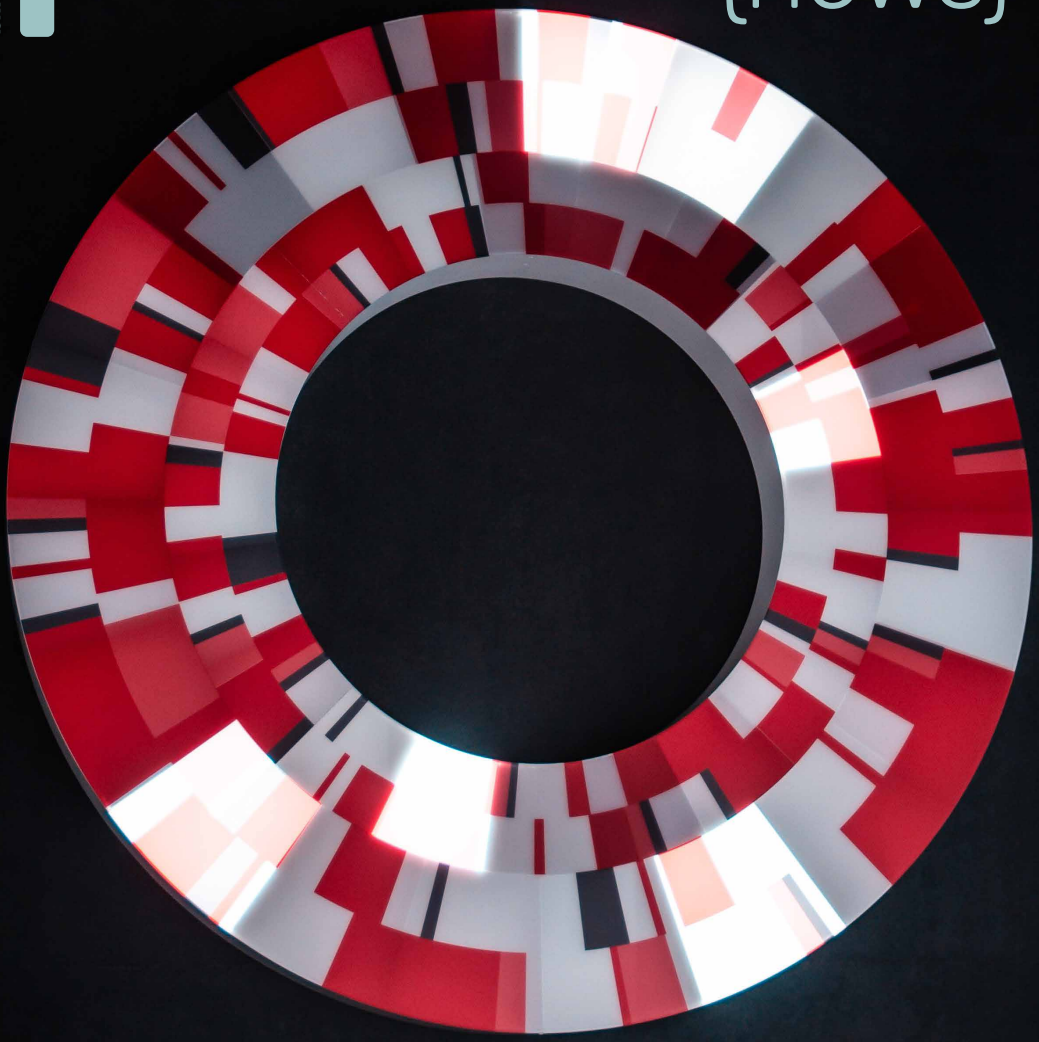
bilingual edition

ptsoc{news}



Existem demasiadas leis para a cibersegurança?

3 Perguntas a Pedro Verdelho

DNSSEC por Eduardo Duarte

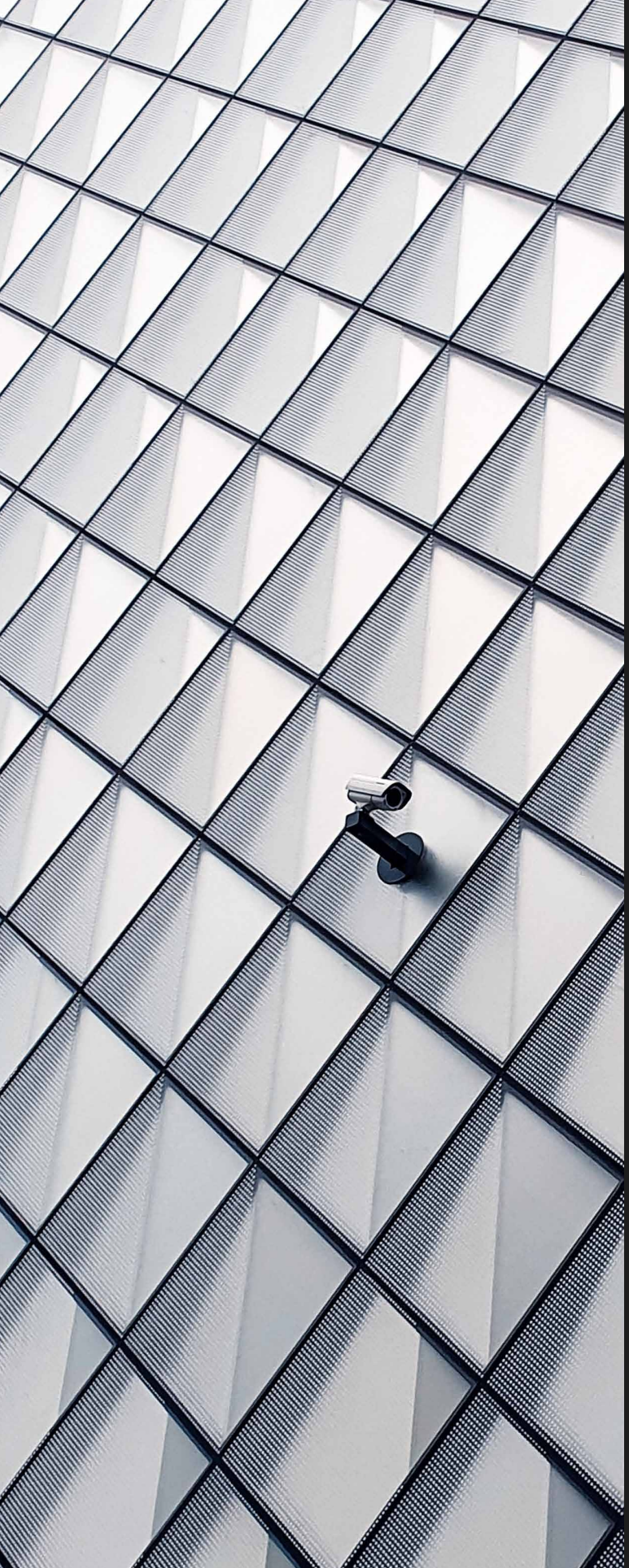
02

Are there too many cybersecurity laws?

3 Questions to Pedro Verdelho

DNSSEC by Eduardo Duarte

.pt



02 **Destaque** Feature

Existem demasiadas leis para a cibersegurança? Are there too many cybersecurity laws?

18 **Estatísticas** Statistics

- Interconectividade internacional de Portugal Portugal's international connectivity
- As principais ciberameaças em 2020 Main cyberthreats in 2020

20 **3 Perguntas a...** 3 Questions to...

Pedro Verdelho

Coordenador do Gabinete Cibercrime da PGR Coordinator of the Cybercrime Office at the Prosecutor General's Office

23 **DNSSEC**

Eduardo Duarte

Diretor Técnico do .PT Technical Director of .PT

26 **Documentos** Documents

- Global Cybersecurity Index 2020
- Gartner Top Security and Risk Trends for 2021
- Perigo nos subdomínios Subdomains in danger
- Ajuda para mitigar ataques de ransomware Help in mitigating ransomware attacks
- Bases de dados expostas Exposed databases

Existem demasiadas leis para a cibersegurança?

Os diplomas legislativos sobre cibersegurança acumulam-se. Portugal tem as suas leis, nacionais, comunitárias ou de organizações com quem estabeleceu relações. Coloca-se assim a natural questão: existem demasiadas leis para a cibersegurança?

Um exemplo recente é o Regime Jurídico da Segurança do Ciberespaço. Ele define, nomeadamente, os requisitos de segurança das redes e sistemas de informação e as regras para notificação de incidentes pela Administração Pública (AP), operadores de infraestruturas críticas ou de serviços essenciais e ainda os prestadores de serviços digitais.

Esta Lei nº 46/2018, de 13 de Agosto, foi regulamentada no final de julho pelo Decreto-Lei nº 65/2021, que alerta para o facto do ciberespaço ser "uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade".

Ambos os diplomas, de origem comunitária, foram acompanhados pela nova perspetiva da Lei Orgânica de Bases da Organização das Forças Armadas, que

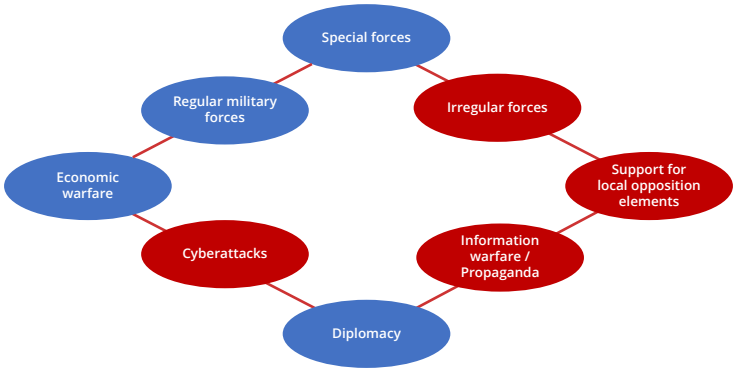
Are there too many cybersecurity laws?

Legislation on cybersecurity is building up. Portugal has its national or community laws or laws from organizations with whom it has established relations. This raises the question: are there too many cybersecurity laws?

A recent example is the Cyberspace Security Legal Framework. It defines, namely, network and information system security requirements and rules for incident reporting by the Public Administration (PA), operators of critical infrastructure, of essential services or digital service providers.

This Law no. 46/2018, of August 13, was regulated at the end of July by Decree-Law No. 65/2021, which alerts to the fact that cyberspace is "(...) a dynamic and fluid reality, in permanent mutation, posing transnational challenges and that crosses several sectors of activity"

Both laws, of community origin, were accompanied by a new perspective of the Organic Law on the Armed Forces,which attributes to EMGFA, among others, the mission of planning, directing and controlling matters relating to cyberdefence.



Componentes principais da guerra híbrida | Main components of hybrid warfare
(Cubeiro, E., 2018, in "Strategic communications as a key factor in countering hybrid threats", STOA, 2021)

atribui ao EMGFA, entre outras, a missão de planear, dirigir e controlar a matéria relativa à ciberdefesa.

A acumulação legislativa tem sido acompanhada por um crescimento nos orçamentos da ciberdefesa e cibersegurança. Os EUA lideram com um valor anual de 2.000 milhões de dólares.

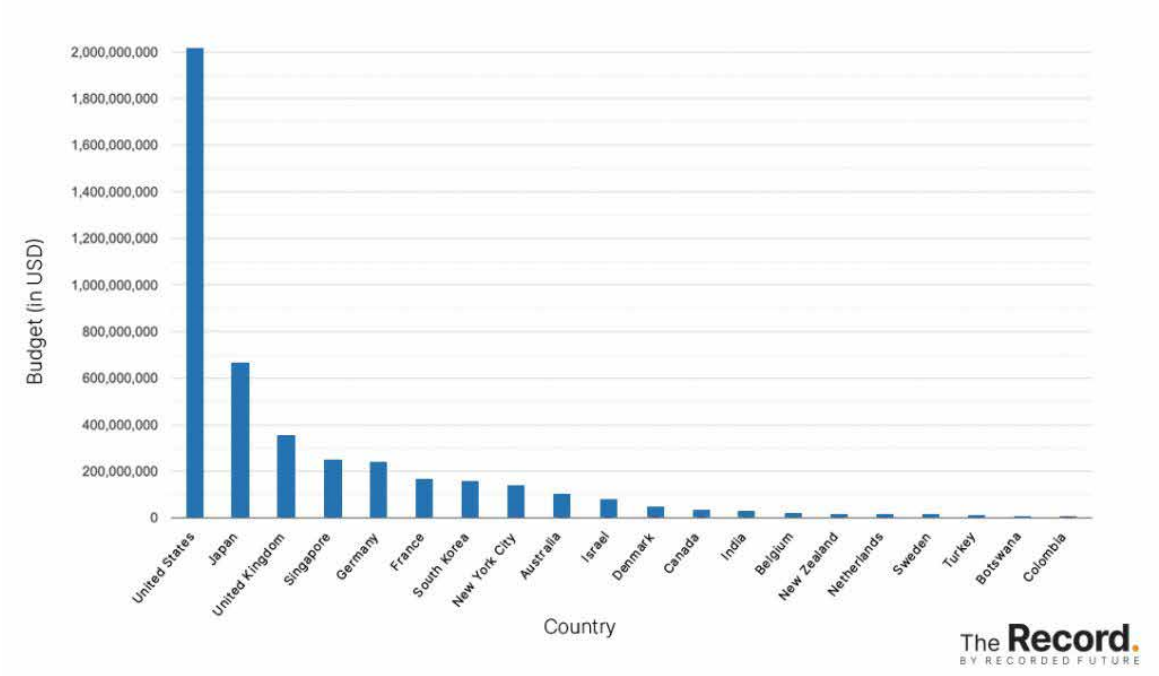
Segue-se o National Center of Incident Readiness and Strategy for Cybersecurity do Japão, com 665 milhões de dólares, quase o dobro do National Cyber Security Centre do Reino Unido (350 milhões) ou do alemão Federal Office for Information Security (240 milhões, quase tanto como Singapura) e longe dos 165 milhões de dólares investidos pela francesa Agence Nationale de la Sécurité des Systèmes d'Information.

No caso europeu, cada país acrescenta ao seu orçamento verbas comunitárias que têm aumentado numa Comissão

Legislative accumulation has been accompanied by a growth in cyber defence and cybersecurity budgets. The US is in the lead, with an annual budget of 2 billion dollars.

Following it is the National Center of Incident Readiness and Strategy for Cybersecurity of Japan, with 665 million dollars, almost double the National Cyber Security Centre of the United Kingdom (350 million) or the German Federal Office for Information Security (240 million, almost as much as Singapore) and far from the 165 million dollars invested by the French Agence Nationale de la Sécurité des Systèmes d'Information [National Cybersecurity Agency].

In Europe, each country adds community funds to its budget, that have been growing in a European Commission (EC) concerned about cyber tension within borders, as revealed by the CERT-EU



Cyber Response Budgets By Country

Europeia (CE) preocupada com a cibertensão dentro de fronteiras, como revelou o "Threat Landscape Report" do CERT-EU em Junho passado.

O número de ataques por ameaças persistentes avançadas (APTs) contra instituições, órgãos e agências da UE aumentou 60% no ano passado em comparação com 2019, para um total de 1.432 incidentes, "o maior número" registado na última década.

Em junho, a CE reconheceu que "a cibersegurança é essencial para o sucesso da transformação digital da economia" e recomendou a criação de uma Joint Cyber Unit (JCU) de coordenação dos esforços europeus em

'Threat Landscape Report' of last June.

Compared to 2019, the number of attacks by advanced persistent threats (APT) against EU institutions, bodies and agencies increased by 60 % last year, to a total of 1 432 incidents, 'the largest number' of attacks recorded in the last decade.

In June, the EC recognised that 'cybersecurity is essential to the success of the digital transformation of the economy' and recommended the creation of a Joint Cyber Unit (JCU) to coordinate European efforts in the event of large-scale cyber incidents, and also for mutual assistance in cybersecurity between public bodies

ciber-incidentes muito graves, e também para a assistência mútua na cibersegurança entre entidades públicas e setor privado.

A JCU agrega estruturas existentes - como a ENISA, Europol e CSIRTs nacionais - num Memorando de Entendimento.

Entre 2014 e 2020, a UE alocou 47,5 milhões de euros em cibersegurança, a que se juntam 11 milhões de euros para 22 projetos em 18 países, no âmbito do programa Connecting Europe Facility. Mais de 1.000 milhões serão ainda entregues pelo Digital Europe Programme para a estratégia da cibersegurança da UE.

Apesar disto, a UE é vista como um "superpoder regulatório", com a recente intervenção no campo da inteligência artificial (IA) a juntar-se ao Regulamento Geral para a Proteção dos Dados, aos Digital Services Act e Digital Markets Act, à Digital Decade, às estratégias para os dados ou para a cibersegurança, à diretiva sobre a segurança das redes e da informação (NIS) e à sua revisão em perspectiva (NIS2).

A resolução aprovada em junho pelo

and the private sector.

The JCU aggregates existing structures - such as the ENISA, Europol and national CSIRTs - in a Memoranda of Understanding.

Between 2014 and 2020, the EU assigned EUR 47.5 million in cybersecurity, to which EUR 11 million were added for 22 projects in 18 countries under the Connecting Europe Facility programme. More than 1 billion euros will still be delivered by the Digital Europe Programme for EU's cybersecurity strategy.

Despite this, the EU is seen as a 'regulatory superpower', with the recent intervention in the field of artificial intelligence (AI) joining the General Data Protection Regulation, the Digital Services Act and the Digital Markets Act, the Digital Decade, data or cybersecurity strategies, the Network and Information Security (NIS) Directive and its prospective review (NIS2).

The resolution adopted by the European Parliament in June on the Cybersecurity Strategy in the Digital Decade highlights another factor regarding human resources and 'the need to match the demand

Parlamento Europeu sobre a Estratégia da Cibersegurança para a Década Digital salienta um outro fator relativo aos recursos humanos e a "necessidade de fazer corresponder a procura de trabalho em cibersegurança com a eliminação das lacunas de competências, prosseguindo os esforços em matéria de educação e formação", mas também de género.

Um parecer do Comité Económico e Social Europeu (CESE) sobre a Estratégia nota como "os ciberataques podem provocar enormes perdas económicas", incluindo a "perda de propriedade intelectual e de informações comerciais confidenciais; fraude e crimes financeiros online, (...) manipulação financeira, com recurso a informações comerciais sensíveis extraviadas sobre potenciais fusões ou conhecimento antecipado dos relatórios de desempenho de empresas cotadas em bolsa; custos de oportunidade, incluindo perturbação da produção ou de serviços, e diminuição da confiança nas atividades online; custos de proteção das redes, como a subscrição de ciberseguros, e pagamentos associados à recuperação após ciberataques; ou danos à reputação e riscos de responsabilidade civil para as

for cybersecurity work with the elimination of skills gaps, continuing education and training efforts', but also gender.

An opinion by the European Economic and Social Committee (EESC) on the Strategy notes how 'cyberattacks can cause huge economic losses', including 'loss of intellectual property and confidential business information; online fraud and financial crimes; (...) financial manipulation, using stolen sensitive business information on potential mergers or advance knowledge of the performance reports of publicly listed companies; opportunity costs, including disruption of production or services, and decreasing trust in online activities; costs with networks protection, such as cyberinsurance underwriting, and payments associated with recovery after cyberattacks; or damage to reputation and civil liability risks for companies targeted by hacking for the respective brand, namely temporary stock exchange losses'.

The Committee cites a report by the Center for Strategic and International Studies, pointing out that 'Europe is where cybercrime has the greatest economic impact, estimated at 0.84 %

empresas visadas por pirataria informática e para a respetiva marca, nomeadamente perdas temporárias no valor em bolsa".

O Comité cita um relatório do Centro de Estudos Estratégicos e Internacionais para fazer notar que "a Europa é a região onde a cibercriminalidade tem maior impacto económico, estimada em 0,84% do produto interno bruto da UE, contra 0,78 % na América do Norte".

Ataques de "disinformation-as-a--service" mais acessíveis

O CESE observa ainda que a estratégia de cibersegurança não aborda a ligação entre esta cibersegurança e a desinformação, cuja propagação "pode ter consequências graves. Os ataques transfronteiras podem visar centros de informações e instituições nacionais ou europeias para propagar a desinformação, bem como diminuir a confiança nos poderes públicos. Por conseguinte, qualquer estratégia de cibersegurança deve destacar a prevenção da desinformação".

Isto quando "existem organizações que desempenham uma função de desinfor-

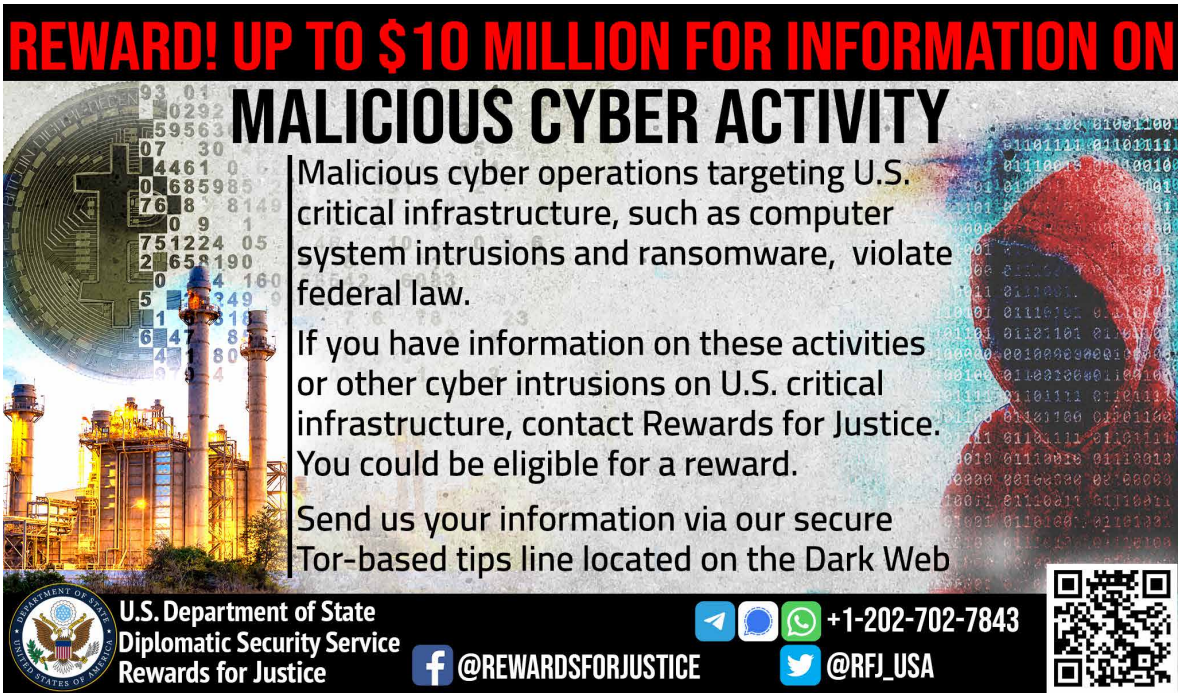
of the EU's gross domestic product, compared to 0.78 % in North America.'

More accessible 'disinformation-as--a-service' attacks

The EESC also notes that the cybersecurity strategy has not addressed the connection between cybersecurity and disinformation, the spread of which 'could have serious consequences. Cross-border attacks can target information centres, governmental or European institutions to spread disinformation and reduce trust in public authorities. Hence, the need to place emphasis on preventing disinformation in any strategy on cybersecurity.'

This happens when 'there are organizations that are playing a disinformation--as-a-service function', said former U.S. cybersecurity head Chris Krebs.

If hiring cyberattack services is now cheaper than ever, it is more expensive to create strategies and resources in cybersecurity. The best strategy is to avoid the attacks, as the United States is discovering.



mação-como-serviço", afirmou o ex--chefe de cibersegurança dos EUA, Chris Krebs.

Se a contratação de serviços de ciber--ataques é cada vez mais barata, mais oneroso é criar estratégias e ter recursos na cibersegurança. A melhor estratégia é evitar os ataques, como estão a descobrir os EUA.

Após o ataque à Colonial Pipeline, o programa Rewards for Justice começou

Following the attack on the Colonial Pipeline, the Rewards for Justice programme began offering rewards up to $10 million 'for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against US critical infrastructure.'

In early June, US President pressured Vladimir Putin on ransomware groups

a oferecer recompensas até 10 milhões de dólares "por informações que levem à identificação ou localização de qualquer pessoa que, enquanto age sob a direção ou sob o controlo de um governo estrangeiro, participa de ciberatividades maliciosas contra a infraestrutura crítica dos EUA".

No início de Junho, o presidente dos EUA pressionou Vladimir Putin sobre os grupos de ransomware que operam a partir da Rússia. "Deixei bem claro que os EUA esperam [que] quando uma operação de ransomware vem do seu solo, mesmo que não seja patrocinada pelo estado, esperamos que [a Rússia] atue".

Para Cyrus Newlin, especialista do Center for Strategic and International Studies, "a questão não é se 'Biden pressionará Putin sobre isso?'" mas antes "o que acontecerá nos meses seguintes? Essa pressão terá algum retorno e a Rússia cessará os ciberataques contra os EUA?"

A 16 de junho, num encontro presencial entre Biden e Putin, este negou qualquer interferência nos ataques aos EUA, afirmando que o seu país também

operating from Russia. 'I made it very clear to him that the United States expects [that], when a ransomware operation is coming from his soil, even though it's not sponsored by the state, we expect [Russia] to act.'

For Cyrus Newlin, a specialist at the Center for Strategic and International Studies, 'the question is not whether "Will Biden pressure Putin on this?", but rather "What will happen in the following months?

Will this pressure have any return and will Russia cease cyberattacks against the US?"'.

On 16 June, at a face-to-face meeting between Biden and Putin, Putin denied any interference in the attacks on the US, claiming that Russia is also targeted by cyberattacks. Both agreed to collaborate to ensure cybersecurity and prevent attacks on critical infrastructure.

'He knows I will act, there will be consequences,' said Biden, while Putin preferred to talk about the agreement: 'We will start negotiations on that. I think that's extremely important.'

é alvo de ciberataques. Ambos concordaram em colaborar para garantir a cibersegurança e evitar ataques a infraestruturas críticas.

"Ele sabe que vou agir, que haverá consequências", disse Biden, enquanto Putin preferiu falar do acordo: "Começaremos as negociações sobre isso. Acho que é extremamente importante".

"As operações ofensivas da Rússia são uma ameaça consistente. Uma ferramenta cada vez mais importante do que a Rússia vê como um 'confronto de informação' a decorrer utiliza ciberoperações com outros meios militares e não-militares para perseguir objetivos estratégicos", escreve-se em "Russia's Strategy in Cyberspace", um documento do StratCom COE.

Neste espaço, "não houve alterações ou contradições significativas nas publicações doutrinárias e conceptuais oficiais da Rússia em relação ao 'confronto de informações' desde o início da presidência de Vladimir Putin em 1999".

Na prática, especifica o documento, "o ciberespaço pode ser usado tanto para ataques físicos às infraestruturas

'Russia's offensive operations are a consistent threat. An increasingly important tool in what Russia views as the ongoing "information confrontation," Russia utilizes cyber operations alongside other military and non-military means to pursue strategic objectives', can be read in 'Russia's Strategy in Cyberspace', a Stratcom COE document.

In this area, 'there have been no significant changes or contradictions in the Russia's official doctrinal and conceptual publications in relation to the "exchange of information" since the start of Vladimir Putin's presidency in 1999.'

In practice, the document specifies, 'cyberspace can be used both for physical attacks on infrastructure, and cognitive attacks such as disinformation,' while 'the front-line of Russia's defensive efforts is its domestic information space, which is tightly controlled by data surveillance and a restrictive legal system aimed at the Kremlin's opponents.' This 'allows not only the protection of society's psychological cohesion from foreign interference, but also protects domestic scientific and technological developments from foreign competition.'

quanto para ataques cognitivos, como a desinformação", enquanto "a linha da frente dos esforços defensivos da Rússia é o seu espaço de informação doméstico, rigidamente controlado pela vigilância dos dados e um sistema legal restritivo a visar os oponentes do Kremlin". Isto "permite não apenas proteger a coesão psicológica da sociedade de uma interferência estrangeira, mas também proteger os desenvolvimentos científicos e tecnológicos domésticos da concorrência estrangeira".

Rússia e China em "confronto de informações"

No âmbito dos ciberataques, a China também é tida como um problema. Em julho, os EUA e aliados como a UE ou a NATO acusaram a nação asiática de "ciberatividades maliciosas e comportamento estatal irresponsável", num padrão "inconsistente com o seu objetivo declarado de ser vista como líder responsável no mundo".

Biden foi mais longe e salientou que os novos desafios na cibersegurança podem desencadear "uma guerra real". "Vimos como as ciberameaças, incluindo ataques de ransomware, são cada vez

Russia and China in 'information confrontation'

In the context of cyberattacks, China is also seen as a problem. In July, the US and allies such as the EU or NATO accused the Asian nation of 'malicious cyber activity and irresponsible state behaviour', in an 'inconsistent [pattern] with its stated objective of being seen as a responsible leader in the world.'

Biden went even further and stressed that new challenges in cybersecurity can trigger 'a real war'. 'We've seen how cyber threats including ransomware attacks increasingly are able to cause damage and disruption in the real world', he stated. Thus, 'a real shooting war with a major power, it's going to be as a consequence of a cyber breach of great consequence.

International treaties for traditional wars seem to have disappeared in the face of this new pattern of conflict. As former US Secretary of State Robert Reich explained, 'the emerging cold war between Beijing and Washington is less about traditional arms than about data – gathering, aggregating, analysing and making maximum use of it to outma-

mais capazes de causar danos e perturbar o mundo real", disse. Assim, "uma verdadeira guerra com uma grandepotência, será em consequência de uma ciberviolação de grandes consequências".

A existência de tratados internacionais para a guerra tradicional parece ter desaparecido perante este novo padrão de conflito. Como explicou o ex-secretário de Estado norte-americano Robert Reich, "a guerra fria emergente entre Pequim e Washington tem menos a ver com armas tradicionais do que com dados - recolha, agregação, análise e máximo uso deles para superar o outro lado. A cibersegurança depende de qual lado tem acesso a mais informações sobre o outro e melhor as pode usar".

O alegado roubo de propriedade intelectual pela China, "apenas para a indústria dos EUA, é estimado em aproximadamente 300 mil milhões de dólares anuais" pela NATO.

A escalada de tensão entre nações revelou também como as amizades são voláteis. Em agosto, a China foi acusada de atacar autoridades da Rússia desde 2020, assim como a Mongólia, Bielorús-

neuver the other side. Cybersecurity comes down to which side has access to more information about the other and can use it best.'

According to NATO, China's alleged theft of intellectual property, 'for US industry alone, is estimated at approximately $300 billion annually.

The escalation of tension between nations also showed how volatile friendships are. In August, China was accused of attacking Russian authorities since 2020, as well as Mongolia, Belarus, Canada and the US were targeted in the first half of this year by the APT31 group - a Chinese 'cyber espionage actor' whose aims are to gain 'information that can give the Chinese government and state-owned enterprises political, economic and military advantages.'

China's cyber capabilities are not consensual. In 'Cyber Capabilities and National Power: A Net Assessment, the International Institute for Strategic Studies states that the nation is 10 years behind the US. But security experts say that 'the report does not take into account cyberattacks by

sia, Canadá e os EUA foram visadas no primeiro semestre deste ano pelo grupo APT31 - um "ator da ciberespionagem" chinesa cujos objetivos passam por obter "informações que podem dar ao governo chinês e às empresas estatais vantagens políticas, económicas e militares".

As cibercapacidades da China não são consensuais. O International Institute for Strategic Studies afirma em "Cyber Capabilities and National Power: A Net Assessment" que a nação está 10 anos atrasada relativamente aos EUA. Mas especialistas em segurança dizem que "o relatório não tem em consideração ciberataques de atores não estatais. Eles dizem que tenta classificar os países em capacidades que são difíceis de medir. E que o relatório não considera adequadamente os poderes defensivos".

Unidos pelos ciberataques

Perante estes cenários, vários países têm mexido na legislação para lidar com ciberataques ou o desvio de propriedade intelectual por alegados ataques da China, Coreia do Norte, Irão e Rússia. No Brasil, o governo instituiu a Rede Federal

non-state actors. They say it tries to classify countries into capabilities that are difficult to measure. And that the report does not properly consider the defensive powers.'

United by cyberattacks

Faced with these scenarios, several countries have been tweaking their laws to address with cyberattacks or the misappropriation of intellectual property due to alleged attacks by China, North Korea, Iran and Russia.

In Brazil, the government instituted the Federal Cyber Incident Management Network, mandatory for federal or local PA. Its purpose is to 'prevent, treat and respond to cyber incidents in order to raise the level of resilience in cybersecurity of your information assets.'

In Canada, Prime Minister Justin Trudeau's government announced laws to protect research and intellectual property and prevent the disclosure of secrets to other countries.

The new policy, similar to that of Australia, makes researchers undertake a risk assessment in state-funded collabora-

de Gestão de Incidentes Cibernéticos, obrigatória para a AP federal ou autárquica. A sua finalidade é a "prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação".

No Canadá, o governo do primeiro-ministro Justin Trudeau anunciou legislação para proteger a investigação e a propriedade intelectual e evitar a divulgação de segredos para outros países.

A nova política, semelhante à da Austrália, obriga os investigadores a uma avaliação de riscos na colaboração financiada pelo Estado envolvendo empresas estrangeiras, nomeadamente em áreas como a computação quântica, IA e aeroespacial.

Nos EUA, o desafio juntou republicanos e democratas na proposta de lei conjunta International Cybercrime Prevention Act, para "permitir que as autoridades confisquem dispositivos de comunicações e outros bens usados para cometer cibercrimes; aumentar a capacidade dos promotores públicos de encerrar botnets e outras infraestruturas digitais usadas para uma ampla gama de atividades

tion involving foreign companies, notably in areas such as quantum computing, AI and aerospace.

In the United States, the challenge brought together Republicans and Democrats in the joint International Cybercrime Prevention Act, to 'allow authorities to confiscate communication devices and other property used to commit cybercrime; enhance prosecutors' ability to shut down botnets and other digital infrastructure used for a wide range of illegal activity; create a new criminal violation for individuals who have knowingly targeted critical infrastructure, including dams, power plants, hospitals, and election infrastructure; and prohibit cybercriminals from selling access to botnets to carry out cyberattacks.'

Despite the 'international' reference, the law is only binding to the US.

In the last 20 years, 92 % of UN members have reformed or are re-adjusting their legislation, according to the Council of Europe's 'The global state of cybercrime legislation 2013 - 2021: A cursory overview'.

dades ilegais; criar uma nova violação-criminal para indivíduos que visaram intencionalmente infraestruturas críticas, incluindo barragens, centrais eléctricas, hospitais e infraestruturas eleitorais; e proibir os cibercriminosos de venderem acesso a botnets para realizar ciberataques".

Apesar do termo "internacional", a lei só vincula os EUA.

Nos últimos 20 anos, 92% dos membros das Nações Unidas reformaram ou estão a re-ajustar a sua legislação, segundo o "The global state of cybercrime legislation 2013 – 2021: A cursory overview" do Conselho da Europa.

Em 2001, esta organização promoveu um dos primeiros acordos globais, a Convenção sobre o Cibercrime (ou Convenção de Budapeste). Até 2024, tem a decorrer o Octopus Project para incentivar, entre outras medidas, o "desenvolvimento de ferramentas online para a realização de atividades de capacitação em cibercrime e prova eletrónica".

Ao abrigo da NATO 2030, a organização anunciou um fundo de 1.000 milhões de

In 2001, this organization promoted one of the first global agreements, the Convention on Cybercrime (or the Budapest Convention). The Octopus Project has been running until 2024 to encourage, among other measures, the 'development of online tools for the delivery of capacity building activities on cybercrime and electronic evidence.'

Under NATO 2030, the organization announced a fund of 1 billion euros to invest in deeptech companies and 'next generation war machines' in the Defence Innovation Accelerator for the North Atlantic (DIANA) civil-military partnership.

In a statement, it revealed that, faced with 'complex, destructive, coercive and ever more frequent' threats, it approved a Comprehensive Cyber Defence Policy, in which 'the answer does not need to be restricted to the cyber domain'. Exactly the same position taken by Joe Biden a month later.

'In addition to the traditional security threats emanating from nation states, the Allies are now also facing new challenges from internationally active terrorist organizations, while cyberattacks

euros para investir em empresas "deep-tech" e na "próxima geração de máquinas de guerra", na parceria civil-militar Defence Innovation Accelerator for the North Atlantic (DIANA).

Em comunicado, revelou que, perante ameaças "complexas, destrutivas, coercivas e cada vez mais frequentes", aprovou uma Comprehensive Cyber Defence Policy, em que "a resposta não precisa de se restringir ao domínio cibernético". Exatamente a mesma posição assumida por Joe Biden um mês depois.

"Além das ameaças tradicionais à segurança que emanam dos Estados-nação, os Aliados agora também enfrentam novos desafios de organizações terroristas ativas internacionalmente, enquanto os ciberataques e as campanhas de desinformação podem ter como alvo a infraestrutura crítica e minar a coesão das nossas sociedades", especificava no ano passado.

É neste cenário que está em preparação um novo tratado internacional. Em maio, a Assembleia Geral da ONU anunciou a criação do Comité Ad Hoc para elaborar uma Convenção Internacional Abran-

and disinformation campaigns can target critical infrastructure and undermine our societies' cohesion,' he specified last year.

It is against this scenario that a new international treaty is being prepared. In May, the UN General Assembly announced the establishment of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, involving participants from each country. Portugal was represented by Prosecutor Pedro Verdelho, Coordinator of the Cybercrime Office at the Prosecutor General's Office.

The Group foresees meetings from 2022 onwards to obtain a prior version of the treaty to be submitted in September 2023.

Pedro Verdelho recalls that, with the Budapest Convention in force, 'Portugal opposed the start of negotiations on a new treaty in this area, which was considered unnecessary. However, since the majority of UN Member States voted to discuss said treaty, Portugal joined the process, volunteering to be Vice-

gente para Combater o Uso das Tecnologias de Informação e Comunicação para Fins Criminosos, envolvendo participantes de cada país, como sucede para Portugal com o Procurador Pedro Verdelho, coordenador do Gabinete Cibercrime da PGR.

O funcionamento do grupo prevê reuniões a partir de 2022 para se obter uma versão prévia do tratado a apresentar em Setembro de 2023.

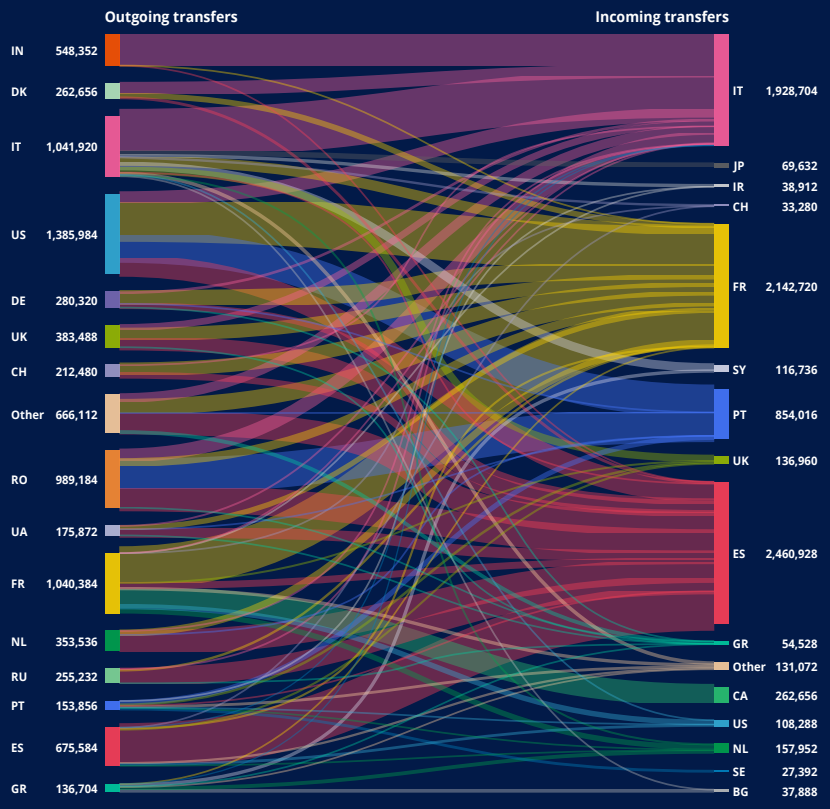
Pedro Verdelho recorda que, estando em vigor a Convenção de Budapeste, "Portugal opôs-se ao início da negociação de um novo tratado nesta área, considerado desnecessário. Porém, tendo a votação da maioria dos Estados Membros da ONU sido no sentido da necessidade de discussão de um tal tratado, Portugal aderiu ao processo, voluntariando-se para ser vice-presidente do Comité", lugar que foi atribuído ao embaixador Almeida Ribeiro (ver "3 Perguntas a...", pág. 20). ■

-president of the Committee', a place assigned to Ambassador Almeida Ribeiro (see '3 Questions to...', page 20). ■

RIPE NCC Internet Country Report: Mediterranean Europe | **2021**

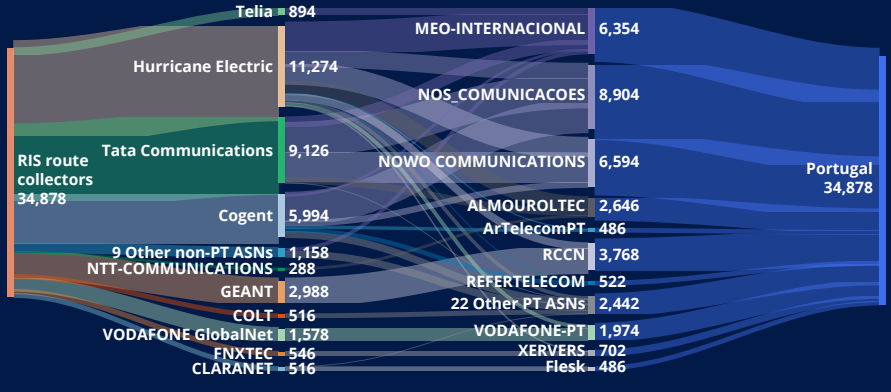
Transferências IPv4 na Europa Mediterrânica entre dezembro de 2016 e maio de 2021

IPv4 transfers within, into and out of Mediterranean Europe between December 2016 and May 2021



Interconectividade internacional de Portugal

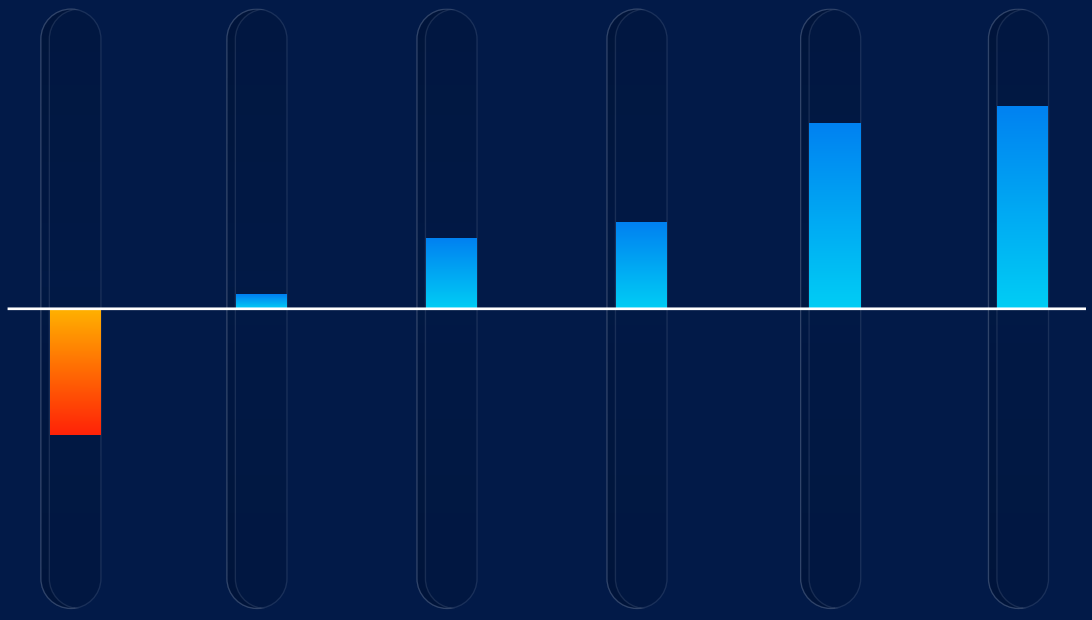
Portugal's international connectivity



As principais ciberameaças em 2020

Main cyberthreats in 2020

MALWARE ATTACKS	ENCRYPTED THREATS	INTRUSION ATTEMPTS	CRYPTOJACKING ATTACKS	RANSOMWARE ATTACKS	IoT ATTACKS
5.6 Billion	3.8 Million	4.8 Trillion	81.9 Million	304.6 Million	56.9 Million



- 43%	+ 4%	+ 20%	+ 28%	+ 62%	+ 66%

Fonte: 2021 SonicWall Cyber Threat Report

3

Pedro Verdelho

Coordenador do Gabinete Cibercrime da PGR
Coordinator of the Cybercrime Office at the Prosecutor General's Office

1. Perante os desafios tão mutáveis do cibercrime, não considera existir demasiada legislação em países e organizações internacionais para agir sobre os responsáveis pelos ciber-ataques?

O combate ao cibercrime supõe a existência de legislação nacional, que puna os comportamentos criminosos. Sem legislação específica, este tipo de atos não será considerado crime e, portanto, não será punido.

Além disso, por esta forma de criminalidade ser, pela sua própria natureza, internacional (exigindo, pois, a sua investigação, recurso à cooperação entre os países), é importante que as diversas legislações, nos diversos países, sejam similares, de forma que a cooperação possa ser efetiva. Sem leis semelhantes, ou pelo menos compatíveis, os países não podem cooperar: um país não pode cooperar com outro se o crime que estiver a ser investigado no outro não for igualmente crime no primeiro.

1. Given the changing challenges of cybercrime, don't you think that there is too much legislation in countries and international organisations to act against those responsible for cyberattacks?

The fight against cybercrime presup-poses the existence of national legislation, which punishes criminal behaviour. Without specific legislation, such acts will not be considered a crime and therefore will not be punished.

Furthermore, as this form of crime is, by its very nature, international (thus requiring its investigation, resorting to cooperation between countries), it's important that the various legislations in the various countries are similar, so that cooperation can be effective. Without similar, or at least compatible, laws, countries cannot cooperate: one country cannot cooperate with another if the crime being investigated in the other isn't also a crime in that first one.

To this extent, it's important that there are international treaties between countries that facilitate, on the one hand, the adoption of similar internal legislation and, on the other, that establish specific cooperation mechanisms. In this regard, it's essential to refer to the Budapest Convention on Cybercrime, the only binding international instrument in this area. 67 countries around the world

Nesta medida, é importante a existência de tratados internacionais entre os países, que facilitem, por um lado, a adoção de legislações internas similares; por outro, que instituam mecanismos de cooperação específicos nesta área. A este respeito, é essencial referir a Convenção de Budapeste sobre cibercrime, o único instrumento internacional vinculativo nesta matéria. Aderiram a ela 67 países do mundo (e estão em processo de adesão outros 10). O texto da Convenção tem sido usado por muitos outros (mais que uma centena) como modelo legislativo interno.

2. Integrando o Comité Ad-Hoc para esta iniciativa, o que se pode esperar de uma convenção da ONU nesta área, que apenas será apresentada na 78ª sessão da Assembleia Geral das Nações Unidas em Setembro de 2023?

Estando em vigor a Convenção de Budapeste, tratado internacional moderno e eficaz para potenciar o combate ao cibercrime (e que, além do mais, está dotado de um sólido conjunto de direitos dos cidadãos e salvaguardas quanto à investigação criminal e ao respeito pelas garantias fundamentais), Portugal opôs-se ao início da negociação de um novo tratado nesta área, considerado desnecessário. Porém, tendo a votação da maioria dos Estados Membros da ONU sido no sentido da necessidade de discussão de um tal tratado, Portugal aderiu ao processo, voluntariando-se para ser

have ratified it (and another 10 are in the process of also joining). The Convention's text has been used by many others (more than a hundred) as an internal legislative model.

2. As part of the Ad-Hoc Committee for this initiative, what can be expected from a UN convention in this area, which will only be presented at the 78th session of the UN General Assembly in September 2023?

With the Budapest Convention in force, a modern and effective international treaty to promote the fight against cybercrime (and which, moreover, has a solid set of citizens' rights and safeguards on criminal investigation and respect for fundamental guarantees), Portugal opposed the start of negotiations on a new treaty in this area, which was considered unnecessary. However, since the majority of UN Member States voted to discuss said treaty, Portugal joined the process, volunteering to be Vice-president of the Committee, to which it was later assigned. Portugal is therefore constructively engaged in this process. The positions adopted and internationally defended by Portugal have been articulated and coordinated with the Member States of the European Union and the States Party to the Budapest Convention (Council of Europe Convention, of which 46 Member States, 45 are Parties to the Convention).

Vice-Presidente do Comité, lugar para o qual foi designado. Portugal está, portanto, construtivamente empenhado neste processo. As posições adotadas e internacionalmente defendidas por Portugal têm sido articuladas e coordenadas com os Estados Membros da União Europeia e os Estados Parte da Convenção de Budapeste (convenção com origem no Conselho da Europa, de cujos 46 Estados Membros, 45 são Parte da Convenção). O Comité Ad-Hoc tem, pois, a tarefa difícil de, por um lado, criar na ONU um "standard" na área do cibercrime, equiparado ao que foi contruído na Convenção de Budapeste: os Estados Parte da Convenção de Budapeste não quererão aderir a um novo tratado mais modesto, nos seus objetivos. Mas por outro lado, o Comité Ad-Hoc tem o desafio de não diminuir (senão o de aumentar) o nível de garantias e salvaguardas dos cidadãos. É, porém, sabido que alguns países pretendem incluir neste novo tratado severas limitações ao direito de livre utilização, pelos cidadãos, das redes de comunicações, abrindo assim portas ao controlo e censura da Internet.

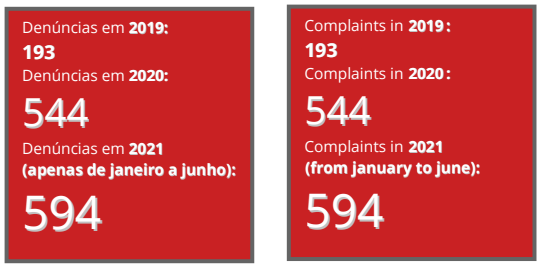
3. Quais foram os principais desafios e eventos na cibersegurança detectados este ano pelo Gabinete Cibercrime da PGR?

Quanto aos desafios na área do cibercrime identificados pelo Gabinete Cibercrime sugere-se a consulta do relatório "Cibercrime em 2021 (1º Semestre)".

The Ad-Hoc Committee has the difficult task of, on the one hand, creating, at the UN, a 'standard' in the area of cybercrime, equated with what of the Budapest Convention: the States Party to the Budapest Convention will not want to join to a new, more modest treaty in their objectives. However, on the other hand, the Ad-Hoc Committee has the challenge of not reducing (but increasing) the level of guarantees and safeguards for citizens. It is well known, however, that some countries want to include severe restrictions on the right of citizens to freely use communications networks in this new treaty, thereby opening the door to Internet control and censorship.

3. What were the main challenges and events in cybersecurity detected this year by the Cybercrime Office at the Prosecutor General's Office?

Regarding the challenges in the area of cybercrime identified by the Cybercrime Office, I refer to the 'Cybercrime in 2021 (1st Semester)' report.



Fonte/Source: Gabinete Cibercrime da PGR

DNSSEC

(DNS Security Extensions)

Eduardo Duarte

Diretor Técnico do .PT
Technical Director of .PT

Nos anos 80 surgiu um dos mais importantes protocolos de comunicação de base na Internet, o Domain Name System (DNS). Este sistema permite a qualquer utilizador aceder a um website ou enviar um email através de um nome de domínio sem ter de memorizar o endereço IP associado a esse serviço.

Como tantos outros protocolos desenhados no início dos anos 80, quando a Internet não tinha a dimensão que conhecemos hoje, a especificação do DNS dá primazia à performance, escalabilidade e redundância em detrimento dos mecanismos de segurança.

Em 2008, Dan Kamisky identificou uma vulnerabilidade que expôs uma falha grave no protocolo DNS e que exigiu da comunidade um "quick fix" para este problema. A exploração maliciosa desta vulnerabilidade tinha como objetivo, através de "cache poisoning", induzir em erro os utilizadores da Internet, alterando os registos de DNS no "resolver", e redirecionando-os a consultar websites, serviços de e-mail ou outros de modo fraudulento. No entanto, este "quick fix" não resolve na totalidade a vulnerabilidade e a solução para esta falha já existia. Estava, contudo, pouco disseminada na comunidade tendo a sua utilização sido fortemente impulsionada nesta altura. Refiro-me às extensões de segurança ao DNS, designadas por DNSSEC (DNS Security Extensions).

In the 1980s, one of the most important communication protocols on the Internet, the Domain Name System (DNS), was created. This system allows any user to access a website or send an email via a domain name without having to store the IP address associated with that service.

Like so many other protocols designed in the early 1980s, when the Internet was not as ample as we know it today, the DNS specification gives priority to performance, scalability and redundancy to the detriment of security mechanisms.

In 2008, Dan Kamisky identified a vulnerability that exposed a serious flaw in the DNS protocol and required a 'quick fix' to the problem by the community. The malicious exploitation of this vulnerability aimed, through cache poisoning, to mislead Internet users by changing the DNS resolver records and redirecting them to consult websites, email services or others in a fraudulent way. However, this 'quick fix' did not fully resolve the vulnerability and the solution to this failure already existed. It was, however, poorly disseminated in the community and its

Mas o que é o DNSSEC? Como referido, o sistema DNS no seu desenho original tinha muito poucas considerações de segurança. O DNSSEC nasce com o objetivo de melhorar a sua confiabilidade, acrescentando uma cadeia de assinaturas criptográficas que parte da raiz, sendo a raiz a única chave universalmente confiável, obtendo-se desta a confiança de todas as outras chaves de segurança. Este conjunto de chaves gera para cada registo de DNS uma assinatura única, possível de validar usando uma lógica de criptografia assimétrica. Refira-se, que ao contrário do que aconteceu na maioria dos protocolos, nomeadamente o HTTP, a segurança não foi obtida adicionando encriptação ao canal de comunicação, mas antes, tendo em conta que a informação do DNS é pública, acrescentando assinaturas aos registos de forma a ser possível validar que a informação não foi alterada em trânsito. Os ganhos para a segurança não têm sido um argumento suficientemente forte para a adoção de DNSSEC já que a sua adição a uma zona de DNS resulta na introdução de maior complexidade na gestão típica do DNS, por exigir processos de re-assinatura dos registos e rotação de chaves. Esta complexidade sempre foi uma barreira à disseminação do DNSSEC e constitui um dos principais desafios dentro da comunidade DNS. Tem sido difícil sensibilizar os administradores de sistemas e gestores técnicos para a adoção das extensões de segurança ao DNS quando pondera a complexidade da sua gestão versus o ganho de

use was strongly promoted at this time. I am referring to DNSSEC, the DNS security extensions.

But what is the DNSSEC? As we mentioned above, the DNS system in its original design had very few security considerations. The DNSSEC was born with the aim of improving its reliability, adding a chain of cryptographic signatures that starts from the root, the root being the only universally reliable key, obtaining from it the confidence of all other security keys. This set of keys generates a unique signature for each DNS record, possible to validate using an asymmetric encryption logic. It should be noted that, unlike most protocols, such as HTTP, security was not obtained by adding encryption to the communication channel, but rather by taking into account that DNS information is public, adding signatures to the records for validation that the information has not been changed in transit. The gains for security have not been a strong enough argument for the adoption of DNSSEC since its addition to a DNS zone results in the introduction of greater complexity in typical DNS management by requiring re-signing processes of the records and rotation of keys. This complexity has always been a barrier to the dissemination of DNSSEC and is one of the major challenges within the DNS community. It has been difficult to raise the awareness of system administrators and technical

segurança. Este contexto justifica que, apesar do DNSSEC ter sido desenhado em 1999, e de ter sido conhecida, em 2008, uma vulnerabilidade que expunha uma falha grave no DNS, só no ano de 2010 é que a zona raiz foi assinada com DNSSEC, e somente após essa data esta extensão de segurança foi totalmente habilitada e operacionalizada, permitindo, a título de exemplo, que o .PT assinasse a sua zona em 2010 e o .COM em 2011. Neste sentido, ainda que a raiz e os TLDs tenham feito um bom caminho até hoje, os donos dos domínios continuam sem grandes incentivos para assinar os seus domínios. À semelhança do que acontece com a generalidade dos ccTLDs, também na zona .PT verifica-se a baixa penetração do DNSSEC, com cerca de 3% de domínios assinados. Não obstante as dificuldades, a comunidade DNS tem vindo a desenvolver várias ações para melhorar a adoção do DNSSEC desde a sua promoção até à melhoria dos processos de assinatura, com a automação dos mesmos. Temos também assistido à evolução de outros protocolos como o DKIM e o DMARC os quais requerem que a zona DNS esteja assinada para serem totalmente eficazes e consequentemente têm também contribuído para o aumento das assinaturas DNSSEC. Desde sempre, o .PT tem acompanhado as melhores práticas e desenvolvido inúmeras ações com vista à promoção do DNSSEC, mantendo-se disponível para apoiar a comunidade da Internet na adoção desde protocolo. ■

managers to the adoption of security extensions to DNS when considering the complexity of its management versus the security gain. This context justifies that, although the DNSSEC was designed in 1999 and a vulnerability that exposed a serious flaw in the DNS was known in 2008, it was not until 2010 that the root zone was signed with DNSSEC, and only after that date was this security extension fully enabled and operationalised, allowing, as an example, that .PT signed its zone in 2010 and .COM in 2011. In this sense, although the root and the TLDs have come a long way, domain owners still do not have much incentive to sign their domains. As with most ccTLDs, the .PT zone also has a low DNSSEC penetration, with about 3 % of domains signed. Despite the difficulties, the DNS community has been developing several initiatives to improve the adoption of the DNSSEC, from its promotion to the improvement of the signature processes, with their automation. We have also seen the development of other protocols such as DKIM and DMARC which require the DNS zone to be signed in order to be fully effective. They have also contributed to the increase of DNSSEC signatures. .PT has always followed the best practices and developed numerous actions to promote the DNSSEC, remaining available to support the Internet community in the adoption of this protocol. ■

Mais informações ou formação especializada sobre a implementação de DNSSEC, contacte-nos através do email info@dnssec.pt
More information or specialised training on DNSSEC implementation, please contact us at info@dnssec.pt

Global Cybersecurity Index 2020

Portugal subiu 28 lugares para a 14ª posição no Global Cybersecurity Index (GCI), uma iniciativa da International Telecommunication Union (ITU), posicionando-se entre a Alemanha e a Letónia. Na região europeia, o país ocupa o 8ª lugar. No anterior relatório, relativo a 2018, Portugal estava em 25º em termos europeus e em 42º a nível global na cibersegurança.

Portugal rose 28 places, placing 14th in the Global Cybersecurity Index (GCI), an initiative of the International Telecommunication Union (ITU), ranking between Germany and Latvia. In Europe, the country ranks 8th. In the previous report for 2018, Portugal was 25th amongst European countries and 42nd globally in cybersecurity.

Gartner Top Security and Risk Trends for 2021

Entre oito medidas propostas, o relatório da consultora Gartner sobre tendências de risco e segurança antecipa a necessidade de colocar um especialista em cibersegurança na administração das organizações, até porque, "em 2023, 30% da eficácia dos CISO será medida diretamente na capacidade da função de criar valor para o negócio".

Among eight measures put forward, Gartner consultant's report on risk and security trends anticipates the need to place a cybersecurity expert in the administration of organizations, not least because, 'by 2023, 30 % of CISO's effectiveness will be directly measured on the ability to create value for the business.'

Perigo nos subdomínios Subdomains in danger

Investigadores da TU Wien e da Ca' Foscari University descobriram uma nova vulnerabilidade de segurança que passa pelo abuso dos subdomínios como "sub.example.com" a partir de "example.com". Asseguram que "é possível assumir o controlo de tais subdomínios", após detetarem 1.520 subdomínios vulneráveis num exame a 50 mil dos endereços Web mais importantes.

Researchers at TU Wien and Ca' Foscari University have uncovered a new security vulnerability, where it's possible to take control of subdomains such as 'sub.example.com' from 'example.com'. They assure that 'it's possible to take control of such subdomains', after detecting 1 520 vulnerable subdomains following an examination carried out to 50 000 of the most important websites.

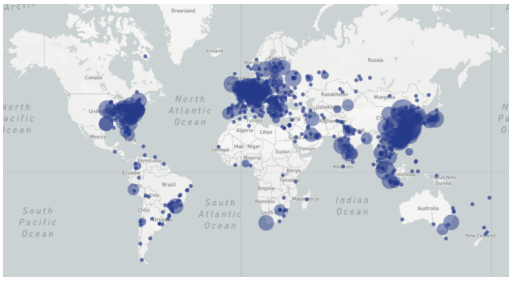
Ajuda para mitigar ataques de ransomware Help in mitigating ransomware attacks

O valor dos resgates pagos no primeiro semestre do ano por ataques de ransomware aproximou-se dos 40 milhões de dólares, segundo o Ransomwhere. Para ajudar a testar a eficácia das redes, a Cybersecurity and Infrastructure Security Agency (CISA) lançou o Ransomware Readiness Assessment, enquanto o National Institute of Standards and Technology (NIST) publicou um conjunto de recomendações para evitar estes ataques.

According to Ransomwhere, the value of ransoms paid in the first half of the year for ransomware attacks was close to $40 million. To help test the effectiveness of the Networks, the Cybersecurity and Infrastructure Security Agency (CISA) launched the Ransomware Readiness Assessment, while the National Institute of Standards and Technology (NIST) released a set of recommended practices to avoid these attacks.

Bases de dados expostas Exposed databases

Milhares de bases de dados (BDs) foram divulgadas na Internet, com mais de 60 a serem atribuídas a Portugal, numa análise dos RedHunt Labs. A fraca segurança e BDs não-autenticadas mas ligadas à Internet são algumas das razões para este panorama que resulta em dados expostos em público: Portugal tem registos com a Memcached (30 casos), Elasticsearch (15), Redis (9), MongoDB (5) e RethinkDB (2).



According to a Redhunt Labs analysis, thousands of databases were exposed on the Internet, with more than 60 from Portugal. Poor security and unauthenticated databases connected to the Internet are some of the reasons for this scenario that results in publicly exposed data: Portugal holds records with Memcached (30 cases), Elasticsearch (15), Redis (9), MongoDB (5) and RethinkDB (2).

Directora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design gráfico | Graphic design
Sara Dias

Tradução | Translation
Sara Pereira

Fotografia (capa e índice) | Photography (cover & index)
Maximalfocus

Publicação trimestral | Quarterly publication
Setembro 2021 | September 2021

Cofinanciado pelo Mecanismo Interligar a Europa - União Europeia