BOLETIM TERTÚLIA

Encontros e Reflexões

SEGURANÇA E DEFESA EUROPEIA

VOLUME 2

CIBERSEGURANÇA

PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

COM O APOIO

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

Índice

Editorial

Dando cumprimento aos objetivos de afirmação e participação da comunidadejovem portuguesa no debate sobre as matérias de segurança e defesa europeia,surge, no âmbito da produção da 4ª Edição das Tertúlias EDJ, o respetivoBoletim Tertúlia.
Procurando cumprir os objetivos a que as Tertúlias EDJ se propuseram, desde o momento da sua criação, tais como: (1) criar debates relevantes e reflexões sobre as matérias de segurança e defesa europeia, (2) promover o encontro e debate geracional da EuroDefense Portugal com os jovens, (3) promover o diálogo e interação com organismos relevantes, e também atividades no seio académico, o Boletim Tertúlia pretende dar continuidade aos mesmos, convidando todos os interessados a produzir um debate escrito sobre os tópicos discutidos durante as Tertúlias. Desta forma, não só se sublinha a importância que as Tertúlias têm, como meio eficaz de produção e discussão de conhecimento, como também se afirmam enquanto um meio de debate geracional e académico de matérias de Segurança e Defesa.

O presente, e segundo volume dará conta da terceira Tertúlia, inserida na 4ª Edição das mesmas, onde se abordou, através da participação do Professor Doutor João Rucha Pereira e do Engenheiro Paulo Moniz, o imenso universo dos desafios que gere o debate pela segurança cibernética das nossas sociedades, cada vez mais vulneráveis a ataques malfeitores a infraestruturas críticas, constituídas com base nos sistemas de gestão digitais.

Resta-me apenas desejar ao caro(a) leitor(a) uma boa leitura e convidar a participar nas futuras Tertúlias e Volumes deste Boletim Tertúlia.

Com elevada consideração e amizade,
Vitaliy Venislavskyy
Presidente EuroDefense-Jovem Portugal

O desafio da guerra cibernética na defesa das infraestruturas críticas

Diogo Alexandre Carapinha, Univ. Autónoma de Lisboa

Resumo

O século XXI viu surgir uma guerra que permite a Estados e atores não-Estatais combater sem armas. O ciberespaço é, assim, o novo campo de batalha, onde os ataques cibernéticos podem ter efeitos comparáveis aos das armas de guerra de outrora. Estes ataques são parte integrante dos conflitos internacionais contemporâneos e têm uma vasta influência na geopolítica e nas relações internacionais, sendo inegável a necessidade de tomar medidas eficazes de cibersegurança.

Palavras-Chave: Ciberguerra; Ciberataques; Infraestruturas Críticas; Segurança

1. Introdução

Os ataques terroristas de 11 de setembro de 2001 mudaram a História e despertaram um clima que não se esperava após a queda do muro de Berlim. Este clima é de insegurança e apreensão, com vulnerabilidades manifestas nos sistemas de defesa, até dos Estados mais poderosos. Adicionalmente, o século XXI viu surgir uma guerra diferente: uma que permite combater sem armas.

O ciberespaço é o novo campo de batalha, onde Estados podem – de forma relativamente fácil e barata – desenvolver um ataque cibernético com efeitos comparáveis aos das armas de guerra de outrora. Todavia, nem só os Estados se movimentam neste espaço. Aqui, há grupos de *hackers* de várias nações que se dedicam a provocar a maior disrupção possível. Desta forma, hoje, a maior ameaça que enfrentamos pode ser oriunda de um indivíduo com más intenções, que possui um computador portátil e a vontade de causar danos.

A guerra cibernética pode considerar-se entre as maiores ameaças à Segurança Nacional da nossa nação, tendo António Guterres, Secretário-Geral da ONU, sublinhado esta mesma preocupação. A verdade é que as possibilidades que um ciberataque bem-sucedido pode alcançar são inquietantes. Uma arma cibernética pode, por exemplo, extinguir toda a rede elétrica de uma cidade, o que, numa sociedade altamente conectada – como é a nossa – terá monstruosas repercussões.

Contemplemos o seguinte exemplo: Lisboa apaga. Primeiramente, todos os bancos fecham, o multibanco deixa de funcionar e instala-se o pânico quando todos se esforçam para levantar dinheiro e não o conseguem fazer. Subsequentemente, as estações de tratamento de águas residuais deixam de funcionar, não havendo água limpa. Ademais, imaginando um ataque semelhante direcionado às forças armadas nacionais – desligando o seu GPS e a sua rede de computadores – estas ficariam essencialmente incapazes de operar, demorando dias ou semanas até se recuperar o controlo. O pânico em massa seria total.

2. A conceptualização

Após esta breve introdução aos potenciais resultados da guerra cibernética, importa agora perceber o que se entende concretamente pelo conceito. Ora, este termo ganhou destaque nos últimos anos e refere-se à utilização da tecnologia digital e da Internet para travar

guerras, efetuar espionagem e perturbar as operações de Estados, organizações e indivíduos. Embora ofereça novas perspetivas para atingir metas militares, políticas e económicas, levanta também várias questões e preocupações.

Em primeiro lugar, há uma enorme dificuldade em atribuir os ataques a atores específicos, uma vez que estes podem ser lançados de qualquer parte do mundo, com um certo grau de anonimato, ao contrário do que acontece numa guerra convencional. Além de dificultar uma resposta eficaz, esta dimensão complica a tarefa de antecipação e prevenção dos ataques. Em segundo lugar, devido à complexidade do mundo digital, os danos colaterais e resultados imprevistos que estão em causa são inúmeros. Por exemplo, uma operação cibernética que vise perturbar a rede elétrica de um adversário pode inadvertidamente afetar infraestruturas críticas, afetando indivíduos inocentes. Adicionalmente, face à sua crescente dependência nas infraestruturas digitais e na Internet, a sociedade contemporânea – países, organizações e indivíduos – encontra-se especialmente vulnerável a ataques cibernéticos, sendo o potencial impacto de uma ciberguerra amplificado por esta interconexão. É importante referir que os efeitos de uma ciberguerra são longos, uma vez que um ciberataque bem-sucedido tem o potencial de perturbar sistemas vitais, prejudicar as economias e quebrar a confiança do público.

Uma outra questão alarmante é que a própria definição do que constitui um ato de guerra no domínio cibernético é relativamente indefinida, sendo que a falta de quadros legais dificulta a dissuasão dos agentes maliciosos. Da mesma forma, sendo que muitas das ferramentas e tecnologias utilizadas na guerra cibernética podem ser usadas tanto para fins ofensivos quanto defensivos, a distinção entre espionagem e operações de *intelligence* passa a ser uma tarefa difícil. Além disso, os Estados podem justificar o desenvolvimento das suas capacidades defensivas em prol da Segurança Nacional, acabando a usá-las para fins agressivos.

Uma vez que o quadro legal e ético para o ciberespaço se encontra em desenvolvimento – não havendo consenso sobre o que é um comportamento aceitável no ciberespaço e como as leis internacionais devem ser aplicadas – é consideravelmente difícil atribuir responsabilidade aos cibercriminosos pelas suas ações. Ao erodir a confiança na implementação das normas, a guerra cibernética tem o potencial de abalar a confiança na própria soberania dos Estados.

Antes de explorar a evolução da ameaça cibernética e as suas implicações na Segurança Nacional, uma breve História da ciberguerra é pertinente. Estudar esta História permite compreender que os ciberataques são cada vez mais comuns e estão cada vez mais sofisticados.

Numa fase inicial, com o surgimento das redes informáticas na década de 1980, o conceito de ciberguerra começa a ganhar forma. Uma das primeiras ocorrências de *software* malicioso foi em 1982 quando os computadores Apple II foram infetados pelo vírus informático "Elk Cloner". Similarmente, o "Morris Worm" causou também problemas em milhares de computadores no final dessa década, demonstrando a possibilidade de ciberataques amplos. Não muito depois, durante a Segunda Guerra do Golfo (1990-1991), o Iraque realizou alguns dos primeiros ataques cibernéticos patrocinados pelo Estado. Todavia, embora tenham tentando, os atores não conseguiram interferir nos sistemas de comunicação militar dos EUA. Mais tarde, em 2007, a Estónia foi alvo de um ataque de negação de serviço distribuído (DDoS) em resposta à deslocação de um memorial de guerra da Era Soviética que prejudicou gravemente o seu governo e sistema financeiro. No seguimento deste ataque, o risco de ciberataques entre Estados aumentou consideravelmente. Em 2009, uma série de ciberataques a grandes empresas norte-americanas, incluindo a Google, ficou conhecida como Operação Aurora. Esta Operação foi atribuído à China e visou roubar propriedade intelectual e informações confidenciais, tendo levantado dúvidas sobre a espionagem industrial patrocinada pelo Estado chinês. Pouco depois, em 2010, foi lançado um dos mais conhecidos ataques cibernéticos da História, o Stuxnet. Este *malware* foi projetado para atingir as instalações nucleares (físicas/cinéticas) do Irão e é tido como um exemplo de que os ciberataques podem causar danos físicos à infraestrutura vital de um Estado.

Mais recentemente, entre 2015 e 2017, a Ucrânia foi alvo de vários ciberataques, incluindo um que visou a sua rede elétrica e um que utilizou o *ransomware* NotPetya. Estes eventos foram associados à Rússia e ilustraram a possibilidade de os ciberataques prejudicarem serviços públicos essenciais. Em 2016, piratas informáticos russos invadiram os servidores de correio eletrónico do Comité Nacional Democrata durante as eleições presidenciais americanas roubando endereços de *email*, o que levantou preocupações sobre a presença de Estados-terceiros no processo democrático norte-americano. Em 2017, os *ransomware* WannaCry e NotPetya causaram danos a empresas

e pessoas em todo o mundo, havendo análises recentes que indicam que os ataques podem ter visado objetivos políticos relacionados a atores Estatais. Por último, em 2020, o ciberataque da SolarWinds atingiu a cadeia de abastecimento de várias agências e empresas estadunidenses. Havendo suspeitas do envolvimento de um grupo patrocinado pelo Estado russo, este é considerado um dos incidentes de ciberespionagem mais importantes da História.

A ciberguerra é uma área em constante mudança e com vasta influência na geopolítica e nas relações internacionais, sendo que a História dos ciberataques acima apresentada demonstra a necessidade de tomar medidas eficazes de cibersegurança. É inegável que a ameaça cibernética tem evoluído significativamente ao longo do tempo, transformando-se numa das preocupações mais prementes em todo o mundo.

A proteção contra ameaças cibernéticas exige uma abordagem multidimensional que envolva não apenas governos, mas também o setor privado e a comunidade internacional. Além disso, um esforço cooperativo internacional robusto e eficaz é essencial para desenvolver normas e acordos que regulem o ciberespaço e combatam as ameaças e agentes cibernéticos. A capacidade de adaptação é crucial para garantir segurança no mundo digital, sendo, para isso, necessário perceber que ameaças estão em jogo e que implicações estas têm para a segurança dos Estados.

As tendências mais recentes apontam para um aumento na sofisticação dos ataques cibernéticos, sendo os cibercriminosos cada vez mais capazes de recorrer a técnicas avançadas de engenharia social, exploração de vulnerabilidades e *malware* personalizado. O *ransomware*, a título de exemplo, tornou-se uma das ameaças mais urgentes a considerar. Similarmente, os alvos têm evoluído de instituições financeiras e empresas para infraestruturas críticas da sociedade, como as redes de energia e água e serviços de saúde. Estes alvos, associados ao envolvimento de Estados-nação – como a Rússia, China, Irão e Coreia do Norte – em atividades cibernéticas ofensivas, torna a ciberguerra numa questão incontestável de Segurança Nacional.

É certo que as implicações para a Segurança Nacional são inúmeras. Com o aumento dos ataques a infraestruturas críticas, a guerra cibernética representa uma ameaça direta à vida quotidiana dos cidadãos e à economia dos países. Da mesma forma, a ciberespionagem está a tornar-se numa ferramenta para Estados recolherem informações estratégicas, o que

pode minar a confiança entre as nações e escalar o conflito cibernético. Hoje em dia, é inegável que a cibersegurança integra a estratégia militar de muitos países e que o ciberespaço é um campo de batalha em potencial.

A ciberesfera tem sido o palco de vários conflitos internacionais contemporâneos. Para melhor compreender as ameaças em causa, abordaremos um dos mais emblemáticos casos de guerra cibernética, analisando as estratégias utilizadas pelos atores Estatais envolvidos e destacando o impacto dos ataques nas operações militares e políticas.

Ora, no conflito entre a Rússia e a Ucrânia – em 2014, antes da Invasão de 2022 – a Rússia realizou vários ataques DDoS que visaram *websites* governamentais e de media ucranianos, dificultando a disseminação de informação e a coordenação das respostas do governo. Ao mesmo tempo, ambos os lados lançaram campanhas de desinformação em grande escala para moldar a narrativa do conflito e atacaram infraestruturas críticas do país rival. A título de exemplo, a Ucrânia direcionou ataques cibernéticos aos sistemas de energia russos, permanecendo o ataque de dezembro de 2015 à Prykarpattya Oblenergo um dos primeiros ciberataques a causar um *blackout* significativo.

Os impactos militares e políticos dos ciberataques na Ucrânia são irrefutáveis. Não só causaram instabilidade política – a desinformação e os ataques a *websites* governamentais afetaram a confiança pública e a coesão nacional – mas desafiaram também as capacidades defensivas, expondo a necessidade de investimento em cibersegurança. É um facto que ambos os lados reconheceram a importância da cibersegurança nas operações militares. Por um lado, a Ucrânia estabeleceu uma nova unidade de guerra cibernética, enquanto a Rússia integrou a cibersegurança nas suas doutrinas militares. Adicionalmente, é importante destacar o potencial de os ataques cibernéticos causarem danos materiais significativos que afetam a população, evidenciando-se a necessidade de proteção das infraestruturas críticas. Da mesma forma, é de salientar que o uso de ataques cibernéticos durante este conflito exacerbou as tensões entre a Rússia, a Ucrânia e a Comunidade Internacional, levantando questões sobre a aplicação do Direito Internacional em conflitos cibernéticos.

3. Conclusão

Este estudo de caso demonstra como os ataques cibernéticos podem desempenhar um papel crucial num conflito internacional, moldando o ambiente político, militar e humanitário. Os efeitos são profundos e evidenciam uma necessidade contínua de desenvolver estratégias de defesa cibernética, promover normas internacionais no ciberespaço e melhor compreender o impacto dos ciberataques nas relações internacionais e na segurança global.

Bibliografia

Geers, Kenneth. "The cyber threat to national critical infrastructures: Beyond theory." *Information Security Journal: A Global Perspective* 18, no. 1 (2009): 1-7.

Harrop, Wayne, and Ashley Matteson. "Cyber resilience: A review of critical national infrastructure and cyber security protection measures applied in the UK and USA." *Journal of business continuity & emergency planning* 7, no. 2 (2014): 149-162.

Maglaras, Leandros A., Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, and Tiago J. Cruz. "Cyber security of critical infrastructures." *ICT Express* 4, no. 1 (2018): 42-45.

Plėta, Tomas, Manuela Tvaronavičienė, Silvia Della Casa, and Konstantin Agafonov. "Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases." *Insights into regional development. Vilnius: Entrepreneurship and Sustainability Center* 2, no. 3 (2020).

Rudner, Martin. "Cyber-threats to critical national infrastructure: An intelligence challenge." *International Journal of Intelligence and CounterIntelligence* 26, no. 3 (2013): 453-481.

Ciberguerra: Defesa das Infraestruturas Críticas

João Rodrigues da Areia Brito da Silva, NOVA IMS

Abstract

This paper addresses the issues of cyber warfare as an increasingly relevant threat with implications at different levels, from loss of life to disinformation; more specifically, it addresses the issue of critical infrastructure and how threats in cyberspace extend to these essential services because of technological development, interconnection and interdependence that are characteristic of today's globalized world.

The topics were analyzed with a focus on Europe, and how the conflict between Ukraine and Russia has given new importance to cyber defense and raised new concerns regarding cyber-attacks in the European Union (EU). At the end, the EU's response to this threat was analyzed, including the different mechanisms (namely the NIS2 directive) and entities (ENISA) involved, which demonstrates a clear priority on the part of the Union, and the member states, to deal with threats to Europe and its citizens in the field of technology.

Keywords: Cyberwarfare; Cyber Defense; Critical Infrastructure; European Union; Europe; Ukraine; Russia

1. Introdução

À medida que o nosso mundo se torna cada vez mais dependente da tecnologia, governos e organizações em todo o mundo estão cada vez mais preocupadoscom a possibilidade de guerras cibernéticas e danos ainfraestruturas essenciais. O funcionamento da sociedade contemporânea é apoiado por serviços vitais, que incluem redes elétricas, sistemas bancários, e redes de transporteque, devido à sua interligação, são também suscetíveis a ciberataques que podem desestabilizar e/ou paralisar países, espalhar desinformação, ser usados como ferramenta de espionagem, entre outros. Este trabalho irá discutir a ideia da ciberguerra, no período da última década, especialmente nos últimos três anos,e como esta se relaciona com o tema das infraestruturas críticas, bem como as medidas que estão a ser tomadas para fazer face a esta realidade, no espaço europeu.

2. Ciberguerra

O rápido desenvolvimento das tecnologias de informação e comunicação nas últimas décadas criou oportunidades para conflitos militares. A guerra cibernética, a utilização de ataques digitais para perturbar ou danificar sistemas informáticos, surgiu como umanova dimensão da guerra no século XXI. As dimensões da guerra cibernética são multifacetadas, desde aspetostécnicos a estratégicos e sociais.Para podermos proceder a uma análise sobre a Ciberguerra,ou *Cyberwarfare*, no Espaço Europeu, e mais especificamente o que é que isso significa em termos de defesa das infraestruturas críticas, é preciso definir os conceitos para melhor compreensão do tema.

Em primeiro lugar, quando se fala em Ciberguerra existem diversos pontos de vista em relação a como a definir. Uma definição possível é “Cyber Warfare is typically defined as a set of actions by a nation or organization to attack countries or institutions' computer network systems with the intention of disrupting, damaging, or destroying infrastructure by computer viruses or denial-of-service attacks.”(Fortinet, 2023) ou seja, uma perspetiva da ciberguerra como um conjunto de ações, por parte de Estados ou atores não estatais, no ciberespaço, com o objetivo de provocar danos em infraestruturas de Estados ou instituições.

Outra definição é "Cyberwarfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems."(Fred Schreier, 2015) Existem outras formas de definir o conceito de ciberguerra, mas todas concordam que se trata de ações com intenção maliciosa no ciberespaço contra as infraestruturas de um Estado.

A ciberguerra tem vindo a ser cada vez mais relevante como forma de conflito ou ingerência entre Estados. A utilização dos meios digitais e a expansão de atividades militares (ofensivas ou defensivas) no ciberespaço apresenta múltiplas vantagens, nomeadamente, o custo reduzido em termos de recursos (monetários, materiais e humanos) envolvido nestas operações em comparação com os recursos convencionais de defesa. Para executar campanhas de ciberguerra não é necessário um elevado número de tropas e de equipamento, qualquer pessoa com acesso a um computador e internet está equipado para participar em operações desta natureza; o facto destas ações se realizarem pela internet permitem maior anonimato e sigilo, o que permite muitas vezes aos Estadosnegação plausível (*plausible deniability*), ou seja, permitem aos Estados negar qualquer envolvimento nas ações; a proliferação dos meios e ferramentas que permitem fazer ataques informáticos é descontrolada e estes são facilmente acessíveis pela internet.

O facto de tudo acontecer no ciberespaço, o quinto campo de batalha (depois da terra, água, ar e espaço) que não é palpável nem visível, faz com que muitas vezes as intrusões passem despercebidas permitindo monitorizações, espionagem, *leaks* de informações, etc. Por sua vez as ramificações destas intrusões podem resultar em destruição de infraestruturas e disrupção de serviços essenciais, obtenção de dados sensíveis e/ou confidenciais sobre essas infraestruturas, o aparelho de defesa do Estado e da população em geral. Estas informações podem ainda ser usadas e alteradas pelo atacante para lançar uma campanha de desinformação.

Com a aceleração do processo de globalização, o uso das tecnologias de informação e a automatização de processos de produção aumentou também, o que inevitavelmente levou a uma maior relevância do campo das tecnologias e à exploração das mesmas com objetivos maliciosos. Quanto maior a dependência e proliferação dos sistemas informáticos e redes aumentam os vetores de risco associados a essas. De acordo com a ENISA (*European Union Agency for Cybersecurity*), no relatório *ENISA Threat Landscape 2022*, em 2021 e 2022, os

ciberataques aumentaram em número e em quantidade de vetores.(European Union Agency for Cybersecurity., 2022)

O relatório mencionado em cima tem como intuito a análise da situação europeia no campo da Cibersegurança, nomeadamente da "paisagem" quanto às ameaças, entre as quais se encontram: o *ransomware*, a desinformação e *fake news*, e os ataques informáticos às cadeias de abastecimento (*supply chain attacks*). De destacar que, no campo da desinformação e *fake news*, o relatório aponta como maior exemplo o impacto que estas tiveram e continuam a ter no desenrolar do conflito na Ucrânia, como ferramenta de ciberguerra.(European Union Agency for Cybersecurity., 2022)

Ainda no âmbito do relatório da ENISA, entre julho de 2021 e junho de 2022, na União Europeia, os dados mostram que os dois setores mais afetados fora o da Administração Pública e dos Serviços Digitais. Em termos dos principais atores relacionados com a cibercriminalidade/ciberguerra, o relatório aponta quatro categorias principais: *state-sponsored actors*, *cybercrime actors*, *hacker-for-hire actors* e *hacktivists*. O meu foco será mais na primeira categoria, por ser aquela que é mais relacionada com a ciberguerra, dado que se trata de organizações diretamente ligadas a Estados.

3. Infraestruturas Críticas

As infraestruturas críticas são os sistemas e redes que são essenciais para o funcionamento das sociedades modernas. Estes incluem sistemas tais como transportes, energia, abastecimento de água, comunicações e finanças. A perturbação ou dano a estas infraestruturas pode ter consequências graves para a economia, saúde pública e segurança, e segurança nacional.

De acordo com a Comissão Europeia, infraestruturas críticas são recursos ou sistemas cuja danificação, por causas naturais ou por atividade maliciosa, teria um impacto significativo na segurança da EU e do bem-estar dos cidadãos europeus.(Home Affairs, 2023)

Uma das principais características das infraestruturas críticas é a sua interdependência. Ou seja, um corte de energia pode afetar não só a rede elétrica, mas também os sistemas de transporte, estações de tratamento de água, hospitais e outros sistemas de

infraestruturas críticas que dependem da eletricidade. Esta interdependência significa que uma única falha ou ataque pode ter um efeito de cascata que tem impacto em múltiplos sectores e sistemas.

Assim, os setores críticos incluem: o setor energético, nomeadamente as centrais e os sistemas que permitem a transmissão de energia; o setor da água; os transportes; comunicações, serviços de emergência (serviços de saúde e de segurança), o setor alimentar (em grande parte relacionado com a distribuição), bem como as áreas relacionadas com as funções mais importantes da administração pública. Cada vez mais é possível considerar o setor financeiro como crítico, visto que sucessivamente aumenta a integração com os setores das comunicações e por ser um pilar das sociedades, ou seja, uma disrupção do setor financeiro regista ramificações em múltiplos outros setores essenciais, ao mesmo tempo, pode ser usada para infligir danos económicos.

Estes setores são fontes preciosas de dados sensíveis dos utilizadores e de informações confidenciais quanto ao estado destas estruturas, que podem ser usadas como intelligence, ou intel, no mapeamento das defesas de um Estado para uma futura ação militar convencional. Essas informações podem ainda ser utilizadas como base para desinformação quanto a intenções que determinado Estado pode ter. Também são alvos muito aliciantes para atacantes estatais, e outras organizações, devido a dimensão dos danos que podem provocar, no caso de ações de sabotagem, ou destrutivas, que impossibilitem a sua CID (Confidencialidade, Integridade e Disponibilidade), que podem ter implicações a níveis estratégicos para os Estados.

4. Panorama Europeu

A 24 de Fevereiro de 2022, a Rússia invade mais uma vez a Ucrânia. Desde então, e até antes da data da invasão, a ciberguerra tem desempenhado um papel fundamental como forma de sabotagem das infraestruturas críticas e na desinformação das populações para efeitos de moralização/desmoralização e como preparação e apoio às atividades militares convencionais no terreno. Isto pode ser observado em ambas as partes participantes do conflito.

No caso da Rússia, de acordo com um relatório da Microsoft(Microsoft, Digital Security Unit, 2022), já a 19 de Janeiro de 2022, cerca de um mês antes da invasão, tinham sido registados ataques informáticos em massa enquanto, em simultâneo, eram encetadas manobras no campo diplomático que se revelaram um fracasso. Os ataques nesta fase tinham como alvo os sites do governo ucraniano e algumas empresas de IT (Information Technology), e o objetivo nesta fase era causar disrupções e destruição de forma a obter concessões por parte do governo de Kyiv, o que não aconteceu. Já nas vésperas da invasão, as operações informáticas ofensivas por parte da Rússia intensificaram-se e vários setores, como o governamental, IT, energia, agricultura, e financeiros ucranianos foram alvos de ataques que resultaram na destruição de mais de 300 sistemas informáticos.

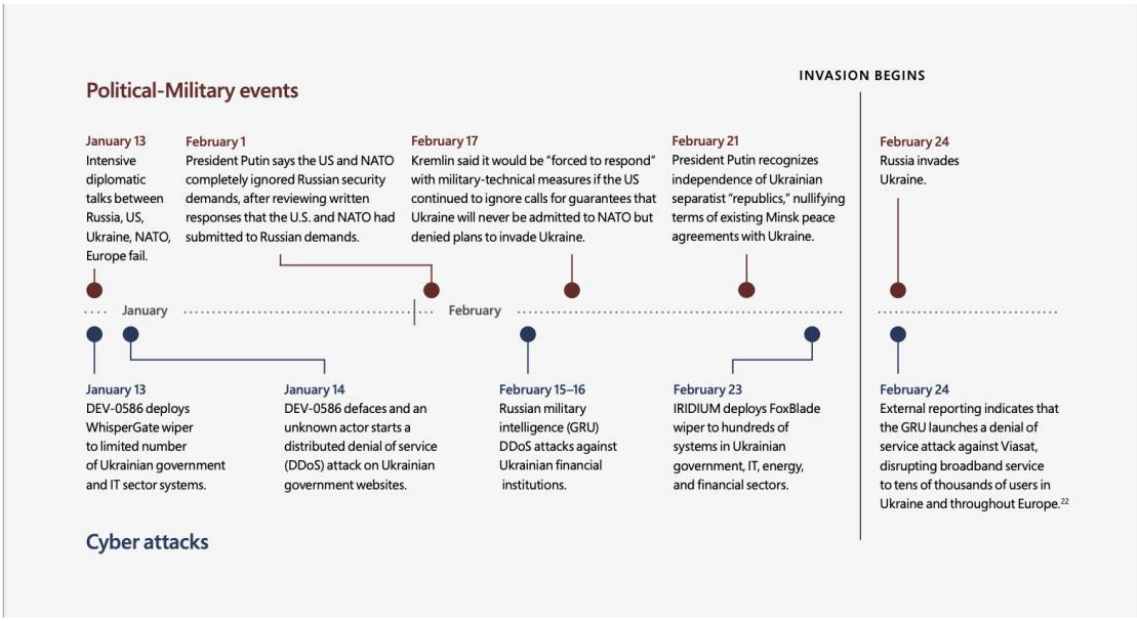


Figura 1 - Cronologia dos Ciberataques e Eventos Políticos Cronologia dos Ciberataques e Eventos Políticos (Microsoft, Digital Security Unit, 2022)(Microsoft, Digital Security Unit, 2022)

Após a invasão, o panorama foi idêntico em termos de ofensivas no ciberespaço. Os ataques contra infraestruturas críticas, por parte de grupos diretamente ligados aos serviços de informações russo, continuaram e muitas vezes em coordenação com as próprias operações militares. Nesta fase, os ataques informáticos pretendiam apoiar as tropas no terreno e/ou degradar e desacreditar o governo, forças armadas e setor financeiro ucranianos (dimensão psicológica).

Segundo o relatório da ENISA (European Union Agency for Cybersecurity., 2022), o início do conflito na Ucrânia também marcou o aumento das ações hostis no ciberespaço

contra os Estados-membro da UE (União Europeia) e da NATO/OTAN (Organização do Tratado do Atlântico Norte) por apoiarem a Ucrânia politica, económica e militarmente, nomeadamente aqueles que estão mais próximos da Rússia. (Anexo A)

No entanto, estas operações não tiveram origem somente a partir da Rússia. Registaram-se operações hostis relacionadas com outros Estados, como a China, como forma de disrupção e ingerência em assuntos internos com o objetivo de prossecução de objetivos estratégicos.

Os Estados europeus têm intensificado a sua colaboração em matéria de segurança cibernética nos últimos anos e reforçado as suas defesas cibernéticas. O Regulamento Geral de Proteção de Dados (GDPR) é uma das iniciativas legislativas que a União Europeia implementou para reforçar a cibersegurança e privacidade. A União Europeia também criou a Agência da União Europeia para a Cibersegurança (ENISA) para ajudar os Estados-Membros da UE na harmonização de medidas de segurança comuns a nível europeu, incluindo na proteção de infraestruturas críticas. Em 2016, a UE já tinha avançado no sentido de se proteger com mais eficácia no ciberespaço, com a aprovação da Diretiva NIS (Network Information Security), que foi a primeira iniciativa vinculativa a todos os Estados-membros da União no que toca a políticas comuns para a proteção de infraestruturas digitais (Thales Group, 2023).

5. Conclusão

A ciberguerra tornou-se uma ameaça cada vez mais significativa para as infraestruturas críticas, tal como demonstrado pelos numerosos ataques cibernéticos que têm visado sistemas críticos nos últimos anos. As consequências de um ataque cibernético bem-sucedido a infraestruturas críticas podem ser graves, desde a interrupção de serviços essenciais, a danos económicos generalizados e perda de vidas humanas. Como resultado, é essencial que governos e organizações do sector privado tomem medidas para melhorar as suas defesas no que toca à cibersegurança e implementem planos de contingência robustos e estratégias para responder a potenciais ataques cibernéticos.

Medidas eficazes de cibersegurança requerem uma abordagem abrangente que aborde os fatores técnicos, operacionais e humanos que contribuem para as vulnerabilidades

cibernéticas. Os governos e organizações do sector privado devem investir em tecnologias de ponta, desenvolver estratégias abrangentes de gestão de risco, e fomentar uma cultura de sensibilização para a cibersegurança entre os seus funcionários, dado que o fator humano é elo mais fraco no que concerne à segurança digital.

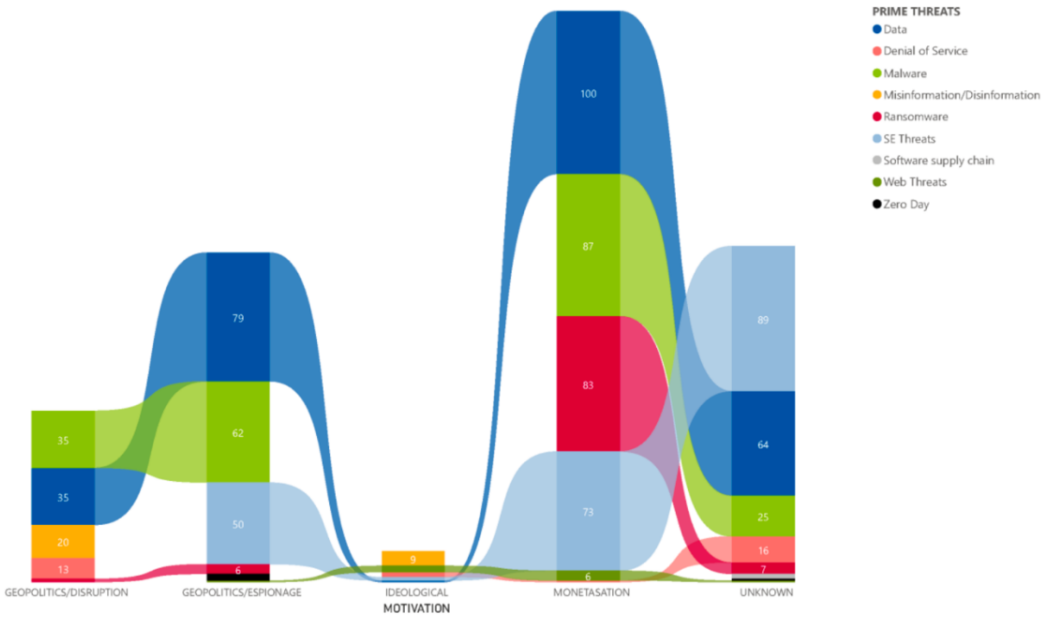
Além disso, a cooperação e a partilha de informação entre governos, empresas privadas e organizações internacionais, como a União Europeia e a NATO podem desempenhar um papel crucial na abordagem da ameaça cibernética às infraestruturas críticas. Ao trabalharem em conjunto e partilharem as melhores práticas, estes intervenientes podem melhorar as suas defesas coletivas de cibersegurança e responder mais eficazmente a potenciais ataques cibernéticos.

De facto, tanto a União Europeia e NATO têm desenvolvido esforços no sentido de acompanhar a tendência crescente da ciberguerra e cibercriminalidade. Todos os dias existem ataques informáticos às mais variadas instituições públicas e/ou privadas, muitos deles bem-sucedidos, outros frustrados, e muitas vezes eles são bem-sucedidos e nem as próprias instituições sabem que foram alvo de uma intrusão.

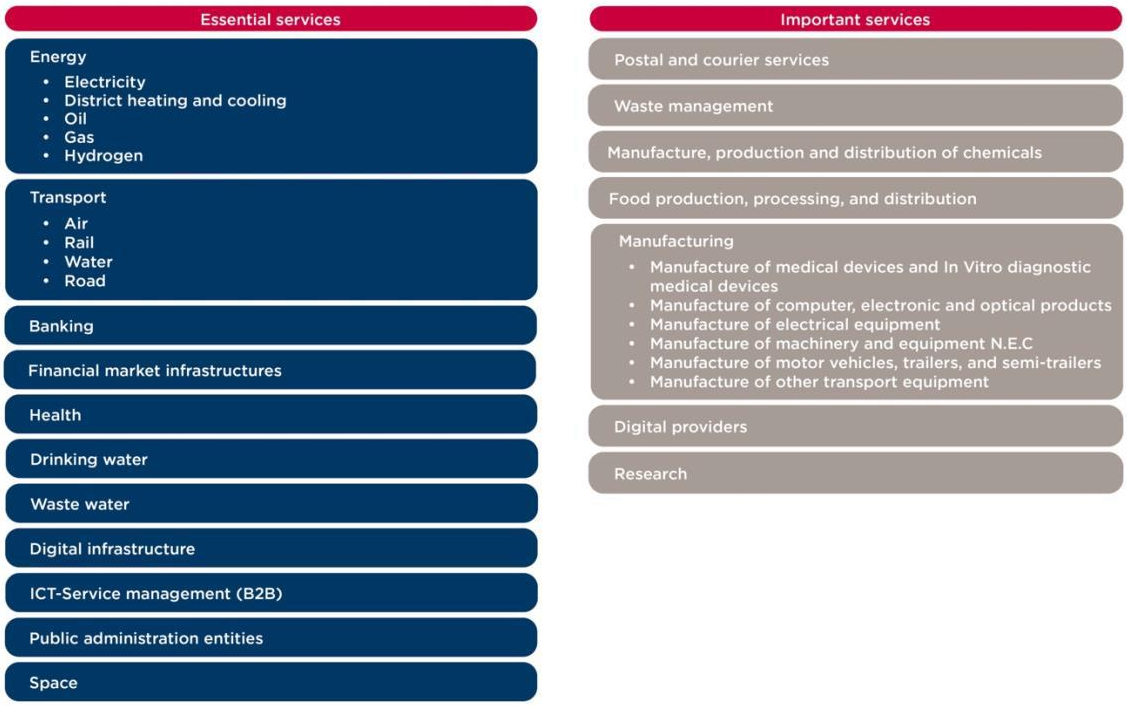
A verdade é que a ciberguerra é uma ameaça que já existe há algum tempo, como vimos com o caso Stuxnet (em 2010), mas tornou-se um fenómeno ainda mais global com o desenvolvimento das tecnologias e da integração que estas tiveram na vida das sociedades, desde o nível particular, empresarial e governamental. É uma ameaça que se intensificou, no território da União Europeia, e na Europa como um tudo, com o eclodir do conflito na Ucrânia pela forma e proporções que tomou e continua a tomar.

Em suma, proteger infraestruturas críticas contra ameaças cibernéticas é um desafio complexo e multifacetado que requer uma abordagem coordenada. Contudo, ao tomar medidas proactivas para reforçar a segurança da informação e fomentar uma cultura de resiliência, os governos e as empresas, nomeadamente as que prestam serviços essenciais, podem reduzir o risco de ataques informáticos e garantir a segurança e estabilidade dos seus sistemas de infraestruturas críticas.

Anexos



Anexo 1 - Motivações dos Ataques e Tipos de Ataques (European Union Agency for Cybersecurity.,



Anexo 2 - Serviços Essenciais e Serviços Importantes, ao abrigo da Diretiva NIS2 (Setterwalls),

Bibliografia

European Commission, 2022. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1680452856715&from=en>.

European Union Agency for Cybersecurity., 2022. ENISA threat landscape 2022: July 2021 to July 2022. [online] LU: Publications Office. Available at: <https://data.europa.eu/doi/10.2824/764318> [Accessed 3 April 2023].

Fortinet, 2023. What Is Cyber Warfare? [online] Fortinet. Available at: <https://www.fortinet.com/resources/cyberglossary/cyber-warfare> [Accessed 8 April 2023].

Fred Schreier, 2015. On Cyberwarfare. Available at: <https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf> [Accessed 2 April 2023].

Home Affairs, 2023. Critical infrastructure. [online] Available at: <https://home-affairs.ec.europa.eu/pages/page/critical-infrastructure_en> [Accessed 8 April 2023].

Microsoft, Digital Security Unit, 2022. An overview of Russia's cyberattack activity in Ukraine. [online] Available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> [Accessed 2 April 2023].

NATO, 2023. Cyber defence. [online] NATO. Available at: <https://www.nato.int/cps/en/natohq/topics_78170.htm> [Accessed 14 April 2023].

Setterwalls, 2023. NIS2 - New EU Cybersecurity Framework. [online] Setterwalls. Available at: <https://setterwalls.se/artikel/nis2-new-eu-cybersecurity-framework/> [Accessed 14 April 2023].

Thales Group, 2023. NIS2 Directive - Enhancing Cybersecurity Across the EU. [online] Available at: <https://cpl.thalesgroup.com/compliance/emea/nis2-directive-goal-enhance-cybersecurity-across-the-eu> [Accessed 12 April 2023].

UK Cyber Security Council, 2023. Glossary of cyber security terminology. [online] UK Cyber Security Council. Available at: <http://ukcsc-www-production-1.azurewebsites.net/glossary/> [Accessed 10 April 2023].

Cibersegurança na União Europeia: Ameaças e Estratégia

Pedro Nuno Morgado Baião, NOVA IMS

Resumo

A Cibersegurança tem cada vez um papel mais ativo na salvaguarda da vida normal da população mundial. A dependência da sociedade da internet trouxe inúmeros benefícios e novas oportunidades, no entanto, criou também novas vulnerabilidades que principalmente no caso de instituições governamentais ou empresas importantes tentam ser capitalizadas com maior frequência por atores com intenções criminosas. A União Europeia sendo um gigante económico e político não é exceção, desde cedo percebeu a importância de aplicar uma sólida estratégia para preservar um ambiente seguro no seu ciberespaço, garantindo um desenvolvimento da economia digital e prevenção de falhas graves que possam ocorrer como consequência de ataques.

Usando o método de investigação proposto por Raymond Quivy e Luc Van Campernhoudt este trabalho pretende, de forma informativa, investigar em que estado se encontra a Cibersegurança na União Europeia percebendo quais as ameaças mais recentes e quais as estratégias aplicadas.

Palavras-Chave: Cibersegurança, União Europeia, ameaças cibernéticas.

1. Introdução

Tendo os seus primórdios na Comunidade Europeia do Carvão e do Aço, a União Europeia atualmente é composta por 27 países que, na sua maioria, partilham uma moeda única, um espaço com fronteiras abertas e objetivos em comum. Mantendo a sua soberania, estes países garantem o sucesso da sua cooperação através de várias instituições, organismos e agências descentralizadas que trabalhando em conjunto procuram salvaguardar os interesses e o futuro dos cidadãos europeus.

Como um dos principais catalisadores do fenómeno da globalização, a internet veio unir o mundo de uma forma nunca vista. Evoluiu de uma simples rede que permitia a troca de informação entre os poucos computadores existentes, para uma ferramenta essencial usada pela grande maioria da população mundial.

Nos dias de hoje, é utilizada nas mais variadas tarefas pessoais, por empresas para venda de bens ou por instituições governamentais para gerir e controlar infraestruturas. Esta realidade em que tudo está à distância de um clique veio criar o conceito de ciberespaço, uma nova dimensão, que dadas as suas inúmeras potencialidades, veio também atrair atores com intenções criminosas.

O passar dos anos veio mostrar que o uso indevido do ciberespaço pode trazer consequências gravosas que chegam mesmo a influenciar o mundo real. A existência de novas vulnerabilidades num gigante da economia e política mundial como a União Europeia é algo que tem de ser colmatado urgentemente. Como tal, embora seja uma ideia algo recente, a Cibersegurança tem estado em constante desenvolvimento e a ganhar cada vez mais importância.

Com este trabalho pretende-se mostrar em que estado se encontra a Cibersegurança na União Europeia referindo as ameaças atuais e o seu planeamento estratégico para combater as mesmas.

2. Enquadramento teórico

"Information and communication technologies are a critical enabler for our economic growth and our societies now rely on the internet in many different ways and on many different levels."

Wolfgang Röhrig e JPR Smeaton

a. União Europeia

O dia 8 de maio de 1945 viu o fim da Segunda Guerra Mundial e uma Europa devastada, pronta a começar uma fase de recuperação. O início de uma nova era de cooperação e da União Europeia (UE) que hoje é conhecida começou pela fundação da Comunidade Europeia do Carvão e do Aço em 1951, seguida instituição da Comunidade Económica Europeia em 1957 com a assinatura do Tratado de Roma (União Europeia, s.d.).

Assente no princípio de Estado de Direito, a União Europeia baseia todas as suas iniciativas em tratados aprovados voluntária e democraticamente por todos os estados-membros da união. Estes são acordos vinculativos que definem os objetivos da UE, regras de funcionamento das instituições, processo de tomada de decisão e relações entre a UE e os estados que a constituem. Os tratados são documentos vivos que podem ser alterados consoante a necessidade (União Europeia, s.d.).

Em constante evolução, o sistema de tomada de decisões da União Europeia é constituído por quatro principais instituições cujos poderes, responsabilidades e procedimentos estão vertidos nos tratados fundadores da UE. O Parlamento Europeu, juntamento com o Conselho da União Europeia, toma decisões sobre leis europeias e aprova o orçamento da UE, o Conselho Europeu, composto pelos Chefes de Estado dos países membros, consegue efetuar alterações a tratados e a Comissão Europeia é o principal órgão executivo, representando os interesses comuns da união. Esta última instituição é capaz de apresentar propostas de nova legislação, gere as políticas e o orçamento da UE e assegura que os países aplicam corretamente a legislação (União Europeia, s.d.).

b. Importância da Cibersegurança

A crescente dependência da sociedade em tecnologias de informação e comunicação mudou drasticamente o mundo. A população, nos dias de hoje, encontra-se à distância de um clique ou de um simples toque num ecrã. A era digital veio trazer enormes benefícios em vários aspetos da sociedade, mas também novas vulnerabilidades (Röhrig & Smeaton, 2015).

Presentemente a internet tanto é utilizada para lazer, como por empresas ou entidades governamentais para controlar estruturas críticas para a sociedade, tornando o ciberespaço um domínio que oferece inúmeras potencialidades. Não é de admirar que o número de incidentes relacionados com o cibercrime tenha aumentado a um nível alarmante e, em certas ocasiões, esteja a afetar a normalidade da sociedade. É possível assumir que os responsáveis por estes incidentes irão continuar a evolução tecnológica com o objetivo de encontrar novas formas de atingir o seu objetivo (Röhrig & Smeaton, 2015).

O aparecimento de advanced persistent threats (APT) veio criar um novo tipo de ameaça, destinta das tradicionais, que deixou de estar ligada unicamente ao domínio militar. Passou a existir um opositor com nível sofisticado de perícia e recursos significativos para criar oportunidades que permitam cumprir com o seu objetivo através de ataques com múltiplos vetores (por exemplo, usando o ciberespaço e o mundo real). Acrescenta-se ainda que os ATP usam técnicas evasivas e furtivas para fazer ataques repetidos durante campanhas de longa duração (Chen, et al., 2014).

A Cibersegurança é responsável por criar um conjunto de medidas que permitem negar as ameaças ou mitigar as consequências das mesmas, tentando garantir um ciberespaço seguro para a utilização da população.

3. Ameaças à União Europeia no ciberespaço

Fundada em 2004 e fortalecida pelo regulamento da UE para Cibersegurança a European Union Agency for Cybersecurity (ENISA) tem como objetivo que haja um nível elevado de Cibersegurança, comum em todos os estados-membros. Esta prepara a UE para

desafios futuros cooperando com os países, instituições ou outras agências, contribuindo para as políticas no ciberespaço, aumentando a confiança em tecnologias de informação e comunicação e prestando serviços e processos de certificação (Cybersecurity, European Union Agency for, 2022).

Publicado anualmente, o relatório ENISA Threat Landscape (ELT) providência uma visão geral do panorama das ameaças no ciberespaço que a UE pode sofrer. Este afirma que durante a metade do ano 2021 e 2022 o número de ataques continuou a aumentar, não só em termos de vetores e número absoluto, mas como no impacto dos mesmos. A crise Rússia-Ucrânia trouxe um novo paradigma com implicações nas normas internacionais para o ciberespaço, para ciberataques patrocinados por Estados e para ataques contra estruturas civis críticas. Segundo o ELT, dada a situação internacional volátil, é expectável observar mais operações no ciberespaço derivadas da geopolítica a curto e médio prazo (Cybersecurity, European Union Agency for, 2022).

O ELT elaborado com informação compreendida entre julho de 2021 e julho de 2022 identifica e foca oito principais grupos de ameaça, devido à sua popularidade e o impacto que se materializou devido a estas ameaças:

• *Ransomware* – tipo de ataque em que os atores tomam controlo de propriedade informática e informação do alvo e pedem um resgate para retornarem o acesso;

• *Malware* – software ou firmware com intenção de efetuar um processo não autorizado que irá ter um impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema. Spyware e algumas formas de adware também são considerados códigos malignos;

• *Social Engineering* – engloba diversas atividades que pretendem explorar o erro ou comportamento humano com o objetivo de ganhar acesso a informação ou redes;

• *Threats against data* – conjunto de ameaças que têm como objetivo ganhar acesso não autorizado a fontes de dados, assim como manipular os dados para interferir com o comportamento dos sistemas, ou seja, podem ser classificadas como data breach ou data leak;

• *Threats against availability: Denial of Service* – a disponibilidade dos serviços é o alvo de uma grande abundância de ameaças ou ataques, estes fazem com que utilizadores de um sistema ou serviço não consigam ter acesso a informação relevante, serviços ou outros recursos. Também são conhecidos como *Distributed Denial of Service* (DDoS);

• *Threats against availability: Internet threats* – este grupo cobre os ataques que têm impacto na disponibilidade da internet, tais como o sequestro do *Border Gateway Protocol*;

• Disinformation/misinformation – estimulado pelo aumento do uso das redes sociais, a informação que gera mais visualizações é aquela que é promovida, mesmo que antes seja validada;

• Supply Chain Attacks – tem como alvo a relação entre as organizações e os seus fornecedores.

Para pertencer a este grupo, tem de existir pelo menos dois ataques. Um que tenha como alvo a organização, outro que tenha como alvo o fornecedor.

Tendo em conta a figura 1 é possível observar que os três maiores alvos durante este período foi a administração pública/governo, empresas que fornecem serviços digitais e a população em geral.

Segundo o ELT os principais responsáveis pelos ataques efetuados durante o período de estudo, foram: atores patrocinados por Estados, atores do cibercrime, *Hacker* contratados e hacktivistas.

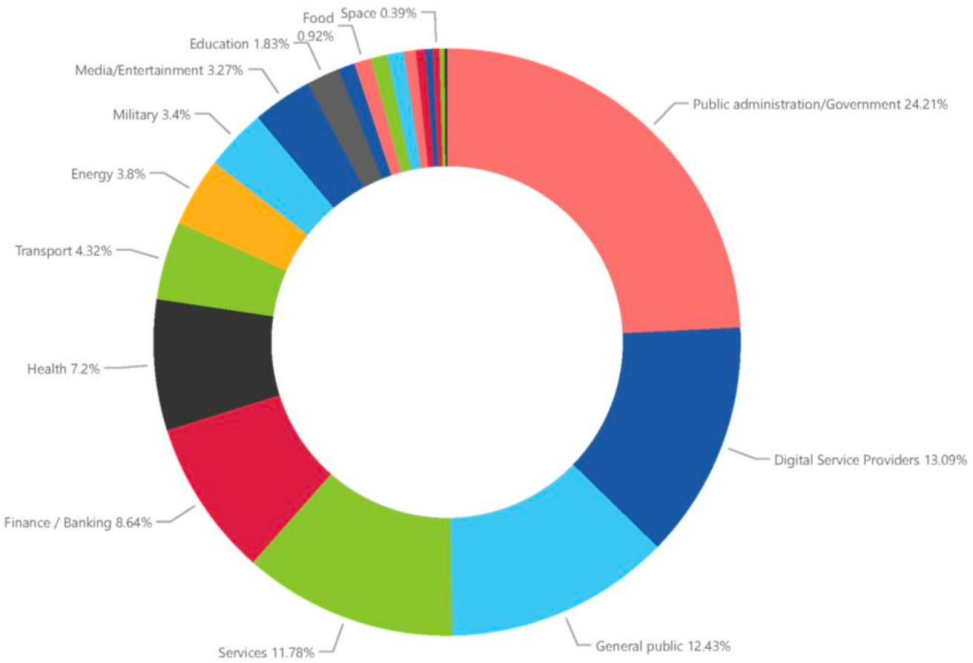


Figura 1 - Setores que sofreram ataques por número de incidentes (julho 2021 - junho 2022) (Cybersecurity, European Union Agency for, 2022).

4. Estratégia para a Cibersegurança na União Europeia

A União Europeia tendo noção da dependência na tecnologia e nos sistemas de informação presentes em todos os segmentos da sociedade e da economia, percebeu o quão catastrófico seria a falha dos mesmos.

Criada em 2013, a estratégia da UE para a Cibersegurança foi publicada em duas partes com o intuito de criar o ciberespaço mais seguro do mundo, de modo a desenvolver a economia digital e prevenir e responder a ataques a sistemas críticos. Esta estratégia foi um passo importante e eficiente para estabelecer as fundações de uma Cibersegurança Europeia unificada (Kovács, 2018).

A primeira parte da publicação da estratégia consistiu no Comunicado por parte da Comissão Europeia e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, enquanto que a segunda parte foi a proposta da Comissão Europeia de uma diretiva sobre a segurança de redes e informação, conhecida como a diretiva NIS

(*Network and Information Systems*)[1]. Os comunicados oficias da UE dão ênfase à ideia que a Cibersegurança é tão importante como a segurança do espaço físico, ficando revertida na estratégia através de cinco princípios: atingir ciber resiliência, diminuir drasticamente o cibercrime, desenvolver políticas e capacidades de Ciberdefesa[2], desenvolver a indústria e os recursos tecnológicos necessários para a Cibersegurança e estabelecer políticas coerentes para um ciberespaço internacional para UE com valores europeus (Kovács, 2018).

De forma a atingir cyber resiliência, a UE pretende que o setor público trabalhe com o sector privado com o intuito de garantir o desenvolvimento de capacidades de Cibersegurança, recursos e eficiência. Contudo, sem melhorar as capacidades de prevenção, deteção e gestão de eventos relacionados com a Cibersegurança a um nível de controlo da UE, em vez de nacional, não é possível cumprir com o primeiro princípio. Tal como é mencionado no capítulo anterior, a ENISA é criada com a intenção de colmatar este problema (Kovács, 2018).

A redução do cibercrime só é possível através da implementação de um ambiente legislativo mais rígido, poderoso e, ao mesmo tempo, efetivo. Embora tenham ocorrido convenções internacionais ainda não houve nenhum avanço significativo na área (Kovács, 2018).

Para garantir métodos de Ciberdefesa que consigam salvaguardar os sistemas informação e comunicação, tanto civis como militares, de ataques sofisticados, a UE tem a assistência da *European Defense Agency* (EDA) e estabeleceu uma cooperação com a *North Atlantic Treaty Organization* (NATO). O principal objetivo é garantir o desenvolvimento da indústria e dos recursos necessários para a Cibersegurança (Kovács, 2018).

[1] Em janeiro de 2023 foi publicada uma nova diretiva, conhecida como Diretiva NIS2, que veio substituir a anterior. Segundo a ENISA, esta veio melhorar a diretiva já existente criando as necessárias estruturas para fazer uma gestão de crises, aumentando o nível de harmonia, encorajando os Estados-membros a introduzir novas áreas de interesse, entre outras.

[2] Ciberdefesa, normalmente associada a Cibersegurança, é um conjunto de medidas que procuram defender de ataques contra os sistemas. Embora não seja o foco deste trabalho, é algo que será brevemente mencionado no subcapítulo da cooperação com a NATO.

a. Cooperação com a NATO

Tendo a UE e a NATO sido criadas com objetivos diferentes e, com algumas exceções, membros diferentes, torna a sua cooperação em torno da Cibersegurança um desafio, no entanto, ambas as organizações consideram o assunto extremamente importante. Em fevereiro de 2016 com a assinatura de um acordo técnico para aumentar a troca de informação entre as duas organizações é mostrado algum interesse em avançar com a união (Ilves, et al., 2016).

O interesse da NATO mantém-se focado na defesa militar, embora tenha reconhecido a importância dos sistemas civis e os riscos que correm, nomeadamente através da ameaça de guerra híbrida, não tem as capacidades legais ou políticas para tentar resolver o problema. Contudo a UE, embora tenha ambições mais modestas na área da defesa, ao criar medidas para nivelar a Cibersegurança de todos os Estados-membros, garantindo coerência com as medidas da NATO, vai resolver o problema mencionado, pelo menos nos membros que têm em comum (Ilves, et al., 2016).

No que toca à Ciberdefesa, uma cooperação entre a UE, os Estados Unidos da Améria (EUA) e a NATO permitiria desenvolver capacidades conjuntas. Os EUA podem fornecer um grande contributo para as ciber operações dos outros dois atores e servir de elo de ligação. Até ao momento as medidas implementadas pela UE e pela NATO são promissoras, mas servem apenas de fundação. As organizações têm de continuar a construir um futuro com partilha de informação, capacidades e estratégias defensivas (Ilves, et al., 2016).

b. Cooperação com os EUA

No final da primeira década do século XXI nota-se um acréscimo das interações entre a UE e os Estados Unidos da Améria no que diz respeito à sua Cibersegurança, culminando em 2010, com a criação de um grupo de trabalho específico. A cooperação entre a UE e os EUA pode ser justificada através de três interesses comuns. O primeiro é o fato que a existência de vários padrões de Cibersegurança na zona transatlântica pode pôr em causa

a economia dos dois atores que se encontra bastante interligada. O segundo é o interesse em moldar os padrões mundiais das regras e políticas da Cibersegurança com base nos ideais Ocidentais, algo que só o peso geopolítico conjunto da UE e dos EUA consegue fazer. O terceiro e último é o confronto de interesses e ideologia entre os dois atores e a China e a Rússia no que toca à administração da internet e os direitos humanos na internet (Anagnostakis, 2021).

A estratégia da UE ao partilhar um conjunto de princípios com a estratégia americana fez com que os dois atores procurassem evoluir no sentido do combate ao cibercrime, proteção de infraestruturas críticas, garantia de direitos humanos no ciberespaço e administração da internet. Foram estabelecidas duas instituições chave, o *European Union (EU)-United States (US) Working Group on Cybersecurity and Cybercrime* e o *EU-US Cyber Dialogue*, de modo a discutir políticas e, potencialmente, coordenar ações. Desde a sua criação as duas instituições têm trabalhado para que ambos os lados do Atlântico consigam ter um decréscimo no cibercrime, nomeadamente contra o abuso sexual de menores online, e na implementação de políticas que promovam a proteção dos direitos humanos no ciberespaço, a capacidade de Cibersegurança em países do terceiro mundo e assuntos relacionados com a segurança internacional no ciberespaço. De uma forma geral, as instituições permitiram a criação de um ambiente rico no qual agentes da autoridade conseguem partilhar experiências e trocar pontos de vista em como agir perante problemas comuns (Anagnostakis, 2021).

5. Conclusão

A Cibersegurança é um tema que, mesmo com o passar do tempo, continua a ser recente. Uma vez que sociedade mundial continua a aumentar a sua dependência das tecnologias de informação e comunicação e a constante evolução da tecnologia permite criação de novos métodos maliciosos que indivíduos ou organizações usam para cumprir os seus objetivos, a Cibersegurança terá de continuar a adaptar-se, evoluir e tentar ficar um passo à frente.

A União Europeia sendo um gigante da economia e política mundial tem a tendência de ser o alvo de diversas entidades. Houve um período em que a UE claramente não estava

preparada para lidar com ciberataques ou ciber incidentes, como ficou provado pelas intervenções indesejadas nos sistemas eleitorais da França e Alemanha.

De acordo com o ELT a União Europeia é alvo de vários tipos de ataques efetuados por diferentes tipo de atores. Embora no último ano praticamente metade dos ataques tenham tido como alvo instituições governamentais, empresas que fornecem serviços digitais/telecomunicações e o público em geral ainda é bastante difícil prever novos ataques dado que os motivos variam assim como o tipo de ataque.

É possível concluir que a situação de ameaças da UE é algo bastante complexo e que o trabalho realizado pela ENISA em estrita cooperação com as organizações nacionais dos Estados-membros e outras agências é essencial.

Quem delineou a estratégia da UE chegou à conclusão de que a cooperação dos países membros é o principal fator de sucesso. O facto que os tipos de ataque que a Cibersegurança pretende impedir ou mitigar são tantos, tão distintos, com diferentes graus de complexidade e podendo ser efetuados por alguém em qualquer parte do mundo faz com que seja essencial estabelecer políticas e leis aceites pela comunidade mundial. Fundamentada em cinco princípios a estratégia europeia procura a um nível micro (comparado à escala mundial) estabelecer, com o auxílio dos EUA e da NATO, um método que permita aos utilizadores utilizarem o ciberespaço em segurança sem pôr em causa os direitos humanos. De referir a importância do setor privado para garantir o sucesso da estratégia da UE.

Forças	**Fraquezas**
• Economia forte; • Estruturas de Governo/Administração organizadas; • Agências que promovem e facilitam cooperação entre Estados-membros.	• Organização composta por 27 Estados-membros; • Capacidade dos Estados-membros não é uniforme; • Pode estabelecer metas e objetivos, mas não controla o avanço.
Oportunidades	**Ameaças**
• Cooperação internacional; • Cooperação com a NATO; • Cooperação com os EUA.	• Atores patrocinados por Estados; • Atores do cibercrime; • *Hacker* contratado; • Hacktivistas.

Tabela 1 - Análise SWOT da capacidade da Cibersegurança da UE (elaboração própria, 2023).

Pretende-se com a tabela 1 resumir as ideias apresentadas ao longo deste trabalho e ao mesmo tempo responder à questão central que iniciou esta breve investigação sobre um tema tão importante para o dia-a-dia que ainda passa despercebido ou desconhecido por muitos.

Por último gostaria de salientar que, dado o foco da estratégia da UE nas vantagens de cooperações internacionais para a transmissão de informação e de conhecimento, a Ucrânia devido ao seu histórico de ataques sofridos e de ser dos primeiros países a participar numa guerra híbrida, será um excelente aliado para desenvolver as capacidades de Cibersegurança e Ciberdefesa da União Europeia.

Bibliografia

Anagnostakis, D., 2021. The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. Journal of Cyber Policy, 22 Abril, pp. 243-261. Anon., s.d. s.l.:s.n.

Chen, P., Desmet, L. & Huygens, C., 2014. A Study on Advanced Persistent Threats. iMinds-DistriNet, pp. 63-72.

Cybersecurity, European Union Agency for, 2022. ENISA Threat Landscape, Atenas: ENISA.

Dimitrova, S., Stoykov, S. & Kochev, Y., 2015. National cybersecurity strategies in member states of the European Union. Administrative and Criminal Justice, pp. 54-58.

Ilves, L. K., Evans, T. J., Cilluffo, F. J. & Nadeau, A. A., 2016. European Union and NATO Global Cybersecurity Challenges. A Way Foward. PRISM, VOL. 6, No. 2, pp. 126-141.

Kovács, L., 2018. Cyber security policy and strategy in the European Union and NATO. Land Forces Academy Review, Março, Volume 23, pp. 16-24.

Quivy, R. & Campenhoudt, L. V., 2005. Manual de Investigação em Ciências Sociais. Quarta Edição ed. Lisboa: Gradiva.

Röhrig, W. & Smeaton, J., 2015. Cyber security and cyber defense in the European Union: Opportunities, synergies and challenges. Cyber Security Review, Maio, pp. 23-27.

União Europeia, s.d. Acordos constitutivos. [Online] Available at: https://european-union.europa.eu/principles-countries-history/principles-andvalues/founding-agreements_pt [Acedido em 23 abril 2023].

União Europeia, s.d. História da UE. [Online] Available at: https://european-union.europa.eu/principles-countries-history/history-eu_pt [Acedido em 23 Abril 2023].

União Europeia, s.d. Tipos de instituições e organismos. [Online] Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/typesinstitutions- and-bodies_pt [Acedido em 23 abril 2023].

Regime Jurídico da Cibersegurança em Portugal: Contributo para a sua análise e compreensão

Emmanuel Carneiro, NOVA IMS

Gonçalo Santos, NOVA IMS

Pedro Vieira, NOVA IMS

Resumo

Num mundo cada vez mais interligado, a importância da cibersegurança não pode ser subestimada, particularmente no contexto das infraestruturas críticas. Com a rápida digitalização de serviços essenciais como as redes elétricas, os sistemas de transporte e as instalações de tratamento de água, a proteção destas redes e sistemas vitais contra as ciberameaças é fundamental.

Os sistemas das infraestruturas críticas estão na base do funcionamento da sociedade moderna, exemplificando a dependência das tecnologias digitais, criando um cenário vulnerável a potenciais ciberataques de impactos devastadores, incluindo perturbações económicas e o comprometimento da segurança pública e mesmo perda de vidas humanas

Palavras-Chave: Cibersegurança; Ciberameaças; Vulnerabilidade; Interligação; Infraestruturas críticas.

1. Introdução

A presente monografia consiste, essencialmente, na análise do Regime Jurídico da Cibersegurança em Portugal, pretendendo-se compreender quais os elementos fundamentais do mesmo, quais as suas inter-relações e lacunas e que novos desafios legais existem à luz da crescente utilização do Ciberespaço. De modo a abordar este tema manteve-se por base os diplomas legais integrantes do Regime Jurídico da Cibersegurança em Portugal.

O presente trabalho divide-se em cinco capítulos, sendo que, num primeiro momento, é feita a introdução ao tema abordado, definindo-se o objeto de estudo, os objetivos que se pretendem com o mesmo, a metodologia utilizada na sua concretização e a estrutura geral do trabalho. O Capítulo 2 identifica e explicita quais são os principais diplomas integrantes do Regime Jurídico da Cibersegurança em Portugal, apresentando uma breve descrição do conteúdo e alcance legal de cada um deles, assim como a sua relação com alguns diplomas comunitários. No Capítulo 3 é estabelecida a relação daqueles diplomas com outros diplomas relacionados com o tema da Cibersegurança como sejam o Regime Geral da Proteção de Dados (RGPD), a Lei da Proteção de Dados e a Lei do Cibercrime. O Capítulo 4 discute alguns novos desafios legais que existem à luz da crescente utilização do ciberespaço. O quinto capítulo faz referência às ameaças e aos atores de ameaças do ciberespaço. Por último, o Capítulo 5 apresenta as conclusões finais.

2. Regime Jurídico da Cibersegurança em Portugal

Incidindo este trabalho sobre o Regime Jurídico da Cibersegurança em Portugal, começa-se, neste ponto, por se identificarem os principais diplomas legais que integram este Regime Jurídico, explicitando o essencial do seu conteúdo e as relações que os mesmos têm com outros diplomas do Direito Comunitário que estão na sua génese ou estão com eles relacionados.

a. Lei n.º 46/2018

O primeiro diploma legal relativo ao regime jurídico da cibersegurança em Portugal é a **Lei n.º 46/2018**, de 13 de agosto, que é designada por Regime Jurídico da Segurança do Ciberespaço e que assegura a transposição da Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016[3] (conhecida como Diretiva NIS ou *Network and Information Security Directive*)[4], estabelecendo medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia.

A Lei n.º 46/2018: Estabelece o Regime Jurídico de Segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148; prevê a elaboração da Estratégia Nacional de Segurança do Ciberespaço; prevê a criação do Conselho Superior de Segurança do Ciberespaço (CSSC) que assegura a coordenação político-estratégica para a segurança do ciberespaço; estabelece o Centro Nacional de Cibersegurança (CNCS) como a Autoridade Nacional de Cibersegurança. Confere-lhe poderes, responsabilidades e competências, nomeadamente no âmbito de supervisão, regulação e certificação; estabelece o CERT.PT como a Equipa de Resposta a Incidentes de Segurança Informática Nacional, assim como o ponto de contacto com a Rede Nacional de CSIRT.

Esta lei aplica-se a várias entidades tal como:

- Administração Pública: Estado; Regiões Autónomas; Autarquias locais; Entidades administrativas independentes; Institutos públicos; Empresas públicas; Associações públicas.
- Operadores de Serviços Essenciais em vários setores e subsetores: energia: eletricidade, petróleo e gás; transportes: transporte aéreo, ferroviário, marítimo e por vias navegáveis interiores, rodoviário; setor bancário; infraestruturas de mercado financeiro; saúde: instalações de prestação de cuidados de saúde; fornecimento e distribuição de água potável; infraestruturas digitais.

[3] É importante notar que esta Diretiva é revogada pela **Diretiva (UE) 2022/2555** do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 - Diretiva NIS 2. Contudo, devido à sua recente publicação, a sua transposição no enquadramento jurídico de Portugal encontra-se ainda por realizar.
[4] Diretiva analisada no Anexo III.

- Operadores de infraestruturas críticas.
- Prestadores de serviços digitais: Serviço de mercado em linha; serviço de motor de pesquisa em linha; serviço de computação em nuvem.
- A quaisquer outras entidades que utilizem redes e sistemas de informação (o que depois não será aplicado no âmbito de Decreto-Lei já a ser apresentado)

No âmbito desta Lei n.º46/2018, o CNCS identifica os operadores de serviços essenciais.« Contudo, as entidades do setor das infraestruturas digitais (OSE) e prestadores de serviços digitais (com a exceção das micro e pequenas empresas) devem comunicar de imediato ao Centro o seu exercício da respetiva atividade.

Ainda no âmbito desta Lei n.º46/2018 são estabelecidos os **Requisitos de Segurança** e **Requisitos de Notificação de Incidentes**:

1. Sobre os Requisitos de Segurança é mencionado que Operadores de Serviços Essenciais, a Administração Pública, Operadores de Infraestruturas Críticas e Prestadores de Serviços Digitais devem aplicar medidas técnicas e organizativas adequadas e proporcionais à gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam;
2. Sobre Requisitos de Notificação de Incidentes, o CNCS deve ser notificado de incidentes com impacto relevante.

b. Decreto-Lei nº 65/2021

O **Decreto-Lei n.º65/2021 (DL)** e as **obrigações das entidades (RJSC)** surge como legislação complementar. Este Decreto tem dois âmbitos diferentes:

- Regulamenta o Regime Jurídico da Segurança do Ciberespaço (aprovado na Lei 46/2018), visto que concretiza algumas medidas e requisitos mencionados na Lei 46/2018;

- Define as obrigações em matéria de certificação de cibersegurança em execução do Regulamento (UE) 2019/8813.

Relativamente à regulamentação do Regime Jurídico da Segurança do Ciberespaço, o DL especifica os Requisitos de segurança das redes e sistemas de informação, assim como as Regras para a notificação de incidentes.

No que toca a disposições comuns: É solicitado que haja indicação (por todas as entidades abrangidas mencionadas anteriormente) de **um ponto de contacto permanente**, de modo a assegurar fluxos de informação de nível operacional e técnico com o CNCS. É designado um **responsável de segurança** para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes. É elaborado um **plano de segurança** devidamente documentado e assinado pelo responsável de segurança. É também elaborado e atualizado um **inventário de todos os ativos essenciais** para a prestação de respectivos serviços, devendo o mesmo ser assinado pelo responsável de segurança. É elaborado um **relatório anual** a ser enviado ao CNCS.

No âmbito da Segurança das Redes e dos Sistemas de Informação, as entidades devem cumprir as medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, devendo, para o efeito, realizar uma **análise dos riscos** em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam. Esta análise de risco deve ser feita de forma global pelo menos uma vez por ano, ou em caso de notificação do CNCS. Pode também ser feita de forma parcial, principalmente durante o planeamento e preparação de alterações nos ativos, ou caso a ocorrência de algum incidente de impacto relevante. A análise de risco pode ser enquadrada através de uma instrução técnica – de **normativo complementar setorial** aprovado pelo CNCS, sem prejuízo da aplicação de outro normativo nacional e da União Europeia em matéria da segurança das redes e dos sistemas de informação. Ou, as instruções da sua realização podem ser consultadas no **Quadro Nacional de Referência de Cibersegurança**, e respectivas disposições complementares, elaborado pelo CNCS.

No âmbito das Regras para a notificação de incidentes, a Lei 46/2018 já indicava alguns critérios para a determinar o impacto, nomeadamente o número de utilizadores afetados, a duração do incidente, distribuição geográfica, nível de gravidade e extensão do impacto nas atividades económicas e sociais. No entanto, o DL vem concretizar quando devem as

entidades notificar este tipo de incidentes ao CNCS e como. Neste sentido solicitam-se três tipos de notificações:

- Notificação inicial. Deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação;
- Notificação de fim de impacto relevante ou substancial. Deve ser submetida ao CNCS logo que possível, dentro de um prazo máximo de duas horas após a perda de impacto relevante ou substancial;
- Notificação final. Dever ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar;
- No caso em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final.

2018/151 da Comissão que concretiza ainda mais medidas de segurança, thresholds e o que é interpretado como incidente de impacto social, assim como aquilo que também é esperado que seja feito a nível setorial ou que se concretize um pouco mais. Então, no âmbito dos prestadores e deste regulamento europeu, o DL trouxe aspetos importantes sobre:

- A segurança dos sistemas e das instalações:
  - Abordagem baseada em avaliações e análises de risco na gestão sistematizada das redes e dos sistemas de informação (recursos humanos, segurança operacional, arquitetura de segurança, segurança dos dados, gestão do sistema no ciclo de vida e, se for o caso disso, encriptação e a gestão), na segurança física e ambiental, na segurança dos fornecimentos e no controlo dos acessos.
- Tratamento dos incidentes:
  - Processos e procedimentos de deteção documentados, testados e aplicados;
  - Processos e estratégias de comunicação de incidentes e de identificação de fragilidades e vulnerabilidades;

- Melhoria contínua

— Planos de contingência baseados numa análise de impacto nas atividades e respectivos testes
— Auditorias e testes

Ainda no âmbito do Regulamento de Execução (UE) 2018/151 da Comissão já tínhamos parâmetros a ter em conta para determinar se o impacto de um incidente é substancial. Isto está também incluído na Lei n.º46/2018, no entanto neste regulamento para os prestadores de serviços digitais já se concretiza quando devem comunicar. Sendo assim os **parâmetros a ter em conta para determinar se o impacto de um incidente é substancial são**:

— número de utilizadores afetados por incidente;
— duração do incidente;
— distribuição geográfica;
— nível de gravidade da perturbação: disponibilidade, autenticidade, integridade, confidencialidade dos dados ou dos serviços conexo;
— extensão do impacto nas atividades económicas e societais: incidente causou perdas materiais ou não materiais significativas aos utilizadores, nomeadamente em termos de saúde, proteção ou danos patrimoniais.

Considera-se **incidente com impacto substancial** quando:

— O serviços prestado pelo prestador de serviços digitais esteve indisponível durante mais de **5.000.000 horas-utilizador**[5];
— Resultou do incidente uma perda de integridade, autenticidade ou confidencialidade dos dados armazenados, transmitidos ou tratados ou dos serviços conexos oferecidos ou acessíveis através de redes e de sistemas de informação do prestador de serviços digitais tendo sido afetados mais de **100.000 utilizadores da união**;
— O incidente gerou um **risco de segurança pública, proteção pública ou morte**;

[5] Hora-utilizador: um utilizador afetado na União durante 60 minutos.

— O incidente provocou danos materiais superiores a **1.000.000 EUR** a, pelo menos, **um utilizador da União**

O CNCS pode, no âmbito das suas competências, **emitir instruções e técnicas complementares** em matéria de requisitos de segurança e de notificação de incidentes, designadamente normativos complementares setoriais. Isto é, à semelhança que existe este regulamento de execução para os prestadores de serviços digitais, espera-se que também exista algum detalhe para estes setores dos operadores de serviços essenciais e de administração pública para concretizar pelos menos os parâmetros de notificação de incidentes e esclarecer também de forma gradual os requisitos de segurança, apesar de estarem muitos deles contidos no Quadro Nacional de Referência para a Cibersegurança e outros que têm vindo a ser publicados.

O Decreto-Lei nº 65/2021 tem também como objetivo definir **as obrigações em matéria de certificação de cibersegurança** em execução do Regulamento (UE) 2019/881.

Assim sendo, o **CNCS é a Autoridade Nacional de Certificação da Cibersegurança (ANCC)**. Enquadra a **implementação de um quadro nacional de certificação da cibersegurança (QNCS)**, sendo que através deste é possível criar, desenvolver e implementar esquemas específicos de certificação da cibersegurança relativos a produtos, serviços e processos de tecnologias de informação e comunicação que não sejam ainda abrangidos por um esquema europeu. Finalmente, o CNCS visa executar as competências no âmbito dos esquemas europeus de certificação de cibersegurança, tal como supervisão e certificação.

Os esquemas europeus são **baseados em risco** e devem especificar:

— As categorias de produtos e serviços abrangidos;
— Os requisitos de cibersegurança, como padrões ou especificações técnicas;
— O tipo de avaliação, como autoavaliação ou de terceiros;
— O nível de garantia pretendido.

Atualmente, os esquemas europeus elaborados ou em processo de elaboração são:

1. EUCC – esquema europeu de certificação da cibersegurança baseado nos Critérios Comuns das TIC – concluído
2. EUCS – esquema europeu de certificação da cibersegurança para serviços de computação na nuvem – em elaboração
3. EU5G – esquema europeu de certificação da cibersegurança para as redes 5G – em elaboração

c. Estratégia Nacional de Segurança do Ciberespaço

O terceiro grande diploma integrante do Regime Jurídico da Cibersegurança em Portugal é a Estratégia Nacional de Segurança do Ciberespaço (ENSC) que foi aprovada através da Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, após audição do Conselho Superior de Segurança do Ciberespaço.

A ENSC começa por definir os conceitos de ciberespaço, cibersegurança, ciberdefesa e cibercrime, nos seguintes termos:

- Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.
- Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.
- Ciberdefesa consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço.
- Cibercrime entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa.

A atual ENSC, que surge na sequência da primeira ENSC, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho, vigora para o período 2019-2023 e está alicerçada nos princípios da subsidiariedade, complementaridade e proporcionalidade e define, de acordo com o interesse nacional, a visão, o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria.

Comparativamente à ENSC anterior, a atual versão deixou de contemplar os princípios da cooperação e sensibilização, embora mantenha estas matérias nos eixos de atuação que se irão referir mais à frente.

Os objetivos estratégicos definidos pela ENSC passam por: maximizar a resiliência; promover a inovação; e gerar e garantir recursos. Associados a cada um dos objetivos estratégicos existem seis eixos de intervenção, que informam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço, sendo estes os seguintes:

- Eixo 1 — Estrutura de segurança do ciberespaço;
- Eixo 2 — Prevenção, educação e sensibilização;
- Eixo 3 — Proteção do ciberespaço e das infraestruturas;
- Eixo 4 — Resposta às ameaças e combate ao cibercrime;
- Eixo 5 — Investigação, desenvolvimento e inovação;
- Eixo 6 — Cooperação nacional e internacional.

3. Relação com outros diplomas

Para além das já mencionadas e notórias relações do Regime Jurídico da Segurança do Ciberespaço e que assegura a transposição da Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016 e do Regulamento do Regime Jurídico da Segurança do Ciberespaço com o Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril de 2019, há ainda inter-relações daqueles diplomas com outros diplomas nacionais e comunitários. Destacam-se a Lei do Cibercrime e o Regulamento Geral de Proteção de Dados.

a. Lei do Cibercrime

A Lei n.º 109/2009, de 15 de Setembro, designada vulgarmente por Lei do Cibercrime, surgiu para acomodar uma realidade recente no âmbito dos crimes e burlas onde estão envolvidos equipamentos informáticos e dispositivos eletrónicos. A Lei transpõe a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

A organização geral da Lei é composta por cinco capítulos, num total de 32 artigos. Os capítulos I e IV referem-se respetivamente aos objetivos e definições e às disposições finais e entrada em vigor da lei. Já os capítulos II, III e IV, que são os mais relevantes, é onde se podem encontrar os artigos que poderão ser acionados num vasto conjunto de crimes que utilizam equipamentos informáticos.

Esses crimes estão representados na figura 1, onde consta também a indicação do respetivo artigo da Lei do Cibercrime.

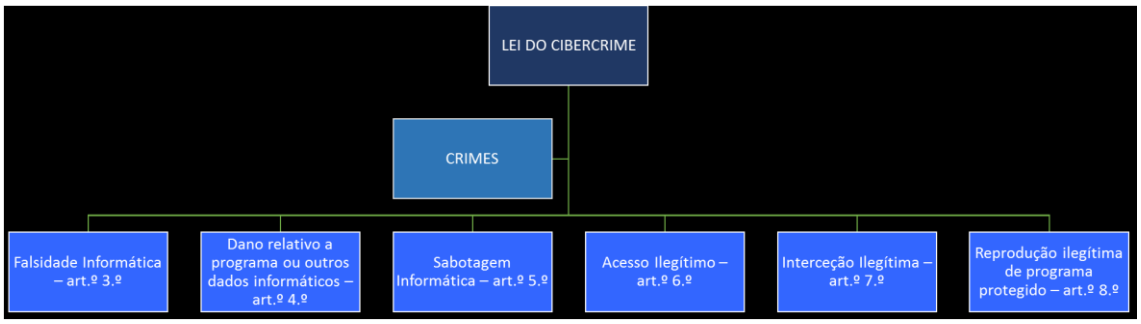


Figura 1 - Crimes tipificados na Lei do Cibercrime.

Não se irá aqui desenvolver em que consiste cada um destes tipos de cibercrimes, nem as penas que a Lei estipula para cada situação. No entanto, pode-se referir que os tipos de ciberataques mais frequentes (*phishing, pharming, spoofing, sniffing, SPAM, hacking*) constituem todos eles cibercrimes que estão enquadrados e são puníveis pela Lei do Cibercrime.

b. Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD) é um regulamento europeu (Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril), que considera a proteção das pessoas singulares, relativamente ao tratamento dos seus dados pessoais, um direito fundamental, independentemente da nacionalidade ou local de residência, contribuindo, assim, para a realização de um espaço de liberdade, segurança e justiça e para uma união económica e social dos cidadãos dos espaço europeu. A Lei 58/2019, de 8 de agosto, ou Lei de Proteção de Dados assegura a execução, na ordem jurídica nacional, do RGPD.

O RPGD reporta-se a vários tipos de dados (pessoais, genéticos, de saúde, biométricos) e autonomiza um conjunto de dados pessoais, que são designados "dados especiais" ou "dados sensíveis", devido à sua natureza sensível do ponto de vista dos direitos e liberdades fundamentais, pelo que o respetivo tratamento pode implicar riscos significativos para esses mesmos direitos e liberdades. Entre estes estão dados que revelem origem racial; opiniões políticas; convicções religiosas; façam tratamento de dados genéticos ou dados biométricos; relativos à vida e orientação sexual.

O RGPD enumera vários princípios relativos ao tratamento de dados pessoais, conforme esquematizado na figura 2.

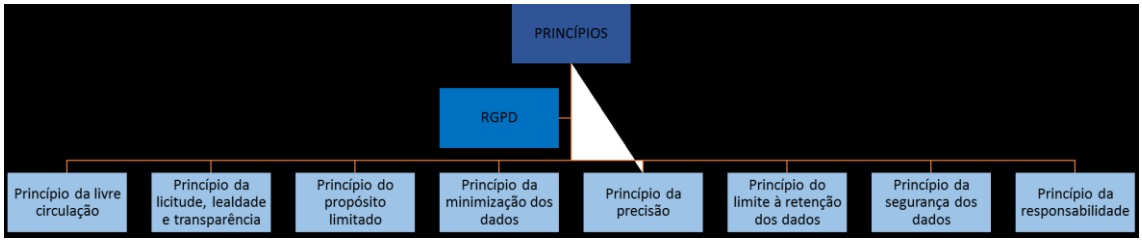


Figura 2 - Princípios do RGPD.

O RGPD contém ainda um conjunto de direitos dos titulares dos dados, de que se destacam o direito à proteção dos dados pessoais, à informação, de acesso, de retificação, de apagamento dos dados, de oposição ou de ser avisado em caso de violação de dados pessoais. A cada um destes direitos cabe uma obrigação, por parte do responsável pelo

tratamento, de tomar as devidas medidas técnicas ou organizativas para corresponder às solicitações que lhe são dirigidas.

Adicionalmente, o Regulamento instituiu também a figura do Encarregado da Proteção de Dados (DPO), cabendo-lhe:

- Informar e aconselhar as organizações (responsável pelo tratamento, subcontratante) acerca das suas obrigações, nos termos do RGPD e de quaisquer outros disposições relativas à proteção de dados na UE ou nos Estados-Membros
- Controlar a conformidade com o RGPD e com outras disposições legais concernentes à proteção de dados;
- Controlar a conformidade com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais;
- Assegurar a repartição das responsabilidade face ao RGPD, nomeadamente quanto ao responsável pelo tratamento, ou ao subcontratante, ou a qualquer outro interveniente;
- Promover ações de sensibilização e formação do pessoal que trata dados pessoais;
- Fazer auditorias;
- Prestar aconselhamento nas ações de avaliação de impacto sobre a proteção de dados;
- Cooperar com a autoridade de controlo;
- Servir de ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento de dados;
- Consultar a autoridade de controlo sobre qualquer assunto que ache útil ou imprescindível.

O RGPD estabelece ainda que devem ser reportadas à autoridade nacional de controlo (em Portugal, a Comissão Nacional de Proteção de Dados) as violações suscetíveis de resultar num risco para os direitos dos titulares. Finalmente, o Regulamento estabelece coimas para empresas e que podem ser:

- Até 10 000 000€ ou 2% do volume do negócio anual ao nível mundial para as violações de disposições legais graves;

— Até 20 000 000€ ou 4% do volume de negócio anual ao nível mundial para as violações de disposições legais muito graves

É ainda referido que cabe aos Estados-Membros estabelecer as regras relativas a outras sanções (para além das coimas), aplicáveis no caso de violação do disposto no RGPD.

4. Lacunas e novos desafios inerentes à utilização do Ciberespaço

Como refere o preâmbulo do Decreto-Lei n.º 65/2021, "a emergência de novas tecnologias disruptivas, como a inteligência artificial, a realidade virtual e aumentada e a Internet das coisas, sublinham a necessidade de assegurar um nível elevado de segurança das redes e dos sistemas de informação que sustentam o uso destas tecnologias, para que decorra num ambiente de confiança e protegido de ameaças que podem ter efeitos desestabilizadores de considerável alcance na vida em sociedade, especialmente em contextos de crise, que tendem a agravar a exploração de vulnerabilidades por parte de agentes de ameaça com motivações diversas."

Torna-se, assim, difícil que o quadro legislativo consiga acompanhar e responder de forma eficaz aos novos desafios emergentes no domínio da cibersegurança.

Assim, cremos que existem algumas lacunas no Regime Jurídico português atual, de que destacamos:

— Ausência de referência na Lei a alguns setores e tipos de entidades importantes

Como já referido, a Lei n.º 46/2018 estipula quais são os setores e tipos de entidades dos operadores de serviços essenciais aos quais a Lei é aplicável (ver Anexo I). Ora, parece-nos que mais tipos de entidades deveriam ser contemplados, especialmente nos domínios da saúde, da água e das infraestruturas digitais. De facto, atualmente, no setor da saúde, apenas estão considerados os prestadores de cuidados de saúde, mas laboratórios e empresas farmacêuticas, por exemplo, também deveriam ser abrangidas pela Lei, pois são algumas das entidades que, mais recentemente, têm sofrido ciberataques importantes e que estão na posse de dados sensíveis à luz do RGPD e muitos apetecíveis do ponto de vista comercial.

Também consideramos que, além dos fornecedores e distribuidores de água destinada ao consumo humano, deveriam ser consideradas as entidades responsáveis pelos lixos, esgotos e tratamento de águas, pois a reciclagem da água é uma realidade cada vez mais presente e as consequências de um ataque, por exemplo, de negação de serviços que implicasse a paragem de estações de tratamento de águas provocaria externalidades muito sérias.

De igual modo, em termos de entidades de infraestruturas digitais, pensamos que os prestadores de serviços de computação na *cloud* e de *data centers* ou os provedores de redes de distribuição de conteúdos, deveriam ficar também sujeitos às imposições legais dada a relevância e realidade incontornável que, por exemplo, os serviços *cloud* assumem.

— Eliminação da exclusão de todas as pequenas e microempresas de prestadores de serviços digitais

Embora possam ser pequenas ou microempresas, existem atualmente prestadores de serviços essenciais que podem ser alvos interessantes para hackers maliciosos e que podem lidar com dados críticos e de importância estrutural para a sociedade, pelo que estas empresas deveriam ser totalmente sujeitas às normas do Regime Jurídico, especialmente os deveres de "tomarem medidas para evitar os incidentes que afetem a segurança das suas redes e sistemas de informação e para reduzir ao mínimo o seu impacto nos serviços digitais, a fim de assegurar a continuidade desses serviços" e de "notificação ao CNCS dos incidentes com impacto substancial na prestação dos serviços digitais."

- Reforço de mecanismos de cooperação internacional

Como se sabe, as ameaças e incidentes "não conhecem fronteiras", pelo é importante melhorar e reforçar a integração e cooperação entre os vários países, até porque, em termos de cibercrime é muito frequente ser necessário recolher informação digital em diferentes países.

- Maior responsabilização

Em termos de *governance*, os responsáveis máximos das organizações públicas ou privadas sujeitas ao Regime Jurídico deveriam poder ser responsabilizados pelas infrações à Lei, por forma a se sentirem mais comprometidos com a necessidade de aprovarem medidas de gestão do risco de cibersegurança.

Ainda a este respeito, refira-se que "a responsabilização apresentará novos desafios: quem é responsável por um crime (ou acidente) diretamente ligado a um sistema de *machine learning*? Talvez quem o desenvolveu, mas e se foi um algoritmo? Talvez quem o "treinou/ensinou/forneceu os dados", mas e se foi o próprio sistema? Talvez quem o operou, mas e se ninguém o operava ou detinha? As respostas a estas questões – e a outras em que algoritmos agem por sua conta - terão de ser encontradas pela sociedade, pela regulação, pelos tribunais, ou mesmo por outros algoritmos" (Alvarenga, 2022).

- Obrigatoriedade de formação

Deveria existir uma obrigatoriedade de ser frequentada e facultada regularmente formação aos trabalhadores e responsáveis das organizações a fim de elevar o nível de literacia dos mesmos, promover melhores práticas de cibersegurança e ciberhigiene e aumentar o nível de resiliência da respetiva organização. Além disso, noutra vertente, é crucial existirem recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço.

Para além destes, podemos identificar os seguintes desafios: os **ataques a sistemas de informação** - com o intuito de roubar dados pessoais para posterior venda, sem que o utilizador se aperceba - como o spam, que serve de veículo para vírus ou espionagem; **a inteligência artificial e os dispositivos que a utilizam**, que apesar das enormes vantagens em termos de facilidades para o quotidiano, apresentam-se como um enorme risco para a segurança e privacidade dos utilizadores; a **crescente utilização de dispositivos móveis**, que são bastante mais fáceis de aceder do que os computadores, principalmente quando conectados através de dados móveis, redes internet partilhadas ou institucionais e aplicações não fidedignas, como alguns jogos ou redes sociais; no entanto, o maior desafio continua a estar relacionado com a **educação e sensibilização dos utilizadores do ciberespaço** para os seus perigos.

5. Caraterização dos seus atores e ameaças

Os ciberataques são levados a cabo por atores criminosos, podendo estes ser grupos ou entidades singulares, com o objetivo de lesar um outro utilizador ou uma entidade pública ou privada, de acordo com os seus interesses. Estes são os agentes de ameaça do ciberespaço, que, segundo o relatório mais recente do CNCS (2022), levam maioritariamente a cabo ações como "a engenharia social para a captura de informação, como o *phishing* (através de email), o *smishing* (SMS) e o *vishing* (telefone). A fraude e a burla online também tiveram relevância no âmbito das técnicas de manipulação do fator humano. Em menor volume, mas com bastante impacto, verifica-se o aumento dos casos, e da sua relevância, de *ransomware*, de comprometimento de contas e de exploração de vulnerabilidades".

De acordo com o mesmo relatório, os atores estatais também tiveram uma atividade relevante no ciberespaço de interesse nacional, visando objetivos geopolíticos e estratégicos, através de ataques de *phishing* e *spear phishing*, do comprometimento de contas, bem como da exploração de vulnerabilidades para a realização de intrusões. Menos relevante, mas a merecer atenção, persiste a ameaça interna negligente, que diz respeito aos colaboradores que inadvertidamente comprometem a sua organização, clicando num link malicioso de um *phishing*, por exemplo. É de referir ainda os *cyber-offenders*, os quais se caraterizam por realizar ações que visam perturbar as suas vítimas ou criar disrupções, mediante, por exemplo, assédio ou destruição de informação. Por fim, também se registaram algumas ações de *hacktivism*, nas quais se procuraram realizar afirmações ideológicas através, por exemplo, de *defacements*.

Para além destes aspetos, são identificadas as principais tendências nacionais - "Para 2022 e 2023 são identificadas como principais tendências em Portugal a propensão para uma maior intervenção de atores estatais, a persistência do uso das fragilidades do fator humano, ataques de *ransomware*, violações de dados relativas a credenciais de acesso, exploração de vulnerabilidades e as tecnologias móveis a serem cada vez mais utilizadas como superfícies de ataque" - e internacionais no contexto do ciberespaço, pelo que nos podemos aperceber de que há claramente uma conexão entre ambas, principalmente ao que concerne às ameaças resultantes do cenário de guerra na Ucrânia, que se tornaram

cada vez mais uma preocupação, uma vez que "o contexto de guerra pode incentivar as ações de atores estatais" e "podem ser portas de entrada para grupos que se confundem na motivação entre os ganhos financeiros, o niilismo político e o vandalismo informático."

No contexto internacional, o cenário foi representado através do esquema constante da figura 3.

Cenários de ameaças próprias de contextos emergentes e/ou permanentes

Cenário 1 - Ameaças típicas do contexto pandémico	**Cenário 2 - Ameaças típicas do contexto geopolítico e estratégico atual**
Agentes de ameaça emergentes neste cenário: cibercriminosos com objetivos económicos.	Agentes de ameaça emergentes neste cenário: atores estatais e paraestatais com objetivos geopolíticos e estratégicos (e ameaças persistentes avançadas); hacktivistas com objetivos ideológicos.
Tipologias de ações hostis emergentes neste cenário*: _ burlas *online*; _ comprometimento de sistemas próprios do trabalho remoto; _ desinformação sobre saúde; _ *phishing* massificado; _ *ransomware*.	Tipologias de ações hostis emergentes neste cenário: _ ciberespionagem; _ comprometimento de cadeias de fornecimento; _ comprometimento de contas; _ comprometimento de sistemas próprios do trabalho remoto; _ DDoS; _ *defacements*; _ desinformação sobre o conflito na Ucrânia; _ exploração de vulnerabilidades; _ intrusões; _ *phishing* e *spear phishing*; _ *ransomware* e/ou sabotagem.
Temas e setores alvo: Banca, Saúde, Serviços de *streaming*, serviços postais e de transporte.	Temas e setores alvo: operadores de serviços essenciais, Administração Pública e Órgãos de Soberania.
Cenário 0 - Contexto permanente: a materialização dos cenários 1 e 2 não obsta a que exista uma dinâmica permanente própria das ameaças ao ciberespaço de interesse nacional para lá da pandemia ou do contexto internacional atual, âmbito no qual certos incidente e cibercrimes tendem a ocorrer.	

Figura 3 - Cenários de ameaças próprias de contextos emergentes. Fonte: CNCS – Relatório Riscos Conflitos, 2022.

6. Conclusões

A Lei n.º 46/2018, de 13 de agosto (Regime Jurídico da Segurança do Ciberespaço), transpôs a Diretiva NIS ou SIR; definiu a orgânica nacional no que respeita ao tema da cibersegurança, criando a ENSC, assim como o CSSC, que, entre outras competências, controla a sua implementação; e estabeleceu o CNCS enquanto Autoridade Nacional de Cibersegurança, sendo principal diploma integrante do Regime Jurídico da Cibersegurança em Portugal.

Este diploma, que é aplicável à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a quaisquer outras entidades que utilizem redes e sistemas de informação, estabeleceu ainda a necessidade de notificação de incidentes, os requisitos de segurança e as contraordenações e sanções aplicáveis pelos possíveis incumprimentos.

Posteriormente, em 2019, foi revista a ENSC, tendo sido publicada uma nova para o período 2019-2023, que fixou nos seus objetivos estratégicos que pretende fortalecer e garantir a resiliência digital, promover a inovação e gerir e garantir recursos. A execução desta pretende contribuir para reforçar Portugal como um país mais seguro e visa aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas.

Por seu turno, o Decreto-Lei n.º 65/2021, de 30 de julho (Regulamento do Regime Jurídico da Segurança do Ciberespaço), que assegurou a execução do Regulamento (UE) 2019/881, relativo à certificação da cibersegurança das tecnologias da informação e comunicação, estabeleceu requisitos mínimos de segurança para as entidades abrangidas pela Lei n.º 46/2018 e implementou um quadro nacional para a certificação de cibersegurança, instituindo novas obrigações como a designação de um responsável de segurança e de um ponto de contacto permanente; a obrigatoriedade de elaboração de um inventário de ativos, de um plano de segurança e de um relatório anual; a realização de uma análise dos riscos; a implementação dos requisitos de segurança; a obrigatoriedade de notificações de incidentes relevantes à CNCS e ainda de um regime sancionatório.

Apesar do atual regime jurídico ter promovido e contribuído fortemente para a implementação de uma cultura de cibersegurança e ciberhigiene nas organizações existem lacunas que carecem de resolução. Neste trabalho, foram identificadas algumas delas, assim como alguns dos desafios existentes à luz da crescente utilização do ciberespaço.

Pudemos identificar alguns desafios derivados da utilização do ciberespaço, tais como os ataques a sistemas de informação, a inteligência artificial e os dispositivos que a utilizam, a crescente utilização de dispositivos móveis, que são mais fáceis de aceder do que os computadores e, por último, a falta de sensibilização dos utilizadores do ciberespaço para os seus perigos.

Para além disso, identificamos, através da análise a vários documentos do CNCS, que as ameaças mais comuns aos utilizadores da Internet em Portugal e na Europa são o *ransomware*, o *phishing*, o *vishing*, o *smishing*, a ciberespionagem, as burlas, as intrusões, os ataques DDoS e o comprometimento intencionado de serviços essenciais, principalmente das infraestruturas públicas.

Bibliografia

Alvarenga A., 2022. Cenários e o futuro do ciberespaço – o desafio da cibersegurança . [online] Available at: <https://blog.exed.novasbe.pt/artigos/cenarios-e-o-futuro-do-ciberespaco-o-desafio-da-ciberseguranca?5fe33004_page=2&de7e1ac7_page=3&ed856a68_page=2&eda8cc54_page=3> [Accessed 20 May 2023].

Araújo, T., 2022. Direito da Sociedade da Informação, Cap.1, 3 e 4, Setúbal, Escola Superior de Ciências Empresariais, Instituto Politécnico de Setúbal (documento não publicado)

Barbas, J. and Reis, M., 2023. Cibersegurança. Enquadramento legal da segurança da informação. Lisboa: Information Management School, Universidade Nova de Lisboa (documento não publicado)

Centro Nacional de Cibersegurança (CNCS), 2019. Quadro Nacional de Referência para a Cibersegurança. [pdf] Lisboa: Centro Nacional de Cibersegurança Available at: <https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf> [Accessed 15 May 2023].

Centro Nacional de Cibersegurança (CNCS), 2023. Perguntas mais frequentes (FAQ). [online] Available at: <https://www.cncs.gov.pt/pt/faq/#e14> [Accessed 15 May 2023].

Centro Nacional de Cibersegurança (CNCS), 2023. Relatório Cibersegurança em Portugal - Riscos e Conflitos, 3ª edição. [ebook] Lisboa: Centro Nacional de Cibersegurança Available throught: Centro Nacional de Cibersegurança website https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf > [Accessed 17 May 2023].

Diário da República Eletrónico (DRE), 2022. Regulamento n.º 183/2022, de 21 de fevereiro. [online] Available at: https://dre.pt/dre/detalhe/regulamento/183-2022-179325870?_ts=1675555200034 [Accessed 20 May 2023]

Diário da República Eletrónico (DRE), 2022. Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro. [online] Available at: <https://dre.pt/dre/detalhe/resolucao-conselho-ministros/106-2022-202899924> [Accessed 17 May 2023]

Imprensa Nacional Casa da Moeda (INCM), 2023. Certificação de maturidade digital. [online] Available at: <https://selosmaturidadedigital.incm.pt/SMD/> [Accessed 22 May 2023]

Procuradoria-Geral Distrital de Lisboa, 2023. Lei da Proteção de Dados Pessoais – Lei n.º 58/2019, de 8 de agosto. [online] Available at: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0014&nid=3118&tabela=lei s&pagina=1&ficha=1&so_miolo=&nversao=> [Accessed 17 May 2023]

Procuradoria-Geral Distrital de Lisboa, 2023. Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (UE) – Regulamento (UE) N.º 679/2016, de 27 de Abril. [online] Available at: https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis&so_miolo= [Accessed 17 May 2023]

Procuradoria-Geral Distrital de Lisboa, 2023. Regime jurídico da segurança do ciberespaço – Lei n.º 46/2018, de 13 de Agosto. [online] Available at: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=2930A0033&nid=2930&tabela=lei s&ficha=1&nversao=> [Accessed 17 May 2023]

Procuradoria-Geral Distrital de Lisboa, 2023. Regulamento do Regime jurídico da segurança do ciberespaço – Decreto-Lei n.º 65/2021, de 30 de Julho. [online] Available at: <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3444A0023&nid=3444&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=> [Accessed 17 May 2023]

Rede Nacional de CSIRT, 2023. Rede Nacional CSIRT [online] Available at: https://www.redecsirt.pt/ [Accessed 20 May 2023]

União Europeia (UE), 2016. Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016. [online] Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016L1148 [Accessed 17 May 2023]

União Europeia (UE), 2018. Regulamento de Execução (UE) 2018/151 da Comissão, de 30 de janeiro de 2018. [online] Available at: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0151> [Accessed 17 May 2023]

União Europeia (UE), 2019. Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019. [online] Available at: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019R0881> [Accessed 17 May 2023]

Anexos

Anexo I: Setores e tipos de entidades dos operadores de serviços essenciais

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais

Setor	Subsetor	Tipo de entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.
Transportes	Transporte aéreo	Transportadoras aéreas. Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos. Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
	Transporte ferroviário	Gestores de infraestruturas. Empresas ferroviárias incluindo os operadores de instalações de serviço.
	Transporte marítimo e por vias navegáveis interiores.	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias. Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos. Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias. Operadores de sistemas de transporte inteligentes.
Bancário	—	Instituições de crédito.
Infraestruturas do mercado financeiro	—	Operadores de plataformas de negociação. Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde.	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável.	—	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
Infraestruturas digitais	—	Pontos de troca de tráfego. Prestadores de serviços de Sistema de Nomes de Domínio (DNS). Registos de nomes de domínio de topo.

Anexo I - Setores e tipos de entidades dos operadores de serviços essenciais. Fonte: Lei n.º 46/2018, de 13 de agosto

Anexo II: Membros da rede nacional de CSIRT

Anexo II - Membros da rede nacional de CSIRT. Fonte: Rede Nacional de CSIRT

Anexo III: Diretiva (UE) 2016/1148

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 em toda a União.A Diretiva foi a primeira peça legislativa de Cibersegurança na União Europeia e fornece medidas jurídicas para aumentar o nível geral de cibersegurança na União, tal como:

- Preparação dos Estados-membros, exigindo que estejam devidamente equipados. Por exemplo, com o *Computer Security Incident Response Team* (CSIRT), Autoridade Nacional competente NIS e Estratégia nacional de segurança das redes e dos sistemas de informação;
- Cooperação entre todos os Estados-membros, mediante a criação do NIS Cooperation Group para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-membros. Dentro deste NIS Cooperation Group existem grupos de trabalho que vão especificar certos setores que vão permitir e facilitar uma harmonização da aplicação desta diretiva
- Uma cultura de segurança em todos os setores que são essenciais para a economia e sociedade e que dependem fortemente das TICs, como energia, transporte, água, bancos, infraestruturas do mercado financeiro, saúde e infraestruturas digitais.

Anexo IV: Regulamento (EU) 2019/881

Regulamento (UE) 2019/881 do Parlamento Europeus e do Conselho de 17 de Abril de 2019 relativo à Agência da União Europeia para a Cibersegurança (ENISA) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança).

O Regulamento Cibersegurança da UE (*Cybersecurity Act*):

- Estabelece o Quadro europeu de certificação da cibersegurança para produtos, serviços e processos TIC;
- A certificação desempenha um papel crucial no aumento da confiança e segurança em produtos e serviços importantes para o mundo digital;
- O quadro de certificação proporcionará esquemas de certificação europeus como um conjunto abrangente de regras, requisitos técnicos, normas e procedimentos;
- Cria condições equitativas como pilares de um mercado europeu de certificação de cibersegurança.

BOLETIM TERTÚLIA

Encontros e Reflexões

SEGURANÇA E DEFESA EUROPEIA

VOLUME 2

CIBERSEGURANÇA

PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

Segue-nos em::

@eurodefensejovem

@eurodefensejovem-portugal5469

linktr.ee/eurodefenseportugal

eurodefenseportugal

Contacta com a EuroDefense-Jovem através de:

jovem@eurodefense.pt

COM O APOIO

REPÚBLICA PORTUGUESA
DEFESA NACIONAL