NOVA SCHOOL OF LAW

CEDIS
CENTRO DE I&D
SOBRE DIREITO E SOCIEDADE

VARIA

#FIQUEEMCASA: PANDEMIA DIGITAL

#StayAtHome: Digital Pandemic

MADALENA MARQUES DA SILVA PEIXOTO
Mestranda em Direito e Segurança

RESUMO

Este trabalho reflete sobre as tipologias e consequências dos recorrentes ciberataques verificados com o aparecimento e propagação da COVID-19. Para além de uma pandemia ao nível da saúde pública, é também uma pandemia digital. Quanto mais tempo passado em casa para conter a propagação do vírus, maior a dependência tecnológica de cada um. Desse modo, estando as pessoas mais expostas a ciberataques, é manifesta a importância da cibersegurança.

PALAVRAS-CHAVE

COVID-19; Ciberataques; Pandemia digital; Dependência tecnológica; Cibersegurança.

ABSTRACT

This paper reflects on the typologies and consequences of the recurring cyber attacks verified with the occurrence and spread of COVID-19. In addition to a public health pandemic, it is also a digital pandemic. The more time spent in the house to contain the spread of the virus, the greater the technological dependence of each person. Thereby, being people more exposed to cyber attacks, it is evident the importance of cybersecurity.

KEYWORDS

COVID-19; Cyber attacks; Digital pandemic; Technological dependence; Cybersecurity.

Siglas e Abreviaturas

C&C	- Command and Control
CERT	- Computer Emergency Response Team
CNCS	- Centro Nacional de Cibersegurança
CoV	- Coronavírus
CSS	- Cascading Style Sheets
CSSC	- Conselho Superior de Segurança do Ciberespaço
COVID-19	- Doença por Coronavírus 2019
DoS	- Denial of Service
ENSC	- Estratégia Nacional de Segurança do Ciberespaço
EU	- União Europeia
EUA	- Estados Unidos da América
ICMP	- Internet Control Message Protocol
IP	- Internet Protocol
MFA	- Multifactor Authentication
OMS	- Organização Mundial de Saúde
RCTS	- Rede Ciência Tecnologia e Sociedade
SARS	- Síndrome Respiratória Aguda Grave
SMS	- Short Message Service
SPAM	- Sending and Posting Advertisement in Mass
SQL	- Structured Query Language
UNCTAD	- Conferência das Nações Unidas sobre Comércio e Desenvolvimento
URL	- Uniform Resource Locator
WEF	- Fórum Económico Mundial

Introdução

A cibersegurança é mais importante que nunca durante a pandemia do coronavírus. O cibercrime disparou após o surto da COVID-19, visto que os cibercriminosos se aproveitam da crescente dependência das pessoas pelas ferramentas digitais. É de assinalar o número de indivíduos que usam o mesmo dispositivo para lazer, finanças pessoais e trabalho, e o número de profissionais obrigados a adotar o regime de teletrabalho.

Ou seja, as medidas para conter a propagação do coronavírus, como o confinamento, levam-nos a passar mais tempo online. Se lhe juntarmos a ansiedade gerada pela crise, podemos deparar-nos com comportamentos online inseguros, fáceis de aproveitar por cibercriminosos.

Através de métodos de *phishing*, instalação de programas maliciosos, entre outros, estes criminosos roubam dados pessoais e acedem aos nossos dispositivos, com o objetivo de aceder a contas bancárias ou até mesmo a bases de dados de organizações.

Este trabalho expõe como esta pandemia digital comprometeu globalmente os sistemas de saúde, económico, educativo, político e social, devido ao aumento do número de ciberataques relacionados com a mesma. Estando mais expostos a esta ameaça, que é invisível em várias vertentes, devemos proteger-nos e contê-la o mais depressa e eficientemente possível.

1. Segurança Cibernética

1.1. Cibersegurança e ciberespaço

A cibersegurança - ou segurança cibernética -, segundo Jorge Bacelar Gouveia, expressa "a proteção que se realiza no ciberespaço contra as ameaças a valores ou direitos da comunidade política, assim perpetrados neste novo ambiente digital"[1].

Para Lino Santos, "... a cibersegurança pode ser vista a partir de duas perspetivas, independentemente de o objetivo da cibersegurança ser o Estado, as organizações ou os indivíduos: a segurança do ciberespaço (na aceção física deste como entidade autónoma) e a segurança da componente "ciber" de um qualquer sistema (segurança do ciberespaço desse sistema)"[2].

O ciberespaço é a "metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras, por exemplo, através de mensagens eletrónicas, em salas de conversa ou em fóruns de discussão"[3], sendo que tanto pode ser um espaço de aproximação, como um espaço de conflito. Como refere o Coordenador do CNCS[4], "O ciberespaço apresenta algumas caraterísticas distintivas. Desde logo, aumenta radicalmente a velocidade e a quantidade das comunicações, ao mesmo tempo que reduz ou elimina a distância entre instituições, entre indivíduos ou mesmo entre nações. Por outro lado, o ciberespaço é aterritorial. (...) Outra caraterística deste espaço virtual diz respeito à

[1] GOUVEIA, J. B. – Direito da Segurança – Cidadania, Soberania e Cosmopolitismo. Lisboa: Almedina, 2018, p. 917.
[2] SANTOS, L. - "Cibersegurança", In Enciclopédia de Direito e Segurança, p. 63.
[3] Associação para a Promoção e Desenvolvimento da Sociedade de Informação.
[4] Centro Nacional de Cibersegurança.

possibilidade de realização de ações de forma praticamente anónima, o que levanta, novamente, dificuldades quanto à atribuição dos atos praticados ou à identificação dos seus autores"[5].

O Direito do Ciberespaço é o subsistema jurídico, com dimensões pública e privada, que visa regular o uso das novas tecnologias digitais e disciplinar as atividades que ocorrem no ciberespaço, dando proeminência à defesa das pessoas e das instituições. Este regula o regime das comunicações eletrónicas, o regime do comércio eletrónico, a proteção dos direitos fundamentais no mundo digital e a punição dos comportamentos que despontem nesse mundo[6]. Contudo, este ramo do Direito ainda não é bem uma realidade nacional, sendo a legislação existente um pouco dispersa[7].

1.2. Ciberameaças

As ciberameaças são ameaças aos valores da comunidade política que sejam perpetrados no ciberespaço e a sua variedade tem vindo a ser multiplicada devido ao desenvolvimento das tecnologias do mundo digital[8].

Os tipos de ciberameaça à segurança nacional são[9]: a ciberguerra - que se traduz na realização de ataques armados contra alvos digitais, ou que se socorre das tecnologias digitais para a realizar, como o uso de veículos não tripulados -, o ciberterrorismo - que se materializa na realização de ataques terroristas contra alvos civis com a utilização de

[5] SANTOS, L. - "Ciberespaço", In Enciclopédia de Direito e Segurança, p. 63.

[6] GOUVEIA, J. B. – Direito da Segurança – Cidadania, Soberania e Cosmopolitismo, p. 918 e 919.
[7] De mencionar a Lei de Proteção de Dados Pessoais - Lei nº 58/2019, de 8 de agosto - na sequência do Regulamento Geral sobre a Proteção de Dados (RGPD), aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.
[8] GOUVEIA, J. B. – Direito da Segurança – Cidadania, Soberania e Cosmopolitismo, p. 925 e 926.
[9] *Ibid*em.

tecnologias digitais -, a ciberespionagem - que se consuma em ações de espionagem que utilizam a infiltração nos meios digitais, acedendo a informação de Estado – e o cibercrime, em que se comete crimes no contexto das tecnologias digitais[10].

2. Ciberataque

2.1. Definição

Um ciberataque é um "ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente"[11].

Os ataques cibernéticos direcionados contra a confidencialidade de um sistema são chamados de espionagem cibernética; os ataques cibernéticos direcionados à integridade e disponibilidade de um sistema são chamados de sabotagem cibernética[12].

2.2. Tipos de ciberataque

O RCTS CERT[13] organiza em quadros[14] as duas principais vertentes relacionadas com os ataques cibernéticos: violações de segurança e métodos de ataque.

Quadro 1 – Violações de Segurança.

[10] Contra o qual se aprovou a Lei do Cibercrime, constante da Lei nº 109/2009, de 15 de setembro.
[11] Disponível em https://www.cncs.gov.pt/recursos/glossario/, consultado em 8 de maio de 2020.
[12] Austrian Cyber Security Strategy (2013), p. 20.
[13] Serviço de Resposta a Incidentes de Segurança Informática da Rede Ciência Tecnologia e Sociedade.
[14] RODRIGUES, F. J. L. – Principais Ameaças no Contexto da Cibersegurança, p. 9-11.

Violação de segurança	Descrição
Falsidade informática	Alegada intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem. Inclui a mistificação de sites Web para roubo de credenciais e a distribuição de mensagens de correio electrónico de phishing.
Interferência em sistema informático	Alegada ação intencional e não autorizada ou a tentativa de impedir ou interromper gravemente o funcionamento do sistema informático, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessível qualquer componente de software ou hardware. Inclui os ataques de negação de serviço.
Acesso ilegítimo a sistema informático	Alegado acesso ou tentativa de acesso intencional e não autorizado à totalidade ou a parte do sistema informático. Inclui roubo de informação, nomeadamente segredo comercial, industrial ou dados confidenciais protegidos por lei.
Interferência em dados	O ato intencional e não autorizado ou a tentativa de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis dados do sistema

	informático. Inclui malware e distribuição do mesmo por correio electrónico.
Recolha não autorizada de informação sobre sistema informático	O ato intencional e não autorizado de reunir informação sobre redes e sistemas informáticos.
Violação de direitos de autor	Alegada violação de direitos autorais, independentemente dos conteúdos serem constituídos por informação, código fonte, projetos gráficos ou quaisquer outros elementos do sistema informático protegidos por direitos de autor.
Mensagem de correio eletrónico não solicitada	Alegada receção/envio de mensagens de correio eletrónico não solicitadas, quer sejam produzidas para efeitos de marketing direto ou sem motivação aparente. Não inclui distribuição de malware ou ataques de phishing.
Outra violação de segurança	Outra alegada violação (da política) de segurança informática.

Quadro 2 – Métodos de ataque.

Método de ataque	Descrição
Ataque físico	Acesso físico a sistema de informação ou outro equipamento
Vulnerabilidade do sistema operativo	Exploração de vulnerabilidade em sistema operativo
Vulnerabilidade de aplicação	Exploração de vulnerabilidade em aplicação (eg. Apache, Acrobat reader, etc.)
Vulnerabilidade de serviço Web	Exploração de vulnerabilidade em serviço Web em linha (eg. SQL injection, CSS, etc.)

Brute-force password attack	Tentativas de acesso ilegítimo - automatizadas, sistemáticas e em número elevado - em que o atacante recorre a dicionários, algoritmos de decifração ou outras ferramentas informáticas para descobrir a password.
Tentativa de login	O atacante tenta descobrir ou contornar a password sem procurar exaustivamente. Habitualmente são experimentadas passwords fracas como “administrador”, “administrator”, “admin” ou “root”.
e-mail flood	Envio massivo (direto ou indireto) de mensagens de correio eletrónico para um ou mais alvos.
Packet flood	Envio massivo de pacotes IP ou ICMP para um ou mais alvos.
Distribuição de malware por e-mail	Envio de mensagens de e-mail contendo código malicioso.
Distribuição de malware via web	Alojamento de código malicioso em site web.
e-mail scam	Envio de mensagem de e-mail configurando uma burla (eg. nigerian scam).
Outro tipo de engenharia social	Recolha e utilização de informações sobre a vítima para melhorar o nível de sucesso de um ataque (eg. envio de e-mail mistificado por forma a levar a vítima a acreditar na sua autenticidade).
Man-in-the middle	O atacante faz-se passar por interlocutor de uma comunicação ou transação ganhando acesso à informação trocada entre os reais intervenientes.
Outro método de ataque	Qualquer outro método de ataque não listado.

O CNCS classifica os ciberataques verificados em território nacional de acordo com a seguinte taxonomia[15]:

Classe Incidente	Tipo Incidente
Malware	Infeção
	Distribuição
	C&C
	Indeterminado
Disponibilidade	DoS/DdoS
	Sabotagem
Recolha de Informação	Scan
	Sniffing
	Phishing
Intrusão	Exploração de vulnerabilidade
	Compromisso de Conta
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de Login
Segurança da Informação	Acesso não autorizado
	Modificação / Remoção não autorizada
Fraude	Utilização indevida ou não autorizada de recursos
	Utilização ilegítima de nome de terceiros
Conteúdo Abusivo	SPAM
	Direitos de autor
	Pornografia infantil, racismo e apologia de violência
Outro	Outro

[15] CNCS.

3. COVID-19

3.1. Origem e precedentes

Uma pneumonia de causa desconhecida detetada em Wuhan, na China, foi reportada à OMS, pela primeira vez, em 31 de dezembro de 2019. O surto foi declarado uma emergência de saúde pública internacional em 30 de janeiro de 2020. Em 11 de fevereiro de 2020, a OMS anunciou um nome para a nova doença de coronavírus: COVID-19[16].

A atual pandemia é causada pelo vírus SARS-CoV-2 (Síndrome Respiratória Aguda Grave Coronavírus 2). Os coronavírus (CoVs) são uma enorme família de vírus, vários dos quais causam graves doenças respiratórias. Exemplo é a Síndrome Respiratória Aguda Grave (SARS), detetada pela primeira vez em 2003, com uma alta taxa de mortalidade[17].

Os CoVs podem também afetar várias espécies animais, sendo que um vírus que é transmitido comummente de um animal para um humano é chamado de vírus zoonótico. Quando um vírus passa de animais para humanos pela primeira vez, ocorre um episódio de transbordamento ("*spillover event*")[18].

O SARS-CoV-2 pertence a um grupo de vírus geneticamente relacionados, que inclui o SARS-CoV e vários outros CoVs isolados de populações de morcegos, especificamente do género *Rhinolophus*. Contudo, atualmente, a fonte zoonótica do SARS-CoV-2 é desconhecida.

[16] **Co**rona**vi**rus **d**isease 20**19.**
[17] Disponível em https://www.who.int/health-topics/coronavirus/who-recommendations-to-reduce-risk-of-transmission-of-emerging-pathogens-from-animals-to-humans-in-live-animal-markets >, consultado em 6 de maio de 2020.
[18] *Ibidem*.

Todas as sequências genéticas publicadas de SARS-CoV-2 isoladas de casos humanos são muito semelhantes, sugerindo que o início do surto resultou de uma introdução pontual na população humana, na altura em que o vírus foi mencionado pela primeira vez em Wuhan. Realizadas várias investigações, uma grande proporção dos casos iniciais no final de 2019 e início de 2020 tinha uma ligação direta ao Mercado de Frutos do Mar de Huanan, na cidade de Wuhan, onde são vendidas várias espécies de animais. Muitos dos pacientes iniciais eram proprietários de tendas, funcionários ou visitantes regulares desse mercado e amostras ambientais recolhidas no mesmo, em dezembro de 2019, apresentaram resultado positivo para SARS-CoV-2.

O SARS-CoV, o vírus que causou o surto de SARS em 2003, e que provavelmente também teve o seu recetáculo ecológico em morcegos, "transbordou" de um reservatório de animais (civeta-africana) para os humanos. De maneira semelhante, e como geralmente há um contacto próximo muito limitado entre humanos e morcegos, é provável que a transmissão do SARS-CoV-2 para seres humanos também tenha ocorrido através de um hospedeiro intermediário, ou seja, outra espécie animal com maior probabilidade de ser tratada por humanos. Contudo, até ao momento, ainda não foi identificado[19].

3.2. Sintomas e transmissão

O nome do vírus, "corona", deriva dos seus espigões em forma de coroa. Uma vez dentro do corpo, os espigões fixam-se às proteínas existentes no exterior das células humanas, dando o vírus instruções às células para produzir mais cópias dele mesmo, podendo depois invadir cada vez mais destas[20].

[19] *Ibidem*.
[20] Netflix - *Coronavirus, Explained* (2020).

O vírus propaga-se através de gotículas, quando se espirra, tosse ou fala, podendo entrar diretamente através dos olhos, nariz ou boca. Também consegue sobreviver em muitas superfícies durante horas, logo, as pessoas podem apanhá-lo nas mãos e infetar-se a si próprias se tocarem na cara. Algo que uma pessoa faz cerca de 20 vezes por hora.

Os sintomas mais comuns são febre, tosse e fadiga, mas existem outros, como falta de ar, dor de garganta, perda de apetite, diarreia, perda de olfato e falta de paladar. Todavia, podemos estar infetados e propagar o vírus sem termos sintomas, ou podemos confundi-los com os da gripe[21].

Há grupos particularmente em risco, como pessoas com doenças crónicas pré-existentes, com idade avançada (65 anos ou mais) ou com um sistema imunitário comprometido[22].

Sendo a origem do vírus ainda desconhecida, resultando na sua imprevisibilidade em termos de imunidade, é mais importante que nunca criar uma vacina.

4. Formas de ciberataque comuns na pandemia

O número de ciberataques tem aumentado exponencialmente desde a declaração da pandemia. Estando as pessoas obrigadas a ficar em casa para conter a propagação do vírus, estas utilizam cada vez mais dispositivos e ferramentas digitais, tornando-se mais vulneráveis a ciberataques. Entre os observados desde o início de fevereiro de 2020, associados ao tema COVID-19, destacam-se as seguintes tipologias[23]:

[21] *Ibidem*.
[22] SNS 24 – Centro de Contacto do Serviço Nacional de Saúde.
[23] Disponível em: https://www.cncs.gov.pt/recursos/noticias/alerta-covid-19-e-as-ciberameacas/, consultado em 9 de maio de 2020.

4.1. Campanhas de "phishing"

Têm sido recorrentes as campanhas de *phishing* (por email, SMS ou por redes sociais) a coberto da imagem de entidades oficiais como a OMS, a UNICEF ou centros de investigação e laboratórios do setor da saúde, com conteúdos fraudulentos alusivos à pandemia. O seu objetivo é o roubo de dados pessoais das vítimas como, por exemplo, dados bancários, ou a infeção dos seus dispositivos com *malware*[24].

4.2. Divulgação de informação falsa através de plataformas e aplicações

Também tem sido notório o aparecimento e divulgação de plataformas digitais e de aplicações para dispositivos móveis que aparentam divulgar informação em tempo real sobre a pandemia (e.g. mapas dinâmicos de contágio), mas que estão, na realidade, orientados para a infeção de dispositivos com *malware*, inclusive da tipologia *ransomware*[25].

Um recente alerta deixado pelo CNCS é para o perigo da aplicação Covid-19 Tracker, que promete aos utilizadores atualizações em tempo real sobre o coronavírus, mas que é,

[24] *Malware* é um termo usado para descrever software malicioso, incluindo spyware, ransomware, vírus e worms. O malware viola uma rede por meio de uma vulnerabilidade, normalmente quando um utillizador clica num link ou anexo perigoso que instala software arriscado. Uma vez dentro do sistema, o malware pode bloquear o acesso a principais componentes da rede (ransomware), instalar malware ou software prejudicial adicional, obter ocultamente informações transmitindo dados do disco rígido (spyware) ou interromper certos componentes e tornar o sistema inoperável.
[25] *Ransomware* é um tipo de software malicioso, também conhecido como malware. Ele criptografa os dados da vítima até que o invasor receba um resgate predeterminado. Normalmente, o invasor exige o pagamento na forma de criptomoeda, como bitcoin. Somente então o atacante enviará uma chave de descriptografia para devolver os dados da vítima.

afinal, um esquema de *ramsomware*. Depois de instalada a *app*, um vírus bloqueia o telemóvel e exige um resgate de 100 dólares em *bitcoin* para que este seja desbloqueado.

4.3. Esquemas de fraude digital

Os esquemas de fraude digital são partilhados por email ou em redes sociais, que divulgam iniciativas de *crowdsourcing*[26] para a recolha de donativos para falsas campanhas de compra de material médico ou de proteção pessoal.

Com a sentida falta de recursos para o combate à pandemia em vários países (como máscaras, álcool em gel, aparelhos respiratórios, entre outros), os cibercriminosos apelam à solidariedade das pessoas para lhes roubar dinheiro.

4.4. SMS falsos de medidas extraordinárias para o combate à pandemia

São comuns os SMS enviados informando que, de acordo com a lei, estão a ser aplicadas medidas extraordinárias para o combate à COVID-19 e que todos os cidadãos nacionais serão vacinados, sendo garantido um reembolso dos custos pelo governo. Para tal, bastaria pagar uma determinada quantia indicada no SMS e através do registo no link enviado, seriam posteriormente ressarcidos.

É importante compreender que ainda não foi produzida nenhuma vacina eficaz contra a COVID-19 e caso tal aconteça, apenas fontes oficiais poderão confirmá-lo e partilhar informação acerca da sua administração e custos associados.

[26] Quando se solicitam contribuições de um largo grupo de pessoas.

5. Consequências dos ciberataques

Mais de 50% da população do mundo está online, aproximadamente um milhão de pessoas fica online pela primeira vez todos os dias e dois terços da população mundial tem um dispositivo móvel. A tecnologia digital tem benefícios económicos e sociais, mas também desvantagens como a desigualdade no acesso à Internet, a falta de uma estrutura global de governação do ciberespaço, que provoca a incerteza geopolítica e geoeconómica, e a insegurança cibernética[27].

Os ciberataques relacionados com a COVID-19 têm várias consequências derivadas desta dependência digital, sendo algumas delas evidentes nos seguintes setores:

5.1. Economia

O choque para a economia global da COVID-19 foi mais rápido e mais severo do que a Crise Financeira Global de 2008 e a Grande Depressão de 1929-39[28]. Além das trágicas consequências humanas, a incerteza económica desencadeada provavelmente custará à economia global 1 trilião de dólares em 2020, afirmou a UNCTAD[29].

Parte deste choque deve-se à forte dependência das infraestruturas financeiras modernas por sistemas informatizados, que as torna particularmente vulneráveis a ataques cibernéticos. A omnipresença da Internet significa que qualquer computador capaz de se conectar à mesma é vulnerável a estes ataques. Segundo o ex-diretor da Inteligência

[27] WEF - The Global Risks Report 2020, p. 7.
[28] Disponível em https://www.weforum.org/agenda/2020/04/depression-global-economy-coronavirus/, consultado em 10 de maio de 2020.
[29] Disponível em https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-cost-economy-2020-un-trade-economics-pandemic, consultado em 10 de maio de 2020.

Nacional dos EUA, Mike McConnell, "os Estados Unidos estão a lutar uma guerra cibernética hoje e estamos a perder... Como a nação mais ligada na Terra, oferecemos o maior número de alvos de importância, no entanto, as nossas ciberdefesas estão terrivelmente ausentes"[30].

Para muitas empresas, códigos de software, propriedade intelectual e infraestrutura tecnológica representam alguns dos mais valiosos ativos da indústria[31]. Embora a quantia total dos custos resultantes desses ataques seja frequentemente difícil de quantificar, esses custos são reais e provocam danos intangíveis e psicológicos. Há que entender que os danos financeiros e psicológicos não são menos devastadores que os danos físicos.[32]

Rui Ribeiro, Diretor Executivo LISS[33], chama a estes ciberataques durante a pandemia de ataques informáticos "Zero Day", uma tipologia de ataques cibernéticos que se espalha a alta velocidade, atacando as vulnerabilidades desconhecidas dos sistemas informáticos das empresas, nas quais os atacantes exploram ao máximo, e em silêncio, até serem descobertos. Até lá, e até à criação da "vacina", por parte do fabricante de software atacado, o *hacker* faz o que quer que, no limite, pode ser até à "morte" da empresa[34]. Em média, um ataque bem-sucedido pode custar até 3,86 milhões de dólares (3,46 milhões de euros) a uma empresa, de acordo com um relatório de 2018 da IBM[35].

5.2. Educação

[30] LIN, T. C. W. - Financial Weapons of War, p. 1393.
[31] *Ibid*., p. 1391.
[32] *Ibid*., p. 1418.
[33] Lusófona Information Systems School.
[34] Disponível em https://jornaleconomico.sapo.pt/noticias/covid-anatomia-de-um-ciberataque-zero-day-557843, consultado em 11 de maio de 2020.
[35] Disponível em https://www.publico.pt/2020/03/31/tecnologia/noticia/pandemia-originar-maior-volume-ciberataques-ja-vimos-1910028, consultado em 11 de maio de 2020.

Em pouco mais de três semanas, cerca de 1,5 bilião de estudantes em, pelo menos, 174 países, ficaram impedidos de ir escola em todo o mundo[36]. O fecho das escolas em todos os países está a impactar mais de 70% da população estudantil do mundo[37].

A melhor opção que os alunos têm é estudar em casa, mas nem todos têm recursos para tal. Em Portugal, duas ferramentas que estão a ser utilizadas para mitigar a situação são o *Apoio à Escolas* - conjunto de recursos para apoiar as escolas no uso de metodologias de ensino a distância, para que elas possam continuar os processos de ensino e aprendizagem - e *Estudo em Casa* - as aulas de TV transmitidas para o ensino básico (1º ao 9º ano) para complementar o uso de ferramentas online[38].

O ensino à distância torna-se ainda mais complicado quando as ferramentas digitais utilizadas sofrem ataques cibernéticos. Um exemplo é a plataforma Zoom, muito utilizada para os professores poderem dar aulas online aos seus alunos durante a pandemia da COVID-19, que esteve envolvida em alguma polémica, visto que as "reuniões" grátis não teriam encriptação, mas apenas a versão *premium* da plataforma. Para além desta polémica, a Check Point Research identificou uma grande falha de segurança na Zoom, porque os *hackers* tinham a capacidade de gerar e ver facilmente os IDs presentes durante as reuniões. Através desta vulnerabilidade era possível espiar as conversas e aceder a todo o conteúdo partilhado durante as mesmas (áudio, vídeo ou qualquer outro tipo de documento)[39]. Entretanto a plataforma já resolveu essas falhas de segurança.

Estes ataques cibernéticos às ferramentas e dispositivos essenciais para a continuação da educação têm várias consequências, entre elas: stress causado aos professores, sendo

[36] Disponível em https://nacoesunidas.org/artigo-a-experiencia-internacional-com-os-impactos-da-covid-19-na-educacao/, consultado em 15 de maio de 2020.
[37] Disponível em https://pt.unesco.org/covid19/educationresponse, consultado em 15 de maio de 2020.
[38] Disponível em https://pt.unesco.org/covid19/educationresponse/consequences, consultado em 15 de maio de 2020.
[39] Disponível em https://www.bit.pt/check-point-descobre-vulnerabilidades-na-plataforma-zoom/, consultado em 16 de maio de 2020.

que as plataformas de ensino à distância tendem a ser confusas e frustrantes**;** desafios na manutenção do ensino à distância, pois a procura e necessidade já são grandes nesta altura de pandemia e já sobrecarregam os portais existentes para a educação remota, quanto mais com ataques que infetam estas plataformas; possibilidade de infeção devido às lacunas no cuidado às crianças, pois muitos pais têm de trabalhar e deixar as crianças sozinhas em casa, sendo que se os dispositivos sofrerem um ataque a criança não saberá o que fazer e pode, sem intenção, permitir aos *hackers* infetar os dispositivos utilizados e roubar dados pessoais; aumento das taxas de abandono escolar, pois a infeção de um dispositivo pode torná-lo inoperável, e o seu utilizador, sendo estudante, pode desistir de tentar aceder às plataformas de educação, comprometendo a sua aprendizagem; aumento do isolamento social, pois estes ataques podem impedir o utilizador de aceder a plataformas de videochamada e fóruns de conversa essenciais para a continuação da experiência educativa e social; por fim, desafios para validar a aprendizagem, pois ataques a plataformas educativas podem impedir que os alunos submetam os seus testes ou trabalhos para avaliação.

5.3. Política

A Internet, com a proliferação de redes sociais como o *Facebook* e o *Twitter*, "restituinos a todos os que as utilizamos uma voz"[40], promovendo descentralização e dando origem a agrupamentos político-sociais inovadores. Contudo, o crime organizado também se tornou mais fácil, já que tem agora meios que antes não tinha para coordenar ações e atividades[41].

[40] GUEDES, A. M. - As "redes sociais digitais", a participação "política" e a segurança, p. 45.
[41] *Ibidem*.

Dessa forma, a dependência digital está a mudar a natureza da segurança internacional e nacional, levantando três questões urgentes: como proteger as infraestruturas críticas, defender os valores da sociedade e impedir a escalada de conflitos entre estados. Períodos em que a Humanidade se encontra mais vulnerável em vários setores - como é o caso da atual pandemia -, são sempre explorados por cibercriminosos ou mesmo atores internacionais que tentam derrubar outros. As tecnologias digitais aparecem cada vez mais na guerra assimétrica, permitindo ataques de países menores e atores não estatais a estados maiores. O ciberespaço tornou-se uma extensão do domínio militar, desencadeando novas corridas a armas tecnológicas [42].

Em termos de soberania, os ciberataques aumentam a pressão sobre questões de jurisdição. A guerra no ciberespaço não tem fronteiras físicas tornando-o "extra-soberano", o que tem sérias implicações ao nível político[43]. Em termos de governação, os ciberataques criam brechas entre estados-nação (e outras partes interessadas) sobre como governar melhor o ciberespaço. Cada um tem a sua visão de qual o melhor modelo de governação do ciberespaço, não existindo assim um consenso internacional significativo. Enquanto os EUA preferem um modelo de cibergovernação de várias partes interessadas - estados, organizações e atores privados -, a China e a Rússia preferem um modelo que dê aos estados, individualmente, a maior parte do poder[44].

Os ciberataques impõem desafios sérios às leis tradicionais, assim como tocam em pontos críticos como soberania e governação.

5.4. Saúde

[42] WEF - The Global Risks Report 2020, p. 65.
[43] LIN, T. C. W. - Financial Weapons of War, p. 1416.
[44] *Ibid*., p. 1420.

Nesta luta contra a pandemia, os *cibercriminosos* percebem que vários sistemas do setor da saúde se encontram mais fragilizados. Hospitais, assim como empresas e órgãos do setor de saúde, como é o caso da OMS, têm-se destacado como os principais alvos destes criminosos. Num cenário como o atual, um ataque cibernético a um hospital ou qualquer outro órgão do setor pode ter consequências muito graves.

Em Espanha, os profissionais de saúde estão a ser alertados para não abrir e-mails suspeitos nos computadores ligados ao sistema informático dos hospitais. Existe um risco de os poderem fragilizar, permitindo um ataque de *malware*. Conforme aviso da Polícia Nacional Espanhola, "todo o sistema informático dos hospitais espanhóis está a ser alvo de um ataque cibernético que utiliza uma enorme campanha de e-mail dirigida aos profissionais de saúde, com e-mails que dizem conter um vírus muito perigoso e malicioso"[45]. Em janeiro de 2020, uma ataque ao Hospital Universitário de Torrejón, em Madrid, afetou a disponibilidade de vários dos seus sistemas. Este ataque foi identificado como *Netwalker Ransomware*. Caso os dispositivos fiquem infetados, o *ransomware* passa a encriptar todos os conteúdos e existe apenas o acesso a um ficheiro de texto que dá instruções à vítima de como deve proceder para pagar o resgate e, supostamente, ter os dispositivos novamente livres[46].

A OMS também sofreu com uma tentativa de ataque cibernético, quando um grupo de hackers, que se pensa ser o DarkHotel[47], ativou um site malicioso que imitava o sistema de e-mail interno da OMS[48]. Este acontecimento levou a organização a publicar um alerta a

[45] Disponível em https://pplware.sapo.pt/informacao/ciberataques-contra-oms-e-hospitais-combate-pandemia-coronavirus/, consultado em 17 de maio de 2020.
[46] *Ibidem*.
[47] Grupo conhecido desde há muitos anos por realizar operações de espionagem cibernética desde, pelo menos, 2007.
[48] Disponível em https://pplware.sapo.pt/informacao/ciberataques-contra-oms-e-hospitais-combate-pandemia-coronavirus/, consultado em 17 de maio de 2020.

informar que os hackers se apresentam como a agência para roubar dinheiro e informações confidenciais.

Segundo a própria organização, desde o início da pandemia do COVID-19, a OMS registou um aumento calamitoso do número de ataques cibernéticos direcionados à sua equipa - vários endereços de e-mail e senhas ativos da OMS foram divulgados online, além de milhares pertencentes a outros que trabalham na resposta ao coronavírus - e ataque por e-mail direcionados ao público em geral - criminosos que personificam a OMS tentam arranjar doações para um fundo fictício. Entretanto, a OMS já tem um sistema de autenticação mais seguro[49].

Os sistemas de saúde também têm vindo a adotar muitas inovações como máquinas de inteligência artificial, sensores, terapias digitais, telemedicina, entre outras. Mas essas novas tecnologias também constituem riscos, podem comprometer a segurança e a privacidade do paciente. Os dados de saúde são especialmente vulneráveis a ataques cibernéticos, com riscos de indivíduos serem identificados mesmo a partir de dados anonimizados[50].

Estes ciberataques afetam o sistema sanitário de um país numa altura em que as unidades hospitalares estão sobrecarregadas, a tratar do aumento de pacientes infetados com o novo coronavírus. Sendo o objetivo destes cibercriminosos afetar principalmente os trabalhadores e as organizações sanitárias, as consequências podem ser devastadoras, pois comprometem a capacidade de resposta à emergência de saúde mundial, pondo em risco a vida de milhares de pessoas. Como afirma Jürgen Stock, Secretário-Geral da INTERPOL, “O bloqueio de sistemas críticos dos hospitais não apenas atrasa a rápida

[49] Disponível em https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, consultado em 6 de maio.
[50] WEF - The Global Risks Report 2020, p. 78.

resposta médica necessária durante estes tempos sem precedentes, como também pode levar diretamente a mortes"[51].

Os sistemas de saúde fazem parte da infraestrutura crítica dos países: são vitais para a sua segurança e crescimento[52]. Se estes se encontram fragilizados, todos os outros setores serão prejudicados também.

5.5. Social

O impacto da pandemia da COVID-19 no crime cibernético tem sido o mais visível e perturbante em comparação com outras atividades criminosas. Os cibercriminosos conseguiram adaptar-se rapidamente e capitalizar o medo das suas vítimas. Ou seja, para além de uma adaptação, foi uma facilitação das suas atividades.

A atividade de distribuição online de material de exploração sexual infantil parece estar a aumentar, com base em vários indicadores; a *dark web* continua a hospedar várias plataformas para distribuir bens e serviços ilícitos, com fornecedores a tentar vender produtos relacionados com a COVID-19; organizações criminosas, estados e atores apoiados por estes procuram explorar esta pandemia para obter lucro ou fomentar interesses geopolíticos; por fim, o aumento da desinformação em torno da COVID-19 continua a proliferar em todo o mundo, com consequências potencialmente prejudiciais à saúde pública e à comunicação eficaz de crises[53].

Estes são apenas alguns exemplos, mas revelam que as consequências ou impactos sociais destes crimes são um conjunto de todos os anteriores. Ataques como estes criam o medo e a incerteza nas pessoas. Para além de infetarem os nossos dipositivos e contas

[51] Disponível em: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware, consultado em 11 de maio de 2020.
[52] WEF - The Global Risks Report 2020, p.79.
[53] EUROPOL - Catching the virus – cybercrime, disinformation and the COVID-19 pandemic, p. 4.

digitais pessoais, atacam organizações e empresas que fornecem bens e serviços básicos, como é o caso dos hospitais, das empresas de telecomunicações, de transportes, de abastecimento de água, de luz, etc. Desse modo, os crimes cibernéticos afetam os setores económico, educativo, político e da saúde, resultando no mau funcionamento da sociedade, criando o pânico e causando perturbações nas vidas das pessoas, colocando-as mesmo em risco.

6. Proteção contra estes ataques

6.1. Proteção institucional

As ciberameaças e os ciberataques atingem vários alvos e obrigam a paralelas respostas por parte das estruturas de segurança internacional e nacional.

Instituições da UE como a Comissão Europeia, a Agência da UE para a Cibersegurança, o CERT-EU e a Europol continuam a trabalhar em prol do rastreio de atividades criminais, da sensibilização e da proteção dos cidadãos e das empresas. É de grande importância 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. Esta tem também solicitado aos operadores de telecomunicações que protejam as redes da UE dos ciberataques[54].

Portugal tem vindo a despertar para a importância da proteção do ciberespaço, tomando algumas medidas para enfrentar estas ameaças, reduzindo as suas vulnerabilidades. Em 2015 foi definida a Estratégia Nacional de Segurança do Ciberespaço (ENSC), aprovada por Resolução do Conselho de Ministros nº 36/2015, a qual se funda "no

[54] Disponível em https://www.europarl.europa.eu/news/pt/headlines/society/20200327STO76003/como-se-proteger-do-cibercrime, consultado em 18 de maio de 2020.

compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (nº 1 da ENSC) e cuja concretização assenta em seis eixos fundamentais: estrutura de segurança do ciberespaço; combate ao cibercrime; proteção do ciberespaço e das infraestruturas; educação, sensibilização e prevenção; investigação e desenvolvimento; cooperação (nº 4 da ENSC).

São de salientar, no plano institucional, os seguintes organismos: Conselho Superior de Segurança do Ciberespaço (CSSC); Centro Nacional da Cibersegurança (CNCS); organismos específicos nas várias dimensões da segurança nacional, como é o caso da ciberdefesa e da cibercriminalidade; ao nível da Defesa Nacional, é de assinalar a Orientação Política para a Ciberdefesa[55].

6.2. Proteção individual

A atual pandemia exige uma mudança no nosso comportamento digital, para que não sejamos alvo de ciberataques nesta altura tão vulnerável.

Devemos rever os nossos hábitos digitais como, por exemplo, verificar se temos uma password longa e complicada (com números, letras e caracteres especiais) para o nosso Wi-Fi de casa e se as *firewalls* do sistema estão ativas no nosso *router*. Também devemos garantir que não reutilizamos passwords na *web* e que usamos uma VPN (Rede Virtual Privada) confiável para acesso à internet. Devemos ainda ser muito cuidadosos quando instalamos softwares, dando as nossas informações pessoais. Não devemos clicar em links de emails. Quando nos inscrevemos em serviços novos, devemos verificar a fonte de cada

[55] Aprovada pelo Despacho nº 13692/2013, de 11 de outubro de 2013, do Ministro da Defesa Nacional.

URL e assegurarmo-nos de que os programas ou as aplicações que instalamos são as versões originais de uma fonte confiável.

Por fim, devemos seguir atualizações oficiais. E assim como prestamos atenção a fontes de informação fidedignas sobre o impacto do COVID-19, devemos assegurar-nos de que atualizamos o nosso sistema de software e aplicações regularmente para reparar alguma vulnerabilidade que possa ser explorada.

Para além destes conselhos, é necessários ter outros cuidados[56], que podem parecer mais simples, mas, por essa mesma razão, são muitas vezes esquecidos.

Devemos estar atentos a e-mails, SMS e chamadas desconhecidos, pois em tempos de crise o criminoso pressiona a vítima a contornar os procedimentos normais de segurança, sendo mais fácil manipular um indivíduo que esteja sob stress e tenha pouco conhecimento do assunto em causa. Também devemos assegurar-nos de que temos um atualizado software de antivírus. Mais, devemos prestar atenção aos que o rodeiam, sendo que as crianças ou outras pessoas podem, acidentalmente, apagar ou alterar informação, ou até infetar o dispositivo que utilizamos para o trabalho, por exemplo.

O teletrabalho é, sem dúvida, essencial nesta matéria, pois o facto de muitas pessoas trabalharem em casa quando não o costumam fazer, leva a que não apliquem as mesmas medidas de segurança que estariam em vigor num ambiente profissional. Também as próprias empresas, por vezes, não implantam as tecnologias ou políticas de segurança corretas. Algumas ideias a adotar são: entender as ameaças à empresa, trabalhando com as equipas de segurança para identificar prováveis vetores de ataque; dar orientações claras e incentivar a comunicação, capacitando os funcionários de tornarem o seu ambiente de trabalho em casa seguro; fornecer os recursos de segurança corretos, garantindo que todos os dispositivos estão equipados com recursos básicos de segurança (autenticação

[56] Disponível em https://www.europarl.europa.eu/news/pt/headlines/society/20200327STO76003/como-se-proteger-do-cibercrime, consultado em 18 de maio de 2020.

multifatorial (MFA), bloqueadores de *malware*, filtração de URLs de domínio malicioso, etc.) [57].

Considerações finais

Dois mil e vinte tem sido um ano desafiante. Começou com tensões entre os EUA e o Irão, passando pelos devastadores incêndios australianos, voltando depois aos EUA com protestos ligados à luta pela justiça relativamente à morte de George Floyd e, consequentemente, contra o racismo. Mas o evento mais marcante globalmente foi, sem dúvida, o surto de COVID-19, que deixou vulneráveis tanto o espaço físico como o ciberespaço.

Medidas para uma robusta cibersegurança são mais importantes que nunca neste tempo de crise e incerteza. Numa pandemia desta escala, a dependência das infraestruturas e comunicações digitais multiplica-se, multiplicando-se assim o número de riscos cibernéticos[58]. A Internet tornou-se quase instantaneamente o meio de interação humana e a principal (por vezes única) maneira de trabalhar e entrar em contato com o outro. Empresas e organizações desenvolvem cada vez mais políticas de teletrabalho e as interações sociais rapidamente se restringem a videochamadas e conversas nos chats das redes sociais.

Neste contexto, um ataque cibernético que priva organizações ou famílias do acesso aos seus dispositivos, dados ou internet pode ser devastador e até mortal: no pior cenário, ataques cibernéticos podem obstruir prestadores de serviços de saúde, sistemas e redes públicos, afetando cidades, países, ou mesmo continentes.

[57] Disponível em https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/, consultado em 10 de maio de 2020.
[58] Ver Imagem 5 em Anexos.

O cibercrime explora o medo. Numa situação de crise, principalmente se prolongada, as pessoas tendem a cometer erros que não teriam cometido de outra forma. Online, cometer um erro em relação ao link em que clicamos ou em quem confiamos os nossos dados pessoais pode custar-nos caro. Para além disso, a grande maioria dos ataques cibernéticos implementa métodos de engenharia social. Os cibercriminosos são extremamente criativos ao conceber novas maneiras de explorar a tecnologia para ter acesso senhas, redes e dados, geralmente aproveitando-se de tópicos ou tendências momentâneas para atrair utilizadores a comportamentos online inseguros, como é o caso da COVID-19.

Mais tempo online pode levar a um comportamento mais arriscado. Vírus digitais espalham-se da mesma forma que os físicos, sendo que os nossos erros online podem muito bem contaminar não só os nossos dispositivos, mas os de outras pessoas numa empresa, numa organização ou outro tipo de comunidade.

As estratégias para manter a segurança cibernética incluem manter uma boa "higiene cibernética", verificar fontes e mantermo-nos a par das atualizações oficiais. É necessária extrema prudência no acesso, na receção e na partilha de conteúdos digitais associados à temática da pandemia COVID-19, devendo dar-se prioridade a fontes oficiais e fidedignas de informação. Não podemos garantir a segurança total de um sistema, mas podemos reduzir a sua insegurança, adotando os comportamentos corretos. E o comportamento de cada pessoa é essencial para prevenir a propagação de infeções tanto no espaço digital como no espaço físico.

Em última análise, muita atenção é dada aos surtos de doenças infeciosas no momento, falando-se muito sobre vulnerabilidades, preparação e resposta. Aconteceu com vírus como o Zika ou a Ébola, mas depois nunca mais ninguém falou sobre esses temas. Estes episódios chamam a atenção das pessoas enquanto acontecem, mas depois essa atenção vai desvanecendo e as pessoas esquecem-se. É preciso tomar medidas preventivas para

que estes ciberataques não aconteçam com tanta frequência da próxima vez que algo do género suceda, é preciso que as pessoas entendem a importância do papel da cibersegurança no mundo em que vivemos, um mundo que está a tornar-se cada vez mais digital, mais tecnológico e, por isso mesmo, cada vez surgem mais desafios ao mesmo. O segredo está não só em combater estes desafios, mas em preveni-los.

Referências bibliográficas e webgráficas

Austrian Cyber Security Strategy [em linha]. Vienna: Federal Chancellery of the Republic of Austria, 2013. [Consult. 7 maio 2020]. Disponível em WWW: < URL: https://bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf >.

Centro Nacional de Cibersegurança PORTUGAL [em linha]. 2020 [Consult. 8 maio 2020]. *Glossário*. Disponível em WWW: < URL: https://www.cncs.gov.pt/recursos/glossario/ >.

Centro Nacional de Cibersegurança PORTUGAL [em linha]. 2020 [Consult. 9 maio 2020]. *Alerta COVID-19 e as ciberameaças*. Disponível em WWW: < URL: https://www.cncs.gov.pt/recursos/noticias/alerta-covid-19-e-as-ciberameacas/ >.

Coronavirus, Explained. [registo em vídeo]. Realização de Claire Gordon e Mark W. Olsen. Netflix, 2020. Documentário de Minissérie (26 min.).

COVID 19: CIBERCRIME EM TEMPO DE PANDEMIA [em linha]. Gabinete Cibercrime Ministério Público, 17 de abril de 2020 [Consult. 11 maio 2020]. Disponível em WWW: < URL: http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/cibercrime_em_tempo_de_pandemia-20-04-2020.pdf >.

EUROPOL [em linha.] 3 abril 2020 [Consult. 11 maio 2020]. *Catching the virus – cybercrime, disinformation and the COVID-19 pandemic*. Disponível em WWW: < URL: https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic >.

GOUVEIA, Jorge Bacelar. *Direito da Segurança - Cidadania, Soberania e Cosmopolitismo.* Lisboa: Almedina, 2018. ISBN: 9789724074924.

GUEDES, Armando Marques - As "redes sociais digitais", a participação "política" e a segurança. *Pessoas & Territórios*. Lisboa. Nº 2 (2009).

INTERPOL [em linha]. 4 abril 2020 [Consult. 11 maio 2020]. *Cybercriminals targeting critical healthcare institutions with ransomware.* Disponível em WWW: < URL: https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware >.

LIN, Tom. C. W. - Financial Weapons of War. *Temple University Legal Studies Research Paper Series.* Minneapolis. ISSN: 2765010. Nº 25 (2016).

Muñoz, Rafael – Nações Unidas Brasil [em linha]. 8 abril 2020 [Consult. 15 maio 2020]. *A experiência internacional com os impactos da COVID-19 na educação.* Disponível em WWW: < URL: https://nacoesunidas.org/artigo-a-experiencia-internacional-com-os-impactos-da-covid-19-na-educacao/ >.

PARLAMENTO EUROPEU [em linha]. 2 abril 2020 [Consult. 18 maio 2020]. *Como se proteger do cibercrime.* Disponível em WWW: < URL: https://www.europarl.europa.eu/news/pt/headlines/society/20200327STO76003/como-se-proteger-do-cibercrime >.

Pequenino, Karla – Público [em linha]. 31 março 2020 [Consult. 11 maio 2020]. "*Pandemia está a originar o maior volume de ciberataques que já vimos".* Disponível em WWW: < URL: https://www.publico.pt/2020/03/31/tecnologia/noticia/pandemia-originar-maior-volume-ciberataques-ja-vimos-1910028 >.

PPWARE [em linha]. 25 março 2020 [Consult. 17 maio 2020]. *COVID-19: Cibercriminosos estão a prejudicar gravemente ação de hospitais e OMS.* Disponível em WWW: < URL: https://pplware.sapo.pt/informacao/ciberataques-contra-oms-e-hospitais-combate-pandemia-coronavirus/ >.

Ribeiro, Rui – Jornal Económico [em linha]. 12 março 2020 [Consult. 11 maio 2020]. *Covid: Anatomia de um ciberataque "Zero-Day".* Disponível em WWW: < URL: https://jornaleconomico.sapo.pt/noticias/covid-anatomia-de-um-ciberataque-zero-day-557843 >.

RODRIGUES, Francisco José Lucas – Principais Ameaças no Contexto da Cibersegurança. *CEDIS Working Paper – Direito, Segurança e Democracia*. Lisboa. ISSN 2184-0776. Nº 48 (2016).

SANTOS, Lino. Cibersegurança, In Gouveia, Jorge Bacelar - *Enciclopédia de Direito e Segurança*. Lisboa, Almedina, 2015. ISBN: 9789724059945.

SNS 24 – Centro de Contacto do Serviço Nacional de Saúde [em linha]. 2020 [Consult. 5 maio 2020]. *Grupos de Risco*. Disponível em WWW: < URL: https://www.sns24.gov.pt/tema/doencas-infecciosas/covid-19/grupos-de-risco/ >.

The Global Risks Report 2020 [em linha]. 15th Edition. World Economic Forum, 2020. [Consult. 10 maio 2020]. Disponível em WWW: < URL: http://reports.weforum.org/global-risks-report-2020/ >.

UNESCO [em linha]. 2020 [Consult. 15 maio 2020]. *Consequências adversas do fechamento das escolas.* Disponível em WWW: < URL: https://pt.unesco.org/covid19/educationresponse/consequences >.

UNESCO [em linha]. 2020 [Consult. 15 maio 2020]. *Suspensão das aulas e resposta à COVID-19.* Disponível em WWW: < URL: https://pt.unesco.org/covid19/educationresponse >.

World Economic Forum [em linha]. 2020 [Consult. 10 maio 2020]. *How to protect yourself from cyberattacks when working from home during COVID-19.* Disponível em WWW: < URL: https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/ >.

World Economic Forum [em linha]. 2020 [Consult. 10 maio 2020]. *This is how much the coronavirus will cost the world's economy, according to the UN.* Disponível em WWW: < URL: https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-cost-economy-2020-un-trade-economics-pandemic >.

World Economic Forum [em linha]. 2020 [Consult. 10 maio 2020]. *This is what the economic fallout from coronavirus could look like.* Disponível em WWW: < URL: https://www.weforum.org/agenda/2020/04/depression-global-economy-coronavirus/ >.

World Economic Forum [em linha]. 2020 [Consult. 10 maio 2020]. *Why cybersecurity matters more than ever during the coronavirus pandemic.* Disponível em WWW: < URL: https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/ >.

World Health Organization [em linha]. 2020 [Consult. 6 maio 2020] *Reducing animal-human transmition of emerging pathogens*. Disponível em WWW: < URL: https://www.who.int/health-topics/coronavirus/who-recommendations-to-reduce-risk-of-transmission-of-emerging-pathogens-from-animals-to-humans-in-live-animal-markets >.

World Health Organization [em linha]. 2020 [Consult. 6 maio 2020]. *WHO reports fivefold increase in cyber attacks, urges vigilance.* Disponível em WWW: < URL:

https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance >.