# A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou Otimista?*

Sofia Martins Geraldes
*Instituto Universitário de Lisboa (ISCTE-IUL), Centro de Estudos Internacionais.*

**Resumo**
O ciberespaço tem sido considerado uma matéria de segurança central, apesar do seu estatuto inicial de simples problema técnico. Na era da conectividade digital, a existência de redes significa que qualquer dispositivo está susceptível à intrusão externa não autorizada e a dependência tecnológica dos Estados e das sociedades cria uma percepção de vulnerabilidade. Este contexto tem justificado a securitização do ciberespaço, com implicações legais, éticas e políticas. Neste cenário, assiste-se à introdução da cibersegurança no topo das agendas políticas dos Estados e das organizações internacionais, como a União Europeia, mas também a uma crescente preocupação com a excessiva regulamentação deste domínio. Deste modo, este artigo, mediante análise de discurso e segundo o modelo proposto por Mark Lacy e Daniel Prince (2018), analisa a evolução da posição discursiva da UE em relação ao ciberespaço enquanto matéria de segurança, para compreender se a estratégia de cibersegurança europeia é catastrofista, realista e/ou otimista.

**Palavras-Chave:** Cibersegurança; Catastrofista; Realista; Otimista; Estratégia de Cibersegurança da União Europeia.

***Abstract***
***Cybersecurity Strategy of the European Union: Catastrophist, Realist and/or Optimist?***

*Cyberspace has been a central security issue, despite its initial status as a simple technical problem. In the era of digital connectivity, the existence of networks means that any device is susceptible to unauthorized external intrusion, and the technological dependence of States and societies creates a perception of vulnerability. This context has justified the securitization of cyberspace, with political, legal and ethical implications. In this scenario, we are witnessing the introduction of cybersecurity at the top of the political agendas of States and international organizations, such as the European Union, but at the same time there is a growing concern regarding the excessive regulation of this domain. Therefore, this investigation, through discursive analysis and following the model proposed by Lacy and Prince (2018), analyses the discursive position of the EU in relation to cyberspace as a security issue, to understand if it presents a catastrophist, realist and/or optimist cybersecurity strategy.*

**Keywords:** *Cybersecurity; Catastrophist; Realist; Optimist; European Union Cybersecurity Strategy.*

* Investigação financiada pela Fundação para a Ciência e a Tecnologia, com a referência de Bolsa de Doutoramento SFRH/BD/140797/2018.

**Introdução**

O ciberespaço[1] tem sido apontado, por atores políticos e militares, como o quinto domínio operacional, à semelhança da terra, do mar, do ar e do espaço (Craig e Valeriano, 2018, p. 85; Steiger *et al.*, 2018, p. 1). Consequentemente, assiste-se à introdução das ciber-ameaças enquanto desafios prioritários nas agendas de segurança nacional e internacional (Craig e Valeriano, 2018, p. 87; Valeriano e Maness, 2018, p. 263; Van der Meer, 2015, p. 193).

Todavia, o ciberespaço nem sempre foi considerado uma matéria de segurança. Inicialmente, a preocupação estava centrada somente na proteção dos sistemas informáticos da intrusão externa não autorizada – segurança informática (Hansen e Nissenbaum, 2009, pp. 1155 e 1160).

No entanto, este espaço foi rapidamente securitizado[2] por atores políticos e governamentais, pelo setor privado e por órgãos de comunicação social, passando a ser, simultaneamente, considerado como matéria de segurança. Na era da conectividade digital, o ciberespaço permeabiliza fronteiras e a existência de equipamentos interligados através de redes significa que qualquer dispositivo pode ser *hackeado* e está suscetível à intrusão externa não autorizada (Valeriano e Maness, 2018, p. 260). Adicionalmente, a dependência tecnológica dos Estados e das sociedades modernas cria, segundo Valeriano e Maness (2018, p. 260), uma perceção de vulnerabilidade, levando ao desenvolvimento de políticas de cibersegurança (Valeriano e Maness, 2018; Eriksson e Giacomelo, 2006).

O debate subjacente à cibersegurança e, nomeadamente à ciberguerra, tem sido exagerado e redutor, o que por sua vez poderá resultar no desenvolvimento de políticas desajustadas que não correspondem à realidade contextual (Valeriano e Maness, 2018, pp. 262-263). Neste sentido, a abordagem proposta por Mark Lacy e Daniel Prince (2018), mediante a identificação de três posições sobre o ciberespaço – catastrofistas, realistas e otimistas – permite ter uma leitura alternativa dos desafios subjacentes ao ciberespaço.

Por um lado, considerando a centralidade que o ciberespaço tem adquirido nas agendas políticas dos Estados e das organizações internacionais, como é o caso da União Europeia (UE) (Cavelty, 2018b, p. 1; Christou, 2018, p. 2; Carrapiço e Barrinha, 2017, p. 1255), urge a necessidade de analisar as políticas de cibersegurança desenvolvidas por estes atores; neste artigo em particular optou-se por analisar o contexto europeu, nomeadamente da União Europeia. Por outro lado, atendendo à

1 Para uma análise mais detalhada sobre o conceito de ciberespaço ver, por exemplo, Nye (2010, p. 3).

2 Para uma análise mais detalhada do conceito de securitização ver, por exemplo, Hansen e Nissenbaum (2009, pp. 1155-1175).

crescente preocupação para com a excessiva regulamentação do ciberespaço, o artigo analisa o processo discursivo através do qual a União Europeia passou a considerar o ciberespaço uma matéria de segurança e averigua a proporcionalidade na sua tradução em políticas e instrumentos. A escolha da União Europeia decorre do seu desenvolvimento e afirmação como ator de segurança que cobre um crescente número de áreas e políticas entre as quais a cibersegurança (Carrapiço e Barrinha, 2017, p. 1254).

O objetivo consiste no estudo da Estratégia de Cibersegurança da UE, averiguando se esta reflete uma posição catastrofista, realista ou otimista tal como ela é descrita na literatura selecionada nesta investigação, através de uma metodologia de análise de discurso. Esta análise permitirá avaliar se posições catastrofistas, que tendem a hipersecuritizar o ciberespaço e a promover o desenvolvimento de contramedidas excessivas, colidem com o sistema de normas, valores e princípios promovidos pela União. Neste contexto analítico, o documento da Estratégia de Cibersegurança de 2013 marca um momento decisivo na identificação do ciberespaço como matéria de segurança no seio da União Europeia (Cavelty, 2018b, p. 8). Assim, a análise será centrada no plano discursivo e não no plano da eficácia das políticas de cibersegurança da União[3].

Neste sentido, este artigo divide-se em três pontos principais. O primeiro ponto analisa o debate subjacente à relação entre o ciberespaço e a segurança, para compreender como uma matéria de natureza técnica assumiu uma dimensão de segurança. O segundo ponto analisa o modelo proposto por Mark Lacy e Daniel Prince (2018) referente às várias posições em torno do debate sobre cibersegurança. O terceiro ponto analisa a evolução da abordagem discursiva da UE sobre o ciberespaço e analisa a Estratégia de Cibersegurança da UE, segundo o modelo proposto por Mark Lacy e Daniel Prince (2018).

## O Ciberespaço: Da Natureza Técnica À Dimensão de Segurança (Inter)Nacional

Os desafios e as ameaças emergentes associadas ao ciberespaço têm tido uma presença indiscutível na agenda de segurança internacional do pós-Guerra Fria, resultante de inovações tecnológicas e de alterações na conjuntura geopolítica (Maness e Valeriano, 2015, p. 2; Hansen e Nissenbaum, 2009, p. 1155; Eriksson e Giacomello, 2006, p. 225).

Todavia, o ciberespaço nem sempre foi considerado uma matéria de segurança. A introdução do termo cibersegurança foi feita pela primeira vez, no início dos anos 1990, por cientistas informáticos. Neste âmbito, a preocupação visava inseguranças

3 Para uma análise mais detalhada sobre a eficácia da UE como ator de cibersegurança ver, por exemplo, Carrapiço e Barrinha (2017).

relacionadas com computadores ligados em rede e alertava para a necessidade de proteger os dados existentes em determinado sistema informático e a integridade dos próprios sistemas informáticos. Deste modo, o foco centrava-se no desenvolvimento de programas e sistemas robustos com o propósito de dificultar a intrusão externa não autorizada – segurança informática (Hansen e Nissenbaum, 2009, pp. 1155 e 1160).

Porém, atores políticos, governamentais, setor privado e órgãos de comunicação social rapidamente securitizaram este problema técnico, reconhecendo os seus potenciais efeitos sociais e implicações para a segurança (Valeriano e Maness, 2018, p. 259; Hansen e Nissenbaum, 2009, p. 1155). Assim, segundo Hansen e Nissenbaum (2009, p. 1160), cibersegurança resulta da adição entre "segurança informática" e "securitização", o ciberespaço deixa de ser um mero assunto técnico e passa a ser considerado simultaneamente como uma matéria de segurança.

A securitização deste domínio pode ser explicada por duas razões principais, uma técnica e uma social: o caráter em rede dos sistemas informáticos (técnica) e a dependência tecnológica dos Estados e das sociedades atuais (social) (Valeriano e Maness, 2018, p. 259; Van der Meer, 2015, p. 195; Hansen e Nissenbaum, 2009, p. 1160).

Por um lado, os sistemas informáticos controlam objetos físicos, como por exemplo transformadores elétricos, comboios, *pipelines*, entre outros. A ocorrência de um ciberataque significa que os sistemas que controlam estes objetos físicos possam ser comprometidos, podendo dificultar ou impedir a distribuição elétrica ou de comunicação, perturbar sistemas de transporte, desativar transações financeiras e, consequentemente, gerar o caos (Hansen e Nissenbaum, 2009, p. 1161). Por outro lado, os avanços tecnológicos, designadamente a conectividade digital, são simultaneamente uma oportunidade, na medida em que contribuem para a distribuição do poder, mas também um desafio, ao reforçarem as vulnerabilidades dos Estados e das organizações (Valeriano e Maness, 2018, p. 259). A crescente dependência tecnológica dos Estados e das sociedades traduz-se numa maior vulnerabilidade às ameaças do ciberespaço. Isto é, um crescente número de atividades fundamentais diárias e interações – transações financeiras, transportes públicos, serviços de saúde, entre outros – depende do domínio digital e, como já mencionado, um crescente número de dispositivos estão ligados em rede, assim, o risco de serem manipulados por partes não autorizadas é igualmente crescente (Van der Meer, 2015, p. 195).

Na disciplina das Relações Internacionais a literatura sobre a securitização do ciberespaço tem sido alimentada, em parte, pelo debate em torno do ciberconflito e da ciberguerra (Valeriano e Maness, 2018, p. 259)[4]. A introdução do debate teve início

4 É possível identificar três fenómenos no debate sobre cibersegurança: ciberterrorismo; cibercrime e ciberguerra, por questões de limites de espaço optou-se por destacar o debate em torno da ciberguerra.

em 1993 por Arquilla e Ronfeldt ao anteciparem que "Cyberwar is coming!" e refletirem sobre o possível uso do ciberespaço com propósitos coercivos no seu sentido convencional. Mediante o desenvolvimento dos conceitos de *netwar* e *cyberwar*, anteciparam a mudança na natureza, "how societies may come into conflict", e o caráter da guerra, "how their armed forces may wage war" (Arquilla e Ronfeldt, 1993, pp. 25 e 27). Os desenvolvimentos tecnológicos iriam perturbar os modelos hierárquicos tradicionais, permitindo a difusão e redistribuição do poder, nomeadamente em proveito de atores tradicionalmente percecionados como mais fracos; mas também iriam redefinir fronteiras e expandir os horizontes espaciais e temporais (Arquilla e Ronfeldt, 1993, p. 26).

No entanto, segundo Rid (2012, pp. 11 e 15), a ciberguerra nunca ocorreu, não está a ocorrer e dificilmente ocorrerá, uma vez que nenhum ciberataque, até então, preencheu todos os requisitos necessários para ser considerado um ato de guerra. Segundo Rid (2012, pp. 8-9), inspirado por um entendimento clausewitziano de guerra, qualquer ação ofensiva ou defensiva, que é ou tenha o potencial de ser considerada um ato de guerra, tem que preencher três requisitos: tem de ter caráter violento, tem de ser instrumental e tem de ter motivação política. Todavia, segundo Stone (2013, p. 101), a análise do ciberespaço expõe a conceptualização precária de conceitos chave dos Estudos Estratégicos. Stone (2013, p. 101) alerta para a ambiguidade no entendimento de conceitos como força, violência e letalidade e, apesar de concordar que a ciberguerra dificilmente terá lugar, não significa que um ciberataque não possa necessariamente ser considerado um ato de guerra. Toda a guerra envolve um ato de força, mas nem todo o ato de força implica letalidade. Assim, a imposição da mudança física (ato de força) poderá ser em indivíduos, matando e assim sendo letal, ou em infraestruturas físicas, o que não implica necessariamente letalidade (Stone, 2013, pp. 103 e 105).

Apesar do debate contestado em torno do futuro da ciberconflitualidade, existe um consenso geral de que a ciberguerra dificilmente terá lugar (Cavelty, 2018a, p. 132). Porém, isto não significa que o ciberespaço não tenha implicações negativas para a estabilidade e segurança internacional. No sistema internacional, a securitização do ciberespaço pode ser explicada por três pressupostos: (1) o potencial do ciberespaço para alterar dinâmicas tradicionais de poder; (2) o potencial ofensivo do ciberespaço; (3) as dificuldades subjacentes às capacidades defensivas no ciberespaço (Kello, 2013, p. 22; Liff, 2012, p. 405).

A acessibilidade e os custos reduzidos associados à ação dos infratores no ciberespaço conferem capacidades e poder a um maior número de atores, desafiando a primazia do Estado e contribuindo para a transição e difusão do poder (Nye, 2012, p. 135; Eriksson e Giacomelo, 2006, pp. 222 e 226). Adicionalmente, partindo do pressuposto que o sistema internacional configura um sistema anárquico, no qual os Estados reconhecem a primazia da necessidade de preservação do interesse

nacional e a estabilidade nas suas relações estratégicas, não reconhecem qualquer autoridade acima da sua própria. Neste contexto, a emergência de atores não tradicionais, que não orientam a sua ação segundo as normas estabelecidas internacionalmente, pode desafiar o equilíbrio da ordem internacional (Kello, 2013, p. 31). Assim, a combinação entre a difusão de poder proporcionada pelo ciberespaço a um maior número de atores e a sua possível indisponibilidade para respeitar as normas internacionais atualmente estabelecidas poderá comprometer a estabilidade e segurança internacional.

No entanto, esta situação não deve ser exagerada, tendo em conta que os Estados, e especialmente os Estados tecnologicamente mais avançados, continuarão a ter vantagem em termos de ciber-poder[5], pelo menos no que diz respeito à capacidade ofensiva. Os Estados permanecerão melhor equipados para tirar partido das ferramentas disponibilizadas pelo ciberespaço, uma vez que têm a capacidade para investir em recursos humanos, investigação e desenvolvimento e educação, para desenvolver ciber-armas suficientemente sofisticadas com capacidade para alterar o *state of affairs* (Valeriano e Maness, 2018, pp. 260-261; Liff, 2012, pp. 410 e 416).

Neste sentido, apesar das oportunidades disponibilizadas pelo ciberespaço a atores não estatais, como organizações de crime organizado e grupos terroristas, as suas ações, até ao momento, têm sido geralmente ineficazes. Isto é, não têm tido um impacto considerável ou são usados como *proxies* pelos Estados, com o propósito de ultrapassar problemas relacionados com a atribuição. Assim, ao usarem outros atores para atacarem, os Estados manipulam a identificação da fonte do ataque (Valeriano e Maness, 2018, pp. 260-261; Craig e Valeriano, 2018, p. 90; Kello, 2013, p. 35; Liff, 2012, p. 413). Assim, apesar de o ciberespaço permitir a transição e difusão do poder, dificilmente alterará significativamente as dinâmicas de poder tradicionais (Nye, 2012, p. 173).

A superioridade ofensiva das ciber-armas, isto é, a facilidade de desenvolver um ciberataque comparativamente à dificuldade de desenvolver capacidades defensivas eficazes no ciberespaço, é um obstáculo à preservação da estabilidade internacional, considerando que contribui para a exacerbação do dilema de segurança. Instaurando uma situação de desconfiança mútua que poderá instigar uma corrida às ciber-armas (Kello, 2013, pp. 32-33). A crescente securitização do ciberespaço é evidente: traduzida na criação de novos comandos militares, como o USCYBERCOMAND; na criação de doutrina militar para o ciberespaço; e no crescente aumento dos orçamentos para a cibersegurança (Craig e Valeriano, 2018, p. 88; Hansen e Nissenbaum, 2009, p. 1157).

A esta realidade associa-se a dificuldade de desenvolver capacidades defensivas suficientemente eficazes (Craig e Valeriano, 2018, p. 88; Kello, 2013, pp. 32-33; Liff,

5 Para uma análise mais detalhada do conceito de ciber-poder ver, por exemplo, Nye (2010).

2012, p. 414), bem como a problemática da atribuição, que é difícil, mas fundamental, para o desenvolvimento de ação e para a sua legitimidade. O ciberespaço permite um elevado nível de anonimato ao atacante, dificultando a identificação da fonte, a sua identidade e localização (Liff, 2012, p. 412). Não obstante a possibilidade de atribuição, através da identificação do IP do atacante, que é a forma técnica mais elementar de deteção do atacante, este pode ser manipulado, condicionando a identificação precisa da fonte e não revela exatamente a identidade do atacante. Adicionalmente, a atribuição, mesmo sendo possível, poderá não acontecer a tempo para retaliar, impedindo ou condicionando a capacidade de resposta e de deter o ataque (Kello, 2013, p. 33).

Porém, apesar do potencial subjacente ao uso hostil do ciberespaço, o seu emprego de forma coerciva convencional tem sido exagerado, considerando o seu poder transformativo limitado, até então, para alterar significativamente o comportamento do alvo. A novidade e o perigo deste novo domínio residem na capacidade que tem para expandir as possibilidades de causar danos, nomeadamente, através de ações de espionagem ou subversão (Valeriano e Maness, 2018, p. 265; Craig e Valeriano, 2018, p. 91). Neste sentido, apesar da baixa probabilidade de um caos global e de escalada para uma situação de conflito armado, esta tecnologia tem multiplicado as possibilidades de causar danos além das conceções tradicionais de guerra, desafiando a estabilidade e a segurança internacional (Kello, 2013, p. 38). A natureza das ciberameaças deverá assim ser devidamente analisada para prevenir a securitização do ciberespaço e levar ao desenvolvimento de políticas de cibersegurança exageradas que não se encontram em concordância com a realidade contextual e criem outras inseguranças (Valeriano e Maness, 2018, p. 262).

Neste sentido, o ponto seguinte analisa um debate alternativo sobre políticas de cibersegurança, nomeadamente sobre como determinadas visões sobre o ciberespaço resultam em determinadas políticas e instrumentos.

**Políticas de Cibersegurança: Catastrofista, Realista ou Otimista**

No artigo intitulado "Securitization and the global politics of cybersecurity" Mark Lacy e Daniel Prince (2018) procuram compreender as políticas de cibersegurança, uma área complexa que compreende desafios técnicos e políticos, e em particular, como diferentes entendimentos sobre o ciberespaço enquanto matéria de segurança justificam o desenvolvimento de determinadas políticas e instrumentos.

Lacy e Prince (2018) propõe três posições: *cyber catastrophist*, *digital realist* e *techno optimist*[6] e alertam para a necessidade de se refletir sobre os vários cenários apresen-

6 Neste artigo, identificados como catastrofista, realista e otimista, respetivamente.

tados em cada posição, considerando a natureza volátil, incerta, complexa e ambígua do sistema internacional atual. Em cada posição é possível identificar questões relevantes sobre a cibersecuritização, as quais devem ser ponderadas, uma vez que se assiste a uma mudança rápida, quer em termos geopolíticos quer em termos tecnológicos. O modelo proposto por Lacy e Prince (2018) procura desenvolver ferramentas que auxiliem a análise do ciberespaço enquanto matéria de segurança de forma a evitar o desenvolvimento de políticas que o hipersecuritarizem[7] (Lacy e Prince, 2018, pp. 100-101 e 111).

Os *cyber catastrophist* têm uma visão pessimista do ciberespaço e acreditam que o desastre digital será uma realidade e uma ameaça central no futuro. Contudo, é recorrentemente pouco valorizada no discurso público sobre desafios geopolíticos. Poucos catastrofistas equipariam as consequências sociais, económicas e ao nível das infraestruturas de um desastre digital à violência das armas de destruição massiva (Lacy e Prince, 2018, p. 104).

A palavra-chave que caracteriza esta posição é ansiedade, alicerçada na premissa de que as hierarquias tradicionais estão a ser perturbadas pelo ritmo da mudança, conferindo oportunidades perigosas a atores não estatais. Neste sentido, por um lado, sobretudo por parte dos catastrofistas que acreditam que a fonte do desastre digital será externa, a preocupação reside na capacidade que atores não estatais poderão desenvolver, podendo atuar com um nível de organização e coordenação semelhante à dos Estados. Por outro lado, a mudança e o progresso tecnológico, sobretudo através da conectividade digital, traduz-se na elevada probabilidade de acidentes e desastres terem consequências além-fronteiras. Consequentemente, esta posição tem tendência a hipersecuritizar o ciberespaço (Lacy e Prince, 2018, pp. 104-105). Esta posição, através de analogias históricas, isto é, mediante a reanimação de eventos passados, especula sobre a ocorrência de um *cyber 9/11* ou mesmo de *cyber Pearl Harbour*, em que sistemas telefónicos poderão colapsar, as redes de transportes poderão parar e o dinheiro de milhares de pessoas poderá fica inacessível (Eriksson e Giacomello, 2006, p. 226). Neste sentido, os *cyber catastrophists* advertem para a possibilidade de se vir a assistir a desastres e catástrofes digitais e para a necessidade de se avaliar o grau de preparação das diferentes organizações responsáveis pela proteção das sociedades (Lacy e Prince, 2018, pp. 101 e 104-106). À semelhança do que sugere Stone (2013), apesar da baixa probabilidade de ocorrência de uma ciberguerra, a posição catastrofista alerta para a necessidade de se considerarem as vulnerabilidades digitais e para a urgência de desenvolver políticas que lhes deem resposta (Lacy e Prince, 2018, p. 113).

7 Hipersecuritizar refere-se à expansão de um problema de segurança para um domínio onde existe o perigo de exagerar ameaças e desenvolver contra-medidas excessivas. Para uma conceptualização mais detalhada ver, por exemplo, Hansen e Nissenbaum (2009).

Os *digital realist*, por sua vez, têm uma visão mais otimista sobre o ciberespaço e criticam o pânico excessivo atualmente existente em torno da ciberguerra (Lacy e Prince, 2018, p. 106). Para os realistas, o cenário catastrofista é altamente improvável, representa um medo excessivo e não uma análise precisa (Eriksson e Giacomello, 2006, p. 226). A visão realista contesta a posição catastrofista e procura combater o exagero subjacente à hipersecutirização do desastre e da catástrofe digital. Adicionalmente, alertam para os benefícios económicos das políticas de cibersegurança (Lacy e Prince, 2018, pp. 106-107).

Thomas Rid é um dos principais autores desta posição, e como mencionado anteriormente, alerta para a problemática subjacente à ideia de ciberguerra, uma vez que é bastante improvável existir um conflito em que um instrumento ciber seja a principal arma. Todavia, isto não significa que o uso hostil do ciberespaço não constitui uma ameaça, mas as suas consequências não devem ser exageradas, uma vez que não resultam geralmente em mortes ou destruição física. Assim, o ciberespaço é visto como um desafio adicional que integra uma longa lista de problemas que as sociedades atuais enfrentam e as suas implicações são, sobretudo, de cariz económico (Lacy e Prince, 2018, pp. 106-107).

Por conseguinte, para os *digital realists*, "cyber is a twenty-first-century nuisance" (Lacy e Prince, 2018, p. 108), e um transtorno relativamente menor quando comparado aos benefícios providenciados pelas tecnologias. Neste sentido, não obstante o reconhecimento da ameaça existente, particularmente, aos dados das sociedades e à propriedade intelectual, os realistas alertam para que se evite a sobrevalorização destes desafios. Adicionalmente, embora exista a possibilidade de atores não estatais acumularem poder de novas formas, não é expectável a concretização de resultados significativos. Deste modo, os *digital realist* admitem a importância de desenvolver estratégias de cibersegurança ofensivas e defensivas, contudo, apresentam-se inquietos quanto ao perigo de qualificar as ciber-armas como *game changers*, que irão transformar o futuro da guerra e desencadear cenários destrutivos e assim justificar hipersecuritizações (Lacy e Prince, 2018, p. 108).

Os *techno-optimist*, ao contrário dos catastrofistas que vêm a evolução tecnológica como um desastre, acreditam que o progresso na condição humana é gerado pela democracia liberal e pelo aparecimento de novas tecnologias. Embora reconheçam as fragilidades da democracia liberal, acreditam que a crítica e a reflexão subjacentes a este modelo permitem e potenciam a aprendizagem, a conectividade positiva e a evolução tecnológica. Neste sentido, os desafios da atualidade são causados pelos sucessos tecnológicos de ontem e as soluções tecnológicas de hoje serão causadores dos problemas de amanhã, gerando assim uma expansão circular de problemas e soluções (Lacy e Prince, 2018, pp. 109-110).

Os otimistas admitem a ocorrência de eventos catastróficos, mas não acreditam nos piores cenários possíveis especulados pelos catastrofistas. Para os otimistas, a capa-

cidade para dar resposta a estas vulnerabilidades será progressivamente aperfeiçoada, permitindo ultrapassar os desafios colocados pelas novas tecnologias. Deste modo, o foco deve estar na investigação, no conhecimento e na educação, uma vez que, por um lado, a investigação fornecerá soluções técnicas para dar respostas às inseguranças da era digital; por outro lado, esta investigação deve ser sustentada pela formação de especialistas em cibersegurança que colaborem na proteção de indivíduos, empresas, Estados e Forças Amadas. Acresce ainda que, para os *techno-optimist*, o risco de ciber-catástrofes será erradicado através de soluções tecnológicas produzidas pela inteligência artificial e por processos aperfeiçoados para colmatar vulnerabilidades (Lacy e Prince, 2018, pp. 109-110).

A principal preocupação desta posição é para com a forma como os governos irão usar as novas tecnologias para vigilância e controlo das populações, sendo, por isso, o maior desafio prevenir a "...militarization or 'Balkanization' of the internet..." (Lacy e Prince, 2018, p. 110). Deste modo, os otimistas centram a sua atenção em esforços que previnam os governos de tornar o ciberespaço, e nomeadamente a internet, num espaço de controlo de populações. O desafio é contrariar a securitização da *everyday life*, isto é, a invocação de ameaças (internas ou externas) para justificar a introdução de novas medidas excecionais para regular a vida digital dos indivíduos (Lacy e Prince, 2018, p. 111).

No próximo ponto, atendendo ao modelo proposto por Mark Lacy e Daniel Prince, analisa-se a evolução discursiva do entendimento do ciberespaço enquanto matéria de segurança na União Europeia, procurando averiguar como este se traduz no desenvolvimento da Estratégia de Cibersegurança. Esta análise é relevante para verificar se há alguma tendência para a hipersecuritizar o ciberespaço a nível europeu que resulte em contramedidas excessivas contrárias às normas, valores e princípios da União Europeia.

## A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista ou Otimista?

### *Da proteção do Mercado Único a uma Estratégia de Cibersegurança*

A cibersegurança tem-se figurado como matéria prioritária nas agendas políticas dos Estados e das organizações internacionais, como é o caso da União Europeia (Cavelty, 2018b, p. 1; Christou, 2018, p. 2; Carrapiço e Barrinha, 2017, p. 1255). Neste cenário, o papel central que as tecnologias de informação e comunicação têm nas sociedades europeias justifica o aprofundamento da cibersegurança no seio da União (Christou, 2018, p. 2; Carrapiço e Barrinha, 2017, p. 1255).

Porém, à semelhança dos desenvolvimentos ocorridos no plano internacional em matéria de cibersegurança, na UE, as preocupações com o ciberespaço tiveram lugar no início dos anos 1990, mas não como matéria de segurança. Ilustradas, por

exemplo, no título de um dos documentos que introduziram este debate no seio da União: *White Paper on Growth, Competitiveness and Employment* (1994). Inicialmente, o discurso era orientado por uma lógica económica associada à edificação e progresso do Mercado Único. A segurança informática era essencial para o desenvolvimento das economias europeias e para a concretização do Mercado Único. Neste sentido, a princípio o ciberespaço não era visto como uma matéria de segurança, mas como um domínio que devia ser protegido por motivos económicos, comerciais e financeiros (Christou, 2018, pp. 5-6; Carrapiço e Barrinha, 2017, p. 1259).

O aparecimento do argumento securitário, em acréscimo à já existente lógica económica, deu-se sobretudo no final dos anos 1990. Esta inclusão foi influenciada por enquadramentos internacionais já existentes em matéria de cibercrime, designadamente pelos Estados Unidos da América, bem como por outras organizações internacionais e regionais como o G8 (Plano de Ação sobre Crime Informático, 1997) e o Conselho da Europa (Convenção sobre Cibercrime, 2001). Neste contexto, surge a e-Europe Initiative (1999) e a Communication on Network and Information Security: Proposal for a European Policy Approach (2001), que destacavam a importância da proteção das infraestruturas de informação para a UE. Adicionalmente, a Comunicação da Comissão Europeia sobre Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-Related Crime (2001) dedicou-se à identificação de medidas a adotar para combater o cibercrime, tanto internamente como internacionalmente, sem colocar em causa o respeito pelos direitos fundamentais dos indivíduos (Christou, 2018, p. 6; Carrapiço e Barrinha, 2017, p. 1259). Deste modo, é possível identificar, desde o início da mitigação dos desafios subjacentes ao ciberespaço no contexto europeu, a configuração de um discurso otimista por parte da União Europeia, uma vez que existe uma preocupação para não hipersecuritizar o ciberespaço e evitar o desenvolvimento de medidas que contrariem os princípios e valores fundamentais da União.

Contudo, apesar da crescente preocupação para com a proteção das infraestruturas de informação e comunicação e para com a necessidade de definir medidas para dar resposta ao cibercrime, a Estratégia Europeia de Segurança da UE de 2003 não fez, surpreendentemente, nenhuma referência ao ciberespaço. Adicionalmente, este racional securitário era sobretudo declaratório, uma vez que, até meados dos anos 2000, nenhum instrumento ou iniciativa juridicamente vinculativa foi consensualizada entre Estados-membros (Christou, 2018, p. 6; Carrapiço e Barrinha, 2017, p. 1259).

Em meados dos anos 2000, a cibersegurança começou a assumir contornos prioritários, próprios das matérias de segurança. A ameaça terrorista do início e meados dos anos 2000 contribuiu para esta mudança de paradigma; reconhecia-se, assim, que as tecnologias e sistemas de informação e comunicação se encontravam vulneráveis a ataques externos e particularmente a ataques de natureza terrorista. Foi

neste contexto que uma lógica de segurança explícita relativa ao ciberespaço se formulou na União Europeia (Christou, 2018, p. 7; Carrapiço e Barrinha, 2017, p. 1260). É também de destacar o papel dos ciberataques na Estónia, em 2007, no desenvolvimento da abordagem ao ciberespaço como matéria de segurança (Cavelty, 2018b, p. 8).

Segundo Carrapiço e Barrinha (2017, p. 1260), esta mudança teve duas implicações centrais em matéria de governação[8] na UE. Em primeiro lugar, a criação de instrumentos juridicamente vinculativos, como por exemplo o Council Framework Decision on Attacks against Information Systems (2005), dando-se assim um "step-change away from a soft law approach...towards...more regulatory interaction" (Christou, 2018, p. 7). Em segundo lugar, o reforço da necessidade de coerência entre várias políticas setoriais da UE, isto é, o caráter transnacional das ameaças atuais leva à integração de preocupações internas e externas de segurança que é um elemento necessário para a eficiência (Carrapiço e Barrinha, 2017, p. 1260).

Deste modo, a explícita perceção de ameaça do crime organizado e do terrorismo à concretização de uma sociedade da informação segura foram elementos chave que contribuíram para o desenvolvimento e aprofundamento da resposta da UE em matéria de cibersegurança (*Ibidem*).

Deste modo, é possível concluir que a evolução do entendimento do ciberespaço enquanto matéria de segurança no seio da União tem sido catastrofista, mas simultaneamente realista e otimista, como sugerido no modelo de Lacy e Prince (2018). É catastrofista, na medida em que identifica a vulnerabilidade da União a ataques externos no ciberespaço, sobretudo de natureza criminosa e terrorista. No entanto, a mitigação destes desafios não deve ser alarmante, nem deve negligenciar a proteção das normas, valores e princípios da UE, sendo por isso realista e otimista.

### *A Estratégia de Cibersegurança da UE (2013)*

Segundo Cavelty (2018b, p. 8), 2013 foi um ano decisivo em matéria de cibersegurança no quadro da União Europeia, uma vez que foi publicada a Estratégia de Cibersegurança (ECS) – Cybersecurity Strategy of the European Union, An Open, Safe and Secure Cyberspace –, resultante de um esforço conjunto entre a Comissária para os Assuntos Internos, Cecilia Malmström, a Alta Representante, Catherine Ashton e a Comissária para a Agenda Digital, Neelie Kroes. Paralelamente, foi proposta uma diretiva sobre a segurança das redes e sistemas de informação – NIS Directive –, adotada em 2016, com uma lógica regulatória que obriga ao reporte de incidentes e ataques no ciberespaço. Estas disposições sinalizam uma transição

8 Governação aqui diz respeito a tradução do conceito de *governance* usado no plano internacional.

para uma postura mais assertiva e regulativa da UE em matéria de cibersegurança, com a criação deste instrumento juridicamente vinculativo (Cavelty, 2018b, p. 8; Christou, 2018, p. 15; Carrapiço e Barrinha, 2017, p. 1260).

A União Europeia entende cibersegurança como:

> "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein" (Comissão Europeia e Alta Representante, 2013, p. 3).

O entendimento de cibersegurança da União Europeia é bastante vago, contudo é evidente a centralidade da necessidade de proteger as redes e as infraestruturas de informação, considerando a sua atual relevância na vida das sociedades.

À semelhança do que aconteceu nos primeiros anos do desenvolvimento da abordagem relativa ao ciberespaço por parte da União Europeia, também na Estratégia de Cibersegurança é possível identificar uma visão algo catastrofista, mas sobretudo otimista. Catastrofista, uma vez que o racional subjacente a esta estratégia assenta na perceção de vulnerabilidade resultante da dependência tecnológica das economias e das sociedades europeias, bem como no crescente número e intensidade dos ciber-ataques (Christou, 2018, p. 13). Otimista, na medida em que reconhece simultaneamente os benefícios do ciberespaço e a necessidade de não adotar medidas que contrariem os princípios que promove no quadro de outras políticas setoriais.

Neste sentido, a União reconhece, por um lado, a perceção de vulnerabilidade resultante da dependência tecnológica das sociedades atuais, sobretudo em termos económicos, e o aumento, a um ritmo alarmante, de incidentes, intencionais e acidentais, no ciberespaço, bem como do cibercrime contra o setor privado e indivíduos. No entanto, por outro lado, admite a existência de aspetos positivos e benefícios do ciberespaço, como espaço que tem contribuído para a inclusão política e social, derrubando barreiras entre países e comunidades; e como espaço que tem funcionado como uma plataforma e contexto de liberdade de expressão.

A posição otimista é confirmada nos princípios que guiam a sua estratégia, ao considerarem a necessidade de promover um ciberespaço seguro sem negligenciar as normas, os princípios e os valores que promove em outras políticas setoriais: (1) os valores centrais da UE também se aplicam no espaço digital; (2) proteção dos direitos fundamentais, liberdade de expressão e privacidade; (3) acesso a todos; (4) governação[9] democrática e envolvimento de atores múltiplos; (5) partilha de

9 Ver nota 8.

responsabilidade. Neste sentido, para a União Europeia, a promoção de um ciberespaço seguro e livre passa por uma proteção de incidentes, atividades maliciosas e uso hostil, que não comprometa os direitos fundamentais, a democracia e o Estado de Direito (Comissão Europeia e Alta Representante, 2013).

A ECS assenta em três pilares principais e evidencia a preocupação da União em abordar esta matéria de forma holística: (1) proteção das infraestruturas de informação crítica; (2) cibercrime; e (3) ciberdefesa. E envolve diversas áreas com mandatos distintos: mercado interno, justiça e assuntos internos, e política externa (Cavelty, 2018b, pp. 8-9; Christou, 2018, pp. 13-14; Carrapiço e Barrinha, 2017, pp. 1260-1261).

A proteção das infraestruturas de informação crítica diz respeito ao conjunto de medidas que procura proteger o funcionamento das instalações e serviços essenciais ao funcionamento de governos e sociedades – saúde, redes de abastecimento de água e energia, telecomunicações, entre outros. As medidas centram-se sobretudo na uniformização da gestão de risco e em mecanismos de reporte de incidentes. O ator institucional chave neste âmbito é a ENISA (European Network and Information Security Agency), criada em 2004, com um mandato inicial de aconselhamento aos Estados-membros e instituições da UE e atualmente com um mandato mais ativo. O segundo pilar da ECS centra-se no combate ao cibercrime, que diz respeito a um leque variado de atividades criminosas que têm como ferramenta principal de ataque, ou como alvo principal, computadores e sistemas informáticos. Neste pilar procura-se fazer com que os Estados-membros criem legislação para dar resposta a este tipo de ataques e que providenciem um entendimento comum de definições neste âmbito, para harmonizar a legislação em matéria de cibercrime no espaço europeu. Adicionalmente, procura-se cooperar em termos políticos e legais com países terceiros, sensibilizando, capacitando, investigando e reforçando a cooperação com o setor privado – os principais detentores não só das infraestruturas digitais, mas também do conhecimento. O ator central nestas matérias é o European Cybercrime Centre, criado dentro da Europol em 2013, que assegura uma resposta coordenada ao cibercrime; serve como plataforma de informação e providencia apoio aos Estados-membros em matéria de investigação. Ao contrário dos outros dois pilares, a ciberdefesa é o pilar menos desenvolvido, e diz respeito à proteção dos sistemas de comunicação e informação que estão na base da defesa nacional (Cavelty, 2018b, pp. 8-9; Christou, 2018, pp. 13-14; Carrapiço e Barrinha, 2017, pp. 1260-1261).

Em suma, o desenvolvimento da Estratégia de Cibersegurança no seio da União Europeia tem sido justificado, segundo Christou (2018, p. 16), pela acumulação de ameaças às redes e sistemas informáticos europeus, que deu lugar a uma crescente perceção de vulnerabilidade, traduzindo-se no desenvolvimento de políticas, institucionalização de órgãos e de procedimentos. Segundo Christou (2018, p. 3), a

securitização do ciberespaço no seio da União Europeia não se tem traduzido em medidas excecionais, mas sim em políticas de rotina, sobretudo a passagem de uma lógica voluntária para uma lógica obrigatória, como é o caso da NIS Directive. Deste modo, as medidas adotadas pela União Europeia têm refletido o seu *modus operandi* e não uma exceção. Adicionalmente, tem-se assistido a processos de de-securitização, como por exemplo com o Regulamento Geral de Proteção de Dados. Neste sentido, o discurso da UE em matéria de cibersegurança tem sido catastrofista no enquadramento dos desafios subjacentes ao ciberespaço, mas otimista na abordagem a estes.

**Considerações Finais**

O ciberespaço tem ganho crescente destaque, enquanto matéria de segurança, nas agendas políticas dos Estados e das organizações internacionais, como é o caso da União Europeia, levando ao desenvolvimento de políticas e estratégias de cibersegurança (Cavelty, 2018b, p. 1; Christou, 2018, p. 2; Carrapiço e Barrinha, 2017, p. 1255). Na União Europeia, o desenvolvimento da Estratégia de Cibersegurança tem sido marcado por uma posição sobre o ciberespaço enquanto matéria de segurança, simultaneamente, catastrofista e otimista.

No início dos anos 1990, à semelhança do que aconteceu internacionalmente, assistiu-se na União a uma preocupação para com o ciberespaço, mas não como matéria de segurança. Inicialmente, a atenção dirigida à proteção dos sistemas informáticos era orientada por uma lógica de proteção do espaço e desenvolvimento económico diretamente ligada à construção e concretização do Mercado Único (Christou, 2018, pp. 5-6; Carrapiço e Barrinha, 2017, p. 1259). Sendo, assim, uma posição mais próxima do pensamento dos realistas, que criticam o exagero em torno da ameaça do ciberespaço e identificam este problema como de cariz económico.

Porém, no final dos anos 1990, embora ainda numa dimensão meramente discursiva, a UE começou a introduzir o racional securitário em torno do ciberespaço, dedicando-se à identificação de medidas a adotar para combater o cibercrime, tanto internamente como internacionalmente, sem colocar em causa o respeito pelos direitos fundamentais dos indivíduos (Christou, 2018, p. 6; Carrapiço e Barrinha, 2017, p. 1259). Deste modo, é possível identificar desde o início da lógica securitária subjacente ao ciberespaço um discurso otimista da União Europeia, na medida que existe uma preocupação para não o hipersecuritizar e evitar desenvolver medidas que contrariem os princípios e valores fundamentais da União.

O início e os meados dos anos 2000 e a crescente preocupação para com a ameaça terrorista e o crime organizado leva a União a adotar uma postura mais assertiva em termos de cibersegurança, culminando, em 2013, com a publicação da Estraté-

gia de Cibersegurança. Neste contexto, a União oscila entre uma posição catastrofista e otimista relativamente à cibersegurança. Catastrofista, uma vez que o racional subjacente a esta Estratégia assenta na perceção de vulnerabilidade resultante da dependência tecnológica das economias e das sociedades europeias, bem como no crescente número e intensidade dos ciber-ataques. Otimista, na medida em que reconhece simultaneamente os benefícios do ciberespaço, bem como a necessidade de não adotar medidas contrárias aos princípios que promove em outras políticas setoriais. Acresce ainda, a identificação da necessidade da tónica na investigação e formação de especialistas.

A securitização do ciberespaço no seio da União Europeia tem, assim, sido feita mediante uma lógica catastrofista, na identificação do problema, mas sobretudo otimista na abordagem ao problema. Isto é, não se tem traduzido em medidas excecionais, mas em políticas de rotina, traduzidas na passagem de uma lógica voluntária para uma lógica obrigatória, através da NIS Directive. Deste modo, as medidas adotadas pela União Europeia têm refletido o seu *modus operandi* e não uma exceção. Adicionalmente, tem-se assistido a processos de de-securitização, como por exemplo com o Regulamento Geral de Proteção de Dados. Neste sentido, o discurso da UE em matéria de cibersegurança tem sido catastrofista no enquadramento dos desafios subjacentes ao ciberespaço, sobretudo na perceção de vulnerabilidade, mas otimista na abordagem a estes, sobretudo na preocupação em não contrariar direitos fundamentais, valores democráticos e o Estado de Direito (Christou, 2018, p. 3).

**Referências Bibliográficas**

Arquilla, J. e Ronfeldt, D., 1993. Cyberwar is Coming! *Comparative Strategy*, 12(2), pp. 141-165.

Carrapiço, H. e Barrinha, A., 2017. The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, 55(6), pp. 1254-1272.

Cavelty, M., 2018a. Revision of "Thomas Rid, Cyber War Will Not Take Place". *ERIS-European Review of International Studies*, 5(1), pp. 131-134.

Cavelty, M., 2018b. Europe´s cyber-power. *European Politics and Society*, 19(3), pp. 304-320.

Christou, G., 2018. The collective securitisation of cyberspace in the European Union. *West European Politics*, 42(2), pp. 278-301.

Comissão Europeia, 2001. *Communication on Creating a Safer Information Society by Improving the Security of Infrastructures and Combating Computer-related Crime*.

Comissão Europeia, 2001. *Communication on Network and Information Security: Proposal for A European Policy Approach.*

Comissão Europeia, 1999. *e-Europe initiative.*

Comissão Europeia, 1994. *White Paper on Growth, Competitiveness and Employment: The Challenges and Ways Forward Into the 21st Century.*

Comissão Europeia e Alta Representante, 2013. *Cybersecurity Strategy of the European Union, An Open, Safe and Secure Cyberspace.*

Conselho Europeu, 2005. *Framework decision on attacks against information systems.*

Craig, A. e Valeriano, B., 2018. Realism and Cyber Conflict: Security in the Digital Age. Em Orsi, D., Avgustin, J. R. e Nurnus, M., eds., *Realism in Practice: An Appraisal*. Bristol: E-International Relations Publishing.

Eriksson, J. e Giacomello, G., 2006. The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, 27(3), pp. 221-244.

Hansen, L. e Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, pp. 1155-1175.

Kello, L., 2013. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 38(2), pp. 7-40.

Lacy, M. e Prince, D., 2018. Securitization and the global politics of cybersecurity. *Global Discourse*, 8(1), pp. 100-115.

Liff, A., 2012. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3), pp. 401-428.

Maness, R. e Valeriano, B., 2015. The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*, 42(2), pp. 301-323.

Nye Jr., J., 2012. *O Futuro do Poder.* Lisboa: Círculo dos Leitores.

Nye Jr., J., 2010. *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs. Disponível em: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf [acedido em 20 de novembro de 2019].

Parlamento Europeu e Conselho Europeu, 2016. *Directive concerning measures for a high common level of security of network and information systems across the Union.*

Parlamento Europeu e Conselho Europeu, 2016. *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

Rid, T., 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), pp. 5-32.

Steiger, S., *et al.*, 2018. Conceptualising conflicts in cyberspace. *Journal of Cyber Policy*, 3(1), pp. 77-95.

Stone, J., 2013. Cyber War *Will* Take Place! *Journal of Strategic Studies*, 36(1), pp. 101-108.

Valeriano, B. e Maness, R. C., 2018. International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain. Em Brown, C. e Eckersley, R., eds.,

*The Oxford Handbook of International Political Theory*. Oxford: Oxford University Press, pp. 259-272.

Van der Meer, S., 2015. Enhancing International Cyber Security: A Key Role for Diplomacy. *Security and Human Rights*, 26(2), pp. 193-205.