MESTRADO EM DIREITO E SEGURANÇA

Dissertação de Mestrado

O "Cyber-empowerment" do indivíduo e (in)segurança nacional

Autora: Alexandra Isabel Ribeiro Quintela Alhais

Orientadora: Professora Doutora Sofia Santos

Lisboa, setembro de 2018

MESTRADO EM DIREITO E SEGURANÇA

Dissertação de Mestrado

O "Cyber-empowerment" do indivíduo e (in)segurança nacional

Autora: Alexandra Isabel Ribeiro Quintela Alhais

Orientadora: Professora Doutora Sofia Santos

Lisboa, setembro de 2018

Declaração de Compromisso de Anti-Plágio

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta de ética e disciplinar.

Lisboa, 6 de setembro de 2018

Declaração de Conformidade

A presente dissertação comporta um total de 171340 caracteres (corpo e notas de rodapé), ou um total de 199805 caracteres completa, cumprindo o estipulado no n. º4 do artigo 7º do Regulamento do Segundo Ciclo de Estudos conducente ao Grau de Mestre em Direito e Segurança (Regulamento nº 402/2016, publicado no Diário da República, 2ª série - nº 80 - 26 de abril de 2016).

Agradecimentos

Agradeço aos docentes do Curso de Mestrado em Direito e Segurança que contribuíram para a minha formação e, em especial à minha orientadora, Professora Doutora Sofia Santos, pela sua compreensão, apoio e exemplo demonstrados.

Reconheço ainda a importância que os docentes que me acompanharam na obtenção da licenciatura em Relações Internacionais na Universidade do Minho, pois foi graças a eles que ingressei neste curso de Mestrado, estando amplamente preparada para o desafio e para os que ainda irei enfrentar.

Demonstro ainda apreço aos meus colegas de mestrado Ariana, Daniel, Rita e Teresa, que enfrentaram esta etapa comigo. Assim como reconheço todo o apoio, contributo e motivação por parte dos meus grandes amigos. Aludo ainda a todos os que me acompanharam no meu dia-a-dia e contribuíram para que eu não desmotivasse ou desfocasse do objetivo primordial.

Por último, agradeço aos meus pais e à minha irmã, que nunca deixaram de acreditar nas minhas capacidades, sem eles este trabalho não seria possível.

Menções Especiais

A presente dissertação segue as normas referentes ao modelo de citação da American Psychological Association (APA) e foi redigida ao abrigo do novo acordo ortográfico. Por opção pessoal, e no intuito de preservar a autenticidade dos autores citados na presente dissertação, serão mantidas as citações de autores e documentos estrangeiros na língua original.

Lista Siglas e Abreviaturas

BYOD – Bring Your Own Device

CEDN – Conceito Estratégico de Defesa Nacional

CNCS – Centro Nacional de Cibersegurança

DLG – Direitos, Liberdades e Garantias

EUA – Estados Unidos da América

FBI – Federal Bureau of Investigation

FSS – Forças e Serviços de Segurança

GCI – Global Cybersecurity Index

IDN – Instituto da Defesa Nacional

IOT – Internet of Things

NATO – North Atlantic Treaty Organisation

NCSC – National Cyber-Security Center

NRA – National Rifle Association

NSA – National Security Agency

OI – Organização Internacional

ONU – Organização das Nações Unidas

RASI – Relatório Anual de Segurança Interna

SETA – *Security education, training and awareness*

SI – Sistema Internacional

TIC – Tecnologias de informação e comunicação

UE – União Europeia

USAID – United States Agency for International Development

WEF – World Economic Forum

Resumo

Vivemos numa era onde a tecnologia se tornou uma grande parte do nosso quotidiano, muitas tarefas, atividades e serviços estão hoje dependentes do funcionamento da rede global e da sua presença no ciberespaço. Num regresso ao passado podemos denotar que antes desta era digital as evoluções tecnológicas e societárias pautavam-se por um maior período de adaptação por parte da sociedade e das próprias economia e indústria. Os vários processos criados e implementados, eram mais morosos e mais duradouros, o que não se revê hodiernamente.

Presentemente, são quebradas novas barreiras em relação ao que existia previamente e estas novas criações acabam por modelar o mundo e a forma como interagimos com o mesmo e com os outros. Nesta dissertação, o foco central do estudo será o papel do indivíduo nestas novas dinâmicas e balança de poder, potenciadas e influenciadas pelas novas tecnologias e pelos seus efeitos e implementação. Assim como o impacto que esse empoderamento poderá ter na Segurança Nacional dos Estados da ordem internacional. De que maneira pode um indivíduo ser uma ameaça maior do que um Estado? Quais as ferramentas ao dispor dos cidadãos que podem melhorar as suas vidas, mas ao mesmo tempo, fazer perigar as vidas de milhares de pessoas por todo o globo? Será que estamos preparados o suficiente, seja individualmente, seja coletivamente, para o poder que um só consegue aglomerar graças à fonte de conhecimento e porta de entrada oferecida pelo ciberespaço?

Palavras-Chave: Indivíduo, Ciberespaço, Segurança Nacional, Novas Tecnologias, Ameaças, Cyber-Empowerment;

Abstract

We are living in an era where tecnology has become a great portion of our everyday life, a lot of tasks, activities and services are liable to the functioning of the global network and their presence on cyberspace. Returning to the past, we can note that before this digital era, the technological and societal evolutions were ruled by a longer adaptation period by society and also economy and industry. The various processes created and implemented, were harder and longer, which does not relate to what we see nowadays.

Presently, new barriers are being broken accordingly to what existed in the past, and these new creations end up modeling the World and the way we interact with it and with others. In the present dissertation, the main focus of the study will be the role of the individual in the briefly stated new dynamics and balance of power, enhanced and influenced by new technologies and its impact and implementation. As well as the impact that that said empowerment may have in the National Security of the international order States. How can an individual become a bigger threat than a State? What are the tools available to citizens that can improve their lifes, but simultaneously, endangering the lifes of thousands around the globe? Are we prepared enough, individually or colectivelly, for the power that only one person can gather thanks to the source of knowledge and gate away offered by the cyberspace?

Keywords: *Individual, Cyberspace, National Security, New Technologies, Threats, Cyber-Empowerment;*

Índice

Introdução

As novas tecnologias trouxeram inúmeras transformações às sociedades hodiernas e cujo impacto pode ser observável nas mais variadas áreas que compõem o mundo atual. A relevância que as mesmas acabam por reunir, especialmente quanto à capacitação dos indivíduos leva a que surjam novas dinâmicas societárias com poder para modelar as próprias entidades estaduais e demais atores do sistema internacional (SI).

De acordo com o referido, rapidamente fora denotado um empoderamento generalizado dos utilizadores das novas tecnologias e uma natural virtualização dos processos e atividades que antes dependiam de procedimentos de caráter mais moroso e que exigiam um maior investimento em termos de tempo, físico ou económico. Este *empowerment*, com génese traçada no uso e implementação das novas tecnologias, pode então ser tido como um *cyber-empowerment* individual. A aquisição de poder, ferramentas ou habilidades que diferem das tidas como tradicionais por parte dos cidadãos, leva a que os mesmos possam transpor barreiras que antes lhes seriam impostas e, conseguem, equilibrar a balança de poder, reclamando valências que antes lhes estariam vedadas e seriam atribuídas a outros atores. Do outro lado da equação, temos os efeitos que a dinâmica de *cyber-empowerment* pode vir a revelar em relação a outros atores, em particular nos Estados, que passam a exercer as suas competências e prerrogativas no seio de sociedades mais informadas e com acesso a novas oportunidades. Seja numa vertente positiva ou negativa, o Estado é diretamente visado pelas dinâmicas aqui elencadas, o que é aplicável à sua própria noção de Segurança Nacional.

A presente dissertação inquire sobre a dimensão do papel individual enquanto ator empoderado, via novas tecnologias, na segurança nacional dos Estados, ambicionando determinar o potencial equilíbrio entre os dois eixos em debate, determinar as suas condicionantes e estabelecer e compilar um mapa relativo às capacidades que a sua dicotomia pode conferir e introduzir naquele que é tido como *status quo* atual, moldando um futuro próximo cujos pilares podem

ser construídos a partir das medidas e das políticas aplicadas no tempo imediato. Além do referido, aludir-se-á através de uma visão crítica ao tipo de ferramentas a serem empregues para se acompanhar o vigor e caráter energético que caracteriza a era tecnológica, a posição do indivíduo na ordem internacional e a nova posição ocupada pelos Estados.

Mediante a influência e indissociabilidade do papel individual enquanto ator *cyber-empowered* e o crescente alerta para com as consequências das mais recentes dicotomias que afetam diretamente a segurança nacional dos Estados, esta temática revela-se pertinente para o mundo contemporâneo e para a sociedade portuguesa em particular. Tendo presente que os efeitos da virtualização quotidiana são generalizados e aplicáveis à totalidade dos atores, convém proceder à indagação sobre os constrangimentos que a mesma poderá adicionar ou subtrair para os atores estaduais e, ainda, para a forma como os mesmos encaram o indivíduo e seu potencial.

Nesta senda, o primeiro capítulo da presente dissertação, terá como finalidade examinar brevemente a dinâmica de *cyber-empowerment* individual, e, em simultâneo, introduzir as novas condicionantes dentro da ideia e conceito de segurança nacional.

O segundo capítulo procurará revelar de que modo o *cyber-empowerment* pode ser vantajoso em relação à segurança nacional de um Estado, seja este *cyber-empowerment* centrado apenas na ação de um indivíduo, ou de uma coletividade distinta da *framework* pública e estatal, mas liderada por um grupo de indivíduos, que podem vir a encabeçar movimentos ou empresas preponderantes em determinadas áreas e matérias e podem conferir à entidade estadual soluções para determinadas questões. Rever-se-á ainda a possibilidade de um só indivíduo poder passar a consistir um *asset* valioso para a estabilidade e para a soberania e segurança nacionais, em tudo o que implica uma ação no ciberespaço e novas tecnologias.

Será destinado ao terceiro capítulo o dissecar da tipologia de ameaças provenientes do *cyber-empowerment* individual, que podem ter como alvo um

Estado, em particular, quatro ameaças, selecionadas devido à sua crescente preponderância em termos de relevância e constrangimentos associados e, reconhecendo a necessidade do estudo que as analise, agregue e especifique entre as inúmeras ameaças existentes neste contexto, qualquer uma delas com potencial de causar danos ostensivos num Estado e sociedade e, poder consistir uma ameaça à própria soberania e segurança nacional. Perante esta temática, será do âmbito deste capítulo ainda uma análise de como estas ameaças e vulnerabilidades acabam por se manifestar de forma distinta em diferentes estados e ainda a sua imprevisibilidade.

O quarto capítulo terá como propósito o examinar dos modos de proteção ao serviço dos estados para conseguir proteger-se e aos seus cidadãos face às ameaças enunciadas no capítulo predecessor. Concomitantemente, outro dos alvos será a investigação das repercussões da concretização efetiva destas ameaças e sua exploração por parte de terceiros ambicionando, posteriormente, refletir sobre as posições adotadas por determinados estados de forma a fazer frente às suas vulnerabilidades e abordagens que tomam e, ainda o perspetivar de abordagens tendenciais que podem vir a alastrar-se a mais Estados da ordem internacional.

O quinto capítulo da dissertação focar-se-á no caso português, no tocante às dinâmicas de *cyber-empowerment* individual e segurança nacional. Aferindo não só a visibilidade que as ameaças elencadas assumem no território português, como também as ferramentas e possibilidades que o nosso Estado possui ou onde deverá investir para dar uma resposta pronta e eficaz.

Por fim, há que elencar que a metodologia utilizada basear-se-á numa visão que se demarca de perspetivas jurídicas, recaindo maioritariamente no prisma e ótica das ciências sociais, em particular das relações internacionais e ângulos político-sociológicos.

Capítulo I – As novas tecnologias, o “*cyber-empowerment*” e a segurança nacional

1 – Das novas dinâmicas societárias à crescente importância e incorporação das novas tecnologias

As novas tecnologias são um tema comum nesta década, especialmente o debate sobre os efeitos que o aumento da sua importância e crescente aplicação na sociedade envolvente têm vindo a registar. Em simultâneo, a esfera do ciberespaço, indestrinçável da revolução tecnológica, assume-se também como uma realidade paralela e complementar da vida moderna.

O ciberespaço assimilou uma porção de atividades que antes teriam sido associadas apenas a um meio físico e palpável, que incluía e requeria um maior envolvimento do indivíduo e mais esforços empreendidos para qualquer que fosse a tarefa. Hodiernamente, este espaço etéreo pesa naquele que é o contexto da ordem internacional, à imagem daquilo que defende Nye, pois a sua influência é notada na balança de poder e mutações resultantes do surgimento deste novo campo de atuação, redefinindo o status quo presente - “*Power depends upon context, and the rapid growth of cyber space is an important new context in world politics.”* (Nye, 2010, p.1) Logo, não é possível descurar-se as repercussões da disrupção da interatividade e do poder que a mesma vem distribuir pelos atores do cenário internacional e a interação entre os mesmos.

O seu papel foi exacerbado devido ao tipo de características que veio imprimir às sociedades cada vez mais globalizadas, que como refere Fernandes, nelas poderão constar a digitalização da maior parte das funções de comunicação humana e transações, um conhecimento/acesso a informação sem igual, uma crescente virtualização dos serviços e do nosso quotidiano, a crescente desintermediação e ainda a imediaticidade. (Fernandes, 2013) Na visão de Desjardins (2018), o vigor perpetuado pela revolução digital fica marcado pela forma como as trocas conseguem ocorrer e pelas assimetrias que esta vem abater entre atores, algo relacionado com a retórica de Nye:“*The low price of entry*,

anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics" (Nye, 2010, p.1) Com isto, retiram-se algumas das condições que levaram à preponderância do ciberespaço e que conduziram à repressão de determinadas barreiras que tradicionalmente consubstanciariam obstáculos ao executar de um grande número de atividades.

As mutações têm vindo a revelar a conversão para uma sociedade em rede - "(…) *pensar o mundo em que vivemos passa por perspetivar uma sociedade em rede, em que a interação entre os homens deixa de ser influenciada por barreiras geográficas e passa a ser condicionada pela disponibilidade e pelo tempo de acesso aos recursos de informação*." (IDN-CEDESEN, 2013, p.8) Ora, rapidamente as sociedades se adaptaram e receberam a novidade tecnológica no seu interior, com mudanças constantes e aceleradas, com a introdução de propriedades que levam ao melhoramento das sociedades e dos indivíduos fisicamente, mentalmente e na sua experiência. As mesmas resultam no desenvolvimento de novas técnicas e métodos de produção, assim como modelos de mercado que se transformam perante uma produção e mercados globais.

São ferramentas cada vez mais utilizadas e adaptadas às necessidades dos atores e cuja utilidade não tem limites. Para Shapiro, esta revela-se como aquilo que ele denomina como uma "Control Revolution", mediante a distribuição de poder que os demais atores podem juntar, exemplificando assim essa mudança: "*Sitting in front of a computer screen in your bedroom or office, it may be hard to see how a click here and there can really affect anything beyond the box, let alone your four walls. But connect that box to an outside line and things start to happen. As you gain access to newly personalized information, your perception of the world changes. Publish online and caucus with fellow travelers, and you can change other people's views. Sign a digital petition and influence the political process. Buy stocks – or groceries – online and affect the economy"* (Shapiro, 1999, p.29). Além das alterações que o autor refere, há que referir também uma maior facilidade no replicar e manipular das informações, o que se transpõe para

um maior poder no lado do utilizador, algo que Mendonça refere como um "efeito de David"(Mendonça, 2012), pois esta transição marca sobretudo aquilo que pode ser tido como um novo mundo para a multiplicidade de atores, configurando-se um empoderamento dos que seriam tidos como mais fracos ou vulneráveis até hoje.

Em termos societários, este empoderamento tem resultado no reformular do funcionamento de todos os processos complementando o mundo físico – "(…) *a crescente informatização em todos estes domínios trouxe novos suportes e os meios de transmissão digitais de informação, que passam a coexistir com os formatos físicos tradicionais.*" (Santos, 2015, p.422) Estas transformações fizeram-se sentir também no papel dos atores do SI, o que por sua vez revelou novas dinâmicas, possibilidades e oportunidades que vêm condicionar a visão contemporânea do mundo.

2 – O *cyber-empowerment* dos cidadãos no mundo atual

O indivíduo enquanto ator, foi dos mais impactados pelas novas dinâmicas, tendo sido alvo de um *cyber-empowerment*[1] que o dotou de faculdades diferentes e que quebram as barreiras à ação tidas como tradicionais, levando ao atenuar de determinadas desigualdades que antes vigoravam nas comunidades que integram – o já referido efeito de David.

Este *cyber-empowerment* é referente ao empoderamento denotado em vários setores de atividade e de envolvimento por parte dos cidadãos. É registada uma maior abertura, exposição à inovação e personalização, que servem os seus interesses e motivações, obtendo uma *ownership* consideravelmente superior sobre o processo de *decision-making* envolvido nas suas vidas – do trivial ao sério, o que nos torna "*(…) masters of our own domains.*" (Shapiro, 1999, p.44)

[1] *Cyber-empowerment* consiste num termo que será referido ao longo deste estudo como um empoderamento por via das novas tecnologias - do acesso e da utilização das mesmas.

Ilustrando esta argumentação e a possibilidade de readaptação e facilitação permitidas pela virtualização das sociedades, Shapiro partilha um exemplo que revela a integração dos cidadãos e de que maneira essa sua interação pode colmatar deficiências e desigualdades que existiam até então. Na sua pesquisa, salientou o caso de indivíduos com autismo, caracterizados por alguma dificuldade em comunicar com outros indivíduos, mas que conseguem fazê-lo por intermédio das novas tecnologias, podendo realmente demonstrar quem são sem estar condicionados. Este caso elenca de forma palpável o impacto gigantesco e a imagem aproximada do empoderamento individual permitido. Sobrepondo-se a este cariz mais individual e privado, os mesmos cidadãos conseguem exercer poder sobre recursos que antes seriam monopolizados por entidades privadas ou Estados, permitindo-lhes antecipar-se e contornar alguns processos, conseguindo benefícios próprios. A progressiva virtualização do mundo leva a que a separação entre espaço físico e ciberespaço seja cada vez mais ténue e, gradualmente, os indivíduos começam a tirar partido da influência que as novas tecnologias podem demonstrar nas suas vidas. As suas ações e comportamentos passam a ter uma influência incomensurável, dependendo das que empreende e de como as perceciona.

Os círculos de influência, comunicação e interligação hoje são mais abrangentes e variados, consoante a atividade ou tópico em que se focam, ou a rede social em que existem - relatando acontecimentos sem ser jornalista, poder escrever e publicar sem possuir ou pertencer a uma editora ou construir e agregar popularidade graças ao tipo de atividade que opera no ciberespaço e, para muitos, até tornar isso na sua ocupação profissional. Para Shapiro, este é um dos pontos fortes na revolução tecnológica, "(…) *the instant ability to spread your unexpurgated words – a piece of yourself, really – to the four courners of the earth.*"(Shapiro, 1999, p.9) Mas indivíduos empoderados continuam a ser diferentes entre si, em termos de valores, interesses ou motivações, o que implica que esse empoderamento tanto possa ter uma vertente positiva como negativa, ou seja, nesta sociedade interligada, podem acabar por estar sujeitos a um novo tipo de ameaças que antes não os assolariam, assim como eles próprios poderão vir a

constituir uma ameaça para outros atores. Veja-se que, o universo de informação a que se tem acesso é variado e pode ser utilizado consoante aquilo que se procura, levando a que muitas vezes surjam indivíduos que podem utilizar esse poder adquirido para explorar outros atores.

A perceção de uma cidade ou meio físico também sofreu alterações, tendo as suas componentes migrado para o universo cibernético, já indissociável da esfera física. Mitigaram-se fraquezas, colmaram-se deficiências e empoderaram-se atores, em simultâneo, abriu-se caminho também para novas ameaças surgidas das novas tecnologias e sua incorporação nas sociedades. Fenómenos que antes seriam apenas hipotéticos ou da literatura fazem parte do leque de oportunidades e de ameaças previstas e sentidas nas sociedades, deixando os atores à sua mercê, pois, denota-se que apesar de se ter abraçado a novidade tecnológica, esta não foi acompanhada de um aumento proporcional da segurança ou preocupações securitárias que as mesmas pudessem suscitar.

Estas condições, contribuíram para o surgimento de um debate correspondente ao *empowerment* em questão e à capacidade que as sociedades têm de combater e proteger-se perante este fenómeno. Para além destas constantes, a equação é complexificada mediante as transformações sociais que os próprios Estados têm enfrentado, passando a ver a sua soberania em determinadas matérias questionada perante legislação supraestadual, sendo que apesar da tradição hegemónica dos Estados como ator preponderante, temos visto tendências para a difusão de poder, especialmente nos anos mais recentes com a globalização do acesso às tecnologias e, com a divisão do palco internacional e de determinadas prerrogativas antes características apenas das entidades estaduais - “*Os Estados são os atores mais relevantes na atual política internacional, mas não detêm o palco internacional exclusivamente para si.”* (Lourenço, Rodrigues, Lopes, Silvério & Costa, 2015, p.48)

O papel e a relevância dos cidadãos tornou-se difícil de ignorar dentro do seu próprio território, podendo influenciar dinâmicas definidoras daquilo que é o comportamento e as medidas reivindicadas pelo próprio Estado que observa os

seus cidadãos ou populações a tomar partido dos conhecimentos e possibilidades que lhes são facultadas pelas novas tecnologias. Nesse sentido e perante as capacidades transformadoras na mão do indivíduo e cuja magnitude pode ser avassaladora, são despertadas novas práticas, visões e políticas.

3 – As novas tecnologias e a Segurança Nacional

Conceitos associados ao poder estadual e à tradição vestefaliana acabam por ser postos em causa mediante a própria revolução tecnológica. Seja o de soberania, que se tem afastado daquele que era o inicialmente elaborado por Jean Bodin e que implicava o Estado como ator preponderante e hegemónico do SI, ainda mantendo a sua relevância: "*(…) o Estado permanece como um ator relevante nas relações internacionais, ainda orientadas em grande parte por lógicas de poder."* (Lourenço, Rodrigues, Lopes, Silvério & Costa, 2015, p.32) Ou o conceito de Segurança Nacional, recorrendo a um conceito do Instituto da Defesa Nacional (IDN) em 1989 que a definia enquanto "(…) *condição da Nação que se traduz pela permanente garantia da sua sobrevivência em Paz e Liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda coletiva das pessoas e bens e dos valores espirituais, o desenvolvimento normal das funções do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas"*(Lourenço, Rodrigues, Lopes, Silvério & Costa, 2015, p.17).

Ora, numa análise cuidada deste último conceito, vemos que Segurança Nacional pressupõe várias componentes que contribuem para a segurança de um Estado, seja por exemplo a sua soberania, a integridade territorial, a proteção dos seus cidadãos e das funções estaduais e o preservar da sua língua, cultura ou valores. Na sua totalidade, são essenciais para a preservação física e ideológica de um país, sendo influenciadas constantemente pelo tipo de contexto que se manifesta num determinado período.

Este conceito de Segurança Nacional passa a incluir um conjunto de ameaças e vetores diferentes daqueles que seriam de esperar em comparação com a época de surgimento do Estado Moderno e Paz de Vestefália já que, nos trâmites da sua origem e na génese da responsabilidade de conferir segurança às populações sobre sua égide, deve ser acrescentada a componente tecnológica à equação, pois continua a ser esperado que o Estado proteja todos aqueles que estejam a seu cargo e continue a zelar por si mesmo - *"Governments, of course, have always exercised authority over their citizens. And much of this sovereign power is a legitimate part of the social contract, the implicit agreement we make to live in a civilized world rather than a barbarous state of nature."* (WEF, The Global Risks Report, 2018, p.) Assim, ao invés de se encarar o ciberespaço apenas como uma plataforma paralela ao "mundo real", deve procurar-se contar com aquilo que esse universo comporta enquanto elo entre os mais variados atores, intenções e conglomerando uma grande diversidade de possibilidades, acabando por colocar em perspetiva aquele que é o real poder de um Estado e como é que este pode assegurar a sua segurança nacional perante uma esfera tão vasta e díspar em termos de conhecimentos, capacidades e objetivos.

Da mesma maneira, o empoderamento de outros atores deve ser uma das preocupações dos Estados, seja para ajudar a desenvolver e enriquecer a educação, a cultura e o conhecimento beneficiando o Estado e o seu funcionamento, seja em termos de poderem constituir outro tipo de ameaças às quais os mesmos não estavam habituados. Em sentido figurativo, se as ações da sociedade se desenvolvessem num oceano observar-se-iam oportunidades e riscos e enquanto uns estão preparados e capacitados a lidar com eles e a tornar-se até predadores, outros, acabam por estar sujeitos a ameaças conhecidas ou desconhecidas e que põem a sua a vida em perigo, tornando-se presas.

Certos Estados[2], revelam uma perspetiva e entendimento baseados em desconfiança quanto a estas mutações, o que consequentemente leva à tentativa de

[2] Aqui, alude-se a Estados que possam ver a recente abertura como algo contrário aos seus ideais, encarando essa difusão de poder como uma nova modalidade de cidadania onde os cidadãos são capazes de diversificar

procurar restringir os efeitos das novas tecnologias nos territórios que tutelam. Aliás, o modo como as ameaças, benefícios das novas tecnologias e do respetivo *cyber-empowerment* dos cidadãos são percecionados difere consoante a agressividade de cada fenómeno na sua ordem interna e até da própria noção de Segurança Nacional[3] atribuída.

É de salientar que tem vindo a apresentar-se uma disparidade quanto à afetação dos Estados, não só por uns comportarem vulnerabilidades de maior significância, ou uma maior preparação e robusteza em termos securitários, mas também tendo em conta o perfil, notoriedade ou interesses que os mesmos possam ter ou suscitar face a terceiros. Uma tipologia de ciberataque ou de investimento pode sustentar resultados com um índice superior de sucesso em determinado Estado enquanto outra abordagem seria preferível para outras entidades estaduais.

Na mesma retórica, as noções relativas ao que é tido como âmbito da Segurança Nacional apresentam algumas diferenças, daí que a categoria de ameaças e potencialidades que podem conglomerar no seio da sua ordem ciberespacial interna possa vir a depender daqueles que são os seus pilares estratégicos e vertentes em que incidem as suas políticas. Numa adenda, veja-se que a Rússia[4] entende a segurança nacional, através da sua Estratégia de Segurança Nacional para 2020 como – "(…) *the situation in which the individual, the society*

---

as suas crenças e interesses, contrariando aquilo que é veiculado pelo governo em questão. É um empoderamento que entendem ter a capacidade de atentar contra o funcionamento correto das suas instituições e sociedade. Um dos casos que melhor transmite esta ideia remete para a China que, de acordo com o *Independent* é acusado por grupos ligados à defesa dos direitos humanos como dos Estados que mais censura os cidadãos no ciberespaço, procurando eliminar tudo aquilo que não corresponda aos padrões sociais e políticos defendidos pelo governo chinês. (Keating, 2017)

[3] Ainda que possam ser apontadas várias diferenças quanto à afetação e ao tipo de prioridades e orientações estratégicas entre os atores estaduais, deve salientar-se os denominadores comuns em que a noção de segurança nacional dos mesmos assenta, nomeadamente a salvaguarda da independência nacional e do funcionamento das instituições competentes. Aliás, na realidade, a componente securitária que se atribui a um Estado acaba por assentar em ideias semelhantes e generalizadas, sendo que difere depois com o desenvolver dos Estados, da sua cultura e das suas prioridades, compartilhando a génese do conceito de segurança nacional que aplicam.

[4] Abordam-se os casos da Rússia e dos Estados Unidos da América (EUA) por serem Estados que mantêm a sua preponderância na ordem internacional, enquanto demonstram divergências nas suas sociedades e ideologias. Por serem os dois Estados que estiveram no palco da Guerra Fria, o seu entendimento da noção de Segurança Nacional foi fortemente influenciado pela história, pelo que transmitem duas perspetivas nacionalistas, mas com prioridades díspares e objetivos demarcados.

and the state enjoy protection from foreign and domestic threats to the degree that ensures constitutional rights and freedoms, decent quality of life for citizens, as well as sovereignty, territorial integrity and stable development of the Russian Federation, the defense and security of the state"(Estratégia de Segurança Nacional Russa, parte I, ponto 6, para.1)– Em simultâneo, no caso dos EUA, a segurança nacional corresponde a um termo que inclui a defesa nacional e as relações externas do país, incluindo por sua vez a obtenção e retenção de uma posição favorável no tocante a relações externas, uma vantagem militar ou defensiva sobre outros estados ou grupos de estados e a salvaguarda de uma postura defensiva capaz de resistir a ações hostis que surjam da ordem interna ou não.[5] Com isto, a abordagem estadual diverge mediante o contexto em que os mesmos operam as suas prerrogativas estaduais, adaptando a resposta consoante aqueles que são os seus valores e objetivos, algo que depois acaba por se traduzir na criação de políticas relativas à sua cibersegurança e segurança nacional.

Os atores começam a impor-se de maneira a conseguir lidar com tudo aquilo que acarretam estas mudanças, reconhecendo-se como fundamental o garante da segurança do ciberespaço, devendo considerar-se como um imperativo nacional.

4 – O *clash* de opiniões face aos efeitos do *cyber-empowerment* individual nos atores estaduais

As dicotomias elencadas suscitam um debate no meio académico sobre a sua influência real nas sociedades e no quotidiano da ordem internacional, surgindo inúmeras reflexões sobre o papel do Estado e dos indivíduos perante a sua intervenção neste novo domínio operacional, que pode ser considerado como o mais recente campo de batalha, suplantando a ideia de guerras tradicionais.

[5] Estas disposições relativas à forma como os EUA encaram a sua segurança nacional vêm elencadas naquele que é a sua Estratégia de Segurança Nacional datada de 2017. Nesse documento, é indicada como responsabilidade fundamental a proteção do povo americano, do território e da forma de vida americana, sendo estipulados como outros pilares essenciais a promoção da prosperidade do país, a preservação da paz através da força e o desenvolver e crescimento da influência americana no mundo. (National Security Strategy of the United States of America, 2017)

Capítulo I – As novas tecnologias, o "*cyber-empowerment"* e a segurança nacional

Algumas das críticas apontadas às Tecnologias de Informação e Comunicação (TIC) e, em particular, ao fenómeno do *cyber-empowerment* individual condenam a sua utilização e demonizam a progressiva virtualização das sociedades. É apontada a incomensurável quantidade de vulnerabilidades e fragilidades que o ciberespaço de um território estatal pode conter, contando com o comportamento dos seus cidadãos, com a atratividade do país enquanto alvo e sua predominância a nível internacional. Estas são algumas das condições que levam muitos teóricos[6] a optar por posições conservadoras em relação à adaptação e evolução dos Estados nesta era digital. Com efeito, os mais céticos culpabilizam a revolução digital pelos fenómenos que hoje condicionam o exercício seguro da cidadania e dão lugar a uma nova tipologia de conflitualidade. Um dos pontos mais vincados é que, tradicionalmente, todos os atores estavam cientes das regras do jogo, ao passo que agora existe uma esfera quase anárquica em que tudo é concretizável e imprevisível, algo a que os Estados não conseguem dar resposta.

É alegado que este ambiente impede o cumprimento das prerrogativas nacionais devido à pluralidade de atores, dificultando qualquer oportunidade de estabilidade dentro das sociedades. Contudo, acresce ainda a ideia de que a incorporação das TIC e empoderamento consequente retira quaisquer obstáculos à ação individual, o que pode ter um cunho negativo devido a demonstrar uma facilidade excessiva na concretização das suas tarefas e interação com a sociedade, algo elencado pelo próprio Aldous Huxley numa reflexão centrada nas alterações societárias a que assistia e que previa para eras futuras: "*Qualquer pássaro que tenha aprendido a esgravatar a sua porção de alimentos sem ser obrigado a usar as asas renunciará a breve trecho ao privilégio de voar e permanecerá para sempre preso ao solo. Com os seres humanos passa-se qualquer coisa de semelhante. Se se lhes der pão de uma maneira regular e abundante três vezes por*

[6] Um dos grandes críticos na literatura é Edward Tenner que menciona até aquilo que classifica como um efeito de vingança que é visível na relação e impacto da adoção das TIC no mundo e sua globalização. Este autor defende que nelas jaz a criação de problemas maiores do que aqueles que veio ajudar a mitigar (Tenner, 1996) Na sua abordagem defendeu que deveria encarar-se com grande ceticismo este *boom* tecnológico devido às possíveis consequências inesperadas.

dia, muitos deles contentar-se-ão em viver apenas de pão – ou pelo menos de pão e circo."(Huxley, 1958, p.154) Ou seja, esta facilitação leva a que os cidadãos não valorizem ou rentabilizem aquilo a que são expostos, conduzindo a que as suas ideias e ações contrariem o exato propósito pelo qual se defendem a abertura da rede global, passando a tomar todas as questões advindas como garantidas e não apresentando uma postura acautelada e dedicada no modo como lidam e interagem na esfera ciberespacial.

Em contrapartida, existem autores[7] que optam por uma abordagem e perceção menos maquiavélica das novas tecnologias e suas consequências, nomeadamente Shapiro, cuja argumentação se foca no facto das novas tecnologias, dispositivos e questões envolventes serem apenas um meio para atingir um fim, uma ferramenta, pelo que não se deve demonizar a mesma devido às ações que indivíduos operacionalizam recorrendo a estas.

A teorização de Shapiro foca-se na culpabilização do agente e não dos "objetos" que lhe facultam tais ações, recorrendo a uma comparação com o debate sobre armas de fogo que tem lugar nos EUA. O autor pressupõe que medidas que tentem mitigar a utilização das TIC são orientadas por propósitos errados, pelo que deveriam antes focar-se na responsabilização daqueles que realmente utilizam estas ferramentas com intenções condenáveis ou de forma descuidada, vincando que "*the way we use guns would seem to be the single most important factor in determining their impact on society*." (Shapiro, 1999, p.13) No seio da comunidade académica argumenta-se ainda que, aliado ao facto deste empoderamento individual ser algo irreversível - apesar de mutável – se deverá apostar nos efeitos positivos que esse mesmo tem, como uma crescente conetividade e espírito de cooperação ou no fomento da pesquisa e desenvolvimento em áreas de interesse humano como a saúde e que são cruciais para a evolução societária.

[7] Um dos autores que reitera os efeitos positivos a retirar é Mulgan, sendo que menciona a existência de ganhos potenciais consideráveis nas aplicações da computação e, das TIC em geral, em setores cruciais. (Mulgan, 2005) Outro autor de referência para estas ideias é o próprio Shirky, cujas contribuições já foram analisadas ao longo deste estudo, pois o escopo da teorização do autor tem como alvo principal os níveis de conetividade e cooperação que as TIC trouxeram para os indivíduos, algo que se traduz no empoderamento dos mesmos e numa contribuição para o desenvolvimento das sociedades.

As duas posições compreendem perspetivas distintas sobre a realidade a que se assiste atualmente, e, na verdade, os dois campos levantam questões válidas sobre a aplicação e influência das novas tecnologias e subsequente empoderamento, pelo que sendo irreversível o progresso crescente da tecnologia e das sociedades, os Estados (que também eles encaram as mudanças com visões divergentes entre si) passam a adotar medidas e políticas que sirvam de instrumentos para a sua adaptação e proteção, salvaguardando as suas capacidades relacionadas com temas de cibersegurança e protegendo as vertentes que podem interligar-se com as suas próprias políticas externas.

Independentemente do tipo de mentalidade em vigor, a abordagem *in casu* deverá sempre atender à proteção das suas populações e à redução dos danos derivados de ciberincidentes. Internacionalmente, organizações internacionais (OI)[8] passaram a dedicar e a estudar as mesmas dinâmicas e a produzir documentos e políticas que ambicionam estabelecer um ordenamento mais conciso e que controle o comportamento dos mais variados atores, enquanto permite e versa sobre o tipo de resposta a ser dadas às tendências globais.

A realidade é que os efeitos têm vindo a fazer-se sentir, especialmente no âmbito da segurança nacional dos Estados, efeitos estes de caráter dual, onde uns têm a capacidade de elevar e transformar as sociedades e seu funcionamento, enquanto outros juntam poder suficiente para perigar a sua sobrevivência.

[8] A Organização das Nações Unidas (ONU) é uma das organizações que tem vindo a debater e analisar os fenómenos aqui estudados, tendo até realizado um estudo que visava a avaliação das defesas e investimentos estaduais na área da cibersegurança, de modo a conseguir perceber quais os Estados que apresentam uma maior ou menos preparação face aos desafios do mundo atual. Na elaboração do relatório relativo ao ano de 2017, apelidado de Global Cybersecurity Index (GCI), não só salientou a necessidade de se criarem estratégias de cibersegurança estaduais, como elencou ser problemática a falta de uma resposta concertada pela comunidade internacional face às temáticas relacionadas com a cibersegurança. (NG, 2017)

Capítulo II – O “*cyber-empowerment”* individual: que contributo para a segurança nacional?

1 – O potencial de indivíduos “*cyber-empowered*” para a segurança nacional

A salvaguarda de novas capacidades e oportunidades transmite-se num contributo individual positivo para componentes de grande valor quanto à segurança nacional de um Estado. Esse *Cyber-empowerment* é manifestado pela capacitação dos cidadãos em melhorar e apoiar a evolução de vários campos de grande importância para um país, para o seu funcionamento e sociedade.

São efeitos que devem ser capitalizados por parte das entidades competentes, de modo a conseguir amplificá-los e o próprio Estado fazer uso de cidadãos independentes, que podem agora trazer algo de novo. Como analisa Shirky, “*The Web created a new ecosystem*” (Shirky, 2008, p.60), salientando a quebra total com a tradicional inclusão dos cidadãos e populações e sua interação com o meio, contando-se alterações radicais na gestão e operacionalização das sociedades, assim como da forma como os cidadãos podem contribuir para o crescimento e evolução das mesmas.

O empoderamento em si, suscita um ancorar de sentimentos de comunidade e de cooperação, resultando em inovações e descobertas ainda mais notáveis. A par da união e democratização do quotidiano, são atores que se influenciam mutuamente num dado período, contribuindo para o surgimento de novos debates e partilha de informação utilizável *a posteriori* por outros cidadãos e demais jogadores do palco internacional.

Na perspetiva individual, pode comprovar-se a existência de um efeito positivo do *cyber-empowerment* individual na Segurança Nacional pois é possibilitada a realização de atividades que melhoram o bem-estar social, promovem a participação na esfera pública, a democratização e apoiam uma maior consciencialização das populações, sendo que todas estas são componentes vincadas direta ou indiretamente na ideia/conceito de Segurança Nacional. São processos que solidificam setores fulcrais para o Estado, cujo interesse deve

sempre ser o progresso, uma verdadeira "arquitetura de participação" - expressão cunhada por Tim O'Reilly e que versa sobre a facilidade com que a interação e partilha ocorrem no ciberespaço (O'Reilly, 2011). Trazem uma maior criatividade e diversidade, antes impossibilitada pela dificuldade de interação e pela falta de voz tradicional dos cidadãos.

Como infere Shapiro, a verdade é que quando se procuram opiniões e soluções num conjunto maior de indivíduos, a probabilidade de obter algo novo, dinâmico e que realmente ofereça melhores factos e ideias sobre uma determinada temática é extremamente superior do que se se continuasse a requisitar apenas a participação de estudiosos ou profissionais (Shapiro, 1999). Desde campanhas que visam a proteção ambiental ou a aplicações que têm como objetivo avisar e virtualizar a via pública de maneira a que os seus utilizadores possam optar pelas opções que comportem maior segurança para si e para as suas deslocações – tornam-se empreendedores, cujas ideias poderão tornar-se vitais para a segurança estadual[9]. Daqui, pode salientar-se por exemplo os contributos derivados da atividade de inúmeras start-ups[10], focalizadas nas mais variadas áreas, desde o ambiente até à cibersegurança, que lançam as campanhas tendo como objetivo a consciencialização e o mitigar dos problemas que estas têm como alvo. Através

[9] No palco internacional, um dos Estados que apostou nas potencialidades que o empreendedorismo e o envolver dos cidadãos na própria sociedade consiste nos EUA, este país promoveu a criação de vários programas dedicados à promoção de parcerias entre empreendedores e entidades governamentais, assim como de apoio e financiamento às start-ups que proliferavam no seu tecido empresarial nacional. Mediante o tipo de especialização de cada negócio ou unidade, conseguem "leverage" que contribui para o crescimento e desenvolvimento de novas políticas, fomentando a inovação em setores da sua segurança nacional. Entre as iniciativas promovidas podem encontrar-se a *USAID'S Grand Challenges for Development* que inclui especialistas, cientistas, pesquisadores e empreendores cujo objetivo é descobrir soluções inovadoras para problemáticas dos desafios de desenvolvimento globais, muitos deles com implicações em áreas com ligação direta à segurança nacional norte-americana e estabilidade internacional ou a iniciativa *Partnering to Accelerate* Entrepreneurship que procura aumentar o investimento no setor privado e ajudar a que determinadas empresas e setores consigam desenvolver-se e dar o retorno devido ao Estado Americano através das suas investigações e descobertas. (GES, 2017)

[10] Dentro do ecossistema em estudo, uma das start-ups cujo âmbito revela uma contribuição significante para campos fulcrais da segurança nacional e das populações corresponde à Protenus. Criada em 2014, centra-se no uso inteligência artificial para proteger os registos eletrónicos de saúde dos pacientes, fazendo ainda a devida monitorização de qualquer tipo de atividade suspeita.É uma tecnologia passível de ser aplicada nas infraestruturas críticas relacionadas com a área da saúde dentro de um dado território, salvaguardando as mesmas e mitigando os danos que qualquer tipo de intrusão poderia criar. Assim, protege os utentes e as instituições, cujo correto funcionamento influencia o bem-estar das populações, contribuindo para a segurança nacional. (Goldman, 2018)

destas campanhas, muitas vezes conhecidas graças à sua promoção online e ao público que conseguem atrair, as entidades competentes acabam por tomar conhecimento de ideias criativas e percecionam as mesmas como alternativas viáveis a alguns dos processos e *modus operandi* de determinados setores de atividade estadual, por exemplo aqueles que lidam com infraestruturas críticas ou permitem melhor utilização dos recursos ao nosso dispor, contribuindo ultimamente, para consolidar as áreas correspondentes a outras linhas de ação da Segurança Nacional.

Além destes fenómenos relatados, contribui ainda para a salvaguarda de trechos da cultura de cada comunidade ou comunidades pertencentes a um país, na medida em que a internet se tornou o veículo de transmissão e preservação de elementos culturais e que levam à valorização dessas características que diferenciam Estados e os tornam únicos. São ações que partem de cada indivíduo, que estima aquilo que o identifica e o une às suas raízes e não deixa que os valores e tradições culturais se percam, perpetuando as imagens, ideais e identidade que compõe os países em questão e que marcam a cultura e história nacionais e devem ser preservadas, algo que corresponde a um dos interesses estatais.

Mediante a hipótese dos Estados não só fomentarem estas dinâmicas como as virem a adaptar às suas realidades, abre-se uma nova etapa no mundo contemporâneo, já que a disponibilidade de financiamento e talento dentro de uma ordem interna poderá ajudar um Estado a assumir-se e assegurar a sua continuidade. É necessário analisar o potencial que este empoderamento individual atrai e de que maneira pode ser absorvido e adotado numa ordem interna, devendo procurar antecipar-se os efeitos positivos que estes fenómenos têm nas áreas de interesse vital para o Estado, não descurando as tendências que os mesmos acarretam.

1.1 – Indivíduos como instrumento de transformação e evolução no funcionamento das sociedades

Graças ao empoderamento e novas acessibilidades de que beneficiam, os indivíduos passam a ter as capacidades necessárias para conseguir influenciar o funcionamento e os processos que anteriormente diriam apenas respeito a infraestruturas estaduais.

Essas dinâmicas são comprovadas pelo registar de movimentos que buscam justiça social ou a reformulação de processos relativos a determinado setor da sua sociedade e que inspiraram mudanças na mesma, revelando-se bem-sucedidos. Uma ilustração destes movimentos enquanto instrumentos de crescimento e sinal de evolução remete para a *The ParoleWatch*, que se focava na reforma do sistema de justiça norte-americano. Nesse domínio, eram proferidas opiniões sobre cada caso, havendo uma análise de candidatos a liberdade condicional e que levava os cibernautas interessados a partilhar a sua "sentença". Porém, movimentos como este facilitavam a opinião sem ter acesso a todas as informações referentes ao caso que se tratava, apesar de ainda assim se poder dizer que consiste uma forma de *empowerment* que, se corretamente utilizada, pode vir a beneficiar e transformar os processos característicos de um Estado*: "If citizens were urged to express their views after being exposed to more thorough and evenhanded information, this level of interest in our criminal justice system would be welcome*."(Shapiro, 1999, p.152) Ao melhorarem e incidirem sobre áreas de atuação e interesse do Estado[11], comprova-se como o *cyber-empowerment* individual tem uma implicância direta na Segurança Nacional, tornando o indivíduo num *asset* valioso. Se capitalizados por parte do Estado, há muito a ganhar, sendo o seu papel e postura determinantes para o tipo de resultados a esperar. O desafio, para Gonçalves, prende-se com a

[11] Na mais recente Estratégia de Segurança Nacional dos EUA, a proteção e desempenho correto das instituições governamentais é vista como uma das prioridades norteadoras das políticas americanas quanto à sua segurança nacional, demonstrando assim o tipo de efeitos que campanhas como *The ParoleWatch* podem ter no desempenhar das funções e evolução deste tipo de entidades americanas (National Security Strategy of the United States of America, 2017). Este tipo de processos e instituições são tidos como fulcrais e, segundo o documento mencionado, devem ser protegidas de modo a salvaguardar o bem-estar social e político americano.

abordagem que os governos deverão ter face ao ciberespaço e novas tecnologias, que é um equilíbrio bem-sucedido da utilização segura e livre por parte dos cidadãos e da simultânea garantia dos Direitos, Liberdades e Garantias (DLG) e cumprimento das prerrogativas estaduais de zelo pela segurança das populações e infraestruturas-críticas.

1.2 – O caso da Wikipedia como exemplo do impacto positivo do empoderamento

Uma das provas dos efeitos benévolos do *cyber-empowerment* individual consta nas dinâmicas coletivas originadas a partir da presença individual no ciberespaço. Ou seja, através de grupos formados graças ao acesso e à ligação criada de acordo com os interesses de cada um, que contribuiu para a aglomeração de cibernautas *like-minded*, e, consequentemente, aproveitam assim a quase não existência de limites ou esforço para se juntar no apoio a causas ou movimentos. Desta distinguem-se ainda outras vias pela qual este *cyber-empowerment* se pode verificar e que, mais claramente, se observa a sua contribuição para a segurança nacional.

Um dos exemplos presentes na literatura é indicado por Shirky e remete para o ataque bombista registado no metro de Londres em 2005. Aquando do sucedido, rapidamente fora criada uma página na Wikipédia, dedicada aos eventos e constantemente atualizada pela população, informando o mundo e, em particular, outros habitantes londrinos, sobre os mais variados detalhes através daquilo a que assistiam. Rapidamente a página se tornou uma ferramenta de comunicação e de entreajuda, permitindo aos que ainda se encontravam nas ruas se pudessem informar sobre o ocorrido e procurar sítios que lhes conferissem a segurança que procuravam - “*The Wikipedia page received more than a thousand edits in its first four hours of existence, as additional news came in; users added numerous pointers to traditional news sources (more symbiosis) and a list of contact numbers for people either trying to track loved ones or simply figuring out how to get home.”*(Shirky, 2008, p.116). A plataforma permitiu ajudar na busca de cidadãos,

na sua identificação e contribuiu para a sua segurança, tudo graças a um esforço de caráter coletivo que levou os mais distintos indivíduos a reeditar a página consoante a informação que tinham e aquilo a que puderam assistir. Neste caso, conseguiam obter informações que não só ainda não estavam disponíveis para a comunicação social, como também ajudaram as autoridades destacadas e encarregues de lidar com o acontecimento, centralizando toda a informação relacionada com o mesmo.

É visível, nesta exposição, o tipo de contributo favorável para a Segurança Nacional, na medida em que foi um movimento que gerou maior estabilidade e ampliou os níveis de segurança em momentos de âmbito mais caótico, como seriam expectáveis no contexto de um ataque terrorista. Demonstrou como os cidadãos "cyber-empowered" podem consubstanciar novos aliados de um Estado, através dos vários "olhos" e perspetivas que podem apresentar perante um acontecimento e suportando uma demarcação face ao que é comunicado pelas entidades dedicadas à comunicação e aquela que é a realidade de facto vivida. Contudo, esta situação verificou-se numa época onde algumas plataformas não existiam ou estavam ainda em processo de criação pelo que atualmente, como verificado aquando de outros ataques terroristas pelo globo, redes sociais como o Twitter[12] ou Facebook são umas das primeiras a noticiar tais eventos, de modo a que se crie uma discussão em torno dos acontecimentos e quase de imediato as informações são partilhadas com o resto do mundo.

1.3 – O papel de indivíduos do setor privado

Para além das capacidades de indivíduos comuns ou de indivíduos que possam estar inseridos em dinâmicas de caráter coletivo, o *cyber-empowerment* é

[12] Em 2009, esta plataforma permitiu a difusão de múltiplos relatos da queda de um avião da *US Airways* no rio Hudson em Nova Iorque, levando a que o mesmo conteúdo fosse instantaneamente partilhado, com atualizações ao segundo, algo característico da mesma (Coyle, 2010). Na eventualidade deste tipo de ameaça ou outras que possam perigar o dia-a-dia dos cidadãos e das infraestruturas públicas e privadas que fazem parte da arquitetura de um Estado, estas ferramentas permitem que possam ser evitadas baixas ou danos superiores aos que seriam registados no caso de não se rever um acesso generalizado.

revelado também no poderio adquirido por parte de indivíduos que tutelem atividades do setor privado, mas cuja atividade seja norteada para áreas de interesse estadual e cujos estudos e inovações podem também ser utilizados pelo Estado em ações futuras. Destarte, poderá idealizar-se um indivíduo que esteja à frente de uma empresa tecnológica e, por sua vez, pode ser um aliado relevante nas questões relacionadas com a cibersegurança de um Estado. São alianças valiosas para o bem-estar e para a segurança, sendo que no caso de se rever uma sinergia sólida, as duas partes beneficiam e ainda permitem uma maior segurança dos cidadãos. Esta é uma dicotomia elencada pelo *World Economic Forum* (WEF), que investiga a partilha de informação e busca de vulnerabilidades entre Estado e setor privado, já que*: “The more government discloses vulnerabilities to the private sector, provided the private sector expeditiously mitigates those vulnerabilities, the more likely software is to be secure against all actors.*” (WEF, Cyber Resilience, 2018, p.13)

Ora, é uma interação saudável que beneficia todos os agentes do ciberespaço, onde por um lado se valoriza a entidade privada e o trabalho desenvolvido pelos indivíduos dedicados a esse setor e, por outro, em conjunto se contribui para o fortalecer e impedimento de determinadas ameaças, mitigando e eliminando as vulnerabilidades que possam ser do seu conhecimento. Este tipo de cooperação, contribui para a responsabilização das partes envolvidas e poderá ser uma das respostas para corresponder às exigências do mundo atual, perpetuando um clima de cooperação, segurança e crescimento que valorize as valências da sociedade enquanto zela por áreas relevantes da segurança nacional.

Capítulo III – O indivíduo "*cyber-empowered*" como ameaça ao Estado e à segurança nacional

1 – Os indivíduos como fonte de instabilidade interna

A outra face da moeda refente ao *cyber-empowerment* pauta-se pelas condições que levam a que este fenómeno consista uma ameaça à Segurança Nacional.

Reconhecendo a incapacidade de elencar de forma justa e exímia a totalidade de vias pelas quais um indivíduo pode - devido às TIC - ser uma ameaça, optar-se-á por uma abordagem mais seletiva, afunilando problemáticas específicas que permitem analisar diferentes modalidades deste tipo de ameaças, estudar a sua influência e consequente intensificação e gravidade atuais. Expondo os vetores consoante a diversidade do impacto e as questões que os mesmos salientam para o estudo do impacto negativo na Segurança Nacional.

Na realidade, admite-se que a vida em sociedade acaba por se desenrolar na esfera ciberespacial, e cujo controlo deixa de estar concentrado apenas numa tipologia de ator:"*The problem for all states in today's global information age is that more things are happening outside the control of even the most powerful states*" (Nye, 2010, p.1). Frisando-se a necessidade de reajustamento a uma realidade onde novos atores conseguem angariar um poderio progressivo e desafiante da balança internacional.

Atinente às ameaças e ciberataques *per se*, o seu impacto beneficia da incapacidade ou lentidão na resposta por parte das vítimas, que por vezes, nem notam que estão a ser alvo de ataques. Tornaram-se na nova normalidade e as suas consequências são exaltadas devido à própria arquitetura do ciberespaço, forma como o mesmo foi introduzido e evoluiu: *"Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense*." (Nye, 2010, p.5)

Com isto, o *cyber-empowerment* individual deve ser motivo de preocupação por parte das entidades governamentais, pelo que é um fenómenos com dois prismas (enquanto oportunidade e enquanto ameaça) e cuja capacidade de infligir dano é enorme e quase sem limites, com capacidade para colocar em causa a segurança e soberania nacionais. De acordo com Moniz, estes podem ser provenientes de fontes díspares e incomparáveis, diferindo em quem as veicula e nos métodos que utilizam, ainda que sempre via ciberespaço (Moniz, 2018)

Ora, isto levanta questões relativas à globalização do uso das novas tecnologias e os seus efeitos nefastos, em particular porque os Estados não estão preparados e continuam a “várias velocidades”, colocando em causa muito mais do que o funcionamento dos governos, mas também o tipo de relações internacionais e cooperação que possam ter como potenciais ou vitais, assim como a própria responsabilização adjacente dos intervenientes.

Todavia, não seria de esperar que todos os cibernautas comportassem os mesmos interesses e intenções e ao apresentar-se este contexto contemporâneo, onde as ameaças já não são os cavalos de Troia clássicos, nem confrontos entre exércitos, a própria postura dos Estados tem vindo a sofrer alterações, até porque diferentes ameaças cibernéticas acabam por afetar os Estados de forma desigual, ainda que todas elas revelam uma tendência notável para se intensificarem. Estas, podem ser destacadas também consoante a sua intencionalidade, demonstrando uma vez mais a diversidade que incutem ao novo ecossistema.

1.1 – As ameaças não intencionais provenientes do “misuse” das TIC

O *Cyber-empowerment* individual, pelo menos o acesso generalizado às TIC contribuiu para que grande parte dos cibernautas seja inconsciente perante as necessidades e preocupações securitárias que deveriam acompanhar o seu trajeto no ciberespaço e os dispositivos que tem na sua posse. Mesmo não sendo intencional, o “misuse” das novas tecnologias, acaba por comportar uma ameaça séria à Segurança Nacional, já que numa rede de dispositivos interconectados, basta um para comprometer todo o funcionamento da mesma.

Estatísticas ilustrativas desta problemática estimam que 41% da população que integra o ciberespaço não consegue sequer determinar se um e-mail consiste num esquema de *phishing* ou não (Jeffries, 2017), o que os leva a agir sem colocar em causa a veracidade do mesmo. Adicionamente, de acordo com um relatório do WEF, a valorização de conteúdo que contenha informações erradas e enviesadas tem vindo a tornar-se outro dos acontecimentos registados, aludindo aos resultados obtidos após um estudo sobre as eleições norte-americanas, proporcionado por esta organização internacional, e em que foi possível determinar que perante um número igual de notícias falsas e notícias verdadeiras, as falsas tiveram melhor performance em termos de interações sociais no ciberespaço em relação às que relatavam os factos verídicos (WEF, The Global Risks Report, 2018, p.48). Ambas, relacionam-se com uma visível falta de escrutínio sobre aquilo com que se deparam durante o uso e tempo que permanecem no ciberespaço, promovendo um ambiente que espalha meias-verdades e, cujo sucesso obtido, pode encorajar outros meios de comunicação a desconstruir alguns factos de modo a torna-los mais apelativos às suas audiências, prejudicando não só os cidadãos mas também as ideias e políticas perpetradas pelo Estado, levando ao condicionamento da opinião pública e debate político. Transversalmente aos condicionamentos enunciados, deve manter-se presente que são comportamentos que impõem limitações à comunicação e relação entre os mesmos e as entidades competentes, tocando em pontos de caráter sério e com implicância real em componentes essenciais para a segurança nacional, sendo elas a democracia e o exercer de uma cidadania, agora minada pela incapacidade revelada em conseguir veicular determinadas informações às suas populações e mostrando-se as mesmas inaptas a contribuir de forma eficaz em processos que modelam o próprio funcionamento do país, das suas infraestruturas e o exercício da cidadania. O estudo sobre as eleições americanas proveniente do *World Economic Forum* é uma das provas das consequências que este "misuse" consegue acarretar, influenciando a atualidade estatal e favorecendo determinadas ideias através de informações manipuladas de forma a veicular ideias erróneas, adulterando em simultâneo aqueles que são alguns dos momentos mais proeminentes no seio de um Estado, como a definição

do seu governante, influenciando assim a sua segurança, bem-estar e independência nacionais.

Outro elemento que espelha o "misuse" redireciona para falta de conhecimentos sobre os processos e aplicações das quais depende a realização de atividades no ciberespaço. Se a esta se juntar uma despreocupação, é criada uma receita suficientemente desastrosa para se traduzir em graves consequências. Numa perspetiva genérica, mediante o reunir destes dois fatores, os indivíduos colocam-se em posições vulneráveis para sofrer ataques de terceiros que minem a sua privacidade, os explorem para fins económicos ou os infetem com qualquer tipo de *malware*. Representam fragilidades para si mesmos e para os círculos que integram, sejam eles profissionais ou privados.

Frequentemente, empregados de determinadas instituições usam até os seus próprios dispositivos para aceder a ficheiros institucionais ou pessoais, confundindo as duas esferas por intermédio do mesmo**.** Embora tenham passado pela formação adequada, perpetuam comportamentos que permitem o corromper de ficheiros institucionais, perdas de informação, deixar que a rede seja alvo de vários tipos de *malware*, ou até levar a que atores externos consigam aceder a informações de cariz privado ou confidencial[13]. São ações que perigam o meio em que decorrem e muitas vezes são desenvolvidas em infraestruturas públicas e críticas - "(…) *présentent un risque pour les entreprises qui les emploient*." (Martin, 1997, p.14) Pegando no caso das fugas de informação, não sendo antecipadas pelas entidades alvo, levam a que a instituição perca a credibilidade junto dos seus pares e clientes/população, informação que é *"para a maioria das organizações o seu bem mais valioso*."(Patrão, 2012, p.199) Posteriormente, veem

[13] Estes eventos materializam-se no mundo físico, não consistindo meramente em projeções de quem busca prejudicar e salientar os perigos que as novas tecnologias incutem nas sociedades. A vulnerabilidade apresentada por estes indivíduos é comprovada pelo registado em 2015 quando um funcionário da National Security Agency (NSA) usou o seu computador pessoal para tratar informações de caráter classificado, dando lugar a uma janela de oportunidade aproveitada por *hackers,* alegadamente apoiados pelo governo russo, que prontamente as roubaram. (Volz & Menn, 2017) Resultaram num perigar de processos e programas essenciais para aquele que era o bem-estar e salvaguarda dos interesses norte-americanos e sua política externa, logo, um claro golpe nas linhas inalienáveis da sua respetiva segurança nacional.

o "fator inovação" em causa, diminuindo o potencial da ambição de vantagens competitivas. Advindo do interior das próprias instituições, os responsáveis não conseguem corresponder no tempo necessário às mesmas, o que resulta numa reação tardia que foca no mitigar dos danos já causados.

As questões relativas ao papel individual nas organizações em que se insere e quanto às suas práticas tecnológicas, vai muito além do mencionado, pois não se prendem apenas com a fuga de informação, perda de confidencialidade e inovação, devendo ter-se em mente que podem gerar condições suficientes para criar danos no próprio funcionamento dessas estruturas públicas ou privadas, privando-as de conseguirem realizar as ações para as quais foram criadas. Uma conduta descuidada de um operador de uma central nuclear pode ser o rastilho necessário para terceiros se aproveitarem, para manchar todo o progresso já feito e para colocar as políticas estaduais em perigo, sendo uma ameaça considerável para a sua segurança nacional. Fora este exemplo, todas as empresas e infraestruturas que estejam ligadas a recursos de elevada importância para a subsistência de um Estado e suas populações, como são a eletricidade ou água, podem ser incluídas nesta vertente.

Ações desta ordem, sendo subvalorizadas, comprometem o meio informático em que decorrem e nem todas as instituições estão propriamente protegidas em termos de políticas e educação dada aos seus funcionários, que por descuido ou desinteresse cometem determinados erros: *"Think of an employee derailing cybersecurity plans by inadvertently clicking on a phishing email because not enough was done to spread risk awareness"* (WEF, The Global Risks Report, 2018, p.57). Na mesma lógica, os seus efeitos que se fazem sentir em áreas importantes para a ordem interna e sobrevivência do Estado, podem ter um caráter catastrófico.

1.2 – O *Cyber-empowerment* individual e o papel das dinâmicas grupais como ameaça à segurança nacional dos Estados

Quando coletividades e outro tipo de associações criam movimentos disruptivos que ponham em causa os valores e o funcionamento das sociedades de um Estado em particular, o governo e suas forças competentes, perceciona esses fenómenos como uma ameaça ao seu bem-estar e segurança nacional. É algo facilmente detetável especialmente no caso de governos de cariz autoritário e opressores dos DLG dos seus cidadãos, pelo que mais facilmente se analisa o *cyber-empowerment* com impacto positivo nos cidadãos, derivado das dinâmicas grupais em escrutínio.

A instabilidade que são capazes de gerar pode originar-se a partir da conetividade do mundo atual, cujas condições possibilitam que indivíduos motivados consigam gerar iniciativas capazes de contagiar um grande número de pessoas e, a partir daí, operacionalizar algo onde possam defender as suas causas, quer estejam na mesma linha dos pensamentos estaduais ou não. (Benkler, 2006)

Um dos exemplos dessa instabilidade proveniente desta tipologia de *cyber-empowerment* provém de Shirky (2008), que relembra os acontecimentos[14] na Bielorrússia em 2006, onde grupos de jovens começaram a comparecer em locais de valor cultural e histórico onde apenas comiam gelados - sim, gelados. Este era um ato banal e do quotidiano que não aparentava qualquer tipo de ameaça concreta, mas a verdade é que consistia num meio de demonstrar a capacidade de organização e união dos cidadãos de todo o país perante um governo autoritário que violava constantemente os direitos fundamentais da população que tutelava. Esses grupos "protestavam" sem cometer qualquer ação pela qual fossem forçados

[14] Os protestos elencados ocorreram após a reeleição de Alexander Lukashenko com cerca de 85% dos votos, resultados esses que para os observadores internacionais teriam sido manipulados, motivando a realização de protestos face a um governante de cariz autoritário. A posição de Lukashenko foi de localizar os opositores e proceder à prisão dos protestantes. Esses eventos acabaram por inspirar a *flash-mob* com recurso a uma prática pacífica e aparentemente inofensiva (gelados), levando as populações à praça pública e demonstrando a capacidade de mobilização grupal que fora possível graças à comunicação permitida pelas TIC à disposição dos cidadãos e que, em simultâneo, ameaçava os ideais perpetrados pelo Estado em questão e sua conceção de segurança nacional.

a sair dessas áreas, pelo menos por justa causa. Porém, isto seria o que acabaria de suceder, tendo passado a circular fotos na internet que mostravam as forças policiais a forçar essa saída, sem causa justificável, procedendo à expulsão dos indivíduos. Resta elencar que, na internet, rapidamente estes conteúdos se tornaram virais e chegaram a instâncias internacionais, demonstrando as violações nos direitos fundamentais de que a população da Bielorrússia estava a ser alvo.

Foi através das novas plataformas do ciberespaço que estes grupos tiveram a possibilidade de se organizar e, pelo facto deste movimento ter sido planeado via *Weblog*, o Estado em questão não tinha meios de detetar todos os que tiveram acesso a esse planeamento, logo, não conseguiria ser eficaz a deter os responsáveis ou a impedir que o mesmo se realizasse, aliado ao ponto de não estar capacitado para determinar quais os que realmente iriam comparecer. O que é importante reter é a possibilidade conferida de se organizarem sem serem detetados e o método pacífico e inocente escolhido para demonstrar a sua união e crenças.

Concomitantemente, na perspetiva estadual, este tipo de organização acabou por ser uma afronta aos valores que o mesmo Estado defendia não pela ação em si, mas antes pela simbologia que a mesma carregava:"*The threat from a group eating ice cream isn't the ice cream but the group.*"(Shirky, 2008, p.168) Ao reagir, os governantes acabaram por atrair a atenção das entidades internacionais, que rapidamente condenaram as ações contra os cidadãos que, por sua vez, fizeram uso da esfera pública para expor a sua realidade.

A dinâmica deste caso particular espelha como os indivíduos conseguem confrontar um Estado expondo o tratamento de que estavam a ser alvo. Isto é um exemplo do poder das tecnologias nos cidadãos e especialmente da sua influência num Estado e na sua Segurança Nacional. O eco internacional foi palpável e mais uma vez veio confirmar o poder da consciência coletiva e organização da mesma.

É visível o impacto de dinâmicas grupais naquele que é o *status quo* em vigor numa determinada sociedade – "*the organization of group effort can be invisible, but the results can be immediately visible."* (Shirky, 2008, p.168)

Portanto, as entidades estaduais podem ter a sua Segurança Nacional comprometida como um todo, ou algumas linhas estratégicas que a componham, sendo criadas novas formas de se exercer e influenciar poder político (Shapiro, 1999).

Aliando-se à crescente conectividade, pluralidade e fluidez de ideias, contribuem para debates sobre temas ainda pouco badalados no seio de sociedades, muitos ainda tabu, mas que, gradualmente, acabam por se alastrar à esfera pública. Daí que um Estado possa ver no *cyber-empowerment* individual e suas dinâmicas grupais adjacentes, um motivo para se sentir ameaçado.

1.3 – Os *Cyber-mercenaries* como ameaça à ordem internacional e Segurança nacional

Uma das ameaças mais recentes e com maior potencial de destruição concentra-se nos chamados *cyber-mercenaries*, fenómeno este que é representado por uma adaptação dos mercenários tradicionais às novas tecnologias e ciberespaço. São a representação do poderio de atores não-estaduais e das capacidades que agregam, outro dos frutos da virtualização progressiva das sociedades e do seu funcionamento. A sua preponderância vem desafiar a ordem e *status quo* presentes, reanimando a luta pelo poder e levantando questões que abalam o cerne do conflito tradicional e intergovernamental que anteriores períodos históricos perpetuavam. Na verdade, “*(...) the [non-state] actors that we look at on a daily and weekly basis have capabilities that actually exceed the capabilities of most nation-states.*” (Segal, 2018, para.4)

Transversalmente, ao inaugurarem uma nova era digital, consubstanciam uma das maiores ameaças globais atuais, pois como alude Weber, se em tempos passados as potências que contassem com a colaboração de mercenários saíam vencedoras, hoje o impacto dos mesmos continua a ser palpável e determinante para o sucesso e persecução dos objetivos estaduais. (Weber, 2018)

Com efeito, são grupos que operacionalizam uma miríade de atividades no ciberespaço, geralmente em busca de lucros económicos[15], fornecendo serviços por todo o universo informático, desde trabalhos mais simples até aos que podem colocar em causa a sobrevivência de populações e Estados. Tal como a tipologia tradicional de mercenários, caracterizam-se por não "vestirem a camisola" de uma força em particular, servindo apenas os seus próprios interesses e os dos seus empregadores/clientes.

Quando se pensa neste fenómeno há que pensar nas potencialidades que os mesmos têm, que são uma arma valiosa pois permitem a terciarização das ações estaduais que se conseguem demarcar das operações e sair impunes face às leis e desconfianças internacionais. Como são grupos que operam através de canais profundos da *Deep Web*, encontram-se em contacto com o negócios mais obscuros e beneficiam de uma invisibilidade que facilita as suas atividades, aumentando exponencialmente a hipótese de não serem nunca localizados, saindo ilesos a par do seu cliente ou empregador.

São vistos como uma área explorável por parte dos Estados, dependendo daqueles que são os objetivos e estratégias nacionais, algo também salientado por Depasquale e por Daly - *"Nation-states are increasingly exploiting this challenge by conducting cyber operations through third-party groups."* (Depasquale & Daly, 2016, para.2) Mediante essa sua utilização, operacionalizam ciberataques que podem ter como alvo outros Estados e minar a sua segurança nacional, seja através de ações contra as suas infraestruturas críticas, populações, espionagem, sabotagem, entre outros.

Tendo em conta a lucratividade destas ações, multiplicam-se os grupos dedicados a este tipo de atividade, alguns deles chegando a operar com o conhecimento das entidades da comunidade internacional, como fora o caso da

[15] Face aos dados apresentados pelo domínio *Hashed Out*, hackers chegam mesmo a auferir cerca de trinta mil dólares por um ou vários trabalhos, sendo os valores dependentes do tipo de trabalho que realizam e de todas as condicionantes que poderão agravar ou dificultar o seu sucesso. (Nohe, 2018)

companhia *Hacking Team*. (Makuch & Tucker, 2016) A companhia em questão vende ferramentas de espionagem e intrusão para várias corporações, governos e forças de serviços e segurança (FSS) e, pese embora inquiram sobre a finalidade dessas aquisições, não podem atestar o tipo de uso que lhes será dado, advogando que estão simplesmente a prestar um serviço, aliás, por essa mesma razão, é que esteve envolvida em polémicas pelo facto de fornecer essas ferramentas a países com um historial de desrespeito pelos DLG dos seus cidadãos. Relativamente à interação entre esta instituição e organismos estaduais, segundo um documentário realizado sobre a atividade, o governo da Etiópia recorreu à mesma de modo a adquirir meios que permitissem a vigilância e persecução de jornalistas que não estivessem de acordo com a mensagem do próprio Estado, tendo mesmo conseguido infiltrar um *malware* nos computadores pessoais dos mesmos.

Todavia, nem todas as ações são viabilizadas por companhias reconhecidas, tornando-se ainda mais indesejáveis, e nem sempre se consegue determinar quem encomenda tais ataques. Ainda assim, ao serem realizados, quer sejam bem-sucedidos ou não, oferecem sempre informação importante sobre o tipo de segurança que a vítima tem ativa (Gelbstein, 2012). Outras das vantagens de que beneficiam é que os seus alvos nem sempre conseguem aperceber-se de que foram vítimas de um ciberataque, pelo que por vezes já é tarde demais para agir e procuram apenas fazer uma gestão das perdas. Após essa fase, quando buscam pela responsabilização dos atacantes encontram vários obstáculos para o sucesso dessa missão, o que cria por vezes constrangimentos dentro dos seus pares pois gera-se um clima de instabilidade e desconfiança.

Alguns atores estaduais que recorrem aos *cyber-mercenaries* são: a Ucrânia que os contrata de modo a conseguir encontrar e atacar os seus inimigos (Wolf, 2015), o Irão que os recruta com o objetivo de lançar campanhas de *hacking* (Farrel, 2018), a China que faz uso destes grupos para conseguir atrair dentro da esfera pública indivíduos capacitados o suficiente para servir os seus interesses e,

um último exemplo concernente à Rússia[16] que financia cidadãos privados para agirem por si nas frentes que constituam prioridades para o país.

Na multipolaridade a que se assiste, o recorrer a estas práticas e grupos permite que dados Estados possam vir a tirar partido das oportunidades que lhes são apresentadas no ciberespaço, de modo a conseguir adquirir vantagens e um novo posicionamento na ordem internacional, como é o caso chinês ou russo. As vantagens referidas podem englobar a aquisição de informações sobre outros atores, a interferência direta ou indireta nos processos referentes a outros Estados, a promoção e o veicular de determinadas ideias que os favoreçam, entre muitas outras aplicações. Estas linhas de ação causam certas tensões no bem-estar e no funcionamento de quem se encontra na posição de alvo destas operações, infligindo determinadas consequências nas componentes da sua segurança nacional e, mascarando-se de forma a dificultar a retaliação por parte da mesma. Ainda que ultrapassada a bipolaridade mundial da era da guerra fria, algumas das tendências internacionais têm vindo a manter-se, denotando-se que a Rússia e os EUA[17] continuam a ser dos mais fustigados e das potências com maior capacidade de enveredar por estes rumos em prol do cumprimento dos seus objetivos estratégicos, sendo ainda impossível de desconsiderar a China como outro dos Estados preponderantes. Os três têm sido apontados como a raiz de muitos dos ciberataques registados, fundamentando-se ainda que se encontram nos bastidores de muitas das operações encabeçadas por ditos grupos de indivíduos nos territórios

[16] Um dos grupos associados à Rússia corresponde à APT28, pois os alvos são entidades que tendem a representar algum interesse para o governo russo, entre eles a North Atlantic Treaty Organization (NATO) ou as entidades competentes da Geórgia, e cujo *malware* pode ser interligado à ação de profissionais russos. Segundo Atkinson (2018) a ação deste grupo pode mesmo ser detetada como proveniente e financiada por ligações ao governo. Evidências de que o governo russo utiliza e apoia estes grupos são reveladas pela inércia perante as acusações de *hackers* russos pela comunidade internacional, agindo apenas se os mesmos tiverem alvos da mesma nacionalidade, algo que Maurer refere como "*a paradigmatic case of passive support for cybercrimes that do not work against the country's interest.*" (Maurer, 2018, p.173)

[17] De acordo com a *Symantec* os EUA são o país que regista um maior número de data breaches, sendo que no ano de 2016 contaram-se 1013 ataques, face a apenas 38 no Reino Unido no mesmo período. Quanto à suscetibilidade a ciberataques no geral, em 2016, cerca de 39% dos cidadãos norte-americanos foram vítimas destes fenómenos.

correspondentes às esferas nacionais desses Estados – desde a alegada interferência russa nas eleições americanas[18], como a propagação de *malware* no ciberespaço norte-americano proveniente de grupos que mantêm ligações próximas com a China.

O rastreio dos atos perpetrados é frequentemente inconclusivo quanto à fonte de emissão dessas campanhas, até porque tendem a corresponder ao tipo de contratos que invoca secretismo de modo a ser protegida a identidade do Estado que se encontra por detrás dessas investidas, evitando o escalar de um conflito internacional. Embora existam essas condicionantes, muitas dessas capacidades acabam por se encontrar fora do âmbito das capacidades e dos recursos disponíveis para as entidades estaduais na sua generalidade, pelo que recorrem a estes indivíduos de modo a contratarem forças especializadas[19] naquelas que são as medidas que pretendem aplicar de modo a servir os seus interesses, amplificando a ação e a importância dos *cyber-mercenaries* enquanto fenómenos e ferramentas. Não obstante o referido, o nível de risco também diminui quando se procura o *outsourcing* em vez de se depender ou apostar apenas nos recursos nacionais de dada entidade estatal, diminuindo a possibilidade de serem descobertas as suas intenções. Veja-se que a intrusão e roubo de informação confidencial e classificada apresenta uma grande ameaça para a segurança nacional de qualquer Estado

[18] As alegações a que se faz referência, surgiram a partir do registo de uma série de ataques direcionados a agências dedicadas aos processos eleitorais e a computadores do partido democrata norte-americano, tendo como intuito o favorecimento de Donald J. Trump, na altura candidato à Presidência dos EUA. (Volz & Menn, 2017) Na perspetiva de Kuchler, este tipo de operações semeiam um sentimento de desconfiança entre os eleitores e governo, suspeição esta que mina os resultados e a própria democracia. Quando os processos e a democracia são postos em causa, a própria noção de segurança e interesses nacionais são ameaçadas, já que são exercícios essenciais para a continuidade e sobrevivência democrática e para a preservação do bem-estar e dos interesses das populações. (Kuchler, 2018)

[19] Para Maurer, este corresponde a um modelo de interação promovido pela necessidade de atrair e procurar talento em qualidade e quantidade, ambicionando um fortalecimento da sua presença mesmo quando não existem no *core* do Estado os especialistas capazes de perpetrar ações de determinada magnitude, algo que é depois conjugado com a negação plausível que conferem. (Maurer, 2018) De maneira a ilustrar estas dinâmicas pode abordar-se o grupo *Dragonfly*, que se crê aliar-se frequentemente a atores estaduais enquanto força especializada, operando através de ataques direcionados a redes elétricas e outras infraestruturas destinadas a lidar com recursos essenciais para o bem-estar social, económico e político dos territórios (Atkinson, 2018) Ao operacionalizarem determinadas campanhas que contam com um nível de exigência considerável, complementam a ação dos atores que os contrataram, perpetrando assim ações que podem ser correlacionadas com os interesses estratégicos de certos Estados.

visado, revelando ser um dos elementos de vantagem mais cobiçados pelos atacantes ou competidores. Quando estes ciberataques são realizados e detetados, o tipo de causas relacionado ao ataque em questão poderá não espelhar a típica motivação ou fundamentos que esses grupos têm na sua origem, o que transmite a racionalização de que terão sido ações de alguma forma encomendadas por outros atores do SI.

No âmbito destes ciberataques, quando estão envolvidos interesses massivos, os setores alvo costumam ser aqueles que ao falharem criam maior debilidade nas regiões adjacentes, sendo que nestas características se contam qualquer tipo de infraestruturas críticas, setores de transportes ou o setor financeiro. (Moniz, 2018) Com a volatilidade das sociedades e sua interação no ciberespaço, podem ocorrer ataques que colocam em causa o funcionamento total do país, por exemplo direcionados às instituições governamentais com o intuito de descobrir e adquirir informações que depois possam ser leiloadas para proveito de quem encomendou o ataque ou dos próprios grupos que perpetraram o ataque. Se bem-sucedidos, muitas vezes, o Estado só sabe que foi comprometido quando as informações que lhe dizem respeito começam a circular. Concomitantemente, por vezes são recrutados de maneira a lançar campanhas de informação para manipular a opinião pública, favorecendo determinados argumentos, candidatos ou posições, através da criação de plataformas online de apoio e disseminação de informação – muitas vezes falsa. Têm em seu poder também os meios suficientes para deixar um rasto que incrimine outros atores, semeando a discórdia e conflito internacionais, prejudicando as relações internacionais de uma série de Estados visados.

O seu impacto na Segurança Nacional é visível pelo tipo de consequências que se tem provado poder advir das suas ações, a sua infiltração pode tornar todas as ações e intenções de um Estado visíveis para o resto do mundo e, ao servirem terceiros, são mais forças alinhadas para a persecução de determinados fins, o que deixa os atores com menos recursos sujeitos a um perigo superior do que se não fosse possível contar com forças de caráter mercenário. Constituem uma das ameaças mais sérias do mundo atual, são imprevisíveis e se contratadas, não olham

a meios para cumprir as suas missões. A sua preponderância pode ser elevada a tal patamar que, as suas ações poderão levar à subvalorização do poder democrático de um determinado país e a um crescente clima de risco, onde a mínima altercação ou fragilidade pode ser o rastilho para deixar que este tipo de atores não-estaduais consigam intrometer-se na ordem interna de um Estado. São sobretudo fruto da arquitetura securitária do ciberespaço, que peca por falta de robustez e por constituir um cenário atrativo para aqueles que buscam enriquecer graças às suas habilidades, que conglomeram uma panóplia de táticas e ferramentas proporcionadas pelo ciberespaço em si e que deixam uma janela de oportunidade que permite a intrusão destes atores para exploração.

1.4 – O *Ransomware* como fenómeno crescente do cibercrime

Uma das ferramentas, que também pode ser considerada uma das ameaças crescentes utilizadas por estes grupos, consiste no *Ransomware*. Pode definir-se como uma categoria de *malware* que impede as vítimas de acederem às suas informações e aplicações, reclamando um resgate de modo a voltarem a ter acesso a esses documentos, algo que nem sempre se regista.

À semelhança de outros fenómenos inseríveis na área do cibercrime, a sua incidência tem vindo a aumentar e, em termos dos alvos característicos, tanto podem ser específicos como qualquer mero utilizador do ciberespaço, sendo que quando são analisados ataques com alvos específicos, geralmente provêm de grupos organizados, como os *cyber-mercenaries*. O *ransomware,* é um ciberataque que provoca a perda de informações por parte das suas vítimas, como altercações económicas, políticas e sociais, já que coloca em cheque os serviços de cibersegurança das vítimas ou de instituições, levantando um debate público sobre o nível de vulnerabilidade que estes atores apresentam atualmente.

Para ilustrar a perigosidade e expansão é importante analisar algumas das estatísticas que aludem ao mesmo e seu impacto, nomeadamente como anuncia um dos relatórios do WEF que concluiu que para além dos custos económicos que acarretam, consistem numa maioria dos e-mails maliciosos enviados no período

em análise: "(…) *some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails*."(WEF, The Global Risks Report, 2018, p.6) Entre outros dados, o site Kraftbusiness enumera outras estatísticas preocupantes, reiterando que, só em 2017, o *ransomware* contra dispositivos móveis registou um aumento de 250% face ao ano anterior e 72% das instituições visadas não teve acesso aos dados no período mínimo de dois dias, sendo que 67% da totalidade das vítimas perdeu a uma porção ou o conjunto total dos dados em questão. (Kraft, 2018).

Quanto a casos proeminentes, em que o poderio e ameaça deste fenómeno é analisável, é fulcral abordar o *WannaCry*. Este ciberataque afetou inúmeros computadores, vedando o acesso a informações necessárias por parte dos proprietários, algo que ocorreu por exemplo em hospitais britânicos e outros locais por todo o globo e levando centenas a pagar o resgate que era pedido (Wickramanayake, 2017) Foi um ataque que marcou uma nova era no tocante aos ciberataques, pois o seu foco incluiu infraestruturas críticas e cujo funcionamento correto era indispensável para o bem-estar das populações[20]. Atraiu a atenção dos atores, mediante aquilo que este significou e danos que produziu: "*It illustrated a growing trend of using cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."* (WEF, The Global Risks Report, 2018, p.6)

Elucidativo da ameaça do *Ransomware*, este caso, traduz com eficácia a perigosidade que estes ataques podem ter no âmbito da Segurança Nacional. Com

[20] Relembrando que uns dos focos centrais e parte da segurança nacional de um Estado é a salvaguarda do bem-estar das populações, assim como das infraestruturas críticas, cujo correto funcionamento é indispensável para o exercício da cidadania e das prerrogativas estaduais, é visível como campanhas como o *WannaCry* podem atentar contra a segurança nacional. As áreas a que estas infraestruturas se dedicam acabam por se relacionar com recursos vitais, o que pode ter como consequência perda de vidas humanas derivadas dos danos gerados nesses locais e em instituições fundamentais para as prerrogativas estaduais e populações. Este ciberataque fora a atribuído a um grupo de *hackers*, que segundo os EUA, estariam ligados à Coreia do Norte (Groll, 2017), pelo que os mesmos indivíduos estavam capacitados para enveredar por uma operação de tal dimensão, o que revela as consequências que o *cyber-empowerment* individual pode ter para os Estados e organismos afetados, e em simultâneo, o tipo de capacidades que os indivíduos passam a conseguir apresentar.

a capacidade de colocar em risco vidas humanas, atacando hospitais, escolas, governos ou empresas que tratem dos serviços hidroelétricos, todos estes exemplos de instituições vulneráveis e, por vezes, incapacitadas para lidar com ataques desta ordem. Veja-se que um ataque que vise uma unidade de saúde pode comprometer informações de diferentes pacientes que possuem diferentes necessidades, assim como o funcionamento de muitos dos seus aparelhos e resultados. Coincidentemente, quando se analisa ao pormenor o seu impacto em diversas infraestruturas críticas, conclui-se que as consequências poderão ser devastadoras: “*Remember, electricity doesn’t just turn on the lights, it also keeps medicine and food refrigerated and runs air conditioning and heating units, without which hundreds of people—or more—could die in the summer or winter. Blowing up transformers could also start wildfires that affect or kill local residents.”* (WEF, Why cyberattacks could be war crimes, 2017, para. 11)

Estes ciberataques, quando aliados à vontade de causar dano e minar o funcionamento da ordem interna de um Estado, conseguem ser armas com efeitos consideráveis nas mãos de atores mal-intencionados. Companhias de transporte aéreo ou férreo que percam total controlo e informação sobre os seus movimentos estão perante uma situação alarmante.

Estes, alimentam uma necessidade de preparação e cautela, assim como de maior sinergia entre atores de modo a conseguiram travar o seu progresso ou diminuir as suas consequências nas sociedades e atores. Salienta-se ainda o dever de reestruturar a arquitetura dos sistemas de informação e blindar as infraestruturas e seus funcionários de modo a conseguirem contrariar as tendências e estar melhor preparados para o exercício das suas obrigações em segurança.

Capítulo IV – As tendências e respostas aos desafios proporcionados pelo *cyber-empowerment* individual e seus efeitos

1 – As novas orientações estaduais face ao *status quo* que enfrentam

A perda de controlo estadual perante os efeitos do *cyber-empowerment* individual suscita assim determinadas respostas por estes atores. Por entre alguns setores alvo de mudanças contam-se o crescente investimento em educação, em parcerias público-privadas e no fortalecimento dos sistemas e redes, na responsabilização multilateral e, até, no uso das vulnerabilidades de certas redes como ponto a seu favor.

Na verdade, uma das respostas passa pela opção por políticas de caráter protecionista, o que infere duros golpes na componente da liberdade do ciberespaço, pelo menos dentro dos seus territórios. Estas manifestam-se principalmente pela afirmação da sua soberania nacional e alastram-se a outras componentes das suas sociedades, nas quais o Estado procura fazer-se sentir, por exemplo, através das suas FSS e estratégias em prática, salientando a importância que é incorporar novos métodos na sua estrutura de segurança interna, o que segundo um relatório do *World Economic Forum,* é motivado pelo potencial destrutivo das ameaças que se têm vindo a verificar e termina com uma quebra na relação e visão que os governos têm com as TIC no geral: "*the proliferation of damaging crossborder cyberattacks might be the most likely trigger for a government-led breakup of the internet into national or regional "walled gardens'*"" (WEF, The Global Risks Report, 2018, p.35). Essa afirmação, diferente consoante o Estado visado, é marcada pelos seus interesses estratégicos e valores nacionais, diferenças que acabam por ser visíveis nas próprias estratégias de cibersegurança[21] ainda que existam aspetos onde o consenso é possível,

[21] A cultura, ideologia e as linhas estratégicas norteadoras de um Estado condicionam a arquitetura das estratégias de cibersegurança que os mesmos criam, espelhando as suas prioridades face aos seus objetivos e vulnerabilidades que possam apresentar. No caso dos EUA, apresentam uma estratégia de caráter colaborativo que inclui organismos governamentais, internacionais e privados, que foca a proteção das suas redes ou a sua aplicação nas suas FSS (ENISA, 2012) Do lado da China, a sua estratégia encara o

nomeadamente quanto à necessidade de alteração e adaptação consistentes com o novo ambiente em que operam, transformando a sua mentalidade, ou seja,"*Rather than hoping that nothing significant will happen, it is best to plan for such attacks so that when they occur (and they will), everyone will know what they should be doing to mitigate the damage."* (Lazarescu, 2016, para.18)

A partir dessa propensão para a afirmação estatal, uma das formas como as entidades competentes têm procurado corresponder é revelada através de uma crescente tentativa de limitar o tipo de *data* que é enviada para fora do seu território, seja através de um esforço de localização da raiz desses dados, ou então de limitar o tipo de informação que consegue entrar no ciberespaço do país Este tipo de barreiras ambicionam um melhor controlo do *flow* de informação e não são algo inédito, pois a novidade prende-se com a aplicação destes métodos na esfera do ciberespaço, isto é, "*content-restrictions that various national governments have established to limit citizens' access to certain websites or content."*(WEF, Cyber Resilience, 2018, p.41) Alguns exemplos palpáveis do *enforcement* destes instrumentos consistem na restrição de conteúdos que possam de algum modo ser uma afronta aos ideiais estaduais e, consequentemente, um foco de instabilidade em pontos importantes na sua ordem interna. A limitação pode visar conteúdos de ordem política, social, securitária ou até de ferramentas cibernéticas que permitam a comunicação ou partilha de informação. Em termos estatais, vários *players* do sistema internacional recorrem a esta tática, entre eles, pode encontrar-se a China[22] enquanto um dos exemplos mais salientes, mas acrescem outros Estados como os EUA, a Arábia Saudita ou a Tailândia (Tikk-Ringas, 2012)

---

ciberespaço como um novo campo de expressão da sua soberania, tendo a estabilidade política como uma das suas linhas centrais, revelando uma narrativa protecionista e que sobrepõe os interesses nacionais a todos os restantes atores do ecossistema informático (Creemers, 2016). Apesar de serem apenas dois de uma miríade de possíveis exemplos, demonstram as diferenças passíveis de serem encontradas na visão aplicada por cada Estado, posteriormente traduzida nas suas estratégias de cibersegurança.

[22] Presente na sua estratégia nacional de segurança do ciberespaço, o protecionismo chinês é visível de na perceção que o país tem do seu regime e do tipo de soberania que o mesmo deve exercer sobre todas as esferas do seu território, inclusive o ciberespaço. O controlo da navegação e de conteúdos é uma das medidas chinesas aplicadas de maneira a impedir e diminuir a difusão de tudo o que transpareça ideologias, cultura ou informações que possam contrariar o tipo de mentalidade que o governo promove e pretende perpetrar no quotidiano estatal.

Em ligação à ideia de restrição e limitação de determinados conteúdos, eis que surge a neutralidade da internet, conceito que continua no cerne de alguns debates devido aos efeitos que suscita e às implicações que a sua prática traz para os cibernautas. O conceito baseia-se na noção de que a totalidade de informação que se encontra a circular deve ser tratada de igual forma, independentemente da sua natureza, sem qualquer tipo de restrições ou preferência por parte dos controladores (Fernandes, 2013). Porém, o núcleo do debate foca algumas tendências dos fornecedores terem a aptidão de abrandar ou bloquear determinados domínios, enquanto procedem ao favorecimento da presença, da velocidade e da relevância de outros, tendo sempre em conta os interesses dessas entidades. (Raposo, 2017). Essa perda de liberdade é visível na medida em que limita o acesso global à informação por parte dos utilizadores, sem que os mesmos se apercebam de tal regulação e, por isso, continuam a navegar através dos seus motores de busca sem suspeitarem que o tipo de resultados que obtêm não são exatamente os mesmos que os utilizadores do país vizinho conseguem visualizar ou aceder.

Num dos seus expoentes máximos, a China para além do estrangulamento e bloqueio de determinados conteúdos, procede ainda a uma análise cuidada da pegada digital dos seus cidadãos, tendo sempre em vista a monitorização, filtragem ou bloqueio de conteúdos tidos como sensíveis. Segundo Fernandes, o caso chinês espelha de forma clara a ideia de que a liberdade no ciberespaço pode encarar-se apenas como uma opção social e política, não sendo de todo algo inevitável e impossível de controlar (Fernandes, 2013). Quanto à União Europeia (UE), estes debates[23] têm também reunido vários especialistas e opinião pública, tendo sido abordada a perspetiva de uma possível constrição futura dos conteúdos disponíveis para os cidadãos da UE e, levando também ao surgimento de movimentos que se

[23] Na UE, é analisado um crescente debate sobre a *net neutrality*, onde por um lado se têm vindo a realizar propostas que contribuem para um mitigar dessa neutralidade e que tem suscitado respostas por parte dos que defendem a continuidade da liberdade online e de um ciberespaço aberto e sem qualquer tipo de limitações por parte dos provedores de serviços. Uma das campanhas criadas para defender a neutralidade corresponde à *Save Your Internet* (James, 2018), porém, e apesar da sua ação, este será um debate que irá continuar na ordem de trabalhos da União Europeia e que poderá evoluir para o eventual estrangulamento da internet no seio dos territórios da UE.

opõem ao que consideram ser um desfigurar da ideia de neutralidade da internet – o que revela a preponderância que certas tendências podem vir a assumir no ciberespaço global.

Além das tendências já abordadas, é analisado um crescimento na ambição de promover o consenso e cooperação internacional nas matérias de cibersegurança. Outros dos vetores de incidência das mesmas abarcam a redução das vulnerabilidades nos sistemas, um crescente investimento em campanhas de sensibilização para temáticas de segurança informática, um maior investimento na formação de profissionais e incentivo de boas práticas em todas as áreas da sociedade que estejam presentes na internet. Para os autores Guedes e Santos dever-se-á apostar na elaboração de uma defesa concertada e cuja arquitetura permita dar resposta às ameaças, mas sobretudo medidas que veiculam um sentido de compromisso generalizado. (Guedes e Santos, 2017)

Consistindo medidas algo generalistas e tomadas a partir da opção de vários Estados, há áreas específicas nas quais se defende a necessidade de transformações. Dizem respeito a inovações que os Estados deverão adotar e adaptar às suas realidades de modo a combater as ameaças à segurança nacional inspiradas pelo *cyber-empowerment* individual, enquanto procuram tirar partido das valências positivas que o mesmo fenómeno acarretou para com as dinâmicas individuais na era contemporânea.

2 – Ferramentas e métodos que têm vindo a ser adotados ou a adotar

2.1 – O papel da dinâmica público-privada e cooperação internacional

O fortalecer das interações e relações entre os vários atores da ordem internacional acaba por ser uma das vias pelas quais podem ser retirados determinados benefícios e onde se deve apostar. Para Suter esta cooperação é ainda mais fulcral quando está em jogo a proteção de infraestruturas críticas, pois são entidades que asseguram a disponibilidade, fornecimento e tratamento de serviços e bens indispensáveis como eletricidade, água, transportes ou telecomunicações. (Suter, 2012). Assim sendo, quer entidades públicas, quer entidades privadas

conglomeram forças que são cobiçadas mutuamente, o que leva a que uma parceria mutuamente vantajosa seja algo apetecível para as duas partes e com uma influência positiva nas áreas estratégicas para o bem-estar das populações e segurança nacional.

A cooperação permite o germinar de um ciberespaço onde as vulnerabilidades são combatidas e investigadas por diversos elementos e que trazem uma maior criatividade à resolução de problemas, combatendo-se o estigma da competição e procurando-se instigar uma contribuição coletiva para o zelo dos interesses gerais. A capacidade destas sinergias entre Estados e privados é explicada por Kostyuk que reitera a necessidade de fortalecimento destes laços: "*As information travels through the space owned by private companies, states should continue to enhance their ties with private companies and establish working agreements under which these companies are obliged to provide key information to investigators."* (Kostyuk, 2013, p.80)

Promovem um ambiente propício ao progresso e desenvolvimento da própria cidadania no ciberespaço, diminuindo o nível de risco envolvido na própria estrutura das redes e serviços. Para tal ser verificado, dever-se-á reconhecer e localizar os seus pontos fracos, já que só depois dessa inspeção poderão recorrer a este tipo de políticas e estratégias, pensadas de maneira a produzir uma maior quantidade de benefícios para a sua ordem interna. Este é o caso da República Checa, que reconhece que o seu setor privado se encontra num nível inferior comparativamente a outros países europeus, recorrendo em vez disso a entidades multinacionais que os consigam auxiliar de forma eficaz a concertar as vulnerabilidades do seu ciberespaço e a melhorar a resiliência das suas infraestruturas críticas.[24]

[24] A República checa conta com o apoio da National Cyber Security Center (NCSC) e da National Security Authority (NSA) para a salvaguarda das suas infraestruturas críticas de informação, recebendo das mesmas a assistência e conhecimento sobre cibersegurança de que necessita, aliando-se ao facto de grande parte dos serviços checos lidarem com a National CSIRT Team of the Czech Republic quanto às matérias de segurança da informação, revelando assim a simbiose na relação entre as componentes públicas e privadas e seu benefício mútuo. (Wiser, 2016)

Um dos modelos de facilitação destas parcerias enfatiza o recurso a incentivos como, por exemplo, melhores acordos com grupos privados cuja rede de segurança informática fosse mais impermeável, inspirando outros atores não-estaduais a perseguir o mesmo caminho e, ultimamente, levar a uma maior consciencialização e aplicação de medidas centradas na segurança dos seus sistemas e proteção dos mesmos.

Quanto à cooperação internacional, é de extrema relevância enquanto ferramenta ao serviço dos Estados para almejar a salvaguarda da sua Segurança Nacional, especialmente no que toca à difusão e peso do cibercrime a nível internacional – que atenta contra o bem-estar e salvaguarda dos interesses nacionais. A cooperação internacional vem facilitar o contra-ataque por parte das entidades estaduais, como registado no derrubar da *Shiny Flakes* na Alemanha e da *Operação Onymous*[25] que contou com a colaboração de entidades como o Federal Bureau of Investigation (FBI), a Europol e o Department of Homeland Security, conduzindo estas iniciativas a um fim de sucesso e salientando a importância e seriedade deste tipo de colaborações (Vogt, 2017).

Uma operação adicional a mencionar é a chamada "Operação Torpedo", que teve na sua génese a iniciativa das forças holandesas e que recorreu a técnicas pouco usuais de modo a localizar os responsáveis. Tendo obtido como indicação o Nebrasca, desencadearam uma operação conjunta com as entidades norte-americanas que permitiram o sucesso da mesma: *"They provided the information to the FBI, who traced the IP address to 31-year-old Aaron McGrath"* (Poulsen, 2014, para.14) A tática usada aqui remete para o chamado *drive-by hack* onde é incorporado no *website* código malicioso que permite ter acesso a informações dos seus visitantes sem requerer qualquer ação da parte dos mesmos. Este ilustra uma clara aplicação da cooperação internacional em prol da generalização de um ecossistema informático mais seguro para todos os seus utilizadores, contribuindo

[25]Ambas demonstraram as potencialidades existentes na cooperação internacional para responder às ameaças que se assinalam à segurança nacional dos atores estaduais. Promoveram um esforço conjunto que levou ao atenuar e término de atividades que perigavam as sociedades em questão e que exemplificam o tipo de criminalidade que é incluída nas ameaças à segurança nacional.

de certa maneira para a salvaguarda e mitigar de algumas vulnerabilidades e perigos que podem ser encontrados por cibernautas e que perigam o seu bem-estar e das populações, tendo implicações diretas na segurança nacional dos Estados envolvidos.

2.2 – A responsabilização multilateral

Outro método disponível para se combater as ameaças e vulnerabilidades apresentadas hodiernamente passa pela responsabilização dos atores pelos seus comportamentos[26]. Isto é, não só reconhecer as boas práticas como condenar as que possam ter efeitos negativos no que toca à segurança da informação, dos sistemas e das infraestruturas. Aqui poderão incluir-se uma miríade de comportamentos, desde a falta de zelo pelos dispositivos pessoais não recorrendo a antivírus e outro tipo de ferramentas disponíveis à generalidade dos cibernautas, até à deteção de indivíduos que incorram em algum tipo de ciberataque e que constitua um motivo de risco devido ao seu comportamento no ciberespaço.

Ao responsabilizar os privados, um Estado consegue conferir padrões de qualidade mais elevados para as operações das mesmas e, consequentemente, um melhor acompanhamento dos termos securitários adjacentes devido à maior precaução instaurada por parte dos privados por saberem que estão sob escrutínio. O papel dos governos aqui é fulcral para o *enforcement* dessas medidas e controlo do setor privado face às suas obrigações e seus comportamentos, pois é necessário

[26]Um dos exemplos desta responsabilização remete para as diretivas a que os Estados-Membros da UE estão sujeitos, existindo medidas que deverão seguir e aplicar na sua ordem interna sob pena de serem responsabilizados pelo incumprimento das mesmas, cuja falta pode resultar numa maior suscetividade das suas infraestruturas e dos seus cidadãos a este tipo de ataques (que se procuram mitigar), assim como a uma menor preparação das suas entidades competentes para lidar com esses desafios (ENISA, 2017). Esta responsabilização pode ainda incidir nos indivíduos ou setor privado, estando os governos cada vez mais a procurar a responsabilização de empresas e outras entidades face ao tipo de políticas de cibersegurança e de formação dos seus funcionários que as mesmas aplicam, pois a partir das diretivas e conselhos dos governos, ao protegerem-se conseguem proteger os outros e contribuir para um ambiente mais seguro, ao passo que se continuarem com comportamentos que salientem as suas vulnerabilidades podem comprometer todo um território (MacEwan, 2017).

incutir-se esse espírito de supervisão e perspetivas de represálias no caso de erros ou incumprimentos.

Reconhece-se como necessário ter *frameworks* e estruturas corretas para ser possível responsabilizar os atores por todos os atos empreendidos, não apenas os intencionais, mas também aqueles que tiveram na sua génese um descuido ou indiferença face às preocupações securitárias que a nova realidade exige. A responsabilização poderá assim efetuar-se de forma multilateral, ao construir-se um plano que vise a deteção e imputação de atos de risco provenientes de qualquer ator e mediante qualquer tipo de ação operacionalizada, sendo que assim mais facilmente se incute a obrigatoriedade e seriedade das questões relativas à cibersegurança.

Com a responsabilização assente nas mentalidades de todos os atores, a precaução e seriedade com que se encara o comportamento online levam assim ao maior sucesso das iniciativas de proteção e segurança das redes informáticas, contribuindo para o mitigar das vulnerabilidades e ameaças que possam assolar um Estado. Tendo-se demonstrado a volatilidade de cada ação, qualquer ator é passível de ser um elemento que contribua com *inputs* positivos ou negativos, tanto que esta corresponde a uma teoria aplicável aos indivíduos, na sua generalidade e em casos particulares, dependendo do tipo de perfil e nível de ameaça que os mesmos provem consistir ou tiverem proporcionado intencionalmente ou não.

2.3 – O papel do investimento na educação e pesquisa enquanto ferramentas

A investigação, o desenvolvimento tecnológico e a reforma nos métodos educacionais consistem numa das vertentes com maior potencial para os atores, sendo que o dito investimento pode partir da iniciativa estadual ou privada, e pode sintetizar-se pela valorização de campanhas, ideias e estudos que beneficiem o papel do indivíduo e o seu contributo para a estabilidade e proteção da Segurança Nacional e qualquer setor que contribua para o aumento e crescimento em termos de cibersegurança global.

Uma das vias pela qual o investimento na educação pode ser delineado passa pela readaptação dos recursos humanos de um Estado, capacitando-os para os novos desafios e exigências da sociedade tecnológica. Contribui para o crescimento económico e desenvolvimento societário face às transformações tecnológicas e permitem a sua adaptação e preparação para um futuro onde dependerão do ciberespaço para operacionalizarem grande parte das suas tarefas. Para esta aspiração ser concretizada, defende-se que deve proceder-se a uma atualização dos planos de estudo[27] aplicáveis pelas entidades responsáveis pela formação escolar, sendo necessária para a adaptação dessas gerações aos novos modelos de produção e funcionamento das sociedades em que se inserem. Logo, a requalificação é algo absolutamente necessário, só com uma população ativa capaz é que um Estado consegue zelar por si e pelos seus cidadãos.

Ao investir nos seus cidadãos, seja num empoderamento digital ou em conhecimentos abrangentes de variadas áreas, premiando os que apresentarem melhor desempenho, consegue valorizar esses recursos e assegurar profissionais preparados e dedicados. Essa valorização tem como efeitos também uma maior cooperação entre os dois lados, levando a que a consulta de indivíduos perante matéria sob as quais os mesmos são especialistas seja cada vez algo mais correspondente à normalidade e permita que surjam soluções diversas, criativas e inovadoras que podem beneficiar o funcionamento do Estado e das suas instituições, algo que Slaughter salienta pela sua importância e pelo valor que pode acrescentar às novas dinâmicas societárias:*"wherever possible, government should invest in citizen capabilities to enable them to provide for themselves in rapidly and continually changing circumstances.(…) It recognizes that citizens are quicker and more creative at responding to change and coming up with new solutions*."(Slaughter, 2017, para. 7 & 13)

[27] Nos EUA foi recentemente implementado um programa que leva a cibersegurança a um dado número de escolas, iniciativa esta promovida pelo Indiana Department of Education e com o objetivo de inserir a educação e treino para a cibersegurança no plano de estudos dos seus alunos. Tendo sido criada em 2017, permanece uma campanha em vigor nesse estado norte-americano, com objetivos claros e que permite iniciar uma revolução na forma como as temáticas da segurança online e da informação são abordadas ao longo do percurso académico dos seus estudantes. (Indiana Department of Education, 2018)

Neste investimento na vertente educacional, a própria sinergia com centros de investigação e universidades acaba por se revelar oportuna face ao novo *status quo*, mediante o facto de estes serem locais onde muitos desenvolvimentos são operados e onde se podem encontrar diferentes abordagens e fóruns que fomentam o debate e enriquecimento da sociedade. Ao incentivar as dinâmicas enumeradas e ao premiar as boas práticas, contribuindo para o enriquecimento curricular e académico coletivo, um Estado consegue tirar partido do *cyber-empowerment* individual, algo necessário se não pretende deixar-se ficar para trás quanto à corrida tecnológica e preocupações em termos de cibersegurança.

No entanto, uma conclusão de extrema relevância remete para a ideia de que uma abordagem e medidas uniformes e aplicáveis de modo geral, deixam de ser uma opção viável, pois, dentro do ciberespaço e no interior de um Estado, exercem a sua cidadania cidadãos completamente diferentes, seja em motivações, interesses, valores ou conhecimentos. Nessa senda, esta lógica implica que uma única política que incida apenas em determinados vetores generalizados não tenha uma taxa de sucesso como seria de esperar. Aliás, com estudos direcionados a tais questões, foi comprovado o impacto que tem uma abordagem que tenha em atenção as diferenças e as personalidades dos cibernautas ou, neste caso, funcionários, tendo chegado a algumas conclusões de relevância para este tema, especialmente tendo em conta a perspetiva que este trabalho já apresentou sobre os sintomas que a ação individual pode imprimir nos atores estaduais ou não estaduais (McBride, Carter, & Warkinten, 2012). Por isso mesmo, verifica-se a necessidade de entender o porquê dos mesmos funcionários, que passaram ou deveriam ter passado todos pelo mesmo tipo de formação a nível informático, implicarem diferentes graus de ameaça e até resultarem no aumento de vulnerabilidades através de erros cometidos, daí que estes autores promovam a ideia de ter em conta os perfis dos funcionários e, a partir daí, fazer-se uma formação adaptada a cada personalidade.

A sua pesquisa concluiu que o perfil e características de cada funcionário pesam na forma como cada indivíduo perceciona a importância dos protocolos de

segurança e seu cumprimento, algo que os atores deverão ter em consideração de modo a empoderá-los para um mundo onde o risco cibernético é algo usual e de presença permanente. Os autores supracitados, cerram o estudo com a premissa de que a abordagem deve ser personalizada o quanto for possível, já que os indivíduos têm uma reação própria a cada elemento a que são expostos: *"(...) we have established that individuals react to cybersecurity threats and deterrents in different ways and that their personality affects the way they approach compliance with cybersecurity policies."* (McBride, Carter & Warkinten, 2012, p.13) Reiterando-se a necessidade desta readaptação de modo a que as organizações e seus recursos humanos possam de facto atingir o seu pleno potencial, repensando e havendo a metamorfose do modelo de um funcionário típico, para uma adoção de um molde com múltiplas incidências e que cubra as diferenças e diversidade dentro da sua estrutura interna. Por outro lado, abordando a aquisição, pesquisa e deteção das *zero-day vulnerabilities*[28], com o espectro da recompensa e valorização do trabalho individual, cresce a vontade de cooperar e é promovido um desempenho com maior qualidade, não apenas na relação entre indivíduo-estado, mas também entre indivíduo-setor privado, já que são externos que muitas vezes conseguem desenterrar tais fragilidades e reportar às entidades.

Todavia, há outros planos de ação a considerar, nomeadamente a necessidade da mentalidade de gestão de risco e consciencialização respetiva. Ao falar-se de gestão de risco, estão implicadas uma mudança de *modus operandi* na maneira como são encarados os assuntos relacionados com os perigos e potencialidades das redes informáticas, na medida em que deverá haver um estudo e subsequente planeamento quanto às consequências de cada ação, criando-se um modelo padrão de como combater esses acontecimentos. Quer-se com isto dizer que, em vez de se planear consoante um cenário hipotético e onde se pensam

[28] Quando se aborda o termo de "zero-day" faz-se referência a uma vulnerabilidade que é descoberta recentemente pelo seu desenvolvedor, tornando esse o momento "zero" até à criação de uma maneira de a solucionar. Sendo desconhecidas pelos seus criadores, oferecem uma porta para atores mal-intencionados que as consigam explorar sem que os organismos competentes estejam na busca de uma forma de fechar a mesma. Logo, nestes casos, os desenvolvedores têm um grande sentido de urgência de modo a impedir danos maiores aos que podem ter já sido verificados.

algumas medidas, deve incutir-se a ideia de que se está a preparar para algo que vai realmente verificar-se e consiste uma ameaça séria, só assim se poderá assumir e detetar as falhas e as necessidades que apresentam todas as infraestruturas e sociedade.

Na linha da necessidade de uma gestão de risco devem referenciar-se os chamados “Penetration tests” cujo objetivo é descobrir qual a real amplitude e alcance das defesas de uma organização em específico. Um dos modos de efetuar este tipo de testes com sucesso é fazê-lo sem o conhecimento dos responsáveis de cibersegurança aí empregados, pois só assim se pode analisar o tipo de resposta que iria ser utilizada na eventualidade de se verificar um ataque real, favorecendo algumas características relacionadas com o trabalho sobre pressão e com riscos sérios de serem causados danos e haver perdas significativas.

A valorização da educação e o investimento na mesma e na investigação de matérias relacionadas com temas ligados à cibersegurança têm de ser uma das prioridades estaduais, pelo que o potencial que representam consegue moldar as respostas e contribuir para a salvaguarda da segurança nacional e do futuro dos Estados propriamente ditos.

2.4 – Quais os casos de sucesso e boas práticas que devem ser tidos em conta?

Assumindo-se a cibersegurança e o seu impacto na sociedade atual como uma das temáticas proeminentes e geradoras de uma crescente preocupação, incumbe também aos atores internacionais analisar os casos de sucesso que têm vindo a surgir. A influência de uma boa estratégia ou ação pode fazer a diferença em termos securitários, o que excede muitas vezes as práticas regulares e verificadas de combate às novas ameaças.

Um dos casos a apresentar vem do Facebook e incide especialmente no treino dos seus trabalhadores – “*One of the biggest efforts to rethink training comes from Facebook Inc., which holds a “Hacktober” event every October to coincide with National Cybersecurity Awareness Month*” (Stone & Janovsky, 2017, para.8)

– onde são simulados diversos cenários de ciberataques e são reconhecidos os trabalhadores bem-sucedidos. Coincidentemente, é com recurso a operações como a enunciada que operam alguns Estados, apostando em exercícios que têm como finalidade investigar as suas defesas e capacidade de resposta, como é o caso de Singapura. Em 2017[29], as instituições competentes deste país chefiaram um exercício dedicado às infraestruturas críticas de informação e que conjugava inúmeras áreas e ações de forma a realizar uma análise pormenorizada. No respetivo exercício foram incluídas sessões de planeamento de cenários hipotéticos, debates e workshops, incidindo sobre um grupo de tópicos abrangente de várias temáticas e localizando os serviços que consistiam alvos mais apetecíveis ou vulneráveis, tentando-se mitigar e extrair todos os resultados desses exercícios de forma a conseguir melhorar a prestação e o posicionamento de Singapura. Este tipo de ações não só demonstram o papel do indivíduo e a sua importância para a organização e para o Estado, como também permitem ao Estado precaver as suas infraestruturas críticas e ambicionar uma maior segurança da informação no seio dos seus territórios, procurando mitigar as suas vulnerabilidades.

Destarte, por intermédio de exercícios e operações criativas, é possível fomentar o engajamento dos indivíduos e atores não-estaduais para com temáticas com impacto significante na Segurança Nacional. A atratividade de um exercício em que sejam envolvidos puzzles ou outro tipo de jogos/desafios agarra a atenção dos visados e suscita a vontade dos mesmos serem bem-sucedidos num clima de competição saudável, daí ser uma das opções que devem ser aplicadas e tidas como exemplo, como o Facebook integra na sua própria realidade.

Porém, a mudança de paradigma só é possível se, desde cedo, se prepararem os mais jovens para uma educação e formação focada nos desafios atuais e expectáveis, procurando incutir na sua formação as devidas temáticas de segurança

[29] Como noticia o website *The Straits Times* este exercício, ocorrido em 2017, veio cobrir uma panóplia de cenários potenciais e serviu para avaliar o tipo de resposta dada pelos participantes, criando uma consciencialização em torno dessas temáticas e sua preponderância quanto à segurança nacional de Singapura. (Hio, 2017). Este tipo de exercícios têm vindo a ocorrer no país, de maneira a acompanhar a evolução das ameaças cibernéticas e a preparação proporcional da sociedade, infraestruturas públicas e privadas e da população.

da informação, programação e derivadas. Só assim é possível capacitar os indivíduos e, assim, gerar um *cyber-empowerment* individual ainda mais impactante e benigno. Na realidade, nos EUA foi comprovado que os alunos conseguiam adquirir essa consciencialização e aprender diversas técnicas graças a um jogo multiplayer[30] criado especificadamente para o efeito e que os capacitava nas áreas de programação e cibersegurança (Stone & Janofsky, 2017). Ao demonstrarem a capacidade que os jovens têm em transpor as medidas securitárias impostas por determinados domínios, organismos e instituições que compõem as infraestruturas ligadas à sua segurança nacional acabam por expor a gravidade das vulnerabilidades presentes na sua sociedade.

Assim, indicam-se a criatividade, a proatividade, a cooperação, a responsabilização, a investigação e ainda a realização de exercícios práticos como algumas das ferramentas que têm vindo a ser aplicadas com relativo sucesso e que levam a uma reavaliação das estratégias aplicáveis no âmbito da cibersegurança estadual. De forma crescente, têm vindo a ser adotadas políticas que dão prioridade à segurança face à inovação, algo que tem sido também trazido pelo tipo de visões protecionistas que também se têm revelado em ascensão e que marcam o *status quo* da ordem internacional

[30] Cabe aos Estados apostarem na promoção deste género de campanhas, sendo que um dos exemplos disponíveis remete para a realização de uma competição no decorrer de uma conferência em Las Vegas em 2018 onde estiveram presentes mais de 300 crianças cuja ambição era ultrapassar os obstáculos que lhes eram impostos e analisar as suas capacidades de *hacking* (Lee, 2018). No seio da mesma conferência, deu-se particular destaque à realização de uma simulação eleitoral onde os objetivos centravam-se no descobrir de vulnerabilidades nas máquinas de voto e outros instrumento (Kuchler, 2018)

Capítulo V – O caso português

1 – O *cyber-empowerment* individual em Portugal

O Estado Português não escapa intacto aos novos fenómenos e seu impacto, especialmente no que toca à respetiva Segurança Nacional, o que exige a própria adaptação dos nossos sistemas, infraestruturas e instituições. Só assim Portugal conseguirá manter-se a par dos desenvolvimentos tecnológicos e estará apto a acompanhar a evolução a que se assiste. As transformações positivas e negativas globais são visíveis a nível interno e, nesse sentido, há uma necessidade de analisar a repercussão desses fenómenos no país e a forma como a Segurança Nacional pode vir a ser reajustada.

1.1 – As contribuições positivas do *cyber-empowerment* individual na ordem interna portuguesa

O *cyber-empowerment* individual assumiu em Portugal uma presença que não é impercetível. Na realidade, a última década testemunhou a capacitação dos indivíduos de todas as gerações e a implicância que essa capacitação e acesso tiveram nas dinâmicas estaduais. A influência que o fenómeno abordado tem no seio da segurança nacional é notada em vários setores, especialmente nas oportunidades que faculta, constituindo ainda um novo meio de transformação em vetores relacionados com a noção de segurança interna ou de defesa nacional[31], ambas indispensáveis para o correto funcionamento e desenvolvimento da sociedade portuguesa, sendo considerados pilares fundamentais (Lourenço,

[31]A segurança interna é entendida como a atividade incumbida ao Estado para garantir a ordem, a segurança e a tranquilidade públicas, algo presente na Lei de Segurança Interna, artigo 1.º. No âmbito da segurança interna estão incluídas ainda a garantia da proteção de pessoas, repressão da criminalidade, o assegurar do regular exercício dos DLG dos cidadãos ou o respeito pela legalidade democrática. Quanto à Defesa Nacional, que se aproxima do conceito de segurança, vem retratar uma defesa contra qualquer tipologia de ameaça, seja interna ou externa, compreendendo enquanto objetivos por exemplo o garantir da soberania e independencia nacionais, o assegurar da liberdade e segurança das populações e aproteção dos valores fundamentais (artigo 1.º da Lei da Defesa Nacional). Após a análise das duas noções, é possível analisar de que modo as mesmas se incorporam no conceito e ideal de segurança nacional em vigor e norteadora do Estado Português, pelo que ambas são essenciais para o cumprimento e promoção da Paz e da Liberdade, assim como permitem o funcionamento e aplicação das prerrogativas estaduais e seus órgãos, assegurando em simultâneo a democracia, os valores e os interesses fundamentais elencados como prioridades nacionais.

Rodrigues, Lopes, Silvério, & Costa, 2015) e, consequentemente, contribuintes para a complementação da noção segurança nacional. A segurança nacional portuguesa acaba então por conglomerar o expoente máximo relativo aos esforços das instituições governamentais e suas atividades em matérias abrangentes tanto de fatores relacionados com a segurança interna, como da defesa nacional, abarcando setores relacionados com a economia, educação ou justiça, todos eles cruciais para o desempenho das prerrogativas, salvaguarda dos interesses, da independência e do bem-estar nacionais (Lourenço, Rodrigues, Lopes, Silvério, & Costa, 2015).

O empoderamento individual nacional permitiu atenuar algumas desigualdades que persistiam no nosso território e que poderiam ser apontadas em particular nas dinâmicas interior-litoral ou áreas metropolitanas e outras regiões, levando a que mais oportunidades pudessem estar à disposição da generalidade da população e não apenas aos que vivem em locais mais desenvolvidos, apesar de não ter erradicado as mesmas. Permitiu ainda um questionar e acesso à informação que transpõe aquilo que é mediatizado, que para muitos era apenas o tipo de informação a que tinham acesso, informação essa condicionada a determinadas visões e agendas.

O envolvimento dos cidadãos em matérias que ultrapassavam as barreiras nacionais passou a ser concretizável, abraçando temas que ressonavam com as suas morais e interesses. Ao estarem mais conectados, conseguem aproveitar os benefícios da virtualização das sociedades para lidar com obstáculos habituais da vida em sociedade.

As TIC, ao beneficiarem as populações, ultimamente, fortalecem uma das vertentes correspondentes e valorizadas no nosso contexto de Segurança Nacional, tendo em conta que o Estado deve zelar pelo bem-estar dos seus cidadãos. Paralelamente, o Estado tira partido desses efeitos desejáveis e aplica o mesmo tipo de tecnologia para auxiliar o exercício da cidadania e ajudar a evoluir as suas infraestruturas e sociedade, até porque as mesmas facilitam o atenuar de dadas vulnerabilidades que podem ser observadas. Um dos exemplos que prova este

ponto remete-nos para o crescente uso por parte dos habitantes da cidade de Braga da tecnologia incorporada na sua rede de transportes públicos (Oggerino, 2018). Partindo da iniciativa de um indivíduo, foram aplicados meios tecnológicos de modo a resolver uma das ineficácias na cidade de Braga tendo a sua ação pavimentado o caminho que levaria à transformação da rede de transportes urbanos bracarenses com uma simbiose entre os transportes públicos e uma plataforma que permite uma maior interação com os seus utilizadores, aliado à facilitação de acesso à internet simultânea. Este caso demonstrou como um indivíduo ou grupo pode ser empoderado graças à ação de outros portugueses, e como o próprio Estado pode depois capitalizar e dar valor ao empreendedorismo dos seus cidadãos, investindo posteriormente na resolução de problemas que assolam os seus populares.[32]

O crescimento e desenvolvimento de espírito empreendedor e de investigação/desenvolvimento valoriza os recursos humanos portugueses e empodera-os, assim como ao Estado Português. É contemplado um enriquecimento mútuo e contínuo, que permite que as duas variantes de atores progridam com auxílio da era digital. Implicando o setor privado ou não, determinadas valências surgem e devem ser aplicadas de modo a que fortaleçam o ideal de Segurança Nacional. Um indivíduo possui uma capacidade consistente e séria de impactar áreas de relevância para o Estado, graças a ideias, criações ou outros projetos, pode criar algo que beneficie o país em determinado sector e ajudar a que Portugal assuma um lugar de inovação e relevância nesses campos, o que não seria tão simples sem indivíduos *cyber-empowered.*

A difusão de ideias, comunidades e eventos permitida pelas novas tecnologias e que tem como consequência uma crescente multipolaridade do quotidiano português leva a que no seio do nosso território passem a revelar-se movimentos que elevam o debate e alertam para dinâmicas que podem minar o

[32] A resolução de problemas enunciada acaba por ser uma das prerrogativas estaduais, como sendo o zelo pelo bem-estar das populações e, indiretamente, este caso espelha o investimento nos cidadãos como forma de transformar e melhorar o funcionamento de áreas e processos que compõem setores fulcrais da sociedade como o dos transportes, revelando um impacto positivo na segurança nacional.

próprio estado. É o caso de grupos dedicados a questões ambientais, que por intermédio do público que atingiram com a sua presença no ciberespaço, passam a adquirir uma voz mais sonante junto das entidades competentes e conseguem criar uma maior consciencialização para problemáticas que são diretamente do interesse estadual e que devem atrair e conquistar a atenção dos cidadãos portugueses.

O Estado Português pode aproveitar esta nova capacitação dos indivíduos pelos quais zela e deverá procurar conseguir captá-los e atraí-los para a sua ordem interna, evitando a chamada "fuga de cérebros" e potenciando as forças que os seus próprios cidadãos podem representar, fortalecendo-se em áreas fulcrais para o assegurar da soberania e segurança nacionais. São habilidades que incidem sobre dinâmicas de desenvolvimento económico, social, securitário e que contribuem para um país mais evoluído e capaz de fazer frente aos desafios premiados pelo *status quo* atual e que se fazem sentir também no território nacional.

1.2 O enquadramento das ameaças provenientes do *cyber-empowerment* individual em Portugal e seus efeitos na segurança nacional

Os efeitos negativos do empoderamento generalizado conduzem as entidades competentes a uma necessidade de reavaliação de estruturas e pilares importantes das áreas que tutelam a cibersegurança ou que possam estar virtualizadas – o que hoje se refere quase à totalidade de infraestruturas e membros da sociedade portuguesa.

Além de constarem no Conceito Estratégico de Defesa Nacional (CEDN)[33] enquanto ameaças, ressalvando a necessidade e tendência para a consciencialização face às mesmas, é tomada como responsabilidade estadual a

[33] É o documento cuja finalidade é definir a adoção e a incorporação, por parte do Estado Português, dos aspetos fundamentais norteadores da estratégia global do país, com vista à consecução daqueles que são os objetivos pensados pela política de segurança e defesa nacional (CEDN, 2013) Ao abarcar o tipo de potencialidades e vulnerabilidades a que o território se encontra exposto, analisa componentes fulcrais para o ideal e salvaguarda da segurança nacional.

ação que verse sobre segurança informática, especificamente no que toca à ambição de mitigar estas ameaças e destruir as vulnerabilidades que possam existir. Aliás, para Nunes, essa segurança do ciberespaço constitui um imperativo nacional, indissociável dos conceitos de segurança e de soberania nacionais, assim como do exercício do poder estadual (Nunes, 2012) Outros autores realçam a mesma ideia de que a segurança do ciberespaço tem de ser considerada uma prioridade nacional (Lourenço, Rodrigues, Lopes, Silvério & Costa, 2015) e terá de ser um setor a responder aos mesmos fundamentos e valores que caracterizam todas as outras áreas integrantes da Segurança Nacional. Mediante este enquadramento, é analisável o tipo de reação que os efeitos negativos do *cyber-empowerment* individual têm vindo a imprimir nas preocupações securitárias e societárias do Estado Português, algo também reivindicado ainda pelo facto salientado pelo Despacho n.º 13692/2013, correspondente à orientação política para a ciberdefesa, de que as atividades norteadas para fins maliciosos têm assumido uma tendência crescente em volume e em qualidade, revelando a necessidade de ação por parte de Portugal, iniciando assim modificações a nível legal e estrutural.

Convém salientar que, apesar de todos os fatores, reações e do Estado Português estar sujeito à mesma turbulência global, não é lesado de igual forma como outros Estados ou atores da ordem internacional. Ou seja, os Estados tidos como "tubarões", devido ao poderio que emanam, acabam por ser vítimas de determinados fenómenos que não assolam na mesma proporção o território, população e ciberestruturas portuguesas – isto pode justificar-se pela ideia de que alguém que consiga perpetrar um ataque com consequências alarmantes nos EUA adquire uma notoriedade muito superior do que se esse ataque tivesse Portugal na mira. Ainda que se encontre nestas condições, Portugal não pode descurar a aptidão obtida por indivíduos em infligir danos em áreas que se revelam cruciais para o funcionamento correto da sociedade portuguesa e segurança da população, sejam esses danos intencionais ou não.

Tendo em conta essa divergência no tocante aos efeitos ou dimensões que as ameaças em discussão apresentam nacionalmente, não deixa de ser necessário manter-se uma postura e perceção séria sobre as mesmas, na medida em que não se deve agir ou reagir conforme a taxa de probabilidade de algo que se provou ter potencial para afligir setores de extrema importância para a sobrevivência e independência nacionais Aliás, acarretando consigo algumas disparidades face a outros atores da comunidade internacional, não significa que Portugal esteja imune às mesmas, pelo que das enumeradas, todas elas têm vindo a manifestar a sua influência na ordem interna portuguesa. Assim, convém fazer uma análise das mesmas de forma a comparar o tipo de impacto que registam na ordem interna e sua preponderência, de forma a investigar de que modo as mesmas infletem danos de maior ou menor gravidade na segurança nacional portuguesa e sendo elas não intencionais ou intencionais.

Dentro das ameaças de índole não intencional, que podem ser derivadas a um uso desmedido e desinformado por parte dos seus utilizadores, é reconhecido que à semelhança do padrão internacional, uma porção significativa da população[34] no ciberespaço não está ciente da importância e precaução que devem acompanhar a sua presença nessa esfera e impacto que as suas ações e descuidos podem ter para si, para quem os rodeia e para o próprio Estado. Seja no papel de profissionais ou cidadãos, são cometidos erros frequentes que podem colocar em causa as infraestruturas críticas nacionais e, cuja virtualização, pode então culminar na exposição de vulnerabilidades que podem ser exploradas por terceiros. Apesar da falta do elemento intencionalidade, são questões que merecem a devida atenção por consistirem num risco de suscitar ataques de grandes dimensões pelo território nacional, sendo que devido ao tipo de comportamentos que demonstram

[34] Esta dinâmica é analisável pela fácil adoção de novos modelos de operacionalização e comportamento online sem existir um pleno conhecimento daquilo que os mesmos implicam e seus efeitos (Afonso, 2017). O mesmo acaba por ser reforçado pelo noticiado pelo sapo que refere que pelo menos 37% dos portugueses já foram vítimas de problemas relacionados com a segurança informática, valor este superior à média europeia em 2011 e com tendências de aumentar a sua frequência e incidência (SAPOTEK, 2011), algo que transparece esta falta de preparação e consciencialização da população portuguesa aqui em estudo.

abrem espaço para uma difusão de perigos e exposição de vulnerabilidades que devem ser evitadas a todo o custo.

Convém salientar que em Portugal não se exibe por enquanto a existência uma cultura de cibersegurança[35], além da educação sobre conceitos e perigos básicos, não é dada à população em geral o apoio e formação suficientes para as acompanhar e alertar para os reais perigos e fenómenos a que estão sujeitas. Considerando que uma porção elevada da sociedade já navega no ciberespaço, independentemente da faixa etária em que se possa inserir, o desconhecimento ou despreocupação podem ser fatais e acarretar custos sociais e económicos para si e para quem os rodeia. Num ambiente de caráter profissional, este desinteresse ou desconhecimento corporifica situações de fragilidade e uma via para a exploração das vulnerabilidades que as empresas ou infraestruturas públicas possam vir a apresentar.

Perante o "misuse" das novas tecnologias, este empoderamento pode ser venenoso para o bem-estar coletivo e estadual, pois no nosso país essas debilidades apesar de terem sido enfrentadas, não foram colmatadas, colocando Portugal à mercê da exploração dos seus cidadãos, empresas e infraestruturas devido a deficiências na sua estrutura de educação, formação e consciencialização. Deve sobretudo apostar-se numa ciberhigiene interna, que promova boas práticas e elimine ou diminua a capacidade destrutiva desta frente de ataque.

Em comparação com outros Estados, Portugal tem um longo caminho a percorrer na capacitação dos seus cidadãos e profissionais, independentemente da sua condição, já que a propagação de *malware* ou fugas de informação, por exemplo, são potenciadas pelos comportamentos desmedidos destes indivíduos e

[35] Apesar das maior parte das atividades ter migrado para esfera do ciberespaço, os indivíduos enquanto clientes, utilizadores ou provedores de serviços, não apresentam uma consciencialização concreta face à importância da segurança dos seus dados e das redes que frequentam (Blog PT Empresas, 2016). Assim como não estão cientes das represálias que algumas ferramentas ou comportamentos que adotam podem trazer no futuro para si. Ainda não se revê uma capacitação generalizada dos recursos humanos quanto à cibersegurança, alertas estes que devem estender-se a todos setores da sociedade portuguesa, que ainda não apresentam estruturas capazes de responder aos desafios e ciberataques, que revelam uma tendência crescente.

podem ultimamente significar danos irreparáveis em componentes cruciais para a nossa ideia de segurança nacional.

Quanto às ameaças de caráter intencional, no que toca às dinâmicas grupais, é analisável uma capacidade de organização e comunicação ao espelho do caso da Bielorrússia e como a mesma pode ser detetável no nosso país, já que as ferramentas são acessíveis por parte dos indivíduos que habitam no território português e, através das delas, conseguem organizar-se de modo a colocar em causa o funcionamento da sociedade mediante aqueles que são os interesses que esses grupos defendem. No recente caso da invasão de Alcochete, às instalações do Sporting Clube de Portugal, os suspeitos usaram plataformas eletrónicas para comunicar, planear e operacionalizar o ataque em questão, o que os levou a apresentar uma linha de ataque com fins de consequências efetivas no meio físico e partiram do ciberespaço. Este é um dos exemplos da capacidade que as dinâmicas grupais passam a agregar em Portugal, perigando outros indivíduos e minando o exercício da sua cidadania num ambiente de liberdade e segurança, algo pelo qual o Estado deve zelar, questão esta com impacto direto em áreas consideradas de interesse para a segurança nacional.

À semelhança do decorrido, outros grupos utilizam as novas plataformas para se organizarem e facilitarem as suas atividades, conseguindo alienar as entidades competentes, passando ilesos graças às faculdades obtidas. Daí que se possa concluir que os movimentos grupais podem consubstanciar consequências com elevada seriedade para a ordem interna portuguesa, revelando-se impactantes das valências da nossa segurança nacional. Apesar de Portugal não se apresentar num contexto semelhante a um estado autoritário ou policial, não implica que o dinamismo coletivo organizado por via cibernética não seja ameaçador, pois como comprovado, pode colocar em causa alguns dos princípios fundamentais da soberania e segurança nacionais. Esta dinâmica poderia ser visível na eventualidade da tentativa de revolução dentro do nosso território, através do uso das TIC, levando a que indivíduos se organizassem sem ser detetados e conseguissem obter via internet ferramentas e métodos que pudessem então aplicar

enquanto procuram atingir o seu objetivo, algo que teria um impacto sério na estabilidade da sociedade e na manutenção da ordem pública, perigando os valores defendidos pela democracia portuguesa e, por isso, atentando contra a segurança nacional portuguesa.

No caso do *Ransomware* em Portugal e as consequências em que o fenómeno se traduz, vêm a revelar uma incidência crescente, sendo motivado não só devido à desinformação e desinteresse, mas também porque esta é uma ferramenta que pode incapacitar setores críticos do Estado com o intuito da obtenção de ganhos por parte dos perpetradores.

Analisando as estatísticas e deliberações providenciadas pelo Relatório Anual de Segurança Interna (RASI)[36]referente ao ano transato de 2017, o *Ransomware* é encarado com a devida seriedade: "O *ransomware, a exfiltração de dados e a exploração de vulnerabilidades de equipamentos vulgarmente conhecidos por Internet das Coisas (IoT) continuam a apresentar índices de ocorrência muito elevados.*" (RASI, 2018, p.73) O alerta deste relatório foca não só a tendência para serem fenómenos registados com maior frequência e gravidade salientando que também os seus alvos têm vindo a ser diferenciados, incluindo entidades diversas: "*Dos incidentes analisados e resolvidos, 17% afetaram direta ou indiretamente entidades do Estado, o que representa um acréscimo de 8% em relação ao ano transato."* (RASI, 2018, p.129)

Mediante as estatísticas apresentadas, é possível notar a posição estadual enquanto alvo deste fenómeno, algo que pode perigar qualquer instituição pública portuguesa e vedar o acesso a documentos, pôr em causa a manutenção de infraestruturas críticas ou a ação de entidades competentes e necessárias para o funcionamento da sociedade e conservação da ordem pública. A seriedade

[36] O RASI corresponde ao documento que analisa a criminalidade num dado período de tempo, investigando a sua progressão e procurando delinear algumas perspetivas face ao futuro. Permite ainda um estudo sobre as vulnerabilidades e preparação que o Estado Português apresenta e, por isso mesmo, oferece uma visão do impacto que determinadas ameaças e ações têm em esferas importantes da segurança nacional.

merecida por parte deste fenómeno e, maioritariamente porque tem aumentado[37] no nosso território, traduz-se na necessidade observável de uma ação concertada e capaz de mitigar a postura e sucesso de campanhas de *ransomware* no nosso país. Só com prevenção, preparação e formação poderá Portugal inverter esta propensão de evolução que acaba por se alinhar com as tendências internacionais em que este fenómeno se assume como uma das ameaças mais preponderantes no seio da cibercriminalidade e que pode debilitar setores fulcrais para a segurança nacional.

Em relação aos *cyber-mercenaries* e sua manifestação, é notável a disparidade com que as suas ações se registam, desigualdades presentes também naquela que é considerada como a probabilidade de Portugal ser um alvo fustigado pelas suas operações. É feita esta afirmação pois em termos de "inimigos" propriamente ditos ou recursos que possam ser cobiçados por outras entidades internacionais, Portugal, não se apresenta como um dos alvos apetecíveis. As operações significantes por parte destes mercenários tendem a envolver Estados ou grupos que procuram vantagens estratégicas ou a destruição e exploração de fragilidades por via de atores apátridas e que juntam capacidades extremas. Não pode por isso dizer-se que Portugal se encaixe neste perfil, por exemplo não tendo programa nuclear, forças armadas de um poderio assustador ou um poder económico gigante, pelo que aquilo que faria o país ser alvo destes fenómenos seriam outras razões e condicionantes. Esse facto não exclui a possibilidade da rota de variados indivíduos ou grupos[38] tidos como mercenários digitais tomarem o

[37] Este aumento é ainda maior no que se refere aos dispositivos móveis, que segundo Guerra, são perspetivadas atividades que tenham como consequência a encriptação completa dos dispositivos em questão, o que acaba por consistir um perigo ao qual a população portuguesa se encontra exposta e não propriamente advertida (Guerra, 2018). Esta situação exalta um grau de risco gigante para todos os utilizadores independentemente do seu estatuto social ou atividade profissional, desde trabalhadores do setor primário até aos responsáveis máximos das instituições democráticas, comprometendo todos os ficheiros e informações que os seus dispositivos possam conter, alguns deles que podem implicar questões relacionadas com setores críticos da sociedade portuguesa.

[38] De acordo com o noticiado pelo Observador, a ação destes grupos é já visível no nosso território, revelando-se que um grupo de *hackers* conseguiu infiltrar-se nos sistemas informáticos do Ministério dos Negócios Estrangeiros, tendo obtido informações confidenciais que não só comprometeram embaixadas e consulados, como também as credenciais utilizadas por funcionários (Agência Lusa, 2018). Isto espelha como Portugal e suas infraestruturas estão sujeitas a este tipo de ataques, com capacidade para perigar o correto funcionamento de instituições importantes para a salvaguarda dos interesses e da independência nacionais e, ultimamente, da segurança nacional.

nosso país como forma de exploração por lucros ou ganhos, já que recorrendo a métodos como o *ransomware* são capazes de causar instabilidade e danos em infraestruturas críticas, debilitar as defesas e o funcionamento de setores fulcrais para a sobrevivência do Estado e da sua população.

A aplicação dos mercenários é uma das vias pelas quais poderíamos ser alvo de espionagem, sabotagem ou exploração económica, com uma escala de gravidade que facilmente ascende a patamares preocupantes[39]. Não se têm, no entanto, verificado no nosso território, pelo menos que seja do nosso conhecimento, ataques com maiores dimensões ou com intuito semelhante aos ataques que se verificam noutras entidades estaduais ou não-estaduais. Caso se reveja o perpetrar de algo com proporções superiores e não for possível uma defesa robusta, resiliente e atempada, é demonstrado o precedente de que somos uma "presa fácil" e outros ataques se seguirão, fazendo sucumbir áreas necessárias e incorporadas nas prerrogativas nacionais. Ao registar-se tal ineptidão irá comprometer-se a posição portuguesa nos eixos fulcrais da sua política externa e, cabe ao Estado fazer uso de todos os meios e ferramentas a seu dispor para conseguir contrariar as tendências de crescimento que foram evoluindo nos últimos anos e combater o impacto negativo do *cyber-empowerment*, valorizando e utilizando as suas vertentes positivas de modo a transformar a arquitetura do ciberespaço nacional a seu favor.

2 – A opinião da comunidade académica sobre medidas que devem ser aplicadas à realidade portuguesa

Face à nova conflitualidade e impacto dos efeitos de *cyber-empowerment* individual, teóricos passaram a investigar e a procurar determinar aquelas que seriam algumas das necessidades proeminentes para o exercer de um poder

[39] São alertas dados pelo próprio RASI, que defende que a atividade destes grupos ameaça: "*a segurança das infraestruturas críticas, de organismos governamentais e de entidades privadas portuguesas*" (Agência Lusa, 2018, para.6).

estadual seguro e estável, que zele pelos DLG dos seus cidadãos e consiga ripostar contra os desafios potenciados pela era tecnológica.

Disposições presentes no CEDN, enunciam determinadas ordens de trabalho enquanto foco para Portugal acompanhar estas dinâmicas, nomeadamente a necessidade de investimento tecnológico, do investimento das FSS na sua presença no ciberespaço, na cooperação internacional e na educação e desenvolvimento. Juntamente a estas medidas, Nunes salienta a importância do Estado ser capaz de garantir a segurança da informação no ciberespaço, salvaguardando os seus interesses e afirmando o seu poder soberano. Outra das prioridades debatidas consiste numa moldura penal adequada à nova criminalidade, à proteção fundamental das infraestruturas críticas portuguesas e a aplicação de políticas e estratégias sólidas que permitam a Portugal desenvolver uma verdadeira cultura de cibersegurança e ciberdefesa (Nunes, 2012).

O próprio Despacho n.º 13692/2013, que infere sobre a orientação política para a ciberdefesa, referiu o crucial da segurança da informação para a defesa do ciberespaço, encarando este como um “*espaço de defesa de valores e interesses, materializando uma área de responsabilidade coletiva”*(Despacho n.º13692/2013, ponto 3, alínea a)) acrescentando que essa segurança da informação deve “(…) *ser estruturada e desenvolvida de forma a prevenir e retardar a rápida progressão dos ciberataques, garantindo a sua deteção antecipada, implementando ferramentas de vigilância e alerta avançado, procurando deste modo conter e limitar potenciais danos.*” (Despacho n. º13692/2013, ponto 3, parte II, para.1) Além destas enunciações, considera o ciberespaço como um domínio estratégico e prioritário para a defesa de valores e interesses nacionais, pelo que os desafios que este comporta devem ser encarados com seriedade. Por fim, salienta a importância da adoção de uma postura proativa, preventiva e que continue a ter os interesses e valores nacionais no cerne das suas preocupações. Estas foram as perspetivas dadas por vários atores perante a necessidade de se promulgarem documentos que consistissem pilares às estratégias que iriam delinear as políticas portuguesas nestas temáticas, tendo influenciado a arquitetura das mesmas.

2.1 – Estratégias, políticas e ambições pensadas para Portugal

Como resposta portuguesa foram tomadas medidas e aplicadas políticas que visam uma postura securitária alternativa à que tinha sido praticada até então. Por essa razão, a arquitetura cibernética de segurança aplicada hoje é a soma do conjunto de capacidades públicas e privadas, tanto nacionais ou internacionais[40] e do respetivo enquadramento normativo (Barbas & Sancho, 2018), algo que se transpõe na criação das mais recentes políticas e promulgação de estratégias que servem como base às nossas estruturas focadas na segurança informáticas, do Estado e dos cidadãos.

Um dos avanços a assinalar foi a promulgação, em 2015, da Estratégia Nacional de segurança no Ciberespaço através da Resolução do Conselho de Ministros n. º36/2015. Este documento surgiu com vários objetivos em mente, nomeadamente "(…) *aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas*."(Estratégia Nacional de Segurança do Ciberespaço, ponto 1) A mesma é norteada por certos princípios nos quais se contam o princípio da subsidiariedade na medida em que há um responsabilização do indivíduo e do Estado face ao modo como usam o ciberespaço, logo acresce à mesma uma ideia de complementaridade que foca a cooperação entre atores e mediante o uso de parcerias público-privadas, sendo que outros dos princípio a elencar centram-se numa ação proporcional e maior sensibilização para a implementação de uma estratégia sólida e capaz. Outros vetores contemplados na estratégia incidem sobre a importância da

[40] Na qualidade de Estado-Membro da UE, Portugal é influenciado pelas diretivas e políticas emanadas da organização supraestadual, que têm vindo a incentivar as mudanças e as estratégias aplicadas recentemente no nosso país e ambicionam o reforço das capacidades de ciberdefesa dentro da União, procurando a diminuição da incidência e consequências dos ciberataques que ameaçam o bem-estar e a segurança dos Estados-Membros (Comissão Europeia, 2017) Assim sendo, a forma como Portugal perceciona e aplica determinadas medidas, estão interligadas com aquelas que são algumas das prioridades determinadas pela UE e suas instituições.

promoção de uma utilização segura e consciente do ciberespaço e das novas tecnologias não esquecendo a proteção dos DLG.

Esta estratégia pensa assim uma estrutura de como o nosso Estado pode corresponder às novas modalidades de soberania e Segurança Nacional exigidas pelas dicotomias contemporâneas, focando ainda o papel da coordenação operacional e autoridades responsáveis pela vigilância e zelo do ciberespaço e infraestruturas nele inseridas, nomeadamente na figura do Centro Nacional de Cibersegurança (CNCS). O CNCS, é então incumbido da coordenação operacional, coordenação essa necessária para a operacionalidade das medidas visadas na estratégia em si , sendo que algumas das responsabilidades deste organismo pautam-se pela promoção de uma cibersegurança com qualidade crescente e promoção da cooperação internacional, devendo mencionar-se outras de grande relevância para o papel do CNCS em Portugal e presentes no Decreto-Lei 69/2014, como: - “(…) *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.”*(Decreto Lei 69/2014, art.2º, ponto 2) - Este organismo serve ainda para investigar e reunir informação sobre as ameaças e vulnerabilidades que são do conhecimento das entidades.

Outro ponto relevante da estratégia nacional de segurança do ciberespaço é a concretização da orientação política para a ciberdefesa, algo já explorado ao longo do presente capítulo, consubstanciando o implementar, desenvolver e consolidar da mesma, reiterando: “*Constituir a ciberdefesa uma área onde é necessário promover sinergias e potenciar o emprego dual das suas capacidades, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão*.”(Estratégia Nacional de Segurança do Ciberespaço, ponto 4, eixo 3, alínea d)) Aplica-se também à capacidade de ripostar e responder aos acontecimentos, evidenciando a extrema importância de uma política de

ciberdefesa com uma implementação sólida. Prevê-se ainda o estabelecimento de um gabinete de gestão de crises e a realização de exercícios como meio de resposta ao crescente *cyber-empowerment* e suas consequências. Em Portugal, estes exercícios deverão realizar-se com o desígnio de permitir a avaliação da preparação e maturidade da multiplicidade de entidades que se encontram em atividade e da sua capacitação para lidar com incidentes consideráveis, potenciando sinergias entre si. São conglomeradas em adição a melhoria generalizada do ambiente de informação e seu conhecimento por parte de todas as infraestruturas e entidades públicas incluindo-se, nas mesmas, planos de proteção enquanto medidas de segurança necessárias reforçando o poder de cada operador ou funcionário e a importância das suas boas práticas no que toca à detenção, manutenção e prevenção no que toca a segurança informática, implementando uma verdadeira cultura de segurança:*"(...) reduzindo a exposição aos riscos do ciberespaço. É fundamental informar, sensibilizar e consciencializar não só as entidades públicas e as infraestruturas críticas, mas também as empresas e a sociedade civil."* (Estratégia Nacional de Segurança do Ciberespaço, ponto 4, eixo 4)

Quanto à política de ciberdefesa em vigor, centra-se em medidas e ações de grande impacto na proteção do Estado Português, reconhecendo as repercussões que os ciberataques da atualidade podem ter no território nacional, salientando-se –"*perdas relevantes no plano económico, de vidas humanas ou constituir uma ameaça séria à Defesa Nacional*"(Orientação Política para a Ciberdefesa, ponto 3, parte II, para.2) – onde veicula a inovação e evolução constantes, tendo como objetivos primordiais a proteção e segurança das infraestruturas críticas, a exploração de caráter proativo do ciberespaço e a contribuição positiva e cooperativa para a totalidade da cibersegurança nacional. Algo importante que a mesma destaca envolve a promoção de uma cultura de gestão de risco e que deve ser complementada pelos princípios basilares da própria estratégia nacional de segurança do ciberespaço, assim como um investimento nas mais variadas áreas de atuação do Estado quanto à mesma esfera, aliando-se não só ao CNCS, mas também ao Gabinete Nacional de Segurança que supervisiona a articulação e a

harmonização daqueles que se têm como procedimentos quanto à informação de caráter classificado a todos os níveis, assim como a salvaguarda desse tipo de informações mediante a perigosidade que estaria envolvida no caso das mesmas serem de alguma forma vulneráveis a ataques ou acessos exteriores às entidades competentes do Estado.

Com isto, contam-se várias áreas onde as políticas e opiniões analisadas salientam algumas deficiências e necessidade de atuação, quer versem sobre a educação e desenvolvimentos tecnológico, ou pela integração de ferramentas e exercícios usados por outros atores que podem vir a ser aplicados na nossa realidade. Enquanto motivação e núcleo prioritário para os anos vindouros, o RASI aponta algumas prioridades norteadoras da ação estadual portuguesa, ditando como foco no “*investimento nas TIC para desmaterializar e simplificar, aumentar a eficácia e a eficiência da atividade operacional, reforçar o acesso à informação operacional e melhorar a relação entre os cidadãos e as FSS.”*(RASI, 2018, p.230) Em acréscimo, adiciona enquanto necessidades a gestão da função informática, melhorando a capacidade das FSS portuguesas na sua ação.

São opções a considerar, especialmente perante uma disrupção de fenómenos que fazem do nosso país um dos potenciais alvos e cuja população tem que acompanhar a evolução com uma consciencialização proporcional aos desenvolvimentos e sua intrusão no seu quotidiano.

2.2 – O papel da investigação, educação e desenvolvimento em Portugal

É importante destacar tópicos como a educação, a investigação e desenvolvimento tecnológicos, a busca de uma consciencialização global e a criação e aplicação de novas campanhas que promovam soluções criativas como exercícios práticos como o tipo de resposta ou áreas onde se deve apostar nacionamente. Têm vindo a registar-se avanços nestes setores de modo a abrir caminho para uma maior estabilidade do ciberespaço português e consequente segurança da informação.

Assim sendo, um dos eixos prominentes graças ao papel crucial que desempenha, versa sobre a investigação e desenvolvimento, assumindo-se como fundamental o apoio e fomento das capacidades tecnológicas de modo a chegar-se a soluções internas que se pautem pela segurança e confiança, que passem a envolver vários atores dedicados à investigação sobre as mesmas. Valorizando este vetor, Portugal passa a conseguir acompanhar o desenvolvimento da tecnologia com respostas proporcionais em termos securitários, algo que deve ser promovido e incentivado em todas as áreas do saber e afirmando a independência nacional nestes campos, aproveitando os recursos a que tem acesso.

Coincidentemente, outra área de atuação converge no papel da educação e tudo o que possa estar subjacente à mesma, algo que Quesado relembra, reiterando como sendo imperativo capacitar as novas gerações "*com os instrumentos de qualificação estratégica do futuro*" (Quesado, 2013, p.111). Esta deve ser percecionada como um investimento valioso, pois dotando e capacitando as populações, aumentam-se em simultâneo a consciencialização e sensibilização no seio da ordem interna portuguesa – ampliando os efeitos positivos advindos da sua presença no ciberespaço e contrariando os negativos. Nesta lógica, a sensibilização, consequentemente, colmata as divergências entre vulnerabilidades surgidas de ações desmedidas e de descuido de determinados atores e vulnerabilidades realmente causadas por terceiros mal-intencionados, sendo que é inclusiva de meios como promoção de campanhas de informação e alerta, o salientar da natureza crucial da segurança informática, o reforço da educação e da formação de forma ampla e alargada e revela a sua necessidade nas dinâmicas decorrentes das linhas estratégicas para a segurança nacional.

Ambas as valências são necessárias para, com as TIC, se contribuir para a salvaguarda do bem-estar das populações e dos interesses nacionais, abrangendo o tipo de confiança que as boas práticas podem gerar na sociedade portuguesa e todos os serviços que nela se incluem, consolidando setores diferenciados da sociedade através do inspirar e reforçar áreas que também contribuem para uma estabilidade económica, política e/ou social.

Nestas áreas, o espírito de colaboração/cooperação é obrigatório para se lutar pelo sucesso das medidas, citando Quesado - *"(...) só há um regresso possível – o do futuro e protagonizado por todos."* (Quesado, 2013, p.110) revendo-se já alterações positivas na estrutura societária. Contudo, existem várias componentes a ter em consideração, estando em jogo o próprio posicionamento português nas instâncias internacionais. É, por isso, fulcral que Portugal invista e fomente uma evolução constante, a sensibilização e proteção dos serviços e infraestruturas que se revelam críticos para a que o próprio Estado consiga corresponder ao cumprimento dos seus deveres, zelando pelas suas populações, pelos seus valores e pelos seus interesses.

Numa nota mais negativa, convém referir que apesar de registarem progressos, estes são ainda insuficientes face à escalada das ciberameaças e à crescente mobilização do crime para o universo do ciberespaço, algo que o nosso país deve atentar e, assim, procurar adaptar-se com urgência de modo a, primeiro, não ficar para trás na corrida e, segundo, a não vir a ser considerado um alvo fácil devido à desconsideração ou ao subestimar da capacidade de destruição que as novas ameaças provenientes do *cyber-empowerment* individual podem imprimir na sua Segurança Nacional.

2.3 – Que ensinamentos pode Portugal retirar de outros Estados ou atores?

Portugal tem ainda um longo caminho a percorrer em termos de segurança informática e capacitação da sua população e profissionais, contudo, denotam-se já determinados meios e ferramentas que são ou se planeiam utilizar para conseguir fazer frente a ameaças e potenciar os recursos totais que se encontram na esfera interna.

Atendendo à análise das estratégias e medidas empreendidas por outros Estados, Portugal pode investigar o tipo de resposta e adaptações que estes estão a priorizar para adotarem uma postura mais adequada face ao status quo que enfrentam. Esse estudo permite que as entidades competentes possam tentar viabilizar adaptações à nossa realidade nacional e mesmo quando algumas não são

exatamente aplicáveis ao contexto português hodierno, convém tomar conhecimento de planos de reação para uma gestão de risco de qualidade.

Através dos erros cometidos e descobertos na forma como os Estados e outros atores da ordem internacional lidam com as matérias de cibersegurança e empoderamento individual, Portugal, pode ainda conseguir mitigar essas vulnerabilidades na sua ordem interna, podendo antecipar-se tendo em conta o sucedido noutros casos de que tomou conhecimento e assim poder ultrapassar esses desafios antes dos mesmos se revelarem como obstáculos. As divergências na abordagem dos Estados acabam por ser evidentes, algo concluído por um relatório da Comissão Europeia de 2017, mencionando: *"Some already have developed national cybersecurity strategies and so are somewhat locked-in to specific choices such as those regarding the division of responsibility between public and private sectors, the types of instruments and incentives to use, etc. Member State strategies are also marked by cultural and political preferences*." (Comissão Europeia, 2017, p.35) Esta divergência e dissemelhança ajuda na definição de medidas mais diversas pois é possível examinar os resultados que cada uma dessas ações teve no Estado que as implementou. Ora, é do interesse português seguir exemplos de boas práticas, tendo em conta o nosso próprio contexto, realidade e sobretudo recursos, de forma a manter políticas atualizadas e capazes de deixar que a defesa seja o mais afinada possível.

Casos como do Facebook, onde são pensadas formas criativas de manter o engajamento dos funcionários para com temáticas de extrema relevância como é o caso de ciberataques, devem ser tidos em consideração para que a nossa inovação também passe por estratagemas que levem alunos e funcionários não só a criarem e aumentarem a sua consciencialização relativamente a estes temas mas, sobretudo, sofrerem um *cyber-empowerment* positivo onde os próprios se tornam instigadores e peças de uma cibersegurança mais sólida e completa, contribuindo ultimamente para a Segurança Nacional.

O Estado Português tem vindo a aplicar essas novas aprendizagens na sua ordem interna, operacionalizando várias estratégias e políticas que lhe permitem

tomar as rédeas e demonstrar a sua presença na realidade do ciberespaço. Deve estar apto a acompanhar a evolução tecnológica e a empoderar todos os atores que efetuam ações dentro daquilo que pode ser considerado o ciberespaço nacional ou cooperativo. Não deve deixar de procurar novas soluções, investigar e investir no desenvolvimento tecnológico, estando obrigado a criar um clima propício à evolução e capacitação de todos os seus indivíduos e funcionários, fortalecendo todos os sistemas que operam sobre áreas tidas como estratégicas e apostando nas parcerias público-privadas e cooperação internacional[41]. Só assim, e seguindo as estratégias nacionais de cibersegurança e política de ciberdefesa, poderá o nosso país cumprir com os seus deveres e zelar pelos interesses estaduais, promovendo a cibersegurança como parte integrante da Segurança Nacional, sendo o ciberespaço o novo teatro de operações e uma *pool* de interação generalizada.

[41] Uma das iniciativas em que o nosso Estado se envolveu remete para uma campanha de combate ao *Ransomware* e que inclui uma cooperação entre a Polícia Judiciária e entidades estrangeiras, entre elas a EUROPOL. A campanha em si defendia a ideia de "No More Ransom", implementada em 2016, aparecendo como uma ferramenta promotora da cooperação e de assistência aos cidadãos visados por este fenómeno. Com o sucesso da mesma, empresas do setor privado também se aliaram à causa e, segundo o domínio TecheNet, nos primeiros meses de atividade, permitiu que mais de 2500 pessoas conseguissem ultrapassar as barreiras criadas pelos ataques de que tinham sido vítimas sem ter de proceder ao pagamento do respetivo resgate, tudo graças aos métodos e medidas estipulados pelo portal correspondente à iniciativa em estudo. (TecheNet, 2016) Este é um dos exemplos em como a cooperação internacional pode ser benéfica para o Estado Português, cujos organismos conseguem adquirir novas competências e ferramentas que permitem uma melhor realização das suas tarefas, e em especial, uma maior capacitação no que toca à defesa e preservação do bem-estar dos cidadãos portugueses. Os cidadãos, por sua vez, passam a ter acesso a ferramentas apoiadas pelo Estado Português, onde recebem a ajuda e apoio necessários para enfrentar e superar este tipo de ameaças no seu quotidiano.

Considerações Finais

O acompanhar da evolução tecnológica tem vindo a tornar-se uma das tarefas essenciais para o bom funcionamento de uma sociedade cada vez mais multifacetada e diversa, que é modelada pela ação de uma multiplicidade de atores. Essa revolução promoveu um reequilibrar do *status quo* e da balança de poder internacional, especialmente devido ao crescente *cyber-empowerment* individual e seus efeitos. As consequências em si, suscitaram uma necessidade de consciencialização e alteração paradigmática, especialmente quanto ao papel estadual.

No âmbito do presente trabalho, frisaram-se as capacidades e a reinvenção de conceitos tradicionais, assim como um empoderamento a nível global que introduziu temáticas inéditas nas preocupações dos atores da ordem internacional. O empoderamento referido teve especial incidência no novo papel do indivíduo enquanto elemento cada vez mais importante na ordem internacional, cuja ação acarreta efeitos com repercussões no funcionamento, proteção e evolução não só dos Estados a que pertencem, mas também a todos os outros atores do SI.

Simultaneamente, elencaram-se algumas das possibilidades trazidas pelo fenómeno de *cyber-empowerment* para o prisma estadual, enquanto se investigaram determinadas ameaças que o mesmo traria numa outra face da moeda. Nesse estudo, algumas das conclusões que podem ser retiradas aludem à importância do capitalizar do potencial dos indivíduos e da criatividade ou inovação que os mesmos podem incutir em áreas de relevância para o progresso estadual e societário, revolucionando o modo como se operacionaliza a interação entre as duas tipologias de atores e o tipo de benefícios com que podem contar mutuamente. Para um correto desenvolvimento e adaptação do quotidiano à evolução tecnológica, será importante apostar fortemente nesses benefícios, com o intuito de construir um ciberespaço e uma sociedade cada vez mais capacitada para os desafios que possa enfrentar e colmatar as vulnerabilidades que possam ser analisadas. No que concerne às ameaças provenientes do mesmo fenómeno,

compreendem um dos maiores perigos da atualidade, devendo ser cada vez mais abordadas por todos os níveis da sociedade, criando uma maior consciencialização e orientando as gerações para o estudo e conhecimento sobre essas matérias que certamente farão parte dos dilemas do amanhã.

Através do estudo de dadas tendências apuradas e algumas das políticas postas em prática, foi possível enumerar uma fração das ferramentas que permitiriam potenciar as vantagens do *cyber-empowerment* individual, consoante aqueles que são os interesses perpetrados e designados por um ator estadual. Conta-se especialmente a crescente tendência para a aplicação de medidas protecionistas que visam uma maior proteção do ciberespaço de cada Estado e da limitação de conteúdos, existindo uma conceção comum da necessidade de aplicar estratégias que promovam um acompanhamento securitário da novidade tecnológica superior ao que tem sido efetuado, especialmente face à dimensão que as ameaças cibernéticas têm vindo a adquirir no palco internacional.

Posteriormente, afunilou-se o escopo da análise, centrando as atenções no caso português face a este fenómeno de *cyber-empowerment* individual, e generalizado, e seu impacto na ordem interna e na Segurança Nacional respetiva. No decorrer da mesma, denotaram-se as fragilidades que podem salientar-se na forma como Portugal lida e encara os novos desafios e dinâmicas que caracterizam o mundo hodierno. Revela-se que Portugal, apesar de não ser afetado de igual modo por estes efeitos, concentra inúmeras fragilidades e demonstra que, sobretudo quanto ao *Ransomware*, se regista um crescimento exponencial a cada ano deste tipo de ciberataques, não invalidando que ataques de maiores dimensões e que periguem setores críticos se possam vir a dar no futuro e para os quais a nosssa sociedade não se encontra preparada. Enquanto isso, é de salientar que Portugal tem vindo a atrair mais investimento e a tornar-se cada vez mais num país que aposta na novidade tecnológica, cujas contribuições académicas devem ser valorizadas e servem como uma nova via de colocar o país na vanguarda tecnológica. Para se verificar um balanço positivo face à dicotomia entre ameaças *versus* potencialidades provenientes do *cyber-empowerment* individual, algumas

das soluções que se podem prever passam pela cooperação internacional e pela crescente aposta em exercícios e modelos de aprendizagem, aplicados desde cedo, para capacitar a sociedade portuguesa para um mundo onde tudo se desenrola no ciberespaço. Uma das propostas que se pretende veicular consiste na ótica de que é imprescindível adotar-se uma postura proativa, com especial incidência na investigação e mitigar das vulnerabilidades observáveis, reforçando a segurança informática estadual e dos cidadãos portugueses. Tendo Portugal já construído os pilares para a arquitetura de uma estrutura securitária e societária mais robusta, esta deverá ser considerada como uma batalha contínua e imprevisível a ser enfrentada pelo nosso país.

Este novo modelo global de operacionalização da cidadania e interação entre atores, denota uma nova fase na evolução humana e tecnológica, ressalvando-se que as novas gerações desenvolver-se-ão num ambiente que desconhece a inexistência destes fenómenos e das novas tecnologias. É comprovada, assim, uma necessidade de se adotarem as medidas devidas atempadamente para as preparar para um futuro marcado ainda pela virtualização, conectividade e interdependência com o meio físico, complementando-se e moldando o percurso desses indivíduos. Persiste uma obrigatoriedade de preparar melhor as gerações - recentes e futuras - de maneira a incorporar uma mentalidade de cautela que deverá ser aplicada a todos os avanços tecnológicos que certamente se avizinham, de modo a que a evolução tecnológica seja acompanhada de evoluções securitárias que permitam, ultimamente, a incorporação das novas criações de forma segura e que salvaguarde os cidadãos e a segurança nacional das entidades estaduais. Isto porque a transformação tecnológica das sociedades continuará, numa mutação expectável e derivada do progresso e investigação associados, o que por sua vez demonstra a importância de se retirar algumas lições dos erros que têm vindo a ser cometidos e da obrigatoriedade de um aproveitamento mais conveniente das mesmas.

Referências Bibliográficas

Barbas, J., & Sancho, C. (2018). CIBERSEGURANÇA E POLÍTICAS PÚBLICAS ANÁLISE COMPARADA DOS CASOS CHILENO E PORTUGUÊS. *IDN Cadernos*(29). doi:344513/12

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom.* Yale, Estados Unidos da América: Yale University Press.

Fernandes, J. P. (2012). Utopia, Liberdade e Soberania no Ciberespaço. *Nação e Defesa: Cibersegurança*(133), pp. 11-31. doi:54 801/92

Gelbstein, E. (2012). Protecting Critical Information Infrastructures. *Nação e Defesa: Cibersegurança*(133), pp. 128-146. doi:54 801/92

Gonçalves, M. E. (2000). Democracia e Cidadania na Sociedade da Informação. *Presidência da República - Os Cidadãos e a Sociedade da Informação.* Portugal: Presidência da República.

Huxley, A. (1958). *Regresso ao admirável mundo novo* (1ª ed.). Antígona.

Loader, B. D. (2000). Reflexões sobre a Democracia Civil na Era da Informação: um estudo de caso do nordeste de Inglaterra. Em Presidência da República Portuguesa, *Os cidadãos e a sociedade de informação.* Lisboa: INCM.

Martin, D. (1997). *La criminalité informatique: cyber-crime : sabotage, piratage, etc. evolution et répression* (1ª ed.). Paris, França: Presses Universitaires de France. Obtido em 28 de maio de 2018

Maurer, T. (3 de julho de 2018). Cyber Proxies and Their Implications for Liberal Democracies. *The Washington Quarterly: Democracy's Vulnerabilities, 41*(2), pp. 171–188. doi:10.1080/0163660X

Mendonça, A. S. (2012). Diplomacia, Tecnologia e Informação. *Nação e Defesa: Cibersegurança*(133), pp. 50-58. doi:54 801/92

Moniz, P. (abril de 2018). Contributos para uma Estratégia Nacional de Ciberdefesa. Em P. Nunes, C. Mendes, L. Santos, L. C. Santos, P. Moniz, & S. Casimiro. Portugal: Instituto da Defesa Nacional. doi:344513/12

Nunes, P. F. (2012). A Definição de uma Estratégia Nacional de Cibersegurança. *Nação e Defesa: Cibersegurança*(133), pp. 113-127. doi:54 801/92

Patrão, B. (2012). Como Manter um Segredo... Secreto. *Nação e Defesa: Cibersegurança*(133), pp. 196-212. doi:54 801/92

Quesado, F. J. (2012). A Chave da Inteligência Competitiva. *Nação e Defesa: Cibersegurança*(133), pp. 104-112. doi:54 801/92

Santos, L. (2015). Segurança da Informação. Em J. B. Gouveia, & S. Santos, *Enciclopédia de Direito e Segurança* (pp. 422-424). Almedina.

Shapiro, A. L. (1999). *The Control Revolution: How the Internet is putting individuals in charge and changing the World we know.* Nova Iorque, Estados Unidos da América: Century Foundation.

Shirky, C. (2008). *Here comes everybody : the power of organizing without organizations.* New York: Penguin Books.

Tikk-Ringas, E. (2012). National Security Zone in International Cyber Affairs. *Nação e Defesa: Cibersegurança*(133), pp. 59-68. doi:54 801/92

Legislação Consultada

Constituição da República Portuguesa (3ª ed.). (2015). Quid Juris?

- Lei n.º 53/2008 de 29 de agosto. Diário da República n.º 167/2008, Série I de 2008-08-29. https://dre.pt/application/file/a/453327

-Lei n.º 31-A/2009 de 7 de julho. Diário da República n. º129/2009, Série I de 2009-07-07. https://www.emgfa.pt/documents/1stcdg49738f.pdf

- Decreto-lei n. º69/2014 de 9 de maio. Diário da República n.º 89/2014, Série I de 2014-05-09. Lisboa: Presidência do Conselho de Ministros. https://dre.pt/application/file/a/25343853

- Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho. Diário da República n.º 113/2015, Série I de 2015-06-12. Lisboa: Presidência do Conselho de Ministros. https://dre.pt/application/conteudo/67468089

- Despacho n.º 13692/2013 de 28 de outubro. Diário da República n. º208. Pág. 31976.

Artigos consultados online e sites

Afonso, S. (2017). *Portugueses descuidados com segurança informática e fraudes*. Obtido em 1 de setembro de 2018, de Renascença: http://rr.sapo.pt/noticia/78447/portugueses-descuidados-com-seguranca-informatica-e-fraudes

Agência Lusa. (2018). *Espionagem é "ameaça real e concreta" contra a segurança nacional*. Obtido em 6 de setembro de 2018, de TSF: https://www.tsf.pt/sociedade/seguranca/interior/seguranca-espionagem-e-ameaca-real-e-concreta-contra-interesses-nacionais---relatorio-9223454.html

Agência Lusa. (2018). *Ministro garante segurança da rede de comunicações dos Negócios Estrangeiros*. Obtido em 5 de setembro de 2018, de Observador: https://observador.pt/2018/08/30/ministro-garante-seguranca-da-rede-de-comunicacoes-dos-negocios-estrangeiros/

Atkinson, B. (2018). *10 Most Powerful (Known) Active Hacking Groups*. Obtido em 25 de agosto de 2018, de TurboFuture: https://turbofuture.com/internet/Most-Powerful-Active-Hacking-Groups

Blog PT Empresas (2016). *A segurança é importante. Não deixe a componente digital da sua empresa desprotegida*. Obtido de Blog PT Empresas: https://blog.ptempresas.pt/a-seguranca-e-importante-nao-deixe-a-35269

Comissão Europeia (2017). *Cybersecurity in the European Digital Single Market.* Comissão Europeia, High Level Group of Scientific Advisors . Bruxelas: Comissão Europeia. Obtido em 15 de março de 2018, de https://ec.europa.eu/research/sam/pdf/sam_cybersecurity_report.pdf

Comissão Europeia. (2017). *Reforçar o setor da cibersegurança na UE*. Obtido em 5 de setembro de 2018, de Comissão Europeia: https://ec.europa.eu/portugal/news/build-strong-cybersecurity-eu_pt

Coyle, J. (2010). *Is Twitter the news outlet for the 21st century?* (A. Press, Editor) Obtido em 29 de agosto de 2018, de ABC News: Is Twitter the news outlet for the 21st century?

Creemers, R. (2016). *National Cyberspace Security Strategy*. Obtido em 25 de agosto de 2018, de China Copyright and Media: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

Democracy Digest (2018). *'Messing with the Enemy': US lacks consistent narrative to counter weaponized information*. Obtido em 30 de maio de 2018, de Democracy Digest: https://www.demdigest.org/tag/cyber-mercenaries-the-state/

Depasquale, S., & Daly, M. (2016). *The growing threat of cyber mercenaries*. Obtido em 1 de junho de 2018, de POLITICO: https://www.politico.com/agenda/story/2016/10/the-growing-threat-of-cyber-mercenaries-000221

Desjardins, J. (2018). *The Rising Speed of Technological Adoption.* Obtido em 2 de março de 2018, de Visual Capitalist: www.visualcapitalist.com/rising-speed-technological-adoption/

Education, I. D. (2018). *Cybersecurity*. Obtido em 25 de agosto de 2018, de Indiana Department of Education: https://www.doe.in.gov/cybersecurity

ENISA. (2012). *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.* ENISA. ENISA. Obtido em 25 de agosto de 2018, de https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

ENISA. (2017). *NIS Directive*. Obtido em 3 de setembro de 2018, de ENISA: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

Estratégia Nacional de Segurança Russa. (2015). Moscovo, Kremlin.

Farrell, N. (2018). *Iran hires cyber mercenaries for wet work*. Obtido de Fudzilla: https://www.fudzilla.com/news/46263-iran-hires-cyber-mercenaries-for-wet-work

Fernandes, J. P. (2013). Da utopia da sociedade em rede à realidade da sociedade de risc. *Análise Social, XLVIII*(207), pp. 260-286. Obtido em 1 de junho de 2018, de http://analisesocial.ics.ul.pt/documentos/AS_207_d01.pdf

GES. (2017). *U.S. Government Support for Entrepreneurship in America and Around the World*. Obtido de Global Entrepreneur Summit India 2017: https://www.ges2017.org/entrepreneurship-resources-1/

Goldman, J. (2018). *20 Cyber Security Startups to Watch in 2018*. Obtido em 28 de agosto de 2018, de eSecurity Planet: https://www.esecurityplanet.com/network-security/top-cyber-security-startups-2018.html

Groll, E. (2017). *Who Is Really to Blame for the WannaCry Ransomware?* Obtido em 4 de setembro de 2018, de Foreign Policy: https://foreignpolicy.com/2017/05/15/who-is-really-to-blame-for-the-wannacry-ranswomware/

Guedes, A. M. (2010). The new geopolitical coordinates of cyberspace - As novas coordenadas geopolíticas do ciberespaço. *Revista Militar* (2503/2504), pp.

823 - 847. Obtido em 1 de junho de 2018, de https://www.revistamilitar.pt/artigopdf/590

Guedes, A. M., & Santos, L. (2017). Estratégias de Cibersegurança. Portugal. Obtido de https://www.academia.edu/36612491/ls_and_amg_Estratégias_de_Cibersegurança_Cybersecurity_Strategies_aula_do_Mestrado_em_Direito_e_Segurança_Masters_on_Law_and_Security_7_de_Maio_2018_?auto=download

Guerra, A. (2018). *Ransomware móvel está em grande crescimento em 2018*. Obtido em 26 de agosto de 2018, de Ntech.news: https://www.ntech.news/ransomware-movel-esta-em-grande-crescimento-em-2018/

Hacking Team. (2018). Obtido em 30 de julho de 2018, de Wikipedia: https://en.wikipedia.org/wiki/Hacking_Team

Hio, L. (2017). *Cyber-security exercise involves all 11 critical information infrastructure sectors*. Obtido em 25 de agosto de 2018, de The Straits Times: https://www.straitstimes.com/singapore/cyber-security-exercise-involves-all-11-critical-information-infrastructure-sectors

How do Zero-Day Vulnerabilities work: #30SecTech. (s.d.). Obtido de Norton: https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

IDN-CESEDEN, I. c. (2013). ESTRATÉGIA DA INFORMAÇÃO E SEGURANÇA NO CIBERESPAÇO. *IDN Cadernos*. (I. d. Nacional, Ed.) Portugal. Obtido em 5 de maio de 2018, de https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf

Instituto da Defesa Nacional. (2012). *Cibersegurança.* Instituto da Defesa Nacional. doi:54 801/92

Internet censorship listed: how does each country compare? (2012). Obtido de The Guardian: https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list

James, V. (2018). *EU sends controversial internet copyright reforms back to the drawing board*. Obtido em 1 de setembro de 2018, de The Verge: https://www.theverge.com/2018/7/5/17535874/eu-copyright-law-article-11-13-rejected-first-vote

Jeffries, D. (2017). *There is No More Encryption Debate: Backdoors Threaten the Whole World*. Obtido em 2 de novembro de 2017, de Hackernoon: https://hackernoon.com/there-is-no-more-encryption-debate-backdoors-threaten-the-whole-world-8e1793ed32be

Keating, F. (2017). *China causes outrage by banning online content of 'abnormal' homosexual relationships*. Obtido em 3 de setembro de 2018, de Independent: https://www.independent.co.uk/news/china-gay-online-ban-homosexual-a7818166.html

Kostyuk, N. (2013). International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic. *Journal of Strategic Security*, *7*(1), 68-82. doi:http://dx.doi.org/10.5038/1944-0472.7.1.6

Kraft. (2018). *12 Terrifying Ransomware Statistics for 2018*. Obtido em 1 de agosto de 2018, de Kraft: https://kraftbusiness.com/cyber-security/terrifying-ransomware-statistics-infographic/

Kuchler, H. (2018). *US midterm election is new battleground for hackers*. Obtido em 27 de agosto de 2018, de Financial Times: https://www.ft.com/content/c01eaf5e-9b79-11e8-9702-5946bae86e6d

Lazarescu, M. (2016). *Hacked by a fridge: The Internet of Things and cyberattacks*. Obtido em 23 de novembro de 2017, de World Economic

Forum: https://www.weforum.org/agenda/2016/10/hacked-by-a-fridge-the-internet-of-things-and-cyberattacks

Lee, D. (2018). *Hacking the US mid-terms? It's child's play*. Obtido em 27 de agosto de 2018, de BBC News: https://www.bbc.com/news/technology-45154903

Lourenço, N., Rodrigues, J. C., Lopes, F., Silvério, P., & Costa, A. (2015). *Segurança Horizonte 2025. Um Conceito de Segurança Interna.* Colibri & GRESI – Grupo de Reflexão Estratégica Sobre a Segurança Interna. Obtido em 20 de maio de 2018, de https://www.researchgate.net/publication/275464581_Seguranca_Horizonte_2025_Um_Conceito_de_Seguranca_Interna

MacEwan, N. (2017). *Responsibilisation, Rules and Rule-following concerning Cyber Security: Findings from Small Business Case Studies in the UK*. University of Southampton, Faculty of Social, Human and Mathematical Sciences. Obtido em 4 de setembro de 2018, de https://eprints.soton.ac.uk/417156/1/Neil_MacEwan_Thesis_final_draft_post_viva_.pdf

Makuch, B., Tucker, B. (Escritores), & Reibling, D. (Realizador). (2016). *Cyberwar: Cyber Mercenaries* [Filme]. Obtido em 15 de julho de 2018, de https://www.youtube.com/watch?v=Ay1JQsjeuJA

McBride, M., Carter, L., & Warkinten, M. (2012). *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policie.* Institute for Homeland Security Solutions. North Carolina: Institute for Homeland Security Solutions. Obtido em 12 de junho de 2018, de https://sites.duke.edu/ihss/files/2011/12/CyberSecurityFinalReport-Final_mcbride-2012.pdf

Mulgan, G. (2005). Reshaping the State and its Relationship with Citizens: the Short, Medium and Long-term Potential of ICT's. Em M. Castells, & G.

Cardoso, *The Network Society: From Knowledge to Policy* (pp. 225-238). Washington, DC: Center for Transatlantic Relations. Obtido em 15 de agosto de 2018, de https://www.researchgate.net/profile/Gustavo_Cardoso5/publication/265108845_The_Network_Society_From_Knowledge_to_Policy_Edited_by/links/57287fff08ae5d0a42a862c6/The-Network-Society-From-Knowledge-to-Policy-Edited-by.pdf

National Security. (2018). Obtido em 30 de julho de 2018, de Wikipedia: https://en.wikipedia.org/wiki/National_security#China

National Security Strategy of the United States of America (2017). The White House of the United States of America, The White House of the United States of America, Washington, DC. Obtido em 27 de agosto de 2018, de https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

NG, A. (2017). *UN finds cybersecurity is a struggle worldwide*. Obtido em 4 de setembro de 2018, de CNET: https://www.cnet.com/news/united-nations-cybersecurity-global-index-united-states-singapore/

Nohe, P. (2018). 2018 *Cybercrime Statistics: A closer look at the "Web of Profit"*. Obtido em 25 de agosto de 2018, de Hashed Out: https://www.thessIstore.com/blog/2018-cybercrime-statistics/

Nunes, D. F. (2018). *Portugal investe 8 milhões em estradas inteligentes*. Obtido em 18 de junho de 2018, de Diário de Notícias: https://www.dn.pt/dinheiro/interior/portugal-investe-8-milhoes-em-estradas-inteligentes-9270118.html?utm_source=dlvr.it&utm_medium=twitter

Nye, J. (2010). *Cyber Power.* Belfer Center for Science and International Affair. Obtido em 1 de maio de 2018, de https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Oggerino, C. (2018). *How Braga, Portugal Is Using IoT and Cisco DevNet to Become a Smart City*. Obtido em 20 de julho de 2018, de Cisco Blogs: https://blogs.cisco.com/developer/iot-braga-portugal#portugal

O'Reilly, T. (2011). Government as a Platform. *Innovations: Technology, Governance, Globalization, 6*(1), pp. 13-40 . doi:https://doi.org/10.1162/INOV_a_00056

Poulsen, K. (2014). *Visit the Wrong Website, and the FBI Could End Up in Your Computer*. Obtido em 10 de junho de 2018, de Wired: https://www.wired.com/2014/08/operation-torpedo/

Raposo, F. (2017). *Paula Simões sobre neutralidade da internet, direitos digitais e direitos de autor*. Obtido em 23 de janeiro de 2018, de Apenas Fumaça: http://apenasfumaca.pt/paula-simoes-sobre-neutralidade-da-internet-direitos-digitais-e-direitos-de-autor/

Relatório Anual de Segurança Interna - Ano 2017. (2018). Portugal: Sistema de Segurança Interna - Gabinete do Secretário Geral. Obtido em 20 de maio de 2018, de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6

SAPOTEK. (2011). *Portugueses mais afectados por malware que a média europeia*. Obtido em 5 de setembro de 2018, de Sapotek: https://tek.sapo.pt/noticias/computadores/artigos/portugueses-mais-afectados-por-malware-que-a-media-europeia

Segal, A. (2018). *Cyber Mercenaries and the Crisis in Ukraine.* Obtido em 30 de maio de 2018, de Council on Foreign Relations: https://www.cfr.org/blog/cyber-mercenaries-and-crisis-ukraine

Slaughter, A.-M. (2017). *3 responsibilities every government has towards its citizens*. Obtido em 5 de maio de 2018, de World Economic Forum: https://www.weforum.org/agenda/2017/02/government-responsibility-to-citizens-anne-marie-slaughter/

Stone, J., & Janofsky, A. (2017). *A Better Way to Teach Cybersecurity to Workers*. Obtido de The Wall Street Journal: https://www.wsj.com/articles/a-better-way-to-teach-cybersecurity-to-workers-1505700120?lipi=urn%3Ali%3Apage%3Ad_flagship3_detail_base%3B%2FB%2FCnZI8SfSPCvYnupABRg%3D%3D

Suter, M. (2012). PPPs in Security Policy: Opportunities and limitations. *CSS Analysis in Security Policy*(111), pp. 1-4. Obtido em 20 de agosto de 2018, de http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analysis-111-EN.pdf

TecheNet. (2016). *Portugal junta-se à iniciativa “No More Ransom” para combater ransomware a nível mundial*. Obtido em 28 de agosto de 2018, de TecheNet: https://www.techenet.com/2016/10/portugal-junta-se-a-iniciativa-no-more-ransom-para-combater-ransomware-a-nivel-mundial/

Tenner, E. (1996). *Why things bite back: Technology and the revenge of unintended consequences.* Nova Iorque: Knopf.

Vogt, S. D. (2017). The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. *Santa Clara Journal of International Law, 15*(1), 102-124. Obtido em 5 de janeiro de 2018, de http://digitalcommons.law.scu.edu/scujil/vol15/iss1/4

Volz, D., & Menn, J. (2017). *Russian hackers stole U.S. cyber secrets from NSA: media reports.* Obtido em 24 de agosto de 2018, de Reuters: https://www.reuters.com/article/us-usa-cyber-nsa/russian-hackers-stole-u-s-cyber-secrets-from-nsa-media-reports-idUSKBN1CA2DO

Weber, V. (2018). *States and Their Proxies in Cyber Operations*. (Lawfare Institute in Cooperation With Brookings) Obtido em 30 de maio de 2018, de Lawfare: https://www.lawfareblog.com/states-proxies-cyber-operations

Wickramanayake, V. (2017). *The Story of Wanna Cry*. Obtido de Cyberon: https://cyberonsecurity.com/2017/11/15/the-story-of-wannacry/

Wiser. (2016). *Czech Republic (CZ)*. Obtido em agosto de 2018, de Wiser: https://www.cyberwiser.eu/czech-republic-cz

Wolf, R. (2015). *Ukraine: Cyber Mercenaries Attack Antiwar.com (Cyber Mercenaries Part 3).* Obtido em 1 de junho de 2018, de Cyrano's Journal Today: http://www.cjournal.info/2015/10/24/ukraine-cyber-mercenaries-attack-antiwar-com-cyber-mercenaries-part-3/

World Economic Forum (2017). *Why cyberattacks could be war crimes.* Obtido em 1 de março de 2018, de Medium: https://medium.com/world-economic-forum/why-cyberattacks-could-be-war-crimes-b81af0ce8777

World Economic Forum (2018). Obtido em 30 de maio de 2018, de http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

World Economic Forum (2018). *Cyber Resilience: Playbook for PublicPrivate Collaboration.* (F. o. Initiative, Ed.) Obtido em 30 de maio de 2018, de World Economic Forum: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

World Economic Forum (2018). *Readiness for the Future of Production Report 2018.* World Economic Forum. Obtido em 1 de junho de 2018, de http://www3.weforum.org/docs/FOP_Readiness_Report_2018.pdf

World Economic Forum (2018). *Towards a Reskilling Revolution: A Future of Jobs for All.* World Economic Forum. Obtido em 1 de junho de 2018, de http://www3.weforum.org/docs/WEF_FOW_Reskilling_Revolution.pdf