
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VII – MAIO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antes de mais, aproveito para anunciar uma nova edição do Curso de Direito do Ciberespaço, em formato novel, a ter lugar em Novembro de 2019. À semelhança do curso anterior, na oportunidade de publicação de alguns artigos, a Revista assumir-se-á como esse veículo de partilha de conhecimento.

No que concerne propriamente às notas desta edição, permitam-me partilhar algumas novidades e preocupações.

No passado dia 23 de maio do corrente, o Conselho de Ministros aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, que ainda carece de publicação em jornal oficial. Não obstante é já do domínio público que o propósito desta nova ENSC visará *garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas, procedendo desta forma à revisão da ENSC de 2015*[1], tendo em atenção a evolução digital ocorrida desde então.

1 https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278
A propósito, neste conspecto, para quem não tenha estado presente, na Conferência – Cibersegurança, na Universidade de Évora, a 14 de novembro de 2018, será interessante dar uma vista de olhos na apresentação "A Estratégia Nacional de Segurança do Ciberespaço 2.0 – Governação e execução", feita e disponibilizada por parte do CALM Gameiro Marques, da Autoridade Nacional de Segurança, cujo conteúdo pode ser encontrado @ https://www.uevora.pt/media_informacoes/agenda/(item)/25903.

Em efeméride de aniversário do Regulamento Geral de protecção de dados, e estando este em vigor desde *o vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia*, naturalmente a «Cyberlaw by CIJIC» não poderia passar ao lado do tema, recorrente dos últimos anos.

De facto, nestes 3 anos volvidos, é inconcebível que Portugal ainda não tenha uma lei de execução do mesmo. De igual forma, é inconcebível que as organizações, públicas ou privadas, só conheçam o "consentimento" como fundamento de licitude para o tratamento de dados pessoais, considerando-o um verdadeiro *canivete-suíço*. Ainda havemos de pugnar por um "*direito ao esquecimento*" sobre o consentimento, pois que a livre revogabilidade do mesmo por parte da pessoa titular dos dados pessoais parece sucumbir ante tanto abuso na sua utilização por parte das mais variadas organizações.

Se a estupefação quanto ao uso abusivo da figura do consentimento não cercear a nossa incredulidade, é igualmente inconcebível que o Estado, hoje, 3 anos após a entrada em vigor do RGPD, tenha dado conta de que, por exemplo, pelo menos, 1977 freguesias estarão obrigadas a nomear um encarregado de protecção de dados. Subam ou desçam na hierarquia do Estado e imaginem a confusão em que se vive. Três anos volvidos e o Mercado Único Digital Europeu à espreita…

Não pensem, contudo que a confusão é exclusivo do sector público. Quando o foco deriva para dados pessoais sensíveis, nomeadamente, dados de saúde, notícias como por exemplo, «*Proteção de Dados condena clínicas que recusam tratar doentes por falta de assinaturas*[2]», revelam parte do preocupante e actual estado de coisas.

Com efeito, se a protecção de dados pessoais era até há pouco tempo tema desconhecido do grande público, num ápice passou a ser o *olho do furacão*, gerando leque preenchido de atropelos e violações de dados dos seus titulares. E a autoridade nacional de controlo continua amarrada a constrangimentos de índole múltipla, desde orçamentais à falta de recursos, humanos e tecnológicos. Imaginem o que escapa ao *mainstream* mediático.

Enquanto isso, a evolução do digital continua em passo acelerado. O nível de ameaça ao estado de direito democrático acompanha esta desenfreada marcha.

2 Disponível em https://www.dn.pt/lusa/interior/protecao-de-dados-condena-clinicas-que-recusam-tratar-doentes-por-falta-de-assinaturas-10901005.html,

Infelizmente, o tempo do direito e da justiça teimam em não se adaptar. Está assíncrono. O que, se por um lado até poderá induzir-nos a alguma prudência, por outro pode indiciar um factor de preocupação acrescido. Até pelo nível de risco em que coloca a sociedade, no seu todo.

Pensemos na utilização do uso de UAV's; na condução autónoma de veículos; na constante violação das propriedades essenciais da informação gerando supremacias informacionais ilegais a certos Estados; na massificação das redes sociais; na disseminação em *live streaming* de ataques a pessoas; na dispersão de conteúdo mentiroso e propagandístico *online* para desvirtuar o resultado de eleições livres e democráticas; na disseminação de ódio e violência *online*; nas novas ameaças a toda a actividade policial e de segurança do Estado; no controlo e rastreio individual *online* e no registo de crédito social em função disto; entre outras. A profusão destas notícias é de conhecimento geral. A *digitalização* humana está em curso. O ciberespaço, aparentemente, evolui para uma antiutopia.

Neste ensamble, vertiginoso e fulminante, é pois inconcebível que dois anos volvidos após um pedido de fiscalização sucessiva intentado junto do Tribunal constitucional português, por parte de um conjunto de partidos políticos, este Tribunal ainda não se tenha pronunciado quanto à constitucionalidade do acesso aos metadados, dados de tráfego e duração de comunicações por parte dos serviços secretos portugueses. É inconcebível e preocupante pois que, por um lado o serviço de informações da república esteja parado ou a trabalhar à margem da lei ante esta omissão do Tribunal; por outro lado, é inconcebível que este Tribunal, por excelência, de garantia dos direitos e liberdades fundamentais das pessoas, esteja dois anos para aferir da constitucionalidade de uma dada lei.

O que tanto demora a tomada de decisão? Falta de preparação temática dos juízes do Constitucional? Má técnica legislativa? Teimosia política? Falta de ameaças concretas, conhecidas do público, à segurança do Estado? Neste particular dos metadados, sublinho, o delírio é a nota dominante. Até porque, se *o Sistema de Acesso ao Pedido de Dados aos Prestadores dos Serviços de Comunicações Electrónicas (Sapdoc), foi declarado operacional pelo CFSIRP desde Março e está a funcionar*, no outro plano da acção, consta que poderá estar na iminência *um novo chumbo dos juízes,*

uma vez que a questão de fundo - violação do artigo 34º da CRP- manter-se-á [3]. Ora, parece-nos que este delírio, portanto, promete e vai continuar. Novo procedimento, novas discussões, nova lei, mais discussões, novo pedido de fiscalização, novo entorpecimento, novo regresso ao ponto de partida, que recordo, é a nota dominante desde que o poder político criou o *novo regime do Sistema de Informação da República Portuguesa*, em 2015.

Óbice daqui, ameaça dali, risco dacolá, não haverá uma luz de esperança que contrarie o delinear desta *antiutopia*?

A bem de todos nós, mesmo que tenha passado despercebido o *Christchurch Call*[4], julgamos decisivo o apelo à acção. Até porque o momento, o tempo e o espaço a tal nos obrigam. Aqui chegados, impõe-se-nos o sublinhar de parte das notas dos proponentes iniciais. Por um lado, o *envisage* do Presidente francês, o sr. Macron: «"*We need to build this new cyberspace, a free, open and secure Internet, which allows everyone to share, learn, innovate, but which also allows us to uphold our values, protect our citizen and empower them*"»; por outro, o apelo à adesão pluriparticipada, mundial, a cargo da Primeiro-Ministra Neozelandesa, a sra. Ardern: «"*From here, I will work alongside others signed up to the Christchurch Call to bring more partners on board, and develop a range of practical initiatives to ensure the pledge we have made today is delivered*"». Por um *mundo*, terreno e digital, melhor, de todos e para todos.

Por fim, num plano nacional, com especial saudação para a ousadia da proposta, arbitramos da pertinência do Projeto de Lei 1217/XIII[5], apresentado pelo partido Socialista, já apelidado de Carta de Direitos Fundamentais na Era Digital.

A Carta deverá corresponder a *lei de protecção de direitos, liberdades e garantias centrada nas pessoas, consagradora de valores democráticos essenciais contra ameaças que não devem ser ignoradas* procurando ir além de mera *lei compilatória das normas que na ordem jurídica portuguesa consagram (alguns) direitos*, que enuncie *um elenco diversificado e abrangente, que inove, clarifique e valha também*

3 https://www.dn.pt/poder/interior/-necessidade-inquestionavel-fiscais-das-secretas-validam-acesso-a-dados-das-comunicacoes--10935824.html

4 https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

5 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768

como programa de ação vinculativo dos órgãos de poder, pode ler-se no enunciado programático do Projeto de lei. Deixo aqui um apelo a uma participação contributiva entusiasta por forma a melhorar este esboço inicial de consagração de uma Carta de Direitos Fundamentais na Era Digital.

Resta-me, a final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 24 de Maio de 2019

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

CIBERAMEAÇAS E (IN)SEGURANÇA

LUÍS ELIAS [1]

1 Superintendente da PSP. Diretor do Departamento de Operações. Doutorado em Ciência Política na Faculdade de Ciências Sociais e Humanas. Licenciado em Ciências Policiais pelo Instituto Superior de Ciências Policiais e Segurança Interna. O presente estudo representa o desenvolvimento da comunicação apresentada no Curso de Pós-Graduação sobre Direito do Ciberespaço, organizado pelo Instituto de Ciências Jurídico-Políticas e pelo CIJIC da Faculdade de Direito da Universidade de Lisboa.

RESUMO

Este artigo reflete sobre o uso intensivo de tecnologias de informação e comunicação e impactos sociais, políticos e na segurança.

Aborda os conceitos de ciberespaço, de cibersegurança, de ciberameaças e de cibercriminalidade. Analisa a Estratégia Nacional de Segurança do Ciberespaço. Sublinha a relevância do Gabinete Nacional de Segurança, do Centro Nacional de Cibersegurança, do Centro de Ciberdefesa e da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica.

Os desafios no futuro decorrente da revolução tecnológica em curso serão certamente maiores e trarão problemas difíceis de ultrapassar para a segurança pública, das redes e dos cidadãos.

Palavras-Chave: Tecnologias de Informação, Comunicação, Ciberespaço, Ciberameaças, Cibercriminalidade.

1. INTRODUÇÃO

A sociedade da informação contemporânea é caraterizada pelo uso intensivo de tecnologias de informação e comunicação. Muitas das empresas atuais defendem a prevalência da rede, face à hierarquia formal, como o modo de organização e de obtenção de melhores oportunidades de mercado. Sustentam também o crescente uso do digital e da mediação de tecnologias que constituem a infraestrutura básica das organizações.

Na sociedade em rede, o poder e a falta dele são avaliados em função do acesso a redes e do controlo dos seus fluxos de recursos, informacionais ou financeiros (Castells, 1998). As redes são portas de acesso onde se sucedem oportunidades. Fora das redes, a sobrevivência é cada vez mais difícil. As grandes empresas de tecnologias de Informação como a *Google*, a *Facebook*, o *Baidu* e a *Tencent* poderá incluir a médio prazo na "transferência de autoridade dos seres humanos para os algoritmos" (Harari, 2018: 103-104), o que cria riscos de acumulação de informação e de conhecimento numa muito reduzida percentagem de peritos em termos globais e num reduzido número de Governos, aumentando o perigo do totalitarismo.

O mundo hoje é altamente conectado, opera em ritmo acelerado e em constante mudança. O facto de vivermos em plena revolução tecnológica e de o devir das nossas sociedades ser permanente tem provocado um enorme impacto na forma como as ameaças encaram este novo ambiente e também no modo como os Estados e as respetivas áreas de soberania (segurança interna, defesa, informações, justiça) se adaptam ao mundo cada vez mais reticular e desafiador dos paradigmas. A evolução das tecnologias de informação e comunicações conduziu ao primado de uma cultura mundial, contribuindo para a ocidentalização dos modelos políticos, económicos e sociais, tornando-os globais e universais (Ramonet, 1998). O sistema político atual torna-se assim "planetário, permanente, imediato e imaterial" (Ramonet, 1998: 67).

Nos últimos anos, as fronteiras físicas entre os Estados têm vindo a ser esboroadas pelo caráter transnacional das ameaças e riscos e os Estados, face à crescente desterritorialização da segurança acelerada ainda mais pela rede global, cooperam internacionalmente, trocam e partilham informações, planeiam e executam operações conjuntas, criam redes de peritos, por forma a prevenirem e combaterem os fenómenos que mais afetam a segurança coletiva.

Fernandes considera que "a internet é uma das grandes forças equalizadoras do mundo. Sendo uma das principais forças motrizes da globalização e do progresso das comunicações, ela fornece meios inigualáveis de intercâmbio cultural, informativo e de ideias. Ela criou um nível antes inimaginável de interligação que beneficia o mundo dos negócios, governos e cidadãos. Contudo, da mesma forma que a internet proporciona acesso à mesma informação a pessoas que vivem em circunstâncias totalmente diferentes, atua também como um equalizador entre governos e atores não-estatais" (Fernandes, 2014: 11).

A *internet* e as redes digitais em geral constituem-se como um novo ambiente para a criminalidade organizada, para o recrutamento, para a radicalização, para a subversão e ativismo politico com as mais diversas causas e conotações ideológicas. Verifica-se uma desterritorialização das ameaças e riscos, fazendo do mundo virtual, uma nova dimensão para a expansão das atividades ilícitas e para a ação das Forças e Serviços de Segurança. A internet "enquadra-se perfeitamente na conceção anárquica do sistema internacional, pois o ciberespaço tornou-se um novo campo de batalha internacional" (Fernandes, 2014: 12).

No mundo cibernético, os conceitos técnicos são desenvolvidos e utilizados por peritos num círculo relativamente fechado. Os analistas têm de dominar estes conceitos, tal como o jargão técnico e ser capazes de comunicar ideias complexas e propostas de solução às hierarquias policiais e ao poder político, com vista à tomada de decisão informada e adequada.

Neste sentido, refletiremos sobre as noções de ciberespaço, de cibersegurança, de ciberameaças e, em concreto, de cibercriminalidade, acerca dos desafios que se colocam aos Estados, instituições e sociedade civil para fazer face aos fenómenos decorrentes de um sistema económico-financeiro, sociopolítico, cultural cada vez mais interconectado e gerador de incertezas.

2. CONCEITOS DE CIBERESPAÇO, DE CIBERSEGURANÇA, DE CIBERAMEAÇAS E DE CIBERCRIMINALIDADE

As palavras ciberespaço, cibersegurança, ciberameaças e cibercriminalidade entraram de forma definitiva no léxico quotidiano, no meio académico e nos textos jurídicos, pelo que, sem intenção de apresentar definições incontestáveis e definitivas, propomo-nos contextualizar cada um destes conceitos de forma sumária.

2.1. Ciberespaço

O ciberespaço não encontra um significado ou definição objetiva e universalmente aceite. De acordo com o dicionário Priberam de língua portuguesa, trata-se do "*espaço ou conjunto das comunidades de redes de comunicação entre computadores, nomeadamente a internet*".

Gibson foi dos primeiros autores a utilizar o termo ciberespaço na década de 80 do século XX, numa perspetiva sobretudo romântica, considerando-o "uma alucinação consensual experimentada diariamente por biliões de operadores legítimos, em todas as nações, por crianças a quem são ensinados conceitos de matemática... Uma representação gráfica de dados extraídos dos bancos de dados de cada computador no sistema humano. Complexidade impensável. Linhas de luz no espaço da mente, grupos e constelações de dados" (Gibson, 1984: 22).

Kuehl sustenta que o ciberespaço "*é um domínio operacional que se carateriza pela utilização da eletrónica e do espetro eletromagnético para criar, guardar, modificar trocar e explorar informação através de sistemas baseados em tecnologia de comunicação de informação interligados e as suas infraestruturas associadas*" (Kuehl, 2009: 24-42).

Outra definição de ciberespaço poderá ser "*a rede global de infra- estruturas de tecnologias de informação interligadas entre si, especial- mente as redes de telecomunicações e os sistemas de processamento dos computadores*" (Fernandes, 2012: 55).

O ciberespaço pode ainda ser apresentado como "*um ambiente em si mesmo, onde se deve ter em linha de conta tanto a sua componente tecnológica, isto é, as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-lo, como os fatores humanos, uma vez que são estes que caraterizam os utilizadores deste ambiente*" (IDN, 2013: 9-10). Para Natário consiste "*no mundo virtual que os utilizadores da internet visitam quando estão online, acedendo aos mais diversos conteúdos, jogando ou utilizando os variadíssimos serviços interativos que a rede mundial de computadores disponibiliza. (...) Mas é*

fundamental distinguir o ciberespaço da infraestrutura física das redes de comunicação, pois existe uma generalizada confusão concetual. As telecomunicações e a informática, a chamada telemática, limitam-se a permitir a comunicação à distância, enquanto o ciberespaço é um ambiente virtual que se serve destes meios de comunicação para o estabelecimento de relações virtuais" (Natário, 2013).

O ciberespaço é, assim, um ambiente virtual ao nível global utilizado para os mais diversos efeitos: para lazer; para a troca e partilha de conhecimento no meio académico e científico ou técnico; para a realização de negócios; para a difusão de ideias e de conceções políticas, sociais, económicas, culturais; para a comunicação entre pessoas, empresas, instituições e Governos; mas também para a prática de uma vasta panóplia de crimes; para a disseminação de ideologias radicais que questionam e combatem os sistemas políticos, económicos e sociais vigentes; para radicalização e recrutamento para o terrorismo; entre muitas outras práticas que questionam a soberania dos Estados e colocam em risco a segurança das comunidades e dos cidadãos.

Em suma, o ciberespaço está ligado às ideias de:

- globalização, na medida em que a comunicação e o acesso a conteúdos de informação à escala mundial permitiram que pessoas ou grupos de diferentes culturas, origens sociais e económicas, de áreas geográficas diversas, interagissem, se conhecessem e mantivessem contacto permanente *online*, trocando e partilhando informação, fazendo negócios, criando laços de amizade, situação que nunca tinha sido possível até hoje na história da Humanidade;

– criação de um universo virtual paralelo ao mundo físico, ou seja, o surgimento e expansão de uma nova realidade onde se operacionalizam fluxos infinitos de informação, embora a distribuição geográfica dos utilizadores da internet seja muito desigual, em função das disparidades socioeconómicas entre os diversos Estados, do desenvolvimento das infraestruturas, das taxas de penetração tecnológica ou do de nível de educação;

– libertarismo, ou seja, a conceção utópica que considera a internet um espaço que não tem fronteiras, que não está condicionado pelos limites impostos pela soberania e domínio dos governos nacionais e onde os cidadãos têm toda a liberdade de expressar as suas opiniões, contactar entre si e estabelecer relações, concretizando assim a sua emancipação do domínio e regulação dos Estados e das suas instituições. A primeira corrente teórica a tratar do "*controlo*" do ciberespaço tem como expoente Barlow, norte-americano, poeta, escritor e ativista da *internet*. As ideias de Barlow prosperaram nos primórdios da expansão comercial da internet, em 1996 e o sentimento de liberdade era a expressão maior da *web*. A visão era a de que as leis do mundo real não teriam validade sobre o ciberespaço, pois este seria "*um*

mundo à parte, mundo esse alheio e indiferente ao direito tradicional". Esta corrente teórica ganhou impulso maior quando Barlow publicou em 1996 a "*Declaration of independence of cyberspace*" (Declaração de independência do ciberespaço), em contraponto às medidas jurídicas adotadas pelo Governo dos EUA com o "*Communications Decency Act*", continuando ainda a inspirar os *hacktivistas* e as conceções mais contestárias em relação ao estatocentrismo, bem como quanto ao controlo e regulação da rede;

– desenvolvimento e de impacto da tecnologia nas sociedades hodiernas, na medida em que a rede global e a inovação exponencial na área das tecnologias tem transmutado a nossa sociedade, a economia de mercado, as relações sociais, a interação dos Estados com os cidadãos e vice-versa, sendo hoje impensável conceber o mundo sem internet, sem plataformas de comunicação e de disseminação da informação de forma instantânea e imediata.

De acordo com o preâmbulo da Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho que aprovou a Estratégia Nacional de Segurança do Ciberespaço, "*as tecnologias são, no entanto, vulneráveis, criando riscos sociais e materiais*". Se, por um lado, trazem claros benefícios à sociedade, por outro lado, vêm aumentar, de forma significativa, os riscos decorrentes da sua dependência e da quantidade de informação armazenada e em circulação, expondo o Estado, as empresas e os cidadãos. O ciberespaço transpõe a vida real para um mundo virtual, com caraterísticas únicas que impõem novas formas de interação e de relacionamento.

Segundo o *site Internet World Stats* de 2017 a Ásia tem 49,7% dos utilizadores da internet no mundo, a Europa 17%, a América Latina e Caraíbas 10,4%, África 10%, América do Norte 8,2%, Médio Oriente 3,8% e a Oceânia 0,7%.

A taxa de penetração da *internet* na população é a seguinte: América do Norte 88,1%, Europa 80,2%, Oceânia 69,6%, América Latina e Caraíbas 62,4%, Médio Oriente 58,7%, Ásia 46,7% e África 31,2%.

A média da taxa de penetração da *internet* em todo o mundo é de 51,7% (cerca de 3 biliões e 885 milhões de utilizadores em todo o globo). Os seis países com mais utilizadores são: 1.º China, 2.º Índia, 3.º Estados Unidos, 4.º Brasil, 5.º Indonésia e 6.º Japão. Os dois países com mais contas da rede social Facebook são a Índia com 241 milhões e os Estados Unidos com 240 milhões.

2.2. Cibersegurança

A cibersegurança pode ser definida como o sistema e processo de vigilância do ciberespaço para identificar os incidentes, as ameaças e as vulnerabilidades da rede digital assim como para assegurar uma proteção e reação eficiente às atividades das organizações criminosas transnacionais nas suas diversas formas, à radicalização e recrutamento para o terrorismo, ao ativismo político radical e subversivo, as quais procuram destruir os fundamentos do Estado de direito e pôr em causa a segurança das comunidades e dos cidadãos. Segundo Ralo, "*na cibersegurança incluem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco o espaço de liberdade individual/coletiva e de prosperidade que ele constitui e cuja responsabilidade de policiamento deve caber às Forças de Segurança e aos Serviços de Informações. A diferença entre a ciberdefesa e a cibersegurança é, por vezes, muito ténue e, devido à natureza de algumas ameaças, acabam por se sobrepor numa larga percentagem*" (Ralo, 2013).

Conforme previsto na Estratégia da U.E. para a Cibersegurança de 7 de fevereiro de 2013, a cibersegurança refere-se, por norma, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar, procurando-se assim manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas.

A cibersegurança é hoje uma área essencial para os Estados e para a sociedade civil, tendo em vista prevenir ataques às redes dos setores público e privado, os quais podem colocar em causa a estabilidade coletiva. Na Estratégia Nacional de Segurança do Ciberespaço, podemos encontrar os elementos fundamentais da cibersegurança, como sejam:

- o conhecimento das ameaças e das vulnerabilidades existentes. Este conhecimento é essencial para a realização de análise de risco, com vista a uma melhor aplicação dos meios e recursos disponíveis para o tratamento dos riscos, bem como para a identificação das lacunas a colmatar;

- desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas públicas e das infraestruturas críticas, com vista à prevenção e à reação de e a incidentes de cibersegurança;

- criar mecanismos de reporte de incidentes de cibersegurança para entidades públicas e para os operadores de infraestruturas críticas, com vista à eficácia operacional e a uma melhor avaliação situacional. A desejada avaliação situacional resulta na criação de condições para a

identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas;

- em articulação com as autoridades competentes e a comunidade nacional de segurança do ciberespaço, criar uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os operadores de infraestruturas críticas, produzir e apresentar um quadro integral e atual dos incidentes, ameaças e vulnerabilidades que pendem sobre o ciberespaço nacional.

2.3. Ciberameaças

As ciberameaças são aquelas que exercem a sua atividade e se difundem na rede fruto da utilização massiva das tecnologias de informação, podendo afetar infraestruturas críticas, o equilíbrio funcional da sociedade – sistemas informáticos dos Governos, das empresas, dos cidadãos em geral -, assim como os sistemas políticos e financeiros internacionais.

Podemos salientar como ciberameaças mais relevantes na atualidade as seguintes: o ciberterrorismo, a ciberespionagem, a cibercriminalidade, o *hacking* e o *hacktivismo*.

O ciberterrorismo consiste no uso das tecnologias de informação para difundir propaganda acerca de uma ou de várias organizações terroristas e da sua atividade, para a disseminação de ideologia radical promovendo o terror e o medo e contestando o modelo de sociedade vigente, para o recrutamento de novos membros e para o financiamento de terrorismo. Pode igualmente executar ataques informáticos com grande impacto nos sistemas e redes de computadores e infraestruturas críticas, bem como outras atividades de sabotagem, de pirataria e de utilização dos sistemas informáticos para provocar prejuízos, perturbar, parar ou destruir a atividade de alvos determinados ou indiscriminados.

A ciberespionagem é caraterizada pela exploração de vulnerabilidades encontradas em redes informáticas e em *sites* para ter acesso a informação sensível e classificada. Pode ser perpetrada por Estados, empresas rivais ou indivíduos que procuram adquirir conhecimentos e recolher informações, que lhe podem conceder uma vantagem estratégica e competitiva sobre terceiros ou ainda para benefícios financeiros provenientes da venda de informação subtraída. Atualmente, existem diversos relatórios de informações que referem o recrutamento de *hackers* por parte de serviços de inteligência de potências internacionais, com vista à espionagem em países rivais, nomeadamente em setores estratégicos nas áreas da segurança e defesa, energia, banca, finanças, tecnologia de ponta, farmacêuticas, entre outros.

A cibercriminalidade pode ser definida como toda e qualquer prática criminosa que tenha associada à sua realização, ou como meio, um aspeto cibernético ou a utilização de

computadores. Chawki refere que o cibercrime pode ser entendido "*como qualquer ação ilegal associada com a interligação de sistemas de computadores e redes de telecomunicações, onde a ausência de tal interligação impede a prática ilícita desta ação*" (Chawki, 2006). Numa outra perspetiva, "*crimes informáticos, crimes relacionados com a informática, crimes relacionados com a alta tecnologia e cibercriminalidade partilham o mesmo significado, na medida em que usam redes de informação e de comunicações que não têm quaisquer limitações em termos físicos ou geográficos e decorrem da circulação de dados intangíveis e voláteis*" (Kierkegaard, 2007: 432-433). A cibercriminalidade é caraterizada pela transnacionalidade, anonimato, tecnologia, organização e impacto (Natário, 2013).

O *United Nations Office on Drugs and Crime* (UNODC) classifica os crimes informáticos como crimes dependentes do âmbito cibernético, necessitando de uma infraestrutura tecnológica, sendo caraterizados pela criação, disseminação e difusão de malware, ransomware, ataques a infraestruturas críticas nacionais e inativando um sítio na *internet*, sobrecarregando-o com dados (um ataque *DDoS*); crimes possibilitados pelo ambiente cibernético, os quais podem ocorrer quando os computadores ou outros dispositivos estão desligados da rede ou quando dependentes da infraestrutura tecnológica, incluindo fraudes *online*, tráfico de drogas e branqueamento de capitais; a exploração e o abuso sexual de crianças, fóruns na *darknet* e a extorsão.

A cibercriminalidade não necessita de uma proximidade física entre a vítima e o agressor/criminoso. As restrições territoriais são irrelevantes no ciberespaço, isto é, os cibercrimes são transnacionais, podem ultrapassar as fronteiras de mais de um Estado, não estão confinados por fronteiras nacionais, o que implica que, para um criminoso na rede, seja tão fácil atacar um alvo em territórios longínquos, como vitimar um vizinho.

O anonimato concretiza-se através da utilização da tecnologia pelos criminosos para alcançarem níveis de dissimulação sem paralelo no mundo real, assumindo uma multiplicidade de identidades falsas ou fazendo-se passar por cidadãos inocentes, dificultando assim a tarefa das autoridades.

A tecnologia – *internet*, redes de computadores ou de telecomunicações – é usada como meio ou como fim para o cometimento de crimes. Possibilita aos criminosos utilizarem a automação, usurparem identidades, praticarem fraudes com cartões de crédito e utilizarem esquemas de cifragem para dificultar o trabalho das autoridades, camuflando eficazmente muitas das comunicações criminosas.

As organizações de cibercriminalidade recrutam jovens universitários, engenheiros informáticos e outros peritos em sistemas de informação, procuram como alvo as instituições financeiras, estabelecem alianças com organizações criminosas de tráfico de droga, tráfico de armas, tráfico de seres humanos, ou transformam-se em organizações que exploram a criminalidade sexual, a pedofilia, as burlas e os tráficos de diversa ordem, visando sobretudo o lucro.

A cibercriminalidade incide sobre as pessoas, a propriedade, as organizações e sobre os Estados. Todavia, não é fácil de definir o verdadeiro impacto da cibercriminalidade. A ausência de estatísticas válidas relativas às consequências financeiras causado pela cibercriminalidade e a persistente confusão acerca da tipificação exata destes incidentes são os maiores obstáculos à existência de uma métrica rigorosa que permita avaliar a verdadeira dimensão e intensidade do cibercrime. Alguns dos fatores apontados para as cifras negras ou baixa taxa de denúncia às autoridades policiais e judiciárias dos crimes cibernéticos relacionam-se com a relutância que as organizações e empresas têm em reportar a ocorrência de intrusões nos seus sistemas, o medo do que isso possa trazer à sua imagem pública e à sua posição no mercado concorrencial e mesmo as reticências dos cidadãos em reportarem as fraudes ou outros ilícitos de que são vítimas. Tudo isto contribui para que as estimativas de ocorrências criminais sejam inferiores à realidade.

Deste modo, "*faz sentido que as Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às atividades relacionadas com o cibercrime e o hacktivismo, que os Serviços de Informações da República atuem em casos de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham de intervir para fazer face a ações de ciberguerra*" (Nunes, 2012: 115).

Os termos *hack* e *hacking* referem-se à reconfiguração ou reprogramação de um sistema de função de forma não autorizada pelo proprietário, administrador ou *designer*. Os vocábulos têm vários significados relacionados com a tecnologia e ciência de computação: podem-se referir a uma correção ou melhoria rápida e inteligente de um problema num programa de computador ou podem significar uma solução deficiente (embora relativamente rápida) para um problema informático como um "remendo". Os termos "*hack*" e "*hacking*" são também usados para se referirem a uma modificação de um programa ou dispositivo para dar ao utilizador o acesso a recursos não disponíveis anteriormente, como adaptações de acessibilidade.

É comum o uso da palavra *hacker* fora do contexto eletrónico/computacional, sendo utilizada para definir não somente as pessoas ligadas à informática, mas também os

especialistas que praticam o hacking em diversas áreas. Assim, segundo alguns autores, *hackers* são pessoas que utilizam os seus conhecimentos de forma legal. Criam programas como *Paint.Net, Photoshop, Microsoft Office*. Os *hackers* foram os peritos informáticos que criaram a internet, desenvolveram o sistema operacional *Unix* e o que ele é hoje, mantem a *Usenet*, fazem a *World Wide Web* funcionar e mantêm a cultura de desenvolvimento livre conhecida atualmente.

Existem diversos tipos de *hackers*: os *white hat* (chapéu branco) que utilizam os seus conhecimentos com o principal interesse em segurança, isto é, procuram a exploração e deteção de erros e de conceitos, em cumprimento da lei; os *gray hat* (chapéu cinzento) utilizam os seus conhecimentos de certa forma parecidos com os *white hat*, mas, por vezes, violam as leis; os *black hat* (chapéu preto) são considerados como o "*lado negro*" de um *hacker*, isto é, *hackers* criminosos, que quebram as leis, abusam dos seus limites; os *newbie* (novatos) são pessoas novas na área, que ainda não têm grandes competências, mas podem ter bons conhecimentos; os *lammer* são pessoas arrogantes que pensam que são peritos, no entanto, não têm grandes conhecimentos.

A diferença entre um *hacker* e um *cracker* é basicamente de ordem ideológica. O cracker é uma espécie de *hacker* com disposição para provocar um dano, subtrair informações, invadir um computador, desfigurar a página principal de uma instituição ou até mesmo prestar serviços ao crime organizado. Os grupos de *crackers* são os potenciais sujeitos ativos de inúmeras atividades delituosas que são viabilizadas através da *internet*, daí o risco de cooptação pelo crime organizado (Neto, 2009: 83). Os *crackers* são indivíduos ou grupos que utilizam os seus conhecimentos de forma ilegal, muitas vezes, sem grandes qualificações ou competências em programação e sem ética, criminosos que quebram a segurança de sistemas, agindo ilegalmente e fora da ética *hacker*. A título meramente exemplificativo, criam programas para copiar ilegalmente *software*, criam *cheats* (batota) para copiar palavras-passe, entre outras.

O *hacktivismo* é um termo controverso e de difícil definição, na medida em que engloba diversos tipos de organizações, de ideologias e formas de ação direta digital. Alguns argumentam que esta palavra é usada para descrever como a ação direta eletrónica pode trabalhar para a mudança social através da combinação de conhecimentos de programação de computadores, aliada ao pensamento crítico. Outros autores usam este vocábulo como sinónimo de um ato ou estratégia maliciosa e atos destrutivos que comprometem a segurança dos computadores na *internet*.

O *hacktivismo* é a ação conduzida por indivíduos ou grupos que utilizam meios informáticos e veem a internet como um veículo para promover e catalisar as suas causas e disseminar a sua mensagem. A ideologia defendida pode ter motivações distintas, desde políticas a religiosas, mas o objetivo final é comum: chamar a atenção da opinião pública para determinado assunto.

O desenvolvimento da tecnologia levou os grupos que formam a sociedade a adaptarem-se a uma nova maneira de divulgar, protestar e aliar-se. Segundo Mathews (1997: 51-52), a revolução das telecomunicações, com o advento da internet, trouxe uma tecnologia barata e de fácil acesso que ajudou a colocar em crise o monopólio da informação, que estava nas mãos dos Governos, além de facilitar a interação por deixar o espaço aberto para a expressão das pessoas na rede, já que a democracia e a descentralização são colocadas em lugar de destaque, enquanto a hierarquia e a burocracia são desvalorizadas. O que começou com o uso de *e-mails*, desenvolveu-se para a divulgação através de sites, com a simplificação do processo de postagem de mensagens e montagem de paginas na *internet*, e chegou às redes sociais e *sites* onde é possível alcançar um número quase infinito de indivíduos através da partilha de mensagens que podem ser divulgadas por conhecidos e desconhecidos, bastando apenas haver alguma ligação, seja por participar do mesmo grupo de interesses, seja por haver algum nível de amizade (Furtado, 2013: 19).

De acordo com alguns autores, o *Twitter* merece um lugar de destaque nas redes sociais, "*amplificado pela utilização de telemóveis, aumentando significativamente a influência dos 'movimentos politicamente motivados' em dois aspetos: exploração da democratização de acesso à internet, já que não é preciso ter um site para divulgar os seus ideais, muito menos dominar a tecnologia para fazê-lo e ainda pela velocidade de atualização dos posts ou mensagens (...). Hoje, com o Twitter, numa questão de segundos é possível postar uma mensagem que poderá ser lida por milhões de pessoas (...) O acesso às redes sociais, a capilaridade (alcance global e local dessa rede e a velocidade com que é possível trocar mensagens nessas plataformas digitais, tornam-nas muito eficientes e atraentes para o ciberativismo*" (Utsonomiya & Reis, 2011: 7),

O *hacktivismo* pode assumir assim diversas facetas. Uma faceta tecno-libertária assente na ideia de que a "*internet* pode contribuir para criar uma nova era de 'transparência' na política (...). Parece ter sido essa a convicção/missão de Julian Assange, o carismático fundador do *site Wikileaks*" (Fernandes, 2014: 57) e ainda uma faceta corporizada pelos "radicais anticapitalistas, a comunidade de ativistas do ambiente, dos direitos humanos e dos revolucionários políticos, designados nos anos 60, como contracultura" (Leigh & Harding,

2011: 56). Os grupos *hacktivistas Anonymous* e os *LulzSec*, por exemplo, contestam o que "percecionam como um abuso de poder dos governos e das empresas, defendendo a necessidade de promover a transparência na política e nos negócios" (Benkler, 2012).

O *hacktivismo* engloba diversos grupos e organizações que defendem os direitos humanos, a transparência política, a descentralização da informação, a cultura de partilha, o livre acesso à informação, a liberdade de expressão, o uso e desenvolvimento de programas e sistemas em código aberto e licenças livres. Por vezes, algumas organizações *hacktivistas* aproximam-se do ciberterrorismo ou da cibercriminalidade, na medida em que causam danos nos sistemas informáticos e equipamentos, espalham vírus e penetram em redes de instituições e empresas, com o objetivo de sub- trair informação classificada e dados pessoais, bem como difundem ideias contestando o nosso modelo de sociedade e fazendo, em alguns casos, a apologia de alteração do seu sistema social e político através da ação direta. As principais missões das organizações hacktivistas consistem na criação de *sites* ou sistemas com objetivos políticos, no desenvolvimento de programas em código aberto, no espelhamento de *sites*, na subtração de documentos dos Governos ou de instituições públicas e privadas, na difusão da cultura *hacker* e da ação direta digital. Desenvolvem também técnicas mais avançadas como *spoofing*, *email-bombing* e uso de *DoS*.

Por isso, a narrativa e evocação de princípios como a liberdade de expressão, o livre acesso a informação, a privacidade individual e a transparência política, confundem-se com práticas tipificadas como crimes pela lei penal, nem sempre sendo fácil distinguir quais os verdadeiros propósitos de algumas organizações ou indivíduos que se autodesignam hacktivistas, constituindo-se como ameaças transnacionais com um potencial avassalador de desestabilização da economia global e da segurança internacional.

3. ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

Portugal tem uma Estratégia Nacional de Segurança do Ciberespaço desde 2015 (Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho), sendo previsível que leve alguns anos a ser concretizada em toda a sua plenitude. A Estratégia assenta sobre os princípios gerais da soberania do Estado, das linhas gerais da Estratégia da U.E. para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa, da Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade, e alicerça-se em cinco pilares: subsidiariedade, complementaridade, cooperação, proporcionalidade e sensibilização.

A Estratégia desenvolve-se de acordo com vários objetivos: promover uma utilização consciente, livre, segura e eficiente do ciberespaço; proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação. Define ainda seis eixos de intervenção, enformados em medidas concretas e respetivas linhas de ação, destinadas a reforçar o potencial estratégico nacional no ciberespaço.

O Eixo 1 (Estrutura de segurança do ciberespaço) é consubstanciado através do estabelecimento da coordenação político-estratégica para a segurança e defesa do ciberespaço; da consolidação do papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas, do CNCSeg; do desenvolvimento da capacidade de ciberdefesa; do desenvolvimento da capacidade nacional de resposta a incidentes; do estabelecimento de um gabinete para gestão de crises no ciberespaço; da definição e implementação de processos de governação da segurança do ciberespaço.

O Eixo 2 (Combate ao Cibercrime) é concretizado através da revisão e atualização da legislação; da agilização das capacidades da Polícia Judiciária.

O Eixo 3 (Proteção do ciberespaço e das infraestruturas) é efetuado através da avaliação da maturidade e a capacidade das entidades públicas e privadas que administrem infraestruturas críticas ou serviços vitais de informação; da adaptação e melhoria contínua da segurança dos sistemas de informação das entidades públicas, dos operadores das infraestruturas críticas e dos serviços vitais de informação, para assegurar uma maior

resiliência (capacidade de sobrevivência) nacional, adaptando-os aos novos riscos e ameaças do ciberespaço; da análise ao ambiente de informação, para tentar antecipar eventuais ataques e tomar as decisões apropriadas, acompanhando os últimos desenvolvimentos tecnológicos e analisando e antecipando ameaças; da aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas; do desenvolvimento da capacidade de deteção de ataques aos sistemas de informação; da promoção da aplicação, por parte das entidades públicas, das medidas necessárias à continuidade das operações, de modo a responder às principais crises que afetem ou ameacem a segurança dos sistemas de informação ou os operadores de infraestruturas críticas; da inclusão de medidas de segurança do ciberespaço nos planos de proteção de infraestruturas críticas nacionais.

O Eixo 4 (Educação, sensibilização e prevenção) concretiza-se através da consciencialização não só das entidades públicas e das infraestruturas críticas, mas também das empresas e da sociedade civil. Por sua vez, é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço.

O Eixo 5 (Investigação e desenvolvimento) tem em vista apoiar, fomentar e potenciar as capacidades tecnológicas, para que sejam desenvolvidas soluções nacionais, seguras e confiáveis, que possam ser certificadas, permitindo assim potenciar a proteção dos sistemas perante as diversidades das ameaças.

O Eixo 6 (Cooperação) concretiza-se através da segurança e defesa do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais ou internacionais. Requer uma abordagem em rede, pelo que a cooperação nacional e internacional nos diversos domínios de atuação é da maior importância.

De salientar o Conselho Superior de Segurança do Ciberespaço criado através da RCM n.º 115/2017 de 24 de agosto que tem por missão assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da Estratégia Nacional de Segurança do Ciberespaço (ENSC) e da respetiva revisão. É presidido pelo Primeiro-ministro ou pelo Ministério em quem ele delegar, sendo composta pela Autoridade Nacional de Segurança, SG/SSI, SG/SIRP, Coordenador do Centro Nacional de Cibersegurança, DG. da Autoridade Tributária e Aduaneira, Ministério Público, Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária, Diretor Geral da Educação, entre outros.

4. GABINETE NACIONAL DE SEGURANÇA

De acordo com o artigo 1.º n.º 1 do Decreto-Lei n.º 3/2012 de 16 de janeiro, o Gabinete Nacional de Segurança é um serviço central da administração do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar. O n.º 2 do mesmo artigo estipula que a Autoridade Nacional de Segurança, dirige o GNS e é a entidade que exerce, em exclusivo, a proteção e a salvaguarda da informação classificada.

O artigo 2.º n.º 1 do mesmo diploma refere que o GNS tem por missão garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exerce a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado – Infraestrutura de Chaves Públicas (SCEE).

É de referir ainda a Resolução do Conselho de Ministros n.º 5/90 de 28 de fevereiro que contém as normas para a segurança nacional, salvaguarda e defesa de matérias classificadas. Constitui um documento relevante e ainda em vigor, mas já algo desfasado face à evolução avassaladora das redes e sistemas de informação. Por exemplo, o glossário de termos de informações e segurança nacional em anexo à resolução já não responde às necessidades, por se encontrar desatualizado.

Aborda, no entanto, questões muito relevantes que apenas precisarão de alguma atualização em termos de nomenclatura e de contextualização, como sejam o estudo da ameaça e as medidas de segurança; a credenciação dos centros de informática do Estado, dos privados e do seu pessoal; a segurança física de instalações; a segurança de suportes físicos; a segurança lógica; a classificação, preparação e segurança de dados e programas classificados; a reprodução, transferência, controlo de segurança e destruição de dados e programas classificados.

A Resolução do Conselho de Ministros n.º 12/2012 atribui ao Gabinete Nacional de Segurança, no âmbito da medida 4 do plano global estratégico de racionalização e redução de custos com as Tecnologias da Informação e Comunicação, a missão de coordenação com as entidades relevantes da definição e implementação de uma Estratégia Nacional de Segurança da Informação, que compreende, entre outras medidas.

5. CENTRO NACIONAL DE CIBERSEGURANÇA

A Comissão Instaladora do Centro Nacional de Cibersegurança (CNCSeg), no cumprimento do mandato que lhe foi atribuído pela Resolução do Conselho de Ministros no 42/2012, aprovou no mês de julho de 2012 um relatório com uma proposta para a criação de um Centro Nacional de Cibersegurança com a missão contribuir para que Portugal use o ciberespaço de uma forma mais livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional.

Com a segunda alteração ao Decreto-Lei n.º 3/2012, efetuada pelo Decreto-Lei n.o 69/2014 de 9 de maio, foi formalmente atribuída a responsabilidade ao GNS pelo Centro Nacional de Cibersegurança. Nos termos do artigo 2.º A do Decreto-Lei n.o 3/2012 de 16 de janeiro , as competências do CNCSeg são as seguintes:

- desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;
- promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- exercer os poderes de autoridade nacional competente em maté- ria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
- contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
- promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- assegurar a produção de referenciais normativos em matéria de cibersegurança;
- apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;
- assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio;
- coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros.

O artigo 2.º n.º 2 do mesmo diploma estipula que o CNCSeg que tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

6. CENTRO DE CIBERDEFESA

Na sequência da Declaração de Praga de 21 de novembro de 2002, os Estados-membros da OTAN tomaram a decisão de reforçar as capacidades de defesa contra cibercrimes e ciberataques, criando e treinando equipas de resposta a eventos ocorridos no espaço cibernético, estabelecendo Capacidades de Resposta a Incidentes de Segurança Informática (CRISIs). Como órgão de coordenação das CRISIs dos diferentes ramos das Forças Armadas temos a Direção de Comunicações e Sistemas de Informação (DIRCSI), sob a alçada do Estado-Maior-General das Forças Armadas (EMGFA) criado pelo Decreto-Lei n.º 184/2014 de 29 de dezembro de 2014, com a missão de "*planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas*". O mesmo documento define ainda que no que concerne à ciberdefesa a DIRCSI contempla a missão de "*coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas. Conforme preceituado no artigo 30.o, ponto 6 alínea d) do Decreto-Lei no184/2014 de 29 de dezembro de 2014, compete ao DIRCSI "assegurar a coordenação e o trabalho colaborativo e integrado com os Núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA*".

O Centro de Ciberdefesa foi criado pelo Despacho n.º 13692/2013, de 11 de outubro de 2013 do Ministro da Defesa Nacional. Constitui o órgão, na dependência do CEMGFA, responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas.

Considera-se, porém, relevante "distinguir a esfera de atuação da DIRCSI e da rede de ciberdefesa do CNCS e da rede CSIRT nacional, que apresentam linhas de ação semelhantes, mas com objetivos distintos, tendo sido atribuída ao CNCS a missão de manutenção da cibersegurança a nível nacional, estando incumbido da proteção de entidades do Estado e infraestruturas críticas, em questões relacionadas com eventos no ciberespaço. Por outro lado, a DIRCSI e as várias CRISIs dos diferentes ramos das Forças Armadas asseguram a proteção do Estado num cenário de ciberguerra, prevenindo e estando pronto a responder a qualquer ciberataque que lhes seja dirigido" (Goncalves, 2016: 76).

7. UNIDADE NACIONAL DE COMBATE AO CIBERCRIME E À CRIMINALIDADE TECNOLÓGICA

Nos termos da alínea l), do n.º 3, do artigo 7.º da Lei da Organização de Investigação Criminal (LOIC) (Lei n.o 49/2008 de 27 de agosto) constitui competência reservada da Polícia Judiciária a investigação dos crimes informáticos e praticados com recurso a tecnologia informática, sem prejuízo da possibilidade de competência deferida a outro órgão de polícia criminal nos termos do seu artigo 8º.

Salienta-se que o Decreto-Lei n.o 81/2016, de 28 de novembro criou a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) no seio da Polícia Judiciária, segundo consta do preâmbulo, "à semelhança da congénere da EUROPOL – EC3", substituindo a Unidade Nacional da Investigação da Criminalidade Informática, a qual foi extinta, alterando assim o Decreto-Lei n.o 42/2009 de 12 de fevereiro que estabelece as competências das unidades da Polícia Judiciária.

Neste diploma são definidas como atribuições da UNC3T as seguintes:

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias relativamente aos crimes previstos na Lei n.o 109/2009, de 15 de setembro;

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes praticados com recurso ou por meio de tecnologias ou de meios informáticos, previstos, designadamente:

i) na Lei de Proteção dos Dados Pessoais; ii) no Código dos Direitos de Autor e Direitos Conexos, incluindo a interferência e o desbloqueio de formas de proteção tecnológica de bens e de serviços;

- prevenção, deteção, investigação criminal e coadjuvação das autoridades judiciárias quanto aos crimes:

i) contra a liberdade e autodeterminação sexual, sempre que praticados por meio ou através de sistema informático; ii) de devassa por meio da informática; iii) de burla informática e nas comunicações; iv) relativos à interferência e manipulação ilegítima de meios de pagamento eletrónicos e virtuais; v) de espionagem, quando cometido na forma de um qualquer programa informático concebido para executar ações nocivas que constituam uma ameaça avançada e permanente.

A UNC3T assegura, no âmbito da cooperação internacional, o ponto de contacto operacional permanente e colabora e apoia de forma direta as ações de prevenção, deteção e

mitigação desenvolvidas pelas entidades nacionais com competências definidas por lei para a segurança nacional do ciberespaço. Cabe ainda à UNC3T:

- assegurar o regular funcionamento de um grupo consultivo informal para debate e aconselhamento estratégico, formativo, jurídico, técnico e científico de questões relacionadas com o cibercrime, com a criminalidade tecnológica e a cibersegurança;

- assegurar a colaboração e participação direta na formação inicial e contínua sobre cibercrime aos quadros do pessoal de investigação criminal e de apoio da Polícia Judiciária, designadamente, nas áreas da segurança da informação e da cibersegurança.

Na UNC3T e sob a dependência da sua direção é criada uma equipa técnica e de investigação digital com as seguintes funções:

- otimizar e gerir as infraestruturas e meios tecnológicos atribuídos à Unidade;

- apoiar e assessorar nos planos técnico, tecnológico e jurídico, o pessoal de investigação criminal nas suas investigações;

- testar e desenvolver ferramentas específicas para a investigação do cibercrime, da criminalidade tecnológica e da decifragem de dados;

- recolher, tratar e difundir dados relativos a ciber-intelligence para apoio às investigações, à cooperação policial internacional e à prevenção de atos de cibercrime;

- desenvolver ações de contrainformação criminal;

- dar apoio em ações de caráter técnico para recolha de prova digital, nomeadamente, ações encobertas e interceção de dados;

- apoiar investigações que exijam conhecimentos técnicos especializados, nomeadamente, redes de anonimização, mercados virtuais, moedas virtuais, análise de programas maliciosos.

A criação desta unidade especializada na PJ está em linha com as diretivas e recomendações da U.E. e permitirá, certamente, melhorar a eficácia da investigação de organizações criminosas e de indivíduos que se dedicam a diversas práticas delituosas na rede, diminuir o impacto económico da cibercriminalidade e incrementar a segurança nas redes e sistemas de informação.

8. LEI DO CIBERCRIME

No artigo 2.º da Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna 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, encontramos algumas definições úteis para caraterizar a complexidade do ciberespaço.

Assim, «sistema informático» é qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção.

Os «dados informáticos» são qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.

Os «dados de trafego» são os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

O «fornecedor de serviço» é qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores.

«Interceção» consiste no ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros.

A «topografia» trata-se uma serie de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independente- mente da fase do respetivo fabrico.

O «produto semicondutor» é a forma final ou intermedia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição

conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica.

Existem diversas tipologias e modi operandi para cometer crimes cibernéticos, podendo uma rede ou sistema ser o meio do ataque ou o alvo do mesmo. Em Portugal, a já referida Lei do Cibercrime, tipifica uma série de ilícitos criminais que se enquadram na definição de cibercriminalidade: a falsidade informática (artigo 3.º), o dano relativo a programas ou outros dados informáticos (artigo 4.º), a sabotagem informática (artigo 5.º), o acesso ilegítimo (artigo 6.º), a interceção ilegítima (artigo 7.º), a reprodução ilegítima de programa protegido (artigo 8.º). Esta tipificação de ilícitos criminais poderá ter que ser revista no futuro, em função da evolução contínua da cibercriminalidade.

Os crimes relativos a pornografia infantil, referenciados na Convenção sobre o Cibercrime, não são contemplados neste diploma visto que se encontram legislados pelo Código Penal Português na alínea c) do artigo 176º, Pornografia de menores, introduzido após a alteração imposta pela Lei nº 59/2007 de 4 de Setembro de 2007, que afirma que quem "*produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio*", fotografias, filmes ou gravações pornográficas é punido com pena de prisão de 1 a 5 anos.

9. TENDÊNCIAS DAS CIBERAMEAÇAS E DA CIBERCRIMINALIDADE

Para a classificação de incidentes de segurança, o CNCS utiliza a taxonomia da Rede Nacional de CSIRTs que estabelece a classe dos incidentes e os tipos de incidentes. Neste sentido, o 'código malicioso' pode resultar em infeção, distribuição, C & C ou outro. Para a classe de incidente 'disponibilidade', podem surgir incidentes como DoS/DDoS e sabotagem. A 'recolha de informação' pode resultar de incidentes como *scan*, *sniffing* e *phishing*. A 'tentativa de intrusão' é causada por exploração de vulnerabilidades e tentativas de *login*. A 'intrusão' resulta da exploração das vulnerabilidades e de compromissos de conta. A 'segurança da informação' está relacionada com incidentes como acesso não autorizado e modificação/remoção não autorizada. A 'fraude' resulta de incidentes como utilização indevida ou não autorizada de recursos e da utilização ilegítima de nome de terceiros. O conteúdo abusivo consubstancia-se em incidentes como *SPAM*, direitos de autor, pornografia infantil, racismo e apologia da violência.

A motivação de base para a maior parte dos cibercrimes em Portugal continua a ser económica (extorsão, *phishing*, fraude) e *hacktivista* (*anonymous* e movimentos semelhantes), sendo que alguns dos principais atores criminais continuam ligados a fraude com cartões de crédito (*carding*). Das investigações em curso parece resultar um aumento significativo dos expedientes que tiram partido de produtos e serviços bancários, como é o caso dos cartões virtuais, também designados de "pré-pagos". Os crimes de extorsão (*ransomware*) registam uma tendência crescente. Em Portugal, não foram detetadas até hoje ocorrências com recurso ao modus operandi designado por "*APT*" (*Advanced Persistent Threat*). A partir dos casos acompanhados, indica-se um crescimento dos danos provocados da atividade de *phishing* com recurso a meios virtuais (incluindo empresas internacionais) e a estabilização do uso de moedas virtuais (*bitcoins* e outras).

Os dados pessoais poderão constituir um alvo crescente dos grupos criminosos. Cabreiro da UN3CT da Polícia Judiciária considera que o crime informático está em permanente mutação, por exemplo, neste momento está a alterar plataformas, passando dos computadores pessoais, para os *iPads* e *smartphones*, com capacidade de recolha de fotos e vídeo. Segundo Cabreiro, "*a generalização da internet torna difícil encontrar um perfil do autor e da vítima de crime informático*". Acrescenta que se pode encontrar "*um escalão etário mais vulnerável devido às tecnologias não fazerem parte da sua rotina*". As crianças utilizadoras de novas tecnologias podem ser vítimas de pornografia infantil e de abuso sexual *online*. Existe um

mercado de produção e distribuição de filmes, encontrando-se Portugal também na rota de circulação e residualmente de produção destes vídeos.

A utilização das plataformas de transmissão de vídeos – por exemplo, o *Facebook Live* ou o *Periscope* do *Twitter*, entre outras – para fins ilícitos, tem tido um grande crescimento em termos internacionais, nomeadamente por predadores sexuais, exibicionistas, *voyeurs* e outro tipo de agressores que assediam menores e vítimas com perfis muito diversificados, transmitem mensagens de ódio, de incitamento à violência, ao suicídio, por exemplo. A empresa *Facebook* refere estar a procurar melhorar a resposta tecnológica para reagir mais eficazmente às denúncias e a recrutar mais pessoal para as equipas que analisam as queixas e monitorizam os vídeos em direto, por compreender a enorme sensibilidade em termos de direitos individuais que decorre da exibição de imagens em tempo real. Quando um vídeo ou um *post* tem várias denúncias, o algoritmo vai alertar os moderadores. A tecnologia pode ser melhorada, admite o *Facebook*, que depende muito da combinação entre inteligência artificial, moderadores humanos e alertas dos utilizadores para monitorizar toda a rede.

No relatório da EUROPOL designado Internet Organised Crime Threat Assessment (IOCTA) de 2017 as infraestruturas críticas encontram-se na atualidade com um grau extremamente elevado de informatização e de automação, sendo, por isso, alvos potenciais de ataques cibernéticos os diversos setores prioritários e respetivas infraestruturas: energia (eletricidade, combustível, gás), transportes (aéreos, ferroviários, marítimos, terrestres), bancos, mercados financeiros, saúde (hospitais públicos e privados), redes de distribuição de água e infraestruturas digitais. Quanto aos tipos de serviços digitais igualmente cobiçados pelos piratas informáticos, salientam-se os mercados *online*, os motores de busca online e os serviços de armazenagem (*cloud*).

No que concerne à criminalidade cibernética, de referir ainda como principais tendências na U.E. as seguintes:

– o *ransomware* é, ao nível global, a ameaça mais proeminente em termos de diversidade das vítimas e da dimensão dos danos provocados. O número de ataques *DDoS* de larga escala tem tendência a agravar-se, sendo originado pela expansão de aparelhos inseguros de uso doméstico e comercial (*internet of things – IoT*). A segurança ineficaz da internet em muitas empresas, instituições e nas residências particulares, resulta no acesso ilegal, na exfiltração e na substração de dados ou informação; as burlas ou fraudes com cartões de crédito estão também em expansão, afetando em particular as companhias aéreas e a indústria hoteleira e facilitando operações de tráfico de seres humanos, de tráfico de droga e de imigração ilegal. Os ataques às redes bancárias, com vista a manipularem os movimentos das contas, a

controlarem as caixas *ATM* ou a transferirem fundos diretamente, representam uma das ameaças emergentes;

- a exploração e coação sexual de crianças na internet continua a expandir-se, quer visando o acesso físico às vítimas, quer a gravação de conteúdos sexuais em vídeo ou fotogramas. A partilha destes conteúdos é efetuada através de redes de ponto a ponto, das redes sociais ou em comunidades de predadores e agressores sexuais alojados na darknet.

- Os mercados criminais *online* utilizam sobretudo a *darknet*, permitindo-lhes uma interconexão com uma vasta quantidade de redes de criminalidade organizada, garantindo o acesso a dados de contas pessoais, documentos falsos, formas fraudulentas de pagamento. Um número sem precedentes de cibernautas utiliza o *TOR* e outros programas similares para navegarem de forma anónima e para o comércio ilegal de estupefacientes, armas e conteúdos relacionados com o abuso sexual de crianças.

A convergência da cibercriminalidade e do terrorismo é outra das tendências hodiernas. Os terroristas continuam a usar sobretudo a internet e as aplicações de comunicação *online* (exemplo: *Whatsapp* e *Telegram*) para a coordenação de ações violentas, propaganda e troca de conhecimentos. A capacidade dos grupos terroristas para lançarem ciberataques, segundo a EUROPOL, aparenta ser ainda limitada. A atividade das organizações terroristas tem sido centrada na internet livre, mas a darknet começa a ser cada vez mais utilizada pelos terroristas para campanhas de angariação de fundos, para o uso de mercados ilegais e para a difusão de ações de propaganda desencadeadas nas redes sociais *mainstream*.

Segundo Klimburg, "*cibercrime, ciberterrorismo e ciber-guerra partilham uma base tecnológica comum, ferramentas, logística e instrumentos. Podem também partilhar as mesmas redes sociais e ter objetivos similares. As diferenças entre estas duas categorias de ciba atividades são frequentemente ténues (...). Na perspetiva de um ciberguerreiro, o cibercrime pode oferecer uma base técnica (ferramentas de software e apoio logístico) e o ciberterrorismo a base social (redes pessoais e motivação) com as quais podem ser executados ataques às redes de computadores de grupos inimigos ou nações*" (Klimburg, 2011: 41).

Os *modi operandi* utilizados pelos piratas informáticos apontam para a transversalidade e transdisciplinaridade dos crimes. A utilização de técnicas de engenharia social é apontada pela EUROPOL como uma tática para o cometimento de crimes informáticos, na medida em que permite a análise do perfil, hábitos, rotinas, locais de residência e de lazer, familiares e amigos, das potenciais vítimas, aumentando as possibilidades de concretização da ação criminosa e respetivo impacto.

O *Bitcoin* continua a ser um facilitador-chave para a cibercriminalidade, aparecendo, entretanto, outras criptomoedas que começam a ganhar popularidade no submundo digital, como a *Monero*, *Ethereum* e a *Zcash*. A facilidade em abrir contas bancárias em alguns países, em particular contas *online*, está a incrementar o branqueamento de capitais.

Os fóruns criminais e as plataformas digitais de comunicação têm-se consolidado como um ambiente ideal para os criminosos cibernéticos, disponibilizando locais de encontro, mercados e acesso a competências e perícia de outros membros da comunidade de cibercriminalidade transnacional.

A utilização de aplicações seguras por criminosos – normalmente de livre acesso e populares entre os cidadãos em geral -, nos mais diversos mercados ilícitos (tráficos, criminalidade violenta, criminalidade financeira, terrorismo, extremismo político-social), proporciona a rapidez e imediatismo dos fluxos de informação, a camuflagem da identidade, a transferência de grandes quantidades de dados e maiores oportunidades de negócio.

Finalmente, segundo a EUROPOL, uma combinação de fatores de ordem legal e técnica, negam aos órgãos de polícia criminal, o acesso, de forma atempada, às comunicações eletrónicas suspeitas e a possibilidade de execução de perícias forenses. Em muitos casos, as dificuldades colocadas pelos sistemas de encriptação e de retenção de dados, reduzem a possibilidade de prossecução das investigações e a recolha da prova digital de forma célere, eficaz e eficiente.

10. CONCLUSÕES

As infraestruturas de informação e o ciberespaço "*são indispensáveis na nossa sociedade, e o seu correto funcionamento assume importância crucial para a livre circulação da informação e dos processos e serviços dependentes desse fluxo*" (Nunes, 2010: 1194).

A cibersegurança foi integrada nas estruturas securitárias preexistentes (nas Forças Armadas, nas Forças e Serviços de Segurança e Autoridades Judiciárias) em muitos países ocidentais, tendo potenciado a adoção de Estratégias Nacionais e ainda a criação de Centros Nacionais para a deteção de ameaças cibernéticas, para apoiarem operações de investigação criminal. Em alguns países, verifica-se o controlo por parte do Estado de redes organizadas de *hackers* que atuam em nome do regime (caso da China) ou numa lógica de *outsourcing* destes peritos para desenvolverem ações de ataque e defesa (Rússia).

A cibersegurança salienta o esbatimento entre o público e o privado. O setor privado está no centro da cibersegurança mundial, sendo proprietário de grande parte das infraestruturas críticas a nível global e parceiro indispensável de Estados e outros atores (incluindo a U.E. e a ONU) no combate às ciberameaças.

A cibersegurança está ainda relacionada com a dificuldade de atribuição de responsabilidades pelos ataques informáticos. Permite a existência de relações internacionais de forma anónima, escondidas do espaço público e sem conhecimento dos resultados, o que é preocupante numa perspetiva de responsabilização política nacional e internacional. O ciberespaço levanta a questão do conceito de poder nas relações internacionais. Não se trata de uma nova forma de poder, nem desafia ainda a integridade da soberania nacional, mas sim de uma certa difusão do poder por novos atores e entidades, o que há pouco tempo era limitado aos governos dos principais Estados do sistema internacional (Barrinha & Carrapiço, 2016: 256-257).

As ciberameaças e a cibercriminalidade em concreto, estão cada vez mais organizadas e transvazam fronteiras geográficas, de soberania política, de origem social e económica e tecnológicas. É, no entanto, necessário pensar em uma estrutura que coordene as diversas dimensões da segurança no ciberespaço em Portugal, evitando iniciativas casuísticas e parcelares. Revemo-nos "na necessidade de prever a existência de um órgão coordenador das áreas ligadas à Cibersegurança e Ciberdefesa do Estado (Conselho Nacional de Cibersegurança), facilitando a definição não só de uma orientação política e estratégica mais coordenada e sinérgica como também uma gestão de crises mais eficaz" (Nunes, 2012: 115). O Conselho Superior de Segurança do Ciberespaço criado através da RCM n.º 115/2017 de

24 de agosto procura fazer essa ligação entre as diversas estruturas do Estado (Forças Armadas, Serviços de Informações, Centro Nacional de Cibersegurança, Polícia Judiciária, Autoridade Tributária e Aduaneira, entre outros), não contemplando, na nossa perspetiva, incorretamente as duas Forças de Segurança com maior implantação territorial (GNR e PSP) e com um papel primordial na prevenção da criminalidade, na sensibilização junto das populações (nomeadamente, as escolas), na ordem pública e na investigação criminal.

A sociedade em rede e a revolução tecnológica em curso criam novas oportunidades e vulnerabilidades decorrentes das interdependências estruturais e funcionais entre setores considerados críticos para o funcionamento da nossa sociedade. Por um lado, as oportunidades podem ser potenciadas pela redundância entre infraestruturas e respetivos sistemas de alerta de segurança, fortalecendo a resiliência global do sistema. Permitem a troca de conhecimentos ao nível global e a cooperação entre as redes internacionais de aplicação da lei. Por outro, aumentam o potencial das ameaças e riscos afetarem mais alvos e os cidadãos em geral, na medida em que podem aproveitar-se das redes e dos sistemas informáticos desprotegidos, afetando instituições estatais, empresas e comunidades. A interdependência entre setores distintos e da rede de ligações, não minimiza o impacto das quebras de segurança, poderá sim contribuir para o amplificar.

Estas organizações criminosas assumem caraterísticas de grande complexidade, de sofisticação, de pesquisa científica e de desenvolvimento de novas ferramentas tecnológicas, de *modi operandi*, de novas formas de iludir os sistemas de segurança e os investigadores criminais, procuram parcerias, fornecedores, clientes, peritos e vítimas para obterem elevados proventos financeiros.

As redes financeiras e as redes multimédia globais "*estão intimamente relacionadas, e esta meta-rede em particular tem um poder extraordinário. Mas não o poder todo (...) ela própria é dependente de outras grandes redes, como a rede política, a rede de produção cultural (...), a rede militar e de segurança, a rede global criminal e a rede global decisiva de produção e aplicação de ciência, tecnologia e gestão do conhecimento. Estas redes não se fundem (...), envolvem-se em estratégias de parceria e de competição, formando redes ad-hoc em torno de projetos específicos. Mas todas elas partilham um interesse em comum: controlar a capacidade de definir as regras e as normas da sociedade através de um sistema político que primariamente responda aos seus interesses e valores*" (Castells, 2013: 25).

A cibercriminalidade irá explorar intensivamente o novo paradigma da computação na nuvem, a computação móvel (por exemplo, os dispositivos moveis de pagamento), as estratégias *DIY, DIWM, BYOD* e a *IoT*

A *Big Data* afigura-se igualmente como uma oportunidade para as empresas, para as Polícias, mas também para a cibercriminalidade, consistindo em informação agregada e combinada de forma global e perspetivando o desenvolvimento de sistemas de análise preditiva e a inteligência artificial associada à videovigilância ou a nano-drones que poderão ser *the next big thing* no setor da segurança eletrónica, mas também para os piratas informáticos.

O estilo de vida digital liga os consumidores cada vez mais à internet e leva-os a adquirir novas tecnologias: computadores pessoais, telemóveis, veículos automóveis com sistemas de navegação eletrónica, eletrodomésticos inteligentes, serviços *online* (contas bancárias, compras eletrónicas), robots domésticos, ou outros. A integração de sistemas de georreferenciação e de informação geográfica (como o *GPS*) e outros aparelhos, como os computadores, telemóveis, automóveis, a armazenagem em nuvens (*clouds*), as redes de acesso sem fios (wifi), criam um novo campo para o comprometimento da nossa segurança e da nossa privacidade.

A obsolescência dos regimes legais dos Estados para fazer face ao desenvolvimento tecnológico, às ciberameaças e em concreto à cibercriminalidade e à sua permanente mutação e capacidade adaptativa, é uma realidade. Os Estados autoritários recrutam peritos para desenvolver capacidades na área da ciberguerra. Torna-se difícil estabelecer com exatidão a base territorial das organizações ou dos peritos que em concreto cometem o crime ou a série de crimes, o meio utilizado, o servidor, as consequências da ação (prejuízos, lucros, informação subtraída, a existência de cavalos de Troia).

Por outro lado, existem regiões no mundo que se constituem como um autêntico paraíso para a atividade destas organizações, devido à falência ou desregulação dos respetivos sistemas de segurança e justiça. A cooperação internacional entre os Estados (e das respetivas entidades judiciais e policiais), assim como a aposta e empenhamento das Organizações Internacionais (ONU, OTAN, U.E.) e das multinacionais privadas na prevenção, proteção, deteção, reação e investigação das novas ameaças e riscos informáticos é crucial.

À medida que a tecnologia avança, surgem novas ferramentas e formas de iludir as autoridades; "*as limitações tecnológicas na deteção, classificação, e vestígios dos ataques, irão (...) complicar, ainda mais, a decisão estadual durante a análise de um ciberataque (...). A responsabilidade de um Estado deve ser julgada pelos factos disponíveis, mesmo se esta resulta numa atribuição errada. Primeiro, enquanto um Estado avalia um ataque com o melhor da sua capacidade técnica e atua com boa-fé face à informação disponível, este cumpre as suas obrigações internacionais. Segundo, Estados que recusam atuar em*

conformidade com o seu dever internacional de prevenir que o seu território seja usado para cometer ciberataques escolheram o risco de serem considerados indiretamente responsáveis, por acidente" (Sklerov, 2009: 76-78).

O século XXI necessita que os Governos e em concreto as Forças Armadas, as Polícias e os Serviços de Informações sejam versáteis, imaginativas, criativas e que adotem estratégias inovadoras para além das conceções tradicionais de segurança. Os desafios da tecnologia são e continuarão a ser avassaladores, dado que podem impactar nos direitos, liberdades e garantias dos cidadãos, mas também na melhoria da segurança coletiva, cabendo às instituições transnacionais e aos governos nacionais a consensualização e coordenação de políticas, o incremento da investigação cientifica de forma a garantirem a liberdade, a reforçarem a segurança e melhorarem a qualidade de vida nas sociedades modernas.

BIBLIOGRAFIA

Aquilla, John & Ronfeldt, David (2013), Ciberwar is Coming in Comparative Strategy, vol. 12, n.o 2 Spring, 141-165.

Barlow, John Perry (2006). Declaração de independência do ciberespaço. Brasília: Ministério da Cultura.

Barrinha, André & Carrapiço, Helena, Cibersegurança. In Segurança Contemporânea (Lisboa: Pactor, 2016)

Benkler, Yochai, Hacks of Valor. Why Anonymous is not a Threat to National Security in Foreign Affairs. April 4, 2012.

Disponível em: http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of- -valor. Consultado em 19 de outubro de 2017.

Castells, Manuel (2013), Redes de Indignação e Esperança. Movimentos Sociais na Era da Internet. Lisboa: Fundação Calouste Gulbenkian.

Fernandes, José Pedro Teixeira (2012). A Ciberguerra como Nova Dimensão dos Conflitos do Século XXI, In RI, n.o 33, março.

Fernandes, José Pedro Teixeira (2014). Ciberguerra. Quando a Utopia Se Transforma em Realidade. Vila do Conde: Verso da História.

Gibson, William, (1984). Neuromancer. Nova Iorque, Ace Books.

Goncalves, João Pinto (2016). Enquadramento legal da Cibersegurança em Portugal e no Mundo O impacto dos crimes cibernéticos no Direito Internacional. Alfeite: Escola Naval.

Kierkegaard, Sylvia (2007). EU Tackles Cybercrime. In Cyber Warfare and Cyber Terrorism. Editors Andrew M. Colarik, Lech Janczewski. Publisher Idea Group Inc (IG)): 431-432.

Klimburg, Alexander (2011). Mobilizing Cyber Power. In Survival: Global Politics and Strategy, vol. 53, n.o 1, fevereiro-março, pp. 41-60.

Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem. F.D. Kramer et al., eds. Potomac Books, Inc. 24–42.

Harari, Yuval Noah (2018). 21 Lições para o Século XXI. Amadora Elsinore.

Leigh, David & Harding, Luke, Wikileaks. Inside Julian Assange's War on Secrecy. London: Guardian Books, 2011.

Mathews, Jessica T., Power Shift. In Foreign Affairs, 76:1, 1997, p. 50-66. Disponível em: http://www.polsci.wvu.edu/faculty/hauser/PS293B/MathewsPowerShiftForA-ff1997.pdf – Consultado em 15 de outubro de 2017.

Natário, Rui (2013), O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço. Lisboa: Revista Militar n.o 2541.

NATO (2010). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organization. Disponível em: http://www.nato.int/lisbon2010/ strategic-concept-2010-eng.pdf. Consultado em 18 de outubro de 2017-10-22

Nunes, Paulo Viegas, (2010). Mundos Virtuais, Riscos Reais: Fundamentos para a definição de uma Estratégia de Informação Nacional. In: Revista Militar. Lisboa: Empresa da Revista Militar, pp. 1169-1198.

Nunes, Paulo Viegas, (2012). A Definição de uma Estratégia Nacional de Cibersegurança. In: Nação e Defesa – Revista Quadrimestral n.o 133. Lisboa: Instituto da Defesa Nacional, pp. 113-127.

Nunes, Paulo Viegas, (2015). Sociedade em Rede, Ciberespaço e Guerra de Informação. Contributos para o Enquadramento e Construção de uma Estratégia Nacional de Informação (Lisboa: Instituto de Defesa Nacional, 2015)

Ralo, Jorge (2013). CiberSegurança e CiberDefesa. In Direcção-Geral de Política de Defesa Nacional. Disponível em: http://dgpdn.blogspot.pt/2013/03/artigo-de-opiniao- -ciberseguranca-e.html. Consultado a 09/11/2015.

Ramonet, Ignacio (1998). Geopolítica do Caos. Petrópolis. Editora Vozes.

Schjolberg, S. (2012). An International Criminal Court or Tribunal for Cyberspace ICTC). East West Institute.

Sklerov, Matthew J. (2009), Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent. In Military Law Revue, vol. 201, pp. 1-85.

Disponível em: http: //www.loc.gov./rr/frd/Military Law/Military_Law_Review/pdf-files/201-fall-2009. pdf Consultado em: 19 de outubro de 2017.

Utsonomiya, Fred Izumi & Reis, Mariza de Fátima. Reflexões sobre o alcance do agir comunicativo da sociedade civil em redes sociais: o ciberativismo em questão. In SIMSOCIAL – Simpósio em Tecnologias Digitais e Sociabilidade – Mídias Sociais, Saberes e Representações – Anais. Salvador, outubro de 2011. Disponível em: http://gitsufba.net/simposio/wp-content/uploads/2011/09/Reflexoes-sobre-o-al- cance-do-agir-comunicativo-da-sociedade-civil-em-redes-sociais-UTSUNOMIYA- -Fred-REIS-Mariza.pdf. Consultado em 14 de outubro de 2017.

Convenção do Conselho da Europa (CCE), de 23 de novembro de 2001 (designada por Convenção de Budapeste), ratificada por Portugal em 2009, através da Resolução da Assembleia da República n.o 88/2009, de 15 de setembro

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

Estratégia Nacional de Segurança do Ciberespaço (Resolução do Conselho de Ministros n.o 36/2015 de 12 de junho).