácil distribuição, recolha e apresentação, são determinantes para o desempenho de pessoas e organizações* (Gouveia e Ranito, 2004)
- As pessoas podem processar informação, enquanto os computadores são competentes a processar dados
  - Permite distinguir entre Sistema de Informação (SI) e Sistema de Processamento de dados (SPD) (Beynon-Davies, 2002)
  - Os indivíduos possuem um papel importante e indissociável no SI e o SPD é potenciado pelo uso do computador (Gouveia e Ranito, 2004)
- Temos assistido à emergência de sistemas automáticos de cognição com recurso à tecnologia de inteligência artificial
  - Implica a existência de capacidade autónoma de computadores e redes

Requisitos que informam a decisão e suportam a ação

- **Qualidade da informação**: informação precisa, simples, completa, concisa e oportuna, de modo a garantir o máximo proveito e rigor nas consequências da sua utilização;
- **Acesso à informação**: como garante quer da igualdade de acesso, quer da preservação e controlo na obtenção de um recurso cada vez mais crítico à atividade humana;
- **Entendimento da informação**: possuir a informação exige saber lidar com ela, compreender e potenciar a sua utilização. É igualmente importante, garantir as **competências** do indivíduo para selecionar, descartar e estabelecer prioridades na utilização deste recurso;
- **Partilha da informação**: prover as facilidades para partilha e obtenção de informação de forma coletiva. Para tal é necessário assegurar identificadores e conceitos comuns e estabelecer processos de gestão da informação que sejam compatíveis ou integráveis;
- **Lidar com o excesso de informação**: como forma de assegurar que questões associadas com a capacidade cognitiva dos indivíduos seja respeitada. Tal aspeto terá necessariamente consequências no que diz respeito à produtividade e à capacidade de trabalho útil de cada indivíduo;
- **Segurança da informação:** garantir a disponibilidade e acesso, mas essencialmente a preservação e salvaguarda da informação nas dimensões de confidencialidade e de integridade. Se não se conseguir assegurar a qualidade da informação e o seu uso operacional, o seu potencial fica perdido e a capacidade de decisão e ação é comprometida

O recurso a computadores e redes permite assegurar um local de trabalho que seja o mais conveniente possível e permita a integração com os diversos sistemas da organização, por mais complexos que sejam

- O local de trabalho constitui-se como um espaço, não necessariamente físico e muito menos síncrono em tempo, que envolve quatro propósitos (Gouveia, 2006):
  - Ligar a organização aos seus colaboradores, clientes, fornecedores e outros parceiros de negócio;
  - Proporcionar aos profissionais da organização acesso fácil a informações internas e externas à organização;
  - Proporcionar aos profissionais da organização uma janela única para as suas aplicações e os seus sistemas, essenciais à resolução de problemas dos processos de negócio;
  - Assegurar a distribuição oportuna de informação aos profissionais e demais colaboradores da organização.

Em Portugal (2015)…

- Existem comportamentos de risco que configuram uma deficiente **cultura de segurança**
- Uma percentagem significativa dos ataques informáticos, quebras de segurança e perda de informação, ocorrem tendo como **vetores os colaboradores internos** de uma organização

https://pplware.sapo.pt/informacao/36-dos-portugueses-ja-partilhou-a-password-do-e-mail/

As organizações e os ciberataques

- Segundo o relatório anual de cibersegurança 2017 da Cisco; as organizações que sofreram um ataque com consequências:
  - 22% das organizações atacadas perderam clientes (40% destas, perderam mais de 20% da sua base de clientes)
  - 29% perderam receitas (30% destas, refere mesmo perdas superiores a 20% das receitas)
  - 23% das empresas atacadas perderam oportunidades de negócio (42% destas, perderam mais de 120%)
- Representa um custo real para um terço e tem implicações na continuidade do negócio para um quarto

https://www.cisco.com/c/pt_pt/about/press/news-archive-2017/20170131.html

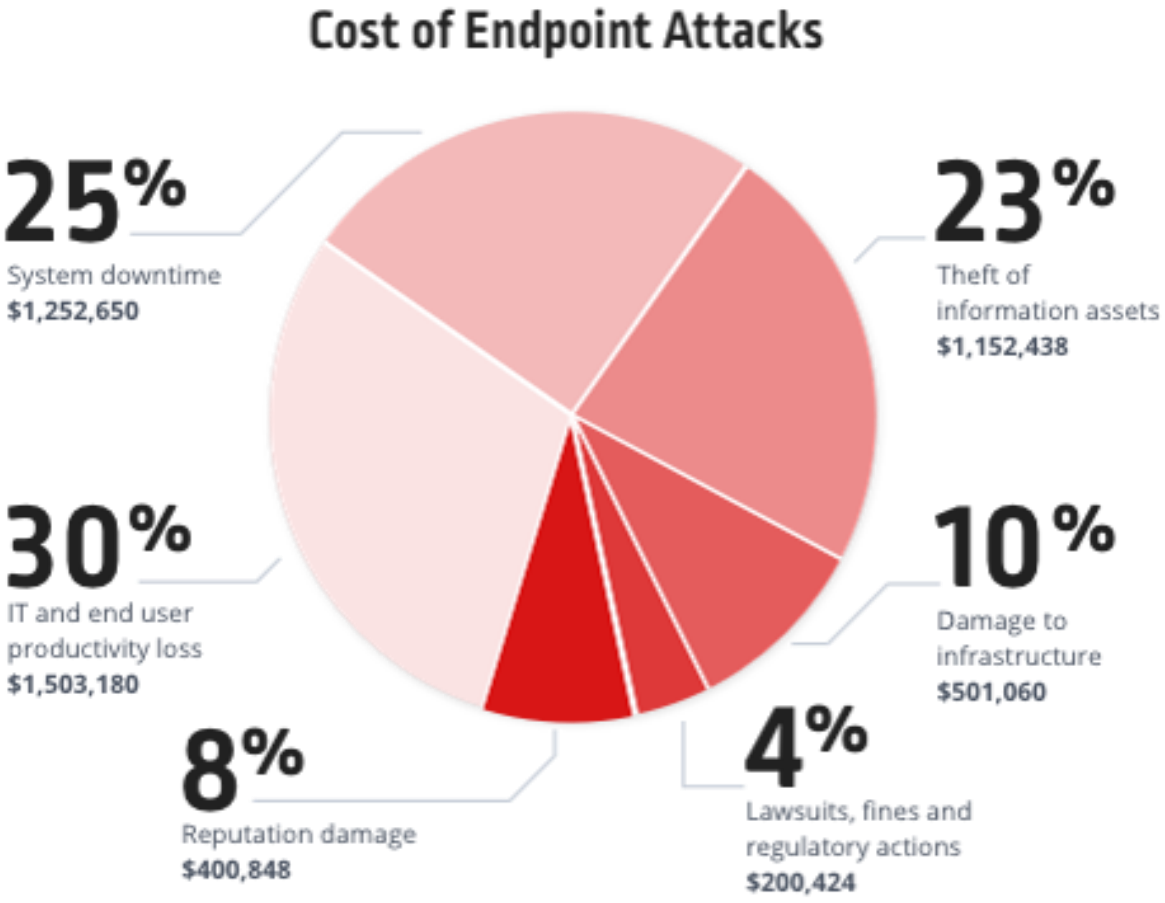
E qual a dimensão do fenómeno (ciber ataques)?

Existe consciência do fenómeno…

- Em 2017, os ciber ataques custam a uma PME, uma média de 2,2 Milhões de Dólares (2017)
- 92,4% do *malware* é enviado por correio eletrónico (2018)
- 60% dos pequenos negócios afirmam que os ataques causam cada vez maior impacto e tem maior sofisticação (2017)
- A proteção avançada de *malware* está a tornar-se uma prioridade de topo para os orçamentos (2017)

https://blog.barkly.com/small-business-cybersecurity-statistics-2018

E qual a dimensão do fenómeno (ciber ataques)?



54%

of companies experienced one or more successful attacks that compromised data and/or IT infrastructure

77%

of those attacks utilized exploits or fileless techniques

https://blog.barkly.com/2018-cybersecurity-statistics

Luís Borges Gouveia, lmbg@ufp.edu.pt

Existe uma consciência generalizada para o risco associado com a cibersegurança na Europa

- Relatório de Segurança de Munique (*Munique Security Report*, *https://www.securityconference.de/fileadmin/images/MSR/MSC_MunichSecurityReport_2018.pdf*)

"Cyberattacks can be more dangerous to the stability of democracies and economies than guns and tanks"

Jean-Claude Juncker, 13/09/2017

… e no mundo (evidenciada pela intervenção do secretário geral das Nações Unidas)

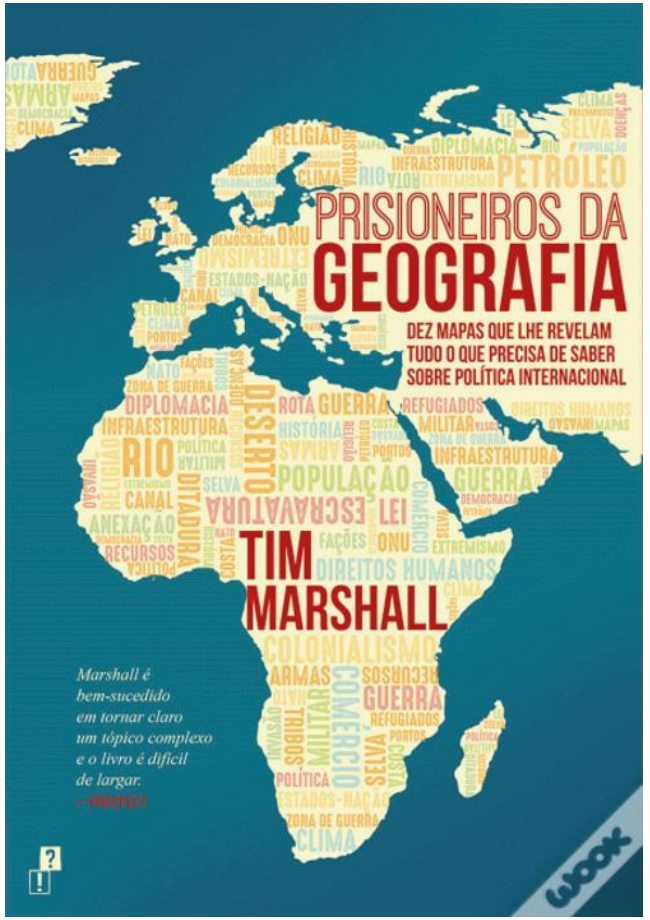
"I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack to destroy military capacity... and paralyze basic infrastructure such as the electric networks"

António Guterres, 19/02/2018

https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4?il=0

A geografia interessa…

- A **geografia** modela a história e condiciona as opções de sustentabilidade (económicas, sociais e ambientais)
  - A obra de Tim Marshall lembra o ártico, toca no espaço, mas esquece o ciberespaço (novas geografias)
- Mesmo num contexto de mudança:
  - Global (a geografia pode determinar)
  - Digital (A geografia condiciona)
- Mesmo mais, porque:
  - Multipolar (mais atores e parceiros inesperados)
  - Complexo (conhecimento em evolução permanente)
  - Instável (impossível de prever, saltos descontínuos)



Luís Borges Gouveia, lmbg@ufp.edu.pt

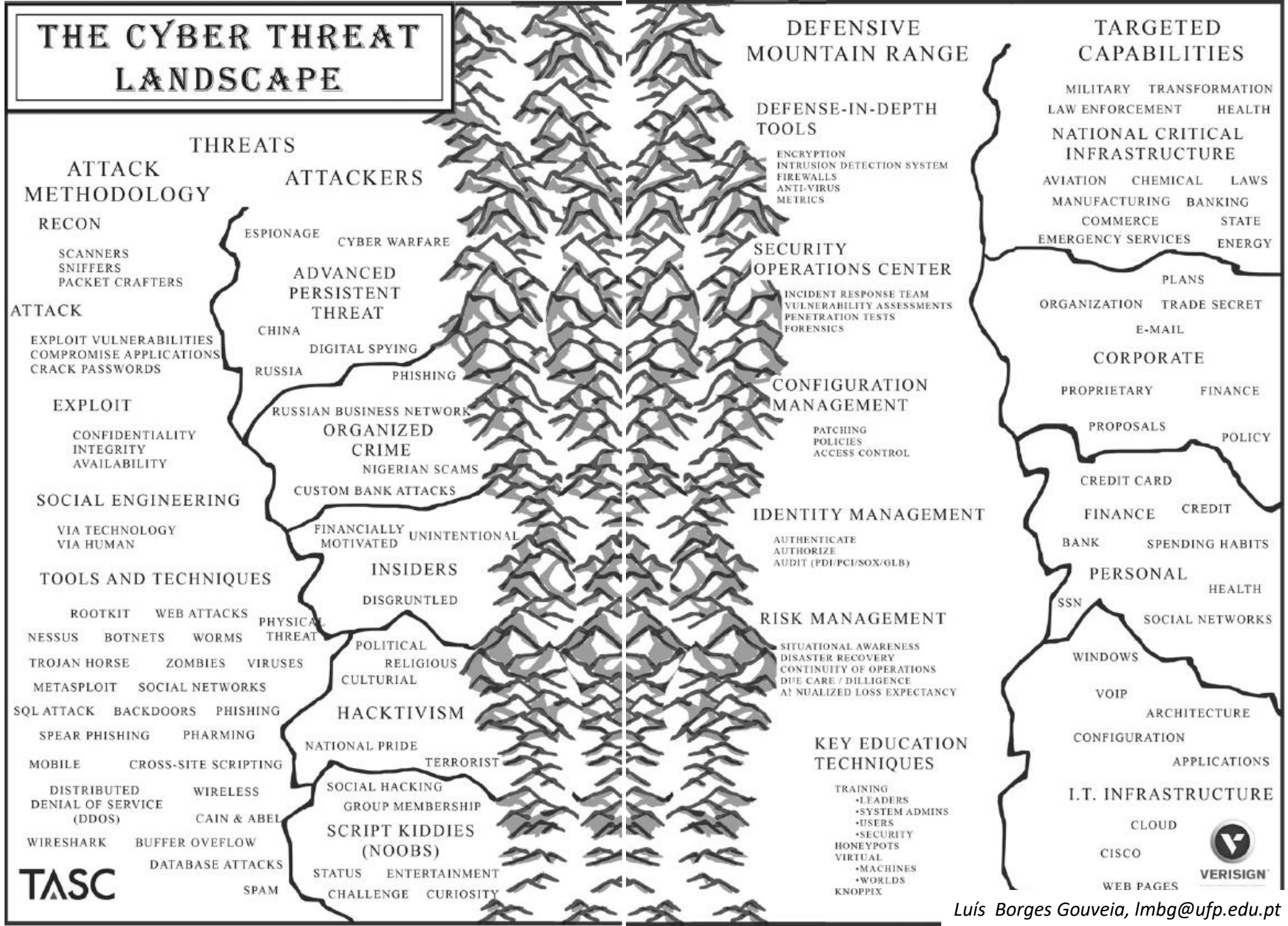
Origens geográficas da Darknet (2008)

Carr, J. (2012). Cyber Warfare. Second Edition. O'Reilly.

*http://stream.**aljazeera**.com/story/201311052102-0023167*

Luís Borges Gouveia, lmbg@ufp.edu.pt

Nova geografia ciber



Luís Borges Gouveia, lmbg@ufp.edu.pt

Segurança…

- Um ativo crítico que não é muitas vezes valorizado
  - Não existindo, sentimos muito a sua falta
  - Existindo, *continuamos como estamos…*
- Não tem retorno direto e funciona para um potencial risco que esperemos que não ocorra
  - Tal como um seguro (em que o risco é normalmente público – acidente. Em oposto a ser privado – incidente)
- Segurança e defesa
  - Conceito associado com muitas outras atividades e que determina a nossa qualidade de vida e nível de proteção
  - Ativo não tangível que afeta confiança (a moeda de esperança da economia…)

Informação…

- Apoia a tomada de decisão e torna possível a ação
  - É abstrato, mas central à atividade humana
- Pode ser um **recurso**
  - E portanto estratégico numa organização (por exemplo, informação comercial de clientes e fornecedores…)
- Pode ser um **ativo**
  - E pode ser transacionado (por exemplo, vender uma base de dados de clientes e suas caraterísticas…)
- Pode ser uma ***commodity***
  - Adquiriu um valor de mercado expetável (por exemplo, saber onde fica determinado lugar…)

Informática…

- Lidar com a informação digital
  - Processada, armazenada e comunicada por dispositivos eletrónicos
- Muito mais do que o computador
  - Dispositivos móveis: *tablets*, *smart phones*, …
  - Sistemas de geolocalização e identificação e controlo de acessos, …
  - Armazenamento de dados: USBs, discos, …
  - Cartões e outros meios de identificação
  - Internet, *Cloud* e plataformas digitais
  - Aplicações , serviços e jogos

Segurança informática

- Vírus e outras formas de ataque a computadores e dispositivos móveis
- Exploração de falhas de software, cada vez mais complexo
- Engenharia social e exploração das caraterísticas humanas (curiosidade, medo, ganância, etc.)
- Falha humana não intencional
  (desconhecimento, relaxamento ou desinteresse)
- Falha humana intencional
  (interesses e atividade criminosa)

Segurança da Informação

- Um maior nível de preocupação que inclui a informação digital, mas também a existente em suportes não digitais
- Preocupa-se com uma abordagem estruturada ao problema e à salvaguarda da informação
  - Qual é a informação crítica?
  - Quais as infraestruturas críticas?
  - O que fazer para assegurar a continuidade do negócio/atividade?
- E temos ainda de lidar com a questão final:
  - *Quem guarda os guardas?*

Quis custodiet ipsos custodes?

Um dilema proposto por Juvenal, poeta Romano (quem guarda os guardas?)

Problema inicialmente colocado por Platão (*A República*, obra sobre governo e moralidade). A sociedade perfeita, descrita por Sócrates (personagem principal da obra), depende de trabalhadores, escravos e comerciantes. A classe guardiã protege a cidade. A pergunta de Sócrates: "Quem guardará os guardiões?" ou, "Quem irá nos proteger dos protetores?“. A resposta de Platão para esta pergunta é que os guardiões irão proteger-se deles mesmos. Segundo Platão, deve ser contada aos guardiões uma "mentira carinhosa." A mentira carinhosa é dizer que os guardiões são melhores do que os que eles servem e que é, então, sua responsabilidade, guardar e proteger aqueles que são menos do que eles. É assim instigado neles um desgosto por poder ou privilégio; eles irão mandar porque o acham ser correto, não porque o desejam.

Luís Borges Gouveia, lmbg@ufp.edu.pt

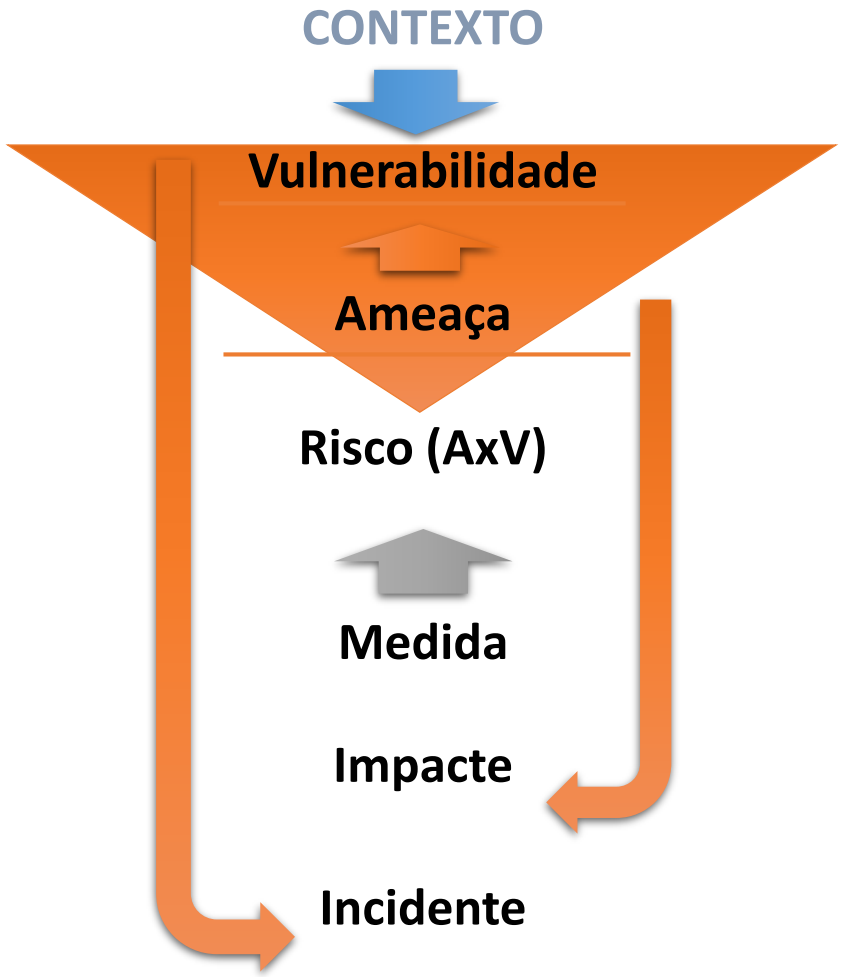
Princípios

- Confidencialidade
  - A informação deve ser salvaguardada de quem não teve autorização para o seu acesso
- Integridade
  - A informação deve ser completa, verificável e verdadeira
- Disponibilidade
  - A informação deve ser fácil de obter onde e quando necessária e de forma entendível
- Não repudiação
  - Não deve ser possível a negação de autoria ou origem da informação

Termos associados: segurança da informação

- Vulnerabilidade
  - Existência de um potencial de falha de segurança
- Ameaça
  - Elementos concretos, potenciadores de exploração de falha de segurança
- Risco
  - Probabilidade efetiva de concretização de ameaças para as vulnerabilidades existentes
- Medida
  - Meio ou procedimento de combate ou minimização do risco
- Impacte
  - Prejuízo em caso de concretização da ameaça
- Incidente
  - Situação efetiva de aproveitamento de uma vulnerabilidade

Termos associados: segurança da informação



Conflitos na era da informação

Informação em contexto de guerra

- Inteligência
- Vigilância
- Reconhecimento
- Clima
- Geográfico
- Outro

Guerra da Informação

- Influenciar atitudes
- Negar/Proteger
- Enganar/Esconder
- Explorar/Atacar

Luís Borges Gouveia, lmbg@ufp.edu.pt

Potenciais vulnerabilidades da sociedade

- **Vulnerabilidades das democracias:**
  - tirando partido de liberdades e garantias e originando informação falsa ou confusa em campanhas organizadas com recurso aos media (imprensa, de massas e redes sociais);
- **Ataque de indivíduos criativos**:
  - com conhecimento, capacidade e determinação para explorar sistemas de comunicações e redes de computadores para ganhos ilegais ou simplesmente sabotar a sociedade;
- **Organizações criminosas:**
  - terroristas, traficantes de armas, ou de mão de obra escrava ou orgãos humanos, que operam entre países;
- **Operações conjuntas:**
  - realizadas de forma combinada com ações militares mais tradicionais, ocultando interesses e atacando alvos considerados críticos para esses interesses;
- **Guerra psicológica:**
  - operações com foco na população de modo a minar a sua confiança nos seus lideres ou na sabedoria da suas ações, muitas vezes explorando clivagens étnicas, sociais, morais dessa sociedade

http://www.iwar.org.uk/iwar/resources/deterrence/iwdAppb.htm

Atores principais na guerra da informação

- **Nações mais poderosas**
  - Depende de sistemas complexos, sujeitos a instabilidade política ou equilíbrios frágeis e possível perda de reputação
- **Organizações multinacionais e redes muito estruturadas**
  - Sujeitos a ações legais, roubo de propriedade intelectual, falha de sistemas e censura pública
- **Indivíduos e redes menos estruturadas**
  - Sujeitos a stresse legal e ilegal por governos e organizações, quando apanhados

O ciberpoder: 3 táticas (*familiares?...*)

- **AA diz a BB o que fazer**
  - se não, BB não o pode fazer…
- **AA não permite a escolha a BB**
  - inclui AA permitir a BB, aplicar as suas estratégias
- **AA molda as preferências de BB**
  - desta forma, BB não considera algumas das estratégias alternativas, como possíveis

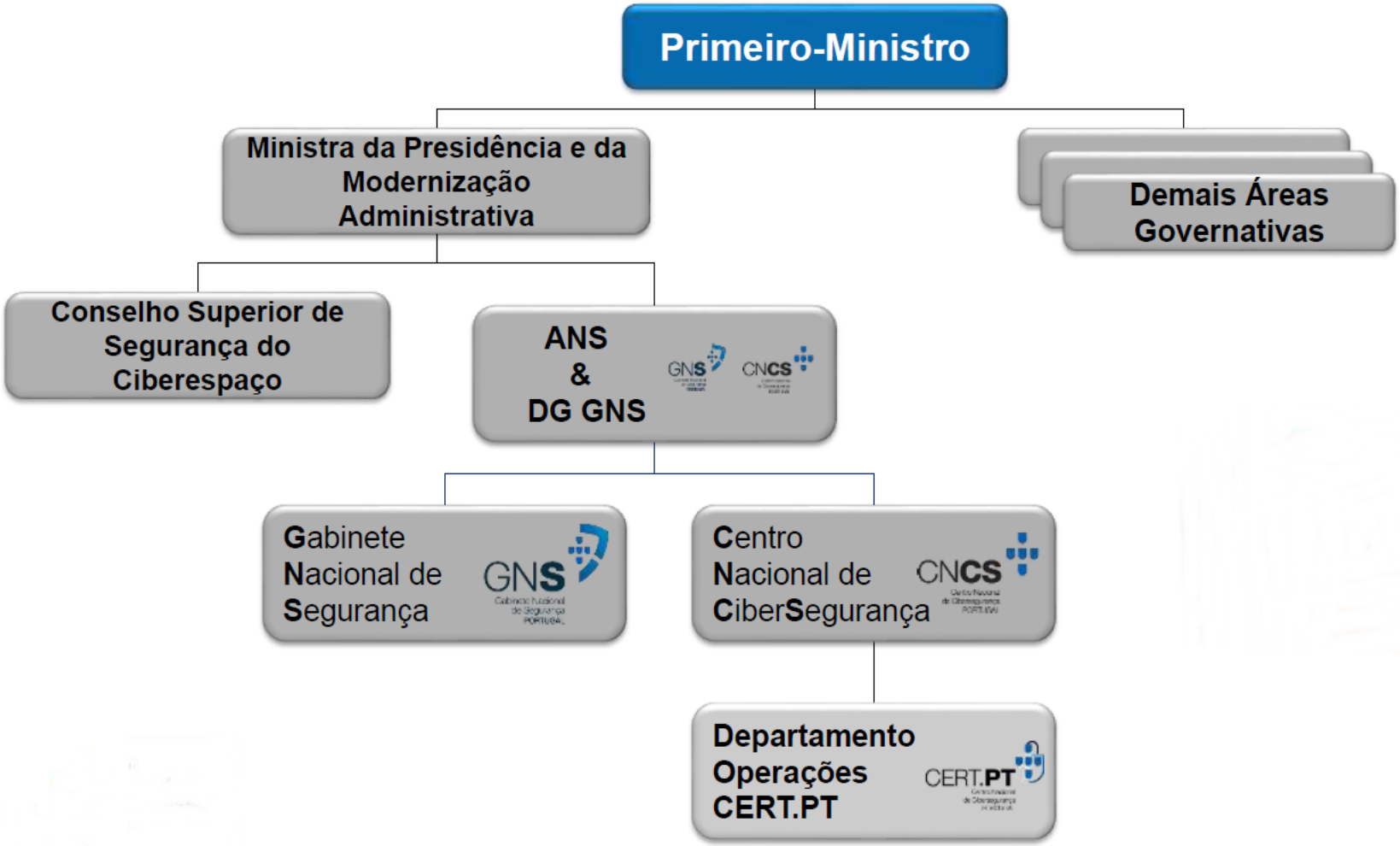
Ciberdefesa

- Conceito militar de resposta à guerra da informação
- Possui 3 componentes:
  - Ciberdefesa **defensiva**: orientada para assegurar a defesa de infraestruturas críticas
  - Ciberdefesa de **exploração**: orientada para explorar e conhecer vulnerabilidade de terceiros e próprias
  - Ciberdefesa **ofensiva**: orientada para realização de ataques a alvos específicos ou como meio de dissuasão (pode incluir o desenvolvimento de ciberarmas)
- Em Portugal, o Centro de Ciberdefesa (CCD, Decreto Regulamentar n.º 13/2015 de 31 de julho) toma estas responsabilidades, estando em revisão a estratégia nacional de segurança do ciberespaço para o CCD assumir operações ativas
  - A NATO possui diversas estruturas associadas com a ciberdefesa; NATO Cyber Defence (*https://www.nato.int/cps/en/natohq/topics_78170.htm*)
  - NATO *Computer Incident Response Capability* (NCIRC) sediada no SHAPE
  - NATO *Cooperative Cyber Defence Centre of Excellence* (CCD CoE) em Talin, Estonia
  - NATO *Communications and Information Systems School* (NCISS) – em mudança de Itália para Portugal

Cibersegurança

- A versão civil da ciberdefesa, orientada para as preocupações de proteger a sociedade nas suas vertentes de serviços públicos, economia e indivíduos
  - Existem ao nível dos Estados, preocupações crescentes com estas questões (em Portugal, é a ***estratégia nacional para a cibersegurança***, *http://www.gns.gov.pt/new-cibersequranca.aspx* da responsabilidade do Gabinete Nacional de Segurança)
  - É organizada em rede e conta com a troca de informação entre interessados e com o reporte de incidentes e práticas de contingência comuns (em Portugal, o **CERT.PT** *http://www.cert.pt/*)
  - A contraparte no contexto europeu é a ENISA (*https://www.enisa.europa.eu/*)
  - Cada um de nós, deve tomar precauções à sua escala…

Contexto de governança nacional para a cibersegurança



Lei 46/2018, de 13 de agosto, requisitos de segurança

- Regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União

https://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html

http://data.europa.eu/eli/dir/2016/1148/oj

Luís Borges Gouveia, lmbg@ufp.edu.pt

Incidentes (alguns exemplos…)

- **Stuxnet** (o caso do ataque com sucesso no Irão) e ?
  - Utilização de software malicioso como ciberarma
- **Wikileaks** e os EUA
  - Classificar informação e proteger informação, parece um ato impossível
  - Ainda existe confidencialidade possível?
- **Snowden** e a NSA
  - Afinal até eu sou espiado, registado e armazenado nas minhas mais diversas dimensões
  - Ainda existe privacidade?
- A **ciberespionagem económica** no caso da China e dos EUA
  - Dos relatórios Mandiant à acusação de Pensilvania
  - Cibersegurança diferente de ciberdefesa?
    E as relações EUA-China?

Numa escala mais humana…

- Como defender:
  - A esfera empresarial
  - A esfera pessoal
- Desafios:
  - Proteção e segurança da informação
  - Privacidade (proteção de dados)
- Mecanismos
  - Trabalho especializado
  - Formação, cautela e experiência

Como fazer?

- Avaliar os ativos de informação
- Classificar a informação
- Listar as infraestruturas críticas
- Listar as vulnerabilidades, as ameaças e os riscos para o contexto
- Formar e enquadrar os recursos humanos
  - Desde o controle de acessos e creditação, até à sensibilização e efetivação de políticas de segurança
- Realizar uma auditoria de segurança
  - Avaliar os riscos e capacidades existentes, refletindo sobre impactes e medidas de contingência
- Rever, partilhar e colaborar
  - A segurança é partilha de informação, rede e conhecimento…

Considerações finais

- A melhor maneira de estar seguro é estar informado
- As proteções tem de ser uma preocupação constante
  - Cada vez mais sofisticadas as ameaças e de maior alcance
  - Sempre em evolução, a exigir uma vigilância contínua
  - Os indivíduos são tão importantes como as empresas
- O conhecimento é a arma e a colaboração a defesa
  - As redes são importantes e o recurso à colaboração e a parcerias, é estratégico
  - O nível de segurança corresponde ao nível associado com o nodo mais vulnerável da rede a que pertencemos

Cenário Actual

- Era da Informação e da Globalização (Sociedade da Informação)
  - Avanços nas tecnologias de informação
  - Avanços nas telecomunicações
  - Maior rapidez na troca de informação
  - Maior exigência das pessoas
- Globalização das ameaças
- Novos riscos e vulnerabilidades

Segurança da Informação

- Proteção da informação e do conhecimento sensíveis para a garantia de continuidade do negócio da empresa
  - *informação* **diferente de** *informações*
- Questões importantes:
  - **O que** deve ser protegido?
  - **Contra o que** será necessário proteger?
  - **Como** será feita a protecção?

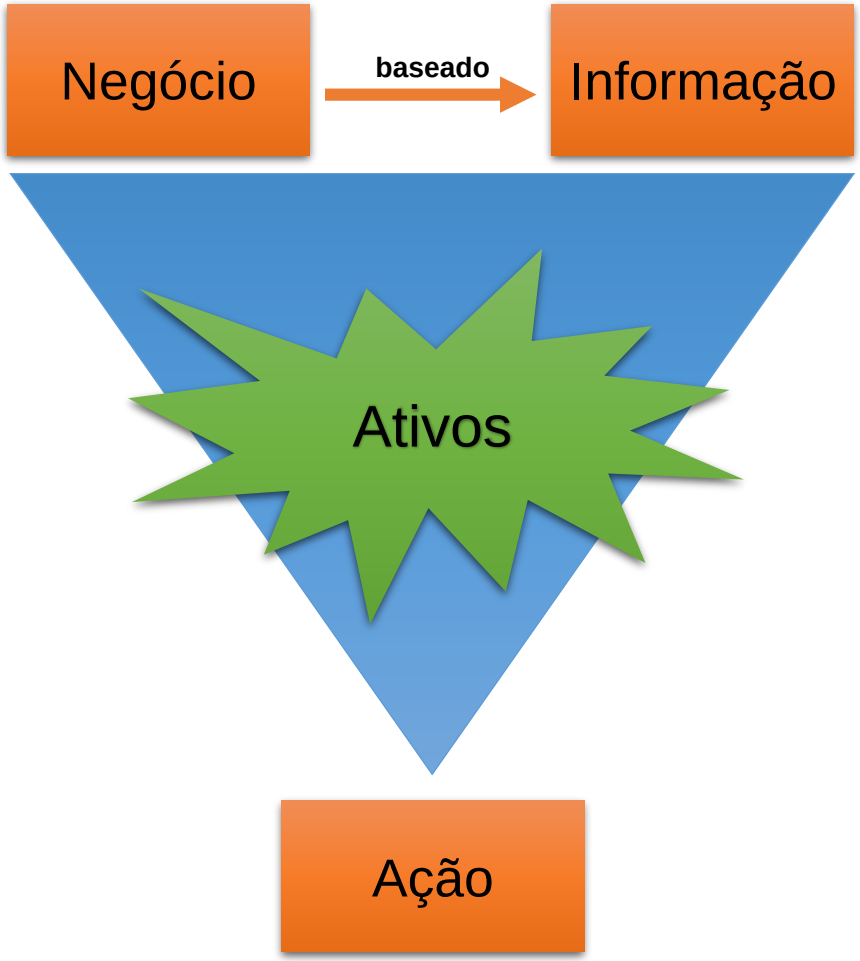
Luís Borges Gouveia, lmbg@ufp.edu.pt

Ciclo da segurança da informação

Luís Borges Gouveia, lmbg@ufp.edu.pt

Ciclo da segurança da informação

Não existe um ambiente 100% seguro, mas um ambiente com menos risco



Nota biográfica: Luis Borges Gouveia
Hab., PhD, MsC, Dip – Sistemas e Tecnologias de Informação

Professor Catedrático na Faculdade de Ciências e Tecnologia da Universidade Fernando Pessoa (UFP)

Coordenador do Doutoramento em Ciências da Informação, Especialidade Sistemas, Tecnologias e Gestão da Informação (UFP)

Consultor, palestrante e autor em sistemas de informação e transformação digital

Auditor de Defesa Nacional, membro do Grupo de Reflexão sobre Resiliência Cibernética, Instituto de Defesa Nacional (IDN)

Membro da Direção Norte da Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI)

Agregação em Engenharia e Gestão Industrial pela Universidade de Aveiro (UA)

Doutoramento em Ciências da Computação pela Universidade de Lancaster (UK, ULancs)

Mestrado em Engenharia Eletrotécnica e de Computadores, pela Faculdade de Engenharia da Universidade do Porto (FEUP)

Licenciado em Matemáticas Aplicadas / Informática pela Universidade Portucalense (UPT)

Possui página na Web (*http://homepage.ufp.pt/lmbg/*)