EuroDefense Portugal

Tertúlia EDJ #02

Outubro 2021

A Segurança do Ciberespaço Europeu

Inês Barbosa Caseiro

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

O projeto Tertúlias EDJ recebeu o patrocínio do Ministério da Defesa Nacional.

A Segurança do Ciberespaço Europeu

1. Notas Introdutórias

Desde cedo, a União Europeia pretendeu ter um papel de liderança na promoção de um ciberespaço à escala mundial aberto, estável e seguro, assente no respeito pelo Estado de Direito, direitos humanos, liberdades fundamentais e valores democráticos. Atualmente, a cibersegurança é uma das principais prioridades da atuação da União e uma pedra angular para uma Europa digital e conectada. No dia 13 de outubro de 2021, a EuroDefense-Jovem promoveu uma Tertúlia sobre a temática da Segurança do Ciberespaço Europeu, que contou com a presença do Sr. Engenheiro Lino Santos, Diretor do Centro Nacional de Cibersegurança. De mencionar igualmente que o evento decorreu no mês Europeu da Cibersegurança, tendo sido integrado nas iniciativas da União Europeia.

2. A Segurança do Ciberespaço Europeu: definições e evolução das políticas de cibersegurança na União Europeia

As últimas décadas demonstraram que ameaças convencionais estão *outdated*. Novas ameaças e riscos para a segurança têm despertado atenção para a necessidade de uma abordagem holística.Embora seja verdade que conflitos convencionais podem ainda ter lugar, novas formas de agressão têm-se revelado tanto ou mais perigosas. As ameaças provenientes do ciberespaço são um dos exemplos.

Os ataques à Estónia e Geórgia em 2007 e 2008, Snowden em 2008 e Stuxnet em 2010 são apenas exemplos do que a atividade maliciosa no domínio cibernético pode originar, bem como das consequências que pode ter, sobretudo devido à elevada dependência da sociedade atual nas novas tecnologias. Em consequência, Estados de todo o mundo têm vindo a reconhecer a importância crescente de promover a segurança e defesa do domínio cibernético.

A União Europeia não é diferente: quer uma sociedade "*powered by digital solutions that are strongly rooted in (…) common values, and that enrich the lives of all of us: people must have the opportunity to develop personally, to choose freely and safely, to engage in society, regardless of their age, gender or professional background*"[1].

[1] EUROPEAN COMMISSION COM (2020) 67 final - Shaping Europe's digital future, p.1

Quer um ciberespaço aberto e acessível a todos, seguro para navegar e estável. Esta realidade só é possível através do investimento, cooperação e coordenação. Neste sentido a União tem, desde o início da década de 2000 e especialmente desde a década de 2010, criado agências, desenvolvido políticas e estratégias, com o objetivo de se destacar no panorama internacional.

Para melhor compreender o caso europeu no que toca à segurança do ciberespaço, é proveitoso fazer algumas considerações sobre o que muitos autores chamam de "quinta dimensão" ou "quinto domínio": o ciberespaço, a fim de perceber porque se trata de um tema tão complicado e porque existe alguma incerteza quando falamos deste espaço.

Em primeiro lugar, deve ser mencionado que o prefixo 'ciber' sugere uma relação entre tecnologia e seres humanos, mais especificamente, a utilização da tecnologia pelos seres humanos. A agitação em torno do ciberespaço começa precisamente com a sua própria definição, no sentido em que não existe uma totalmente aceite e cada autor tende a dar-lhe o seu cunho pessoal. Isto é ilustrado pelas dezenas, senão mesmo centenas, de significados que lhe têm vindo a ser atribuídos. Como Santos[2] salienta, não há acordo geral sobre o seu alcance e natureza dinâmica, o que torna muito difícil formular uma definição clara e precisa. De acordo, Strate[3] refere que "*because cyberspace is everywhere, and through widening usage, threatens to become everything, the term has become increasingly more vague and drained of meaning*."

As suas caraterísticas revelam um espaço particular e complexo. É artificial, não material. É utilizado por milhares de milhões de pessoas de forma diferente e para fins diferentes. É recente e, embora o seu território (virtual) não esteja muito bem delineado, "*involves worldwide connectivity irrespective of geopolitical borders*", como refere Schmitt[4]. É possível, por exemplo, o acesso remoto a computadores que se encontrem do outro lado do mundo. Assim, o ciberespaço reduz ou elimina as distâncias que podem ser encontradas, como nos diz Santos[5]. O ciberespaço oferece formas extremamente rápidas de comunicar, a uma velocidade inimaginável. O anonimato que a atividade cibernética permite é também digno de menção. Alguns sistemas escondem a identidade dos seus autores, o que cria um problema de atribuição e responsabilização, algo de elevada relevância no caso de ciberataques. Sharief[6] acrescenta que a falta de interação física permite que os indivíduos expressem apenas algumas partes da sua identidade, nenhuma de todo, ou que criem até identidades falsas.

O ex-Presidente da Comissão Europeia Jean-Claude Juncker[7] salientou, em 2017, que os ciberataques podem ser mais perigosos para a estabilidade das democracias e das economias do que armas e tanques. Isto porque hoje assistimos à informatização de uma grande parte das operações e processos que compõem as atividades individuais, empresariais e governamentais, como salienta Santos[8]. De acordo com dados da União Europeia[9], os cidadãos e empresas europeias dependem de serviços e tecnologias digitais, e embora acreditem que isto é algo positivo, têm também receio de eventualmente serem vítimas de crimes no ciberespaço. Por exemplo, 80% das empresas europeias sofreram pelo menos um incidente em 2016. A Internet e o ciberespaço estão cada vez mais presentes na nossa vida quotidiana, tanto a nível individual como societal.

Sliwinski[10] diz-nos que "*the beginning of the 21st century has seen the emergence of cybersecurity as a major issue of international security*", uma vez que se trata do "*policy-issue of the hour*", de acordo com Cavelty[11]. O nosso quotidiano, direitos fundamentais, as interações sociais e até a economia dependem de um bom funcionamento das tecnologias de informação e comunicação.

[2] SANTOS, Lino – Ciberespaço, p. 61.
[3] STRATE, Lance – The Varieties of Cyberspace: Problems in Definition and Delimitation, p.383.
[4] SCHMITT, Michael - Tallin Manual 2.0 on the International Law Applicable to Cyber Operations, p. 563.
[5] SANTOS, Lino – Ciberespaço, p. 63.
[6] SHARIEF, Kamran - What is Cyberspace? Definition, Features and More.
[7] Mencionado em BENDIEK, Annegret (et al.) – The EU's Revised Cybersecurity Strategy, p. 1.
[8] SANTOS, Lino – Contributos para uma melhor Governação da Cibersegurança em Portugal, p 225-226.
[9] Cybersecurity Factsheet.
[10] SLIWINSKY, Krzysztof F. – Moving Beyond the European Union's Weakness Cyber-Security, Agent, p. 468.
[11] CAVELTY, Myriam D. – A Resilient Europe for an Open, Safe and Secure Cyberspace, p. 3.

O facto de as sociedades estarem cada vez mais dependentes do ciberespaço em quase todos os aspetos não pode ser ignorado, bem como as ameaças e vulnerabilidades que daí resultam. Como é salientado na Estratégia da União Europeia ciberataques continua a aumentar, estes são mais sofisticados do que nunca, provém de uma vasta gama de fontes dentro e fora da União, e visam áreas de vulnerabilidade máxima.

A UE nunca deixou de reconhecer que, de facto, o domínio cibernético é muito importante, e a sua proteção é crucial. Há, neste sentido, uma grande necessidade de desenvolver estruturas que protejam o ciberespaço. Introduzimos assim o termo 'cibersegurança'.

Santos[13] salienta que definir cibersegurança pode ser mais ou tão complicado como definir segurança. O autor também menciona que, dado o elevado nível de interdependência entre cibersegurança e outros domínios, a cibersegurança pode ser vista como a segurança do ciberespaço, como é vulgarmente conhecida, ou a segurança de qualquer componente cibernética de qualquer sistema.

Como define a União Europeia a cibersegurança? A Estratégia de Segurança Cibernética de 2013 da União Europeia[14] define-a 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 independent networks and information infrastructure (...) strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*". A ENISA[15], Agência da União Europeia para a Cibersegurança, conceptualiza o termo como: "*the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment*". A cibersegurança é um conceito em constante alteração e tem evoluído através dos muitos incidentes que têm ocorrido no ciberespaço. Continuará certamente a evoluir.

É reconhecido que "a cibersegurança é parte integrante da segurança europeia"[16], a par da segurança em todos os outros domínios físicos. É necessário, portanto, criar condições para manter um "ciberespaço global, aberto, estável e seguro, onde todos possam viver em segurança as suas vidas."

A União Europeia começou a preocupar-se com as questões cibernéticas e a reconhecer a sua importância quando, em 2001, o Conselho da Europa propôs a Convenção sobre o Cibercrime, bem como uma estratégia de segurança da informação e das redes. Em 2004, foi criada a Agência Europeia para a Cibersegurança, como um centro de especialização em segurança de redes e informações para a UE, os seus estados-membros, o sector privado e os cidadãos da Europa.

Fovino (et al)[17] mencionam que o grande ímpeto teve lugar em 2016, quando a União Europeia aumentou significativamente a sua ação "*with the adoption of the NIS Directive which pushes industry and relevant players to reduce vulnerabilities and to strengthen resilience*". Estes incluem, por exemplo, o *Cybersecurity Act*, que define processos e normas de certificação de cibersegurança para produtos de TIC, a *Cyber Diplomacy Toolbox*, que fornece os meios para coordenar uma resposta dos Estados-Membros da UE a atividades cibernéticas maliciosas e o *Blueprint*, uma recomendação sobre a abordagem a incidentes graves e em larga escala.

Em 2013, a União Europeia apresentou e adotou a sua primeira Estratégia de Cibersegurança, com o objetivo de tornar o seu domínio cibernético o mais seguro do mundo. Esta delineava 5 prioridades:

- Alcançar resiliência cibernética,
- Redução drástica da cibercriminalidade;
- Desenvolver a políticas e as capacidades de defesa cibernética relacionadas com a Política Comum de Segurança e Defesa (PCSD);
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança;

[13] SANTOS, Lino – Cibersegurança, p. 63.
[14] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, p. 3.
[15] The European Union Agency for Cybersecurity.
[16] The EU's Cybersecurity Strategy for the Digital Decade, p.1.
[17] FOVINO, Igor N. (et al.) – Cybersecurity, Our Digital Anchor, p. 27.

- Estabelecer uma política internacional coerente em matéria de ciberespaço para a União Europeia e promover os valores fundamentais da EU.

No domínio global, a UE ambicionou preservar um ciberespaço aberto, livre e seguro, juntamente com parceiros e organizações internacionais relevantes, o sector privado e a sociedade civil, promovendo ao mesmo tempo os seus valores fundamentais e defendendo-os. A cooperação internacional, por exemplo com a ONU, OSCE, OTAN, UA ou ASEAN, tal como a cooperação entre os Estados Membros, é um fator fundamental. Como é referido, a responsabilidade de um ciberespaço mais seguro cabe a todos os atores da sociedade global da informação, desde os cidadãos aos governos.

Por mais importante que esta Estratégia e o pacote de reformas de 2017 tenham sido, muitos foram os pontos em que não foi concreta. Bendiek (et al.)[18] referem que deixaram em aberto "*a number of questions as to how its objective of an 'open, safe and secure cyberspace' will be credibly defended, both internally and externally*". Primeiramente, como Sliwinski[19] aponta, "*the European Union suffers from lack of collective vision on cybersecurity*". O autor refere que o problema passa por não existir uma visão coletiva, uma vez que muitos estados-membros da UE têm as suas próprias estratégias e conceptualização de cibersegurança. A questão financeira é igualmente importante, uma vez que o investimento é essencial. Como resultado da reticência dos Estados para focar-se nesta área, como Carrapico e Barrinha[20] referem, "*the allocated resources are often extremely low when compared with other security areas and other parts of the world*".

Em 2020, a Comissão Europeia e o Alto Representante para os Negócios Estrangeiros e a Política de Segurança elaboraram uma nova Estratégia: "The EU's Cybersecurity Strategy for the Digital Decade". Integra o plano de recuperação da Comissão, a Estratégia de Segurança 2020-2025, a Estratégia Global para a Política Externa e de Segurança da UE, e a Agenda Estratégica 2019-2024 do Conselho Europeu. O seu principal objetivo é regular como a União "*will shield its people, businesses and institutions from cyber threats, and how it will advance international cooperation and lead in securing a global and open internet*." Como a Estratégia de 2013 apontava, o tempo de agir é agora. Embora um pouco tarde, a União Europeia dá atualmente mais um passo na direção certa, mesmo que os resultados práticos ainda não sejam visíveis. Neste momento a prioridade da União Europeia mantém-se: aumentar a ciber-resiliência; combater a cibercriminalidade; fomentar a ciber-diplomacia; reforçar a ciber-defesa; impulsionar a investigação e inovação; e proteger infraestruturas críticas.

O documento salienta algumas questões em que a União deve refletir, propondo instrumentos para concretizar as suas prioridades (que serão explorados no ponto seguinte):

- Os setores dos transportes, energia e saúde, telecomunicações, finanças, segurança, os processos democráticos, espaço e defesa dependem muito de redes e sistemas de informação que estão cada vez mais interligados;
- O cenário de ameaças é agravado por tensões geopolíticas sobre a Internet, nomeadamente sobre o controlo destas tecnologias;
- Infraestruturas críticas são o alvo de muitos ciberataques, o que representa um enorme risco global;
- As preocupações com a segurança são um grande desincentivo à utilização de serviços online, o que atrasa a digitalização da sociedade;
- A investigação de quase todos os tipos de crime tem uma componente digital, pelo que a sua segurança deve ser assegurada;
- Os serviços digitais e o sector financeiro estão entre os alvos mais frequentes de ciberataques, juntamente com o sector público e a indústria, mas a *readiness* e a *awareness* das empresas e indivíduos permanecem baixas, e verifica-se uma grande escassez de

[18] BENDIEK, Annegret (et al.) – The EU's Revised Cybersecurity Strategy, p. 2.
[19] SLIWINSKY, Krzysztof F. – Moving Beyond the European Union's Weakness Cyber-Security Agent, p. 469.
[20] Mentioned in ANNAMÁRIA, Beláz – The Changing Role of the EU in Cybersecurity, p. 26.

competências em matéria de cibersegurança.

3. Contributos da Tertúlia com o Engenheiro Lino Santos, Diretor do Centro Nacional de Cibersegurança

A sessão iniciou com uma exposição por parte do Engenheiro Lino Santos, seguida de um período de questões do público.

O convidado começou por explorar a Estratégia da União para o Ciberespaço de 2020, expondo alguns dos dilemas identificados e instrumentos e alterações relevantes que introduz.

Salienta que o principal problema é talvez a falta de visão coletiva e *situational awareness* do que são as principais ameaças resultantes do ciberespaço. A Estratégia propõe três instrumentos: de regulamentação, de investimento e de política — para intervir em três domínios de ação da UE: 1) resiliência, soberania tecnológica e liderança; 2) criação de capacidade operacional para prevenir, dissuadir e responder; e 3) promoção de um ciberespaço mundial e aberto. As principais alterações, para além de a nível de financiamento e de soberania tecnológica, passam por:

- Regulamento relativo à segurança da informação nas instituições, organismos e agências da União, relativo a regras comuns em matéria de cibersegurança para as instituições, organismos e agências, tanto as áreas mais clássicas como 'de ponta'.
- Reformar as regras relativas à segurança das redes e da informação (SRI), centrais no mercado único da cibersegurança. A Comissão propõe rever a Diretiva SRI, com o intuito de incrementar o nível de ciberresiliência de todos os setores, quer públicos quer privados, que desempenham uma função importante para a economia e a sociedade. A proposta de diretiva revista é apresentada juntamente com uma revisão da legislação em matéria de resiliência das infraestruturas críticas, prevendo mínimos de segurança.
- A ideia de coordenação e cooperação é bem definida: é essencial a troca de informação entre os vários *stake-holders* no que toca a ameaças. A Comissão propõe desenvolver uma rede de centros de operações de segurança em toda a União, uma Rede de Centros Nacionais de Coordenação, bem como apoiar a melhoria dos centros existentes e o estabelecimento de novos. A finalidade gerar conhecimento coletivo e partilhar boas práticas. A figura da Autoridade Nacional de Cibersegurança ganha pertinência, tendo um *oversight* sobre tudo o que acontece e sendo muito relevante para a construção de uma visão coletiva a nível da União.
- Criação de um ciberescudo que assenta na ideia de reunir o maior número de informação possível sobre ciberameaças e produzir um quadro situacional. Assim, é salientada a importância dos centros de partilha e análise de informações, dos CSIRT, e dos centros de operações de segurança.
- Criar uma infraestrutura de comunicação ultrassegura, desenvolvendo uma infraestrutura de comunicação quântica (EUROQCI) para fins de troca de informação, como por exemplo conectar sistemas de justiça a nível europeu;
- Impulsionar a sua Estratégia Industrial e o papel de liderança nas tecnologias digitais e na cibersegurança em toda a cadeia de abastecimento digital. Igualmente, apoiar as sinergias entre as indústrias civis, da defesa e do espaço.
- Igualmente, a ciberliteracia deve ser desenvolvida, contribuindo para uma 'mão de obra da EU ciberqualificada'.
- Concluir o quadro europeu de gestão de crises de cibersegurança e definir o processo, as metas intermédias e o calendário para a criação de uma *Joint Cyber Unit*, para melhorar a preparação, sensibilização e resposta às ameaças.
- Rever o Quadro Estratégico para a Ciberdefesa e intermediar a conceção de uma «Visão e Estratégia Militar para o Ciberespaço como Domínio da Atividade Militar» para as missões e operações militares da PCSD;
- A nível internacional, a União deve definir e promover um conjunto de objetivos nos processos de normalização internacional, desenvolver a segurança e a estabilidade internacionais no ciberespaço, nomeadamente através de uma proposta relativa a um programa de ação para fomentar o

comportamento responsável dos Estados no ciberespaço (Programa de Ação) na ONU, formular orientações práticas sobre a aplicação dos direitos humanos e das liberdades fundamentais no ciberespaço, reforçar e promover a Convenção de Budapeste sobre a Cibercriminalidade e, por fim, alargar o ciberdiálogo com os países terceiros e as organizações regionais e internacionais, incluindo através de uma rede informal de ciberdiplomacia da UE.

Várias questões foram colocadas ao Engenheiro Lino Santos por parte do público:

A promoção de um espaço cibernético necessita da confiança entre gigantes digitais como o bloco americano e chinês? Não será este um grande desafio para a diplomacia europeia?

Sem dúvida. A questão passa por perceber como afirmar e exigir respeito pelos valores europeus perante gigantes informáticos norte-americanos e chineses não se consegue sem existir negociação e concertação. Isto é evidente na aplicação do RGPD - o Supremo Tribunal de Justiça Europeu que veio salientar que os prestadores de serviços norte-americanos não cumprem de forma suficiente o RGPD e respeito pelos valores europeus, o que leva a que alguns desses serviços não possam ser utilizados por cidadãos europeus. A primeira reunião de trabalho entre a Comissão Europeia e os Estados Unidos para abordar a livre circulação de bens e serviços e a transmissão de dados lugar esta semana [13 de outubro de 2021]. É necessário muito trabalho, diálogo e cooperação, inclusive com o bloco chinês.

Quais são os principais desafios da implementação da nova Estratégia de 2020 e de que forma é que a interoperabilidade será a palavra-chave, ultrapassando lacunas e obstáculos?

O foco não será a interoperabilidade, mas sim a harmonização, onde se encontra precisamente a grande dificuldade. Desde logo, existem diferentes graus de maturidade nos vários Estados-Membros. Por outro lado, relativamente a alguns dos temas mais fraturantes, temos perspetivas muito distintas e mais céticas, sobretudo no que toca à afirmação de autonomia estratégica da União. O desafio é encontrar o denominador comum para criar a harmonização necessária para a implementação das linhas de ação e medidas previstas na Estratégia.

Qual é *improvement* relativamente à Estratégia de Cibersegurança lançada em 2013 e reformas de 2017? É um *step-forward* ou não servirá para resolver as lacunas deixadas pela anterior estratégia?

Esta estratégia oficializa instrumentos introduzidos pela anterior Estratégia como 'experiências' que foram implementadas até 2020, e demonstra uma visão muito pessoal da nova Comissão Europeia da necessidade e pertinência de uma colaboração multidisciplinar. Corrige alguns aspetos que correram menos bem, existindo um grande esforço dos instrumentos desta nova estratégia para harmonizar a ação de todos os Estados-Membros.

4. Referências

ANNAMÁRIA, Beláz – The Changing Role of the EU in Cybersecurity. Safety and Security Sciences Review. Budapest: Biztonságtudományi Szemle. ISSN 2676-9042. 1:2 (2019). 17-30.

BENDIEK, Annegret (et al.) – The EU's Revised Cybersecurity Strategy. Siftung Wissenschaft und Politik Comments. Berlin: German Institute for International and Security Affairs. ISSN 1861-1761. 47 (2017). 1-7.

CAVELTY, Myriam D. – A Resilient Europe for an Open, Safe and Secure Cyberspace. UI Occasional Papers. Stockholm: The Swedish Institute of International Affairs. 2013.

COM (2020) 605 final, Eu Strategy For Union Security. European Comission, 2020.

COM (2020) 67 final - Shaping Europe's digital future. European Comission, 2020.

Cybersecurity Factsheet. European Comission, 2017.

FOVINO, Igor N. (et al) - Cybersecurity, our digital anchor. Luxembourg: Publications Office of the European Union, Luxembourg, 2020. ISBN 978-92 -76- 19957-1.

JOIN (2020) 18 Final. The EU's Cybersecurity Strategy for the Digital Decade. European Comission, 2020.

JOIN(2013) 1 Final, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Comission. 2013.

SANTOS, Lino – Ciberespaço. In: GOUVEIA, Jorge Bacelar e SANTOS, Sofia – Enciclopédia de Direito e Segurança. Coimbra: Almedina, 2015. ISBN 978-972-40-5994-5. 60-63.

SANTOS, Lino – Cibersegurança. In: GOUVEIA, Jorge Bacelar e SANTOS, Sofia – Enciclopédia de Direito e Segurança. Coimbra: Almedina, 2015. ISBN 978-972-40-5994-5. 63-67.

SANTOS, Lino – Contributos para uma melhor Governação da Cibersegurança em Portugal. In: GOUVEIA, Jorge Bacelar – Estudos de Direito e Segurança: Volume II. Coimbra: Almedina, 2017. ISBN 978-972-40-5836-8. p. 217-307.

SCHMITT, Michael - Tallin Manual 2.0 on the International Law Applicable to Cyber Operations. 2aEd. Cambridge: Cambridge University Press, 2017. ISBN 9781316822524.

SHARIEF, Kamran - What is Cyberspace? Definition, Features and More. Computer Tech Reviews. 2019.

SLIWINSKY, Krzysztof F. – Moving Beyond the European Union's Weakness Cyber-Security Agent. Contemporary Security Policy. Oxfordshire: Routledge. ISSN 17438764. 35:3 (2014). 468-486.

STRATE, Lance - The Varieties of Cyberspace: Problems in Definition and Delimitation. Western Journal of Communication. Oxfordshire: Taylor & Francis. ISSN 1057-0314. 63:3 (1999). 382-412.

Vídeo da Tertúlia EDJ #2 ddisponível em:
https://www.youtube.com/watch?v=yYKzBgZChro&t=604s

Faça o Scan do QR CODE para assistir ao vídeo

VEJA AGORA

EuroDefense Portugal

https://eurodefense.pt/

EuroDefense-Portugal

EuroDefense-Portugal

eurodefense@defesa.pt

EuroDefense Jovem-Portugal

@eurodefensept

EuroDefense-Portugal

eurodefense@defesa.pt

Centro de Estudos de Segurança e Defesa Europeia

EuroDefense-Portugal

eurodefense@defesa.pt

Palácio Bensaúde—Estrada da Luz, 151

1600-153 Lisboa | Portugal