AS TECNOLOGIAS DISRUPTIVAS NUM CONTEXTO DE AMEAÇAS HÍBRIDAS

Relatório de Seminário

7 de novembro de 2024

Índice

Sumário Executivo

O seminário "As Tecnologias Disruptivas num Contexto de Ameaças Híbridas", realizado no Instituto da Defesa Nacional em 7 de novembro de 2024, reuniu especialistas de áreas tecnológicas e de segurança para analisar como o avanço acelerado de novas tecnologias — da computação quântica à biotecnologia — está a transformar o ambiente estratégico e a ampliar a vulnerabilidade dos Estados a ameaças híbridas. O evento enquadrou-se nos trabalhos do Grupo de Estudos EuroDefense Portugal dedicado à transformação digital e inovação.
O seminário confirmou que a convergência entre tecnologias disruptivas e operações híbridas está a gerar um ambiente de segurança caracterizado por complexidade, ambiguidade e elevada interdependência entre setores civis e militares.
As principais conclusões destacam:

1. Aceleração tecnológica e novos riscos

Os oradores sublinharam que tecnologias como computação quântica, inteligência artificial (IA), *blockchain*, sistemas autónomos, biologia sintética e ciber-capacidades estão a multiplicar oportunidades — mas também vulnerabilidades — especialmente quando combinadas com operações de influência, espionagem, sabotagem ou desinformação.

2. Fragilidade da dissuasão clássica

A dificuldade em atribuir ataques no ciberespaço ou operações de manipulação informacional enfraquece os mecanismos tradicionais de dissuasão. A "zona cinzenta" que daqui resulta permite que atores estatais e não estatais explorem lacunas normativas e institucionais, atuando abaixo do limiar da guerra.

3. Setores críticos sob pressão

As apresentações evidenciaram riscos significativos em diferentes domínios:

- **Quantum**: potencial transformador em criptografia e comunicações seguras, mas também ameaça à encriptação atual.

- **Cyber**: crescente complexidade dos sistemas, baixa barreira de entrada e forte potencial de disrupção em infraestruturas críticas.
- **Espaço** & IA: aumento exponencial de satélites, privatização do espaço, e dependência de sistemas automatizados para vigilância, operação e tomada de decisão.
- **Biotecnologia**: rápido progresso na manipulação biológica, com ausência de supervisão em Portugal e riscos sérios para defesa biológica.

4. Impacto das ameaças híbridas

O segundo painel demonstrou que as ameaças híbridas atuam simultaneamente nos domínios político, social, económico, energético, informacional e militar, afetando a coesão social e a confiança nas instituições democráticas. Os casos analisados incluíram:

- dependência energética europeia;
- campanhas de desinformação;
- degradação dos media tradicionais;
- limitações legais ao acesso a metadados;
- vulnerabilidades das infraestruturas críticas.

5. Lições estratégicas

Emergiram várias linhas de ação para fortalecer a resiliência nacional e europeia:

- Necessidade de uma governação antecipatória, capaz de lidar com velocidade tecnológica e incerteza.
- Reforço da literacia digital e da comunicação estratégica para mitigar a manipulação informacional.
- Cooperação reforçada entre serviços de informações civis e militares.
- Aproximação entre políticas tecnológicas, industriais e de defesa, garantindo soberania em tecnologias críticas.
- Desenvolvimento de capacidades de negação e punição adaptadas ao contexto híbrido.
- Estabelecimento de uma autoridade nacional de defesa biológica.

6. Conclusão geral

O seminário concluiu que a combinação de tecnologias disruptivas com ameaças híbridas coloca os Estados perante um ambiente de segurança sem precedentes: altamente dinâmico, opaco e permeável. Mitigar estes riscos exige abordagens integradas, cooperação internacional, inovação contínua e um reforço da resiliência societal.

Como sublinhado repetidamente durante o evento, as tecnologias em si podem ser neutras — mas a sua instrumentalização nunca é.

1 – Introdução

Este relatório documenta o seminário "As Tecnologias Disruptivas num contexto de Ameaças Híbridas", organizado em parceria entre o EuroDefense-Portugal e o Instituto da Defesa Nacional (IDN), decorreu nas instalações do IDN, em Lisboa, no dia 7 de novembro de 2024. O evento surgiu na sequência dos trabalhos do Grupo de Estudos EuroDefense Portugal (GEEP) n.º 4, dedicado à transformação digital e inovação.

1.1 – Objetivo

O objetivo do seminário "As Tecnologias Disruptivas num contexto de Ameaças Híbridas" foi a abordagem das questões mais pertinentes deste tema por especialistas das várias áreas, para compreender a sua interação, assim como partilhar perspetivas que apontem para o desenvolvimento de estratégias de mitigação dos riscos associados.

1.2 – Questão Central

"Quais as principais oportunidades e riscos que as tecnologias disruptivas oferecem aos Estados, numa perspetiva de conflito com outros agentes, abaixo do limiar da guerra?"

1.3 – Conceito

A época atual é caracterizada por uma aceleração no desenvolvimento de um conjunto de tecnologias, apoiadas por processos automáticos, que terá consequências em todos os setores da sociedade. Em virtude disso, a economia, a saúde, o trabalho, a educação e a vida social serão completamente modificados. Da biotecnologia ao ciberespaço, do espaço à produção de energia, passando pela agricultura, todas as atividades poderão sofrer transformações radicais proporcionadas pelas tecnologias digitais. Avanços na inteligência artificial, tratamento de megadados, aprendizagem automática, cadeia de blocos

(*blockchain*), Internet das Coisas e computação quântica podem revolucionar segmentos industriais, melhorar a eficiência e criar novas oportunidade para a inovação. No entanto, estas tecnologias também podem abrir a porta a novas vulnerabilidades e desafios, em especial quando articuladas com outros atos de ação maliciosa.

A corrida pelo domínio de áreas-chave das novas tecnologias fez emergir uma competição geopolítica cujos contornos ainda estão em redefinição. Dado o alcance, penetrabilidade e interligação de países, empresas e outros atores de relevo na cena política internacional, as organizações internacionais concebidas numa outra era mostram-se inoperantes para resolver os problemas mais urgentes da humanidade, que vão desde o controlo de armamento, às questões das alterações climáticas ou à regulação do espaço exterior. Deste modo, potências emergentes e outros atores políticos sentem-se inclinados a explorar os novos domínios e a conceber novas modalidades de ação que tirem partido das vulnerabilidades dos sistemas políticos e sociais do Ocidente.

A dissuasão clássica, nuclear ou convencional, revela fragilidades acrescidas, dada a dificuldade em estabelecer mecanismos desencorajadores nos novos ambientes de conflito, assim como atribuir claramente as ações a um protagonista específico.

Uma série de questões como a energia, os fluxos migratórios, os ataques cibernéticos, as pandemias, o comércio internacional, a comunicação e as notícias falsas podem ser convenientemente instrumentalizadas e orquestradas para provocar efeitos ou alterar a decisão individual e coletiva de modo a ser favorável a um agente hostil, sem que o alvo dessa ação tenha plena consciência da natureza intrincada do ataque, até ser demasiado tarde. Vivemos no mundo das ações ditas cinzentas. O desenvolvimento de planos de contingência setoriais será fortemente condicionado pela possibilidade de confluência e cruzamento de acontecimentos em diferentes domínios que normalmente não exigiriam harmonização.

A convergência de tecnologias disruptivas e ameaças híbridas cria um emaranhado de interdependências e vulnerabilidades. Por um lado, a evolução tecnológica pode proporcionar melhorias nas capacidades defensivas, mas também pode ser utilizada para instrumentalização cruzada que amplifique as intenções de um potencial agressor, provocando surpresas estratégicas e eventualmente devastação sem precedentes.

A compreensão da natureza dual das tecnologias disruptivas é crucial para a formulação de respostas às ameaças híbridas, pelo que é urgente um entendimento abrangente e colaborativo em ordem ao reforço da resiliência de uma sociedade perante os riscos e ameaças atuais. As tecnologias até podem ser inocentes. A sua instrumentalização nunca é!

1.4 – Programa do Seminário

09:00
Sessão de Abertura
Isabel Ferreira Nunes, Diretora do Instituto da Defesa Nacional
09:15 – 10:00
Intervenção Principal Desafios Tecnológicos à Segurança no Séc. XXI,
Filipe Arnaut Moreira
Moderação: Embaixador Joaquim Ferreira Marques

10:00 – 11:15
Painel 1 – Tecnologias Disruptivas em Portugal Quantum
Manuel Nolasco Pinto, Universidade de Aveiro Cyber
Paulo Moniz, Digital Global Unit Security & IT Risk da EDP Espaço e Inteligência Artificial
João Montenegro, CEO Darkmatter Biotecnologia
Carlos Penha Gonçalves, Estado-Maior do Exército
Moderação: António Eugénio, IDN

11:15 – 11:30
Intervalo

11:30 – 12:45
Painel 2 – Dissuasão e Resiliência às Ameaças Híbridas Uma Nova Era de Dissuasão
António Eugénio, IDN Segurança económica e energética,
Filipe Santos Costa, IPRI-UNL Redes sociais e informação pública,
João Carlos Barradas, Jornalista Informações na Nova Era,
Helena Fazenda, Juíza Conselheira Moderação:
Agostinho Cunha, EuroDefense Portugal

12:45
Encerramento
Luís Valença Pinto, Presidente do EuroDefense Portugal

1.6 Notas Biográficas dos Intervenientes

Professora Isabel Ferreira Nunes

Diretora do Instituto da Defesa Nacional. Ingressou nos quadros do Ministério da Defesa nacional em 1989. No Instituto da Defesa Nacional e antes do atual cargo, desempenhou diversas funções, com destaque para a chefia da Equipa Multidisciplinar do Centro de Estudos e Investigação. Especializou-se nas áreas de política externa, segurança e defesa europeia, política externa dos pequenos Estados e teorias das Relações Internacionais. É doutorada em Ciência Política pela Universidade de Twente e possui um pós-doutoramento em Relações Internacionais pela Universidade de Groningen. É mestre em Estratégia pelo Instituto de Ciências Sociais e Políticas da Universidade Técnica de Lisboa, e licenciada em História pela Faculdade de Letras de Lisboa. É investigadora do Observatório de Relações Exteriores da Universidade Autónoma de Lisboa. Em 1994 recebeu o Prémio de Defesa Nacional pelo melhor trabalho de investigação (dissertação de mestrado), subordinada ao tema "Delineamento de uma Estratégia Diplomática Portuguesa – Portugal na 2ª Guerra Mundial". Foi auditora do Curso de Defesa Nacional do Instituto da Defesa Nacional entre 1995-1996.

Embaixador Joaquim Ferreira Marques

Natural de Vila Nova de Gaia, tem uma longa e diversificada carreira diplomática. Iniciada em 1976, incluiu missões nas embaixadas portuguesas em Dublin, Moscovo, Nova Deli, Buenos Aires e Atenas. Foi Cônsul-Geral pela na Cidade do Cabo, Assessor do Secretário de Estado dos Negócios Estrangeiros e da Cooperação, Assessor do Secretário de Estado das Comunidades Portuguesas, Representante Permanente Adjunto, Missão de Portugal na UNESCO, Diretor do Departamento dos Assuntos Económicos, Secretário Geral Adjunto do Ministério dos Negócios Estrangeiros, Representante Especial para a Tanzânia, Maurícias e Seychelles, Presidente do Júri do Concurso de Admissão de Adidos de

Embaixada, Representante Especial para Segurança Marítima e Presidente do G7-FoGG (Friends of the Gulf of Guinea). Foi promovido a embaixador "full rank" em abril de 2014.

Major-General José Filipe da Silva Arnaut Moreira

É licenciado em Ciências Sócio-Militares pela Academia Militar e Licenciado em Engenharia Electrotécnica e Computadores pelo Instituto Superior Técnico.
Na sua passagem pelo Ministério da Defesa foi Subdiretor-Geral de Política de Defesa Nacional e Chefe de Gabinete do Ministro da Defesa Nacional.
Foi *Intelligence Officer* no Quartel General da NATO em Madrid, Director de Comunicações e Sistemas de Informação do Exército e Professor de Geopolítica e Geoestratégia na Universidade Nova.
É autor do livro "O Domínio do Poder", publicado em outubro de 2023. É autor, com a jornalista Maria João Simões, do programa semanal "O Domínio da Guerra" na Rádio Observador.

Professor Doutor Armando Nolasco Pinto

Armando Nolasco Pinto é Professor Catedrático do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro e lidera o grupo de Comunicações Quânticas do Instituto de Telecomunicações em Aveiro.
É autor de trabalhos publicados e apresentados em mais de 200 revistas e conferências científicas internacionais. O trabalho por si realizado e pela equipa que coordena foi distinguido com mais de 23 prémios científicos. Detém quatro patentes internacionais e participou em 57 projetos de investigação, tendo sido coordenador global de 24. Atualmente, é coordenador de um projeto da União Europeia e de um projeto da NATO, ambos na área das tecnologias de comunicação quânticas.
É membro do Conselho Editorial das revistas "Scientific Reports", publicadas pela *Nature*, e das revistas "Optical and Quantum Electronics" e "Quantum Communication", publicadas pela Springer e pelo Institute of Engineering and Technology, respetivamente.
É o Presidente da Comissão Técnica de Normalização CTE JTC 22 – Tecnologias Quânticas, a funcionar no âmbito IEP - Instituto Eletrotécnico Português.

É membro Sénior do Institute of Electrical and Electronics Engineers e membro Sénior da Optica Society.

Engenheiro Paulo Moniz

Com uma experiência de cerca de 28 anos no mundo das tecnologias de informação, iniciou a carreira como administrador de sistemas na EDP Distribuição, tendo posteriormente transitado para a EDINFOR onde participou em diversos projetos internacionais de desenvolvimento de soluções como analista, programador e formador. Mais tarde assumiu funções de gestão de projeto tendo abraçado a área de Segurança em 2008, quando assumiu a liderança da Security Practice na Logica Iberia. Atualmente, desde 2010, é diretor pela área de Segurança da Informação e Risco IT no Grupo EDP, atuando como CISO (Chief Information Executive Officer) global no Grupo EDP.
Concluiu em 1995 a licenciatura em Engenharia Eletrotécnica e de Computadores pelo Instituto Superior Técnico, tendo mais tarde concluído uma Pós-Graduação em Sistemas de Informação (POSI) na mesma instituição. Possui também um MSC em Information Security pela Universidade de Carnegie Mellon e um Mestrado em Segurança Informática pela Faculdade de Ciências da Universidade de Lisboa. Posteriormente, concluiu com sucesso o Executive MBA da AESE. Atualmente é Doutorando em Ciências Políticas no ISCSP (Instituto Superior de Ciências Sociais e Políticas).

Dr João Montenegro

João Montenegro é um designer premiado com trabalho em vários setores incluindo: aeroespacial, automóvel, impressão 3D, educação e IA. O seu trabalho inclui:
• O fato espacial StarKnight, vencedor do concurso de design de fatos da Agência Espacial Europeia (ESA);
• A Cápsula Espacial Nazaré, para fabricação no espaço;
• A Base Lunar Rosas, apresentada no IAC 2021 em Dubai, que transforma uma Starship da SpaceX numa base lunar;
• Fundou a ubbu.io, agora utilizada por professores em mais de 30 países;
• A impressora 3D Beethefirst, da Beeverycreative, premiada pelo design inovador.

Como CEO da Darkmatter, desenvolve ferramentas de IA personalizadas para melhorar as capacidades das empresas com foco no Espaço.Desenvolveu várias ferramentas "open-source" para o setor espacial, disponíveis no seu github.
João Montenegro tem Licenciatura e Mestrado em Design de Produto e Estudos Espaciais. Estudou na Universidade de Aveiro, onde lecionou, Politécnico de Milão, e International Space University.

Coronel Carlos Penha Gonçalves

É licenciado em Medicina Veterinária pela Universidade de Lisboa (1984), Mestre em Biologia Molecular pela Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa (1992), Doutorado em Imunologia pela Umea University, Suécia (1999) e prestou provas de Agregação na Faculdade de Farmácia da Universidade de Lisboa (2007).
Ingressou no Quadro Permanente de Medicina Veterinária do Exército em 1986 no posto de Tenente e recebeu a promoção ao posto de Coronel em 2008. Entre outras funções foi Chefe do Laboratório de Bromatologia e Defesa Biológica, Chefe do Centro Militar de Medicina Veterinária e Sub-Diretor do Serviço de Saúde do Exército.
Entre 2000 e 2001 foi investigador convidado no Cambridge Institute of Medical Research, Universidade de Cambridge, Reino Unido. Dirigiu a Unidade de Genómica do Instituto Gulbenkian de Ciência de 2002 a 2018 e, desde 2003, é Investigador Principal do Instituto Gulbenkian de Ciência.
Foi Professor Associado convidado da Faculdade de Farmácia da Universidade de Lisboa (2010-2018) e leitor em diversos cursos de mestrado e doutoramento em Portugal. Orientou oito investigadores de pós-doutoramento e nove teses de doutoramento no Instituto Gulbenkian de Ciência e mais de duas dezenas de teses de mestrado.
Fez parte das delegações portuguesas nas reuniões anuais da Convenção das Armas Biológicas e publicou vários artigos de revisão e de divulgação na área da defesa biológica.
Os seus interesses de investigação científica e inovação técnica centram-se nas doenças inflamatórias e infeciosas e na defesa biológica e bio-segurança. A sua atividade de investigação recebeu apoio de múltiplas agências de financiamento nacionais e internacionais e foi reconhecida com o 1º prémio Pfizer para

investigação clínica em Portugal (2010), a bolsa Génese da Gilead (2019) e a bolsa de Inovação da Ferring Pharmaceuticals (2020).
Foi Presidente da Associação dos Antigos Alunos de Medicina Veterinária de Lisboa (2013-2016) e Presidente da Sociedade Portuguesa de Imunologia (2021-2024).
Publicou mais de cem artigos científicos em revistas internacionais, principalmente nas áreas de doenças infeciosas, imunológicas e metabólicas.

Coronel António Beja Eugénio

É atualmente assessor de estudos no Instituto da Defesa Nacional, onde coordena matérias relacionadas com as tecnologias emergentes na área da Defesa Nacional e a Economia de Defesa. Tem uma carreira de mais de quarenta anos como oficial da Força Aérea Portuguesa, que incluiu experiência de voo em exercícios e operações nacionais e NATO. Recentemente, desempenhou funções conjuntas como Chefe de Estado-Maior do Comando Operacional dos Açores. Tem experiência em cooperação no domínio da defesa, com missões em Angola e Moçambique. Desenvolveu, também, uma carreira académica, com destaque para a docência nos institutos superiores de ensino militar. É autor de diversos artigos e capítulos em livros sobre temas de estratégia, tecnologias, inovação e relações transatlânticas. Além da formação de índole militar, tem uma licenciatura em Gestão pela Universidade Lusíada, duas pós-graduações (em Sistemas e Tecnologias de Informação para as Organizações, pelo Instituto Superior de Economia e Gestão (ISEG), e em Estudos da Paz e da Guerra nas Novas Relações Internacionais, pela Universidade Autónoma de Lisboa), um mestrado em Gestão de Sistemas de Informação (ISEG), a componente letiva do doutoramento em Ciência Política e Relações Internacionais da Universidade Católica de Lisboa, e uma graduação em *Advanced Security Studies* pelo George C. Marshall European Center for Security Studies, na Alemanha.

Dr. Filipe Santos Costa

Quadro da AICEP - Agência para o Investimento e Comércio Externo de Portugal, a que presidiu de 5 de junho de 2023 a 7 de junho de 2024, promovendo Portugal como destino de investimento e as exportações nacionais. A AICEP é uma entidade pública empresarial tutelada pelos Ministérios da Economia, dos

Negócios Estrangeiros e das Finanças, responsável pelas Secções Económicas e Comerciais das Embaixadas e Consulados-Gerais de Portugal pelo mundo.
De 2018 a 2023 presidiu à AICEP Global Parques - Gestão de Áreas Empresariais e Serviços, S. A., gerindo o Albiz - Parque Empresarial de Sintra, o BlueBiz - Parque Empresarial da Península de Setúbal e a ZILS - Zona Industrial e Logística de Sines, onde lançou programas de atração de novos investimentos no âmbito da dupla transição energética e digital, Energia Sul e Sines Tech. Na AICEP Global Parques lançou ainda a ferramenta oficial de seleção de localizações para investimentos, Portugal Site Selection, e a Associação Portuguesa de Parques Empresariais.
Funcionário permanente da AICEP foi, nesse âmbito, Delegado da AICEP em São Francisco, Califórnia, EUA (2015-2018) e antes disso em Xangai, China (2011-2015).
Foi Encarregado da Estrutura de Missão para a Gestão dos Fundos Comunitários no Ministério da Administração Interna (2009-2011) gerindo o Eixo Prevenção, Gestão e Monotorização de Riscos do Programa Operacional Temático Valorização do Território (POVT/QREN 2007-2013) e o Programa-Quadro Solidariedade e Gestão de Fluxos Migratórios (SOLID 2007-2013) da União Europeia em Portugal.
Na AICEP, em Lisboa, foi Técnico da Direção Comercial PME Sul e dos Projetos PIN (de Potencial Interesse Nacional) e Custos de Contexto (2008-2009).
Foi Chefe de Gabinete do Ministro da Justiça (2005-2008).
Foi coordenador das organizações não-europeias nas relações externas da ANACOM, (2000-2005) sendo plenipotenciário à União Internacional de Telecomunicações (UIT, ONU em Genebra) e representante do acionista Estado Português na Inmarsat (Londres), na Eutelsat (Paris) e na Intelsat-ITSO (Washington, D. C.).
Desempenhou várias outras funções públicas, como de Adjunto do Ministro de Estado e do Equipamento Social e Chefe do Gabinete do Secretário de Estado da Cultura.
No setor privado trabalhou em jornalismo e consultoria.
Participou em missões de paz e democracia (sistemas políticos e eleitorais), pela ONU e pela OSCE, a países como Turquia, Croácia, Guiné-Bissau, Marrocos ou Iraque. Fez o "*Programme de visite des personnalité d'avenir*", do Ministério dos Negócios Estrangeiros francês em 2003, e o "*International Visitor Leadership Program*", do Departamento de Estado dos EUA em 2005.

É vice-presidente do Conselho Português do Movimento Europeu e vogal do conselho fiscal da Comissão Portuguesa do Atlântico. É conferencista convidado do Instituto de Defesa Nacional (IDN) em "Energia". É investigador no Instituto Português de Relações Internacionais (IPRI-NOVA), doutorando em "Estudos de Segurança e Estratégia" na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa e mestre em "Desenvolvimento e Cooperação Internacional" pelo ISEG da Universidade de Lisboa.
É fluente em inglês, espanhol e francês; com conhecimentos de italiano, chinês e alemão.

Dr. José Carlos Barradas

Licenciado em História, com atividade profissional de jornalista desde 1982. Desempenhou diversas funções de repórter, coordenador, editor e comentador em empresas de rádio, televisão, jornais, revistas e na Agência Lusa. É colaborador da revista Sábado.

Juíza Conselheira Helena Fazenda

Magistrada do Ministério Público durante 40 anos, com intervenção nas áreas criminais (criminalidade grave, violenta, organizada, transnacional). Também em direito civil, de menores e família. Desempenhou funções na área da formação, inicial e contínua, de magistrados do Ministério Público e judiciais. Tem experiência no âmbito da relação institucional direta, com Forças e Serviços de Segurança, no quadro do processo penal, como dirigente e como entidade coordenadora e de controlo na segurança interna. Também tem experiência de relação e interação institucional com as Forças Armadas. No contexto da União europeia, destaque para o desempenho na luta contra a fraude e a corrupção atentatórias dos interesses financeiros da UE. Experiência de fiscalização de órgãos da União Europeia. Experiência em cooperação internacional. Após concurso público, em 2020 foi graduada como Juíza Conselheira, tendo desempenhado funções no Supremo Tribunal de Justiça - secção criminal. Atualmente encontra-se na situação de jubilada.

Coronel Phd Agostinho Paiva da Cunha

Coronel do Exército Português na reserva, especializado em política de defesa e segurança, planeamento estratégico e gestão, com uma vasta experiência na UE e na NATO. O seu percurso inclui o trabalho em organizações multinacionais militares e civis, como os quarteis-generais da KFOR e na Bósnia e Herzegovina, para além de ter sido conselheiro docente no Colégio de Defesa da NATO em Roma e membro do Conselho Académico Executivo do Colégio Europeu de Segurança e Defesa em Bruxelas. É doutorado em Ciência Política e Governo pela Universidade La Sapienza de Roma.

2 – Sumários das Intervenções e Debate

2.1 – Sumário Painel 1 – "Tecnologias Disruptivas em Portugal"

Neste painel foram discutidas algumas das potencialidades das Tecnologias Disruptivas em Portugal.
Na primeira intervenção, o Prof. Armando Pinto falou sobre Quantum, representando o grupo da Universidade de Aveiro do Instituto de Telecomunicações, onde trabalha com tecnologias quânticas baseadas na "não clonagem", "sobreposição" e "entrelaçamento", explorando luz com poucas partículas. Referiu o trabalho a desenvolver em geradores de números aleatórios e sistemas de distribuição de chaves quânticas para segurança e defesa. Elaborou sobre a sua participação em projetos europeus e da NATO, com redes quânticas e aplicações em cenários militares e genómica, focando-se na privacidade e cooperação internacional.
O Eng Paulo Moniz centrou a sua intervenção na questão Ciber. Realçou que a nossa sociedade é profundamente dependente da tecnologia, enfrentando riscos associados à sua crescente complexidade. No ciberespaço, a projeção de poder é facilitada pela baixa barreira de entrada, anonimato e plasticidade geográfica, mas também comporta ameaças como o crime financeiro, terrorismo e guerra híbrida. A solução passa por regulação equilibrada, cooperação, educação em ciber-riscos e o uso responsável da inteligência artificial para lidar com a complexidade e aumentar a resiliência. O futuro depende da nossa adaptação e inovação.

O Dr. João Montenegro falou sobre Inteligência Artificial. A intervenção abordou o papel da inteligência artificial (IA) na resolução de problemas complexos, especialmente no setor espacial. Enfatizou a aplicação de IA para melhorar o design, operação e tomada de decisões em sistemas avançados, sem substituir o trabalho humano, mas complementando-o. Destacou tendências como o aumento de satélites em órbita, a redução dos custos de lançamento e a criação de data centers espaciais. Salientou a colaboração entre IA e humanos como essencial para enfrentar desafios e explorar novas oportunidades neste mercado emergente.
Para finalizar, o Coronel Carlos Penha Gonçalves falou de Biotecnologia. A biotecnologia está a moldar o século XXI, com avanços como o design de organismos artificiais e a criação de proteínas sintéticas através de inteligência artificial, permitindo aplicações revolucionárias e riscos significativos. O mercado global cresce rapidamente, com a China a liderar em biologia sintética. Portugal carece de infraestruturas e de uma autoridade nacional para a defesa biológica, sendo vulnerável em situações de crise. A falta de supervisão adequada contrasta com a urgência em abordar as implicações de tais tecnologias.

2.2 – Sumário Painel 2 – "Dissuasão e Resilência às Ameaças Híbridas"

Nesta Painel ada orador apresentou uma perspetiva própria sobre as ameaças híbridas, abordando temas que foram desde a segurança económica e energética até a influência das redes sociais na informação pública.
O Coronel Beja Eugénio iniciou a sua intervenção destacando a complexidade das ameaças híbridas na era contemporânea, traçando uma analogia com a Guerra Fria, onde a dissuasão nuclear e clássica desempenhou um papel crucial para evitar confrontos diretos entre superpotências. Refletiu sobre a transição para o novo século, onde a dissuasão se tornou um exercício especulativo, especialmente no contexto de guerras irregulares e terrorismo. Identificou também a postura revisionista da Rússia nas últimas duas décadas como um fracasso da dissuasão clássica, mencionando ainda que a emergência de novos atores, como a China, Coreia do Norte e Irão, aumentou a instabilidade no sistema internacional. Defendeu que as ameaças híbridas, embora não sejam uma novidade, são hoje exacerbadas pelo uso de tecnologias emergentes, introduzindo desafios inéditos. Visando proporcionar uma melhor compreensão sobre este desafio, utilizou como exemplo o modelo do Centro Europeu de

Excelência para Combate às Ameaças Híbridas (*Hybrid COE*) organizado em quatro pilares: atores e os seus objetivos, instrumentos utilizados, domínios de atuação, e fases das operações. Explicou que o propósito central destas ameaças é manipular a capacidade de decisão dos Estados-alvo, sendo a dissuasão um instrumento psicológico que procura convencer o agressor de que os custos das suas ações superam os benefícios. Já a fase de preparação é, na sua conceção, a mais relevante em termos de dissuasão, pois permite a deteção antecipada da interferência e influência hostil. Abordou também a chamada "zona cinzenta", onde se cruzam comportamentos aceitáveis e inaceitáveis, dificultando a deteção precoce da interferência hostil. Sublinhou que estas ameaças afetam os fundamentos da dissuasão: a comunicação, a capacidade e a credibilidade. A dissuasão pode ser alcançada tanto pela negação – através da proteção de infraestruturas críticas — como pela punição, de forma a dissuadir o agressor. Cada Estado deve, assim, definir os seus limiares de reação com base numa análise rigorosa de riscos e vulnerabilidades. O orador apresentou, ainda, as propostas de dissuasão dos Estados Unidos, com enfoque na "dissuasão integrada e *campaigning*", e dos países nórdicos, que priorizam a segurança societal e a resiliência nacional. Advertiu sobre os perigos inerentes ao uso da inteligência artificial, exemplificando com o ataque do Hamas a Israel e a resposta do sistema israelita *Lavender.* António Eugénio finalizou a sua intervenção ressaltando a importância de uma abordagem integrada e colaborativa para enfrentar as ameaças híbridas, com vista a aprofundar o estudo da dissuasão e a compreensão dos seus mecanismos.

Na intervenção seguinte, o jornalista João Carlos Barradas contribuiu para a discussão, explanando o papel e a influência das redes sociais sobre a informação pública e analisando os riscos que as tecnologias digitais representam para os regimes democráticos.

Para tal efeito, começou por definir as redes sociais como plataformas digitais de acesso livre ou restrito para publicação e partilha de conteúdos e informação pública como qualquer mensagem de acesso livre. Com vista a explorar o papel das redes sociais em conflitos, Barradas argumentou ser crucial classificar o teor do conteúdo divulgado nas redes, identificar os emissores e compreender os seus objetivos e estratégias de financiamento. Posteriormente, o jornalista recorreu à definição de guerra de Carl von Clausewitz – "ato de violência destinado a forçar o adversário a submeter-se à nossa vontade" – para ilustrar a

vertente de mobilização como um dos domínios da luta, onde as redes sociais podem ser vistas como uma "antecâmara ideológica da guerra".
Apontou igualmente a propagação de desinformação e a difusão de opiniões prejudiciais como sendo parte integrante das campanhas de propaganda híbrida, servindo-se da ideia de Walter Lippmann sobre estereótipos como base do conhecimento indireto para discutir o "condicionamento da opinião pública".A concluir João Carlos Barradas apresentou o exemplo da "*Rumor Clinic*", criada pelo *Boston Herald* durante a Segunda Guerra Mundial, como uma iniciativa pioneira para combater a disseminação de boatos. Referiu, adicionalmente, o estudo seminal de Gordon Allport e Leo Postman, que definiu o boato como uma "proposição de crença disseminada na ausência de provas substanciais", identificando três fases distintas na sua propagação: nivelação, onde a mensagem é simplificada; acentuação, em que detalhes específicos são amplificados; e assimilação, momento em que o boato é alterado para se ajustar às crenças e preconceitos dos indivíduos. Em complemento, Barradas justificou que as redes sociais devem ser vistas como parte integrante dos sistemas mediáticos e não apenas como disruptivas. Apresentou evidências empíricas que demonstram que, nos Estados Unidos, o consumo de notícias televisivas ainda supera o *online* e que a exposição a notícias falsas é limitada, ocorrendo maioritariamente entre grupos ideologicamente motivados. Salientou o crescimento da desconfiança nos *media* tradicionais, por contraponto ao aumento da credibilidade das redes sociais, embora o consumo destas seja inferior ao dos *media* convencionais. Concluiu aferindo que, em democracias, os *media* tradicionais ainda ditam os critérios de publicação e possuem maior impacto que outras formas de difusão. A principal ameaça, segundo o orador, equivale à degradação da qualidade e à redução da influência desses meios.
O Dr. Filipe Santos Costa dedicou a sua abordagem à segurança económica e energética no contexto das ameaças híbridas, iniciando a sua apresentação com uma referência ao ataque a Pearl Harbor e dando ênfase à importância dos recursos energéticos nas guerras. Discutiu a dependência europeia do gás russo e contrastou com a situação de Portugal, que importa gás natural liquefeito (GNL) através de terminais, beneficiando de 48,5% da capacidade de receção e gasificação da Península Ibérica. O orador citou o exemplo do Japão, que, de modo igual, não depende de gasodutos russos e investe em terminais de GNL e tecnologia de hidrogénio liquefeito. Santos Costa referiu ainda que a Guerra na Ucrânia impulsionou a evolução tecnológica na produção de energia na Europa,

uma vez que a União Europeia implementou medidas legislativas como o *Fit for 55*, o *RepowerEU* e o Quadro Temporário de Transição e Crise 2023, que ambicionam o incentivo da criação de terminais de GNL, a aposta no nuclear e o desenvolvimento de infraestruturas de hidrogénio. Em complemento, alertou para o aumento exponencial do consumo de eletricidade, impulsionado pela eletrificação dos transportes e construção de *data centers*, estipulando que o consumo em Portugal poderá duplicar ou triplicar até 2031. Asseverou que a dependência do mundo ocidental em relação ao exterior é menor do que se pensa. Portugal, como membro da UE, tem uma taxa de abertura da economia de 25%, a mesma dos EUA. Indicou que Portugal tem alcançado sucesso na transição energética, reduzindo a dependência de energia importada e diversificando as suas fontes, sendo que, em 2023, Portugal importou menos 6 mil milhões de euros em petróleo e gás do que no ano anterior, o que contribuiu para um *superávit* comercial de 3,3 mil milhões de euros. O orador deu especial destaque ao afastamento tecnológico da Europa face à Rússia, com os Estados Unidos e a União Europeia a investirem na produção de semicondutores de modo a diminuírem a dependência de Taiwan. O *European Chips Act 2023*, por exemplo, prevê um investimento de 43 mil milhões de euros para esta finalidade. Em Portugal, prevê-se um investimento de 1.000 milhões de euros em projetos de refinação de lítio, produção de baterias de lítio para veículos elétricos e uma nova fábrica de cobre e níquel para baterias. Por fim, Santos Costa referiu a importância da eletricidade verde para a produção de hidrogénio verde e as necessidades energéticas da refinaria de Sines, que poderiam representar até 12% do consumo elétrico nacional.

A Juíza Conselheira Maria Helena Fazenda iniciou a sua intervenção contextualizando as ameaças híbridas, definindo-as como ataques complexos que combinam diferentes táticas para atingir objetivos específicos. Sublinhou que este tipo de ameaça requer uma abordagem integrada e abrangente nas políticas de segurança e defesa, abarcando tanto esferas civis quanto militares. Defendeu a necessidade de transparência, literacia mediática e comunicação clara como meios cruciais para combater a desinformação. Reforçou, ainda, a importância da monitorização constante, da cooperação internacional e da robustez das infraestruturas críticas. A participação ativa da sociedade civil e a implementação de políticas eficazes de contenção também foram apontadas como fundamentais. Maria Helena Fazenda citou o Relatório de Avaliação da Ameaça do Sistema de Informações da República Portuguesa de 2023, que

identifica a propaganda e as operações de manipulação informacional como ameaças híbridas capazes de minar a coesão social e a capacidade decisória das instituições. Observou que a disseminação de desinformação, muitas vezes facilitada por inteligência artificial, continua a proliferar no espaço euro-atlântico. Sublinhou o papel vital dos serviços de informações — no sentido anglo-saxónico de *intelligence* — na mitigação de ameaças híbridas, focando-se na sua função de reduzir a incerteza estratégica para os decisores em segurança, defesa nacional e política externa. Especificou, nesse momento, oito etapas críticas na produção de informações: recolha, análise, elaboração de relatórios, disseminação, monitorização, capacitação, integração de dados e proteção de informações sensíveis. Enfatizou, de modo igual, o papel transformador dos serviços de informações na conversão de dados em conhecimento utilizável para a tomada de decisões estratégicas, ressaltando a necessidade de reforçar a cooperação entre os serviços civis e militares. Questionou a adequação da infraestrutura atual e a preparação dos serviços para enfrentar os desafios tecnológicos. Levantou a questão do acesso a fontes classificadas, defendendo um alargamento controlado, sujeito a escrutínio democrático e judicial, como forma de melhorar a avaliação de ameaças. Nesse plano, criticou a fragmentação das regulamentações vigentes. Argumentou, seguidamente, que os metadados são essenciais para a antecipação e análise precisa de ameaças, sem que isso comprometa os direitos e liberdades fundamentais. Referiu que as restrições impostas pelo Tribunal Constitucional sobre o acesso aos metadados enfraquecem a segurança coletiva e geram insegurança jurídica, ao reduzir o período de armazenamento de dados pelas autoridades. Finalmente, ponderou se a integração do Centro Nacional de Cibersegurança na estrutura do Sistema de Segurança Interna, sob a coordenação do Secretário-Geral, poderia otimizar a recolha e a produção de informações, contribuindo para uma resposta mais ágil e coordenada perante ameaças complexas.

Após as intervenções dos oradores convidados, o moderador, Coronel Agostinho Cunha retomou a palavra para apresentar algumas considerações finais sobre as ameaças híbridas, sublinhando que, embora situadas abaixo do limiar de conflito armado, estas ameaças têm a capacidade de evoluir para guerras híbridas, com implicações significativas para as estratégias de defesa. Caracterizou as guerras híbridas como uma forma de conflito multifacetada, que integra guerra convencional, irregular, de informação e cibernética, com ataques

que vão desde o uso de dispositivos explosivos improvisados até armas de destruição em massa, como as nucleares, biológicas e químicas. Essa nova dinâmica exige que as Forças Armadas desenvolvam estratégias inovadoras e flexíveis, capazes de lidar com adversários que utilizam todos os recursos ao seu dispor.

Agostinho Cunha finalizou a sessão abrindo espaço para uma questão do público. Essa questão foi dirigida à Juíza Conselheira Maria Helena Fazenda, abordando o controverso tema do acesso a metadados pelos serviços de informações. A questão girou em torno da necessidade de equilibrar a segurança nacional com os direitos individuais, num contexto em que a coleta de dados pode ser crucial para a análise e prevenção de ameaças. Em resposta, a Juíza Conselheira sublinhou que, na sua visão, os serviços de informação devem ter acesso a metadados, tal como estava previsto antes da última decisão do Tribunal Constitucional. Destacou que, com o crescimento das ameaças híbridas, a capacidade de monitorizar dados de localização é fundamental para avaliar o grau de risco e assegurar a comunicação entre as autoridades competentes e os decisores políticos. Para a oradora, a restrição ao acesso a esses dados, que não revelam o conteúdo das comunicações, mas apenas a localização de um indivíduo, é excessiva e prejudica a segurança nacional.

Além disso, enfatizou as consequências da decisão do Tribunal Constitucional, que impactou negativamente as investigações criminais, provocando a anulação de decisões judiciais e criando um clima de insegurança jurídica. A situação, segundo Helena Fazenda, compromete a eficácia das instituições de segurança no combate às ameaças, dificultando a tomada de decisões adequadas num cenário de crescente complexidade.

3 – Transcrições do Seminário "As Tecnologias Disruptivas num Contexto de Ameaças Híbridas"[1]

Assistente do Seminário

[1] Link para a gravação online em: https://youtu.be/PP71fAed-2U?si=GNpzByJaQT3BhXXB

Bom dia, vai ter início o seminário "As Tecnologias Disruptivas num Contexto de Ameaças Híbridas". Uma iniciativa conjunta do Instituto de Defesa Nacional e do Centro de Estudos EuroDefense-Portugal, estando integrado nos trabalhos do Grupo de Estudos EuroDefense-Portugal n.º 4, dedicado à transformação digital e inovação. Vai usar da palavra a diretora do Instituto de Defesa Nacional, Professora Doutora Isabel Ferreira Nunes.

3. 1 – Abertura – Prof. Doutora Isabel Ferreira Nunes

Muito bom dia, Excelentíssimo Senhor General Luís Valença Pinto, Presidente do EuroDefense-Portugal, entidades civis e militares presentes neste auditório, caros oradores e moderadores, minhas senhoras e meus senhores.
Queria dar-vos naturalmente as boas-vindas a este seminário sobre tecnologias disruptivas num contexto de ameaças híbridas e que resulta de uma parceria entre o Instituto de Defesa Nacional e o EuroDefense-Portugal. Agradeço também ao Senhor General esta iniciativa e a abordagem que fez ao Instituto no sentido de promovermos conjuntamente esta atividade.
Aos nossos oradores e moderadores queria agradecer muito a sua disponibilidade para estarem presentes connosco neste seminário e a todos os que nele participam quero desejar uma excelente troca de perspetivas e um profícuo debate.
Muito obrigada.
A relação entre a emergência de novas tecnologias e o seu emprego em ambiente híbrido não é um tema novo na agenda de segurança. Contudo, dois desenvolvimentos permitiram uma expressão mais ampla desta interação. Por um lado, a intensificação da competição geopolítica entre potências tradicionais e potências emergentes gerou novas expressões de poder e de influência, nas quais a inovação tecnológica confere hoje a melhor vantagem competitiva a competidores internacionais. Por outro lado, a questão da revolução digital, que acelerou o processamento da informação e uma maior conectividade entre Estados e sociedades, tornando-os simultaneamente mais vulneráveis aos efeitos desta nova interdependência.
No contexto europeu, o desenvolvimento tecnológico, associado aos desafios híbridos, tem tido consequências sobre a forma como é percecionado coletivamente pela União Europeia, mas também pelos Estados-membros, com repercussão na arquitetura institucional da União Europeia no seu tecido

regulativo e no fomento da inovação tecnológica.
A afirmação de uma maior autonomia estratégica da União Europeia e a sua soberania tecnológica implicarão a salvaguarda da posição da Europa e dos Estados-membros no contexto das tecnologias críticas emergentes e disruptivas. A institucionalização de novas plataformas de recolha e análise de dados, iniciativas legislativas e a adoção de estratégias como a cibersegurança, uma estratégia industrial para a Europa, uma estratégia para o espaço, de segurança marítima e de energia, até à lei das matérias-primas críticas, bem como a implementação de programas como o de proteção de infraestruturas críticas que, inclui hoje, as redes 5G, os sistemas de dados do espaço Schengen e os sistemas eleitorais e a operacionalização de planos de ação como aprovado para as sinergias entre indústrias civis, defesa e espaço são essenciais à harmonização regulativa e à mitigação de posições hostis às políticas e às iniciativas instituídas pela União Europeia.
A Comissão Europeia tem recorrido a roteiros tecnológicos no apoio ao planeamento, financiamento e desenvolvimento de sinergias civis-militares que associam a segurança a defesa e o espaço ao desenvolvimento de tecnologias críticas no domínio da segurança e da defesa. Em 2023, a União Europeia lançou a Iniciativa Diálogo Digital, com o propósito de acompanhar a posição da União Europeia sobre inovação e governação no domínio das tecnologias emergentes com efeito disruptivo, como os sistemas de inteligência artificial, as tecnologias quânticas, a biotecnologia ou o ciberespaço e lançou a iniciativa dos *hubs* para a inovação digital europeia que congrega pequenas e médias empresas, grandes indústrias, aceleradores e investidores.
Organizações como a NATO e a União Europeia têm vindo também a adaptar-se ao surgimento de novos fenómenos decorrentes de ameaças assimétricas de desafios no contexto cibernético e híbrido e da presença disruptiva de novas tecnologias num ambiente de competição estratégica à escala global. A introdução de novos domínios operacionais como cibernético, híbrido ou o espacial são um bom exemplo desta adaptação. A crescente digitalização da defesa tem sido acompanhada por uma preocupação euro-atlântica em apoiar condições que acelerem a inovação e o desenvolvimento tecnológico e industrial com o apoio do Fundo de Inovação da NATO e do Fundo Europeu de Defesa. Numa perspetiva política, tal sinaliza a forma como as organizações de defesa e segurança reconhecem a importância das tecnologias emergentes e disruptivas, criando o necessário enquadramento normativo e incentivos financeiros ao seu

fomento.
Do ponto de vista operacional, sublinhe-se a intenção do desenvolvimento de uma capacidade coletiva para proteger e responder rapidamente a uma nova tipologia de riscos e ameaças à segurança internacional. A eficiência da cooperação euro-atlântica tem resultado na combinação entre instrumentos regulativos, económicos e financeiros da União Europeia e uma robusta presença dissuasora da NATO, tornando-as mais aptas a enfrentar o atual contexto de conflitualidade, em que a guerra de atrição coexiste hoje, com sofisticação e a manipulação tecnológica de natureza disruptiva e híbrida.
A face mais visível da ameaça híbrida surge sob a forma de ataques cibernéticos, da desinformação, da polarização política ou da disrupção ou negação do normal funcionamento de serviços críticos necessários ao funcionamento dos Estados, das sociedades e das economias.
A dimensão menos visível, mas não menos disruptiva, manifesta-se sobre a forma de operações subversivas que podem comprometer a prossecução dos objetivos de política interna e externa dos Estados e a sustentabilidade dos setores e serviços públicos e privados. O emprego de tecnologias disruptivas, em contexto de ameaças híbridas, ocorre em ambientes de ambiguidade, dificultando, como sabem, a identificação da sua origem, a atribuição e consequentemente a sua mitigação podendo impactar muito negativamente sobre a confiança pública nas instituições e nas políticas públicas de segurança e defesa.
As campanhas de desinformação e os ciberataques conduzidos na sequência da eclosão da pandemia Covid-19, a invasão da Ucrânia pela Rússia e da subsequente crise energética, são exemplos desta nova realidade.
Concluiria, dando nota de que, no curto prazo, o emprego de tecnologias disruptivas em contexto híbrido implicará a necessidade de uma governação antecipatória centrada na inovação adaptativa na perspetiva estratégica e no desenvolvimento de processos de decisão não-lineares, aptos a lidar e gerir a incerteza e a complexidade. Implicará também uma maximização dos mecanismos de soberania partilhada em benefício da segurança comum e da segurança coletiva da Europa. Implicará, por outro lado, estruturas mais integradas, com melhores recursos de planeamento e capacidade de reação e de recuperação, logo estruturas mais resilientes, reduzindo-se o tempo de resposta e a eficácia na aplicação de medidas de mitigação ou de contenção de danos. Por último, uma melhor literacia digital como uma condição para a

desconstrução da ambiguidade em que a disrupção ocorre, do mesmo modo que, uma melhor comunicação estratégica contraria e mitiga os propósitos da interferência externa.
Durante o seminário de hoje, os nossos oradores irão analisar o impacto das tecnologias, da computação quantum, do cyber, do emprego da inteligência artificial, da biotecnologia, todos em contextos de segurança e defesa. Avaliarão os desafios e as oportunidades decorrentes da presença de tecnologias disruptivas num contexto de dissuasão da segurança económica e energética, das redes sociais e das informações.

Assistente do Seminário

Seguiu-se a intervenção principal deste seminário, subordinado ao tema "Desafios Tecnológicos à Segurança no Século XXI", tendo como orador o Major-General Filipe Arnaut Moreira e moderada pelo Excelentíssimo Senhor Embaixador Joaquim Ferreira Marques.

3.2 – Intervenção Principal - "Desafios Tecnológicos à Segurança no Século XXI"

Embaixador Joaquim Ferreira Marques

Muito bom dia. Em primeiro lugar, gostaria de apresentar os meus agradecimentos à Senhora Diretora do Instituto de Defesa Nacional, Professora Isabel Ferreira Nunes, por nos acolher aqui e ao Senhor. General Valença Pinto pelo trabalho que tem tido à frente do EuroDefense que nos conduziu a este seminário e, se me permitem, sobretudo, ao trabalho do Senhor Coronel Beja Eugénio pelo esforço que desenvolveu e que nos conseguiu fazer no grupo de estudos do EuroDefense-Portugal sobre transformação digital e inovação, o seminário que aqui nos reúne hoje. Gostaria também de agradecer ao Senhor General Arnaut Moreira pela amabilidade de nos falar sobre "Desafios Tecnológicos à Segurança no Século XXI". O Senhor General não precisa de apresentações, é um homem que nos entra pela casa dentro quase todas as noites e que nós ouvimos na rádio. Portanto, vou evitar falar no seu trajeto desde a Academia Militar ao Instituto Superior Técnico, a sua passagem por Madrid, na parte da *intelligence* da NATO e, portanto, gostaria de uma vez mais agradecer

a sua presença.
Se me permitem, só dois pequenos apontamentos: hoje podíamos quase considerar este seminário numa situação de *day after*, não sei se podemos considerar o fim do que se considerou, durante quase 80 anos, na Europa, como Pax Americana. A proteção americana de que a Europa teve oportunidade de usufruir poderá chegar ao fim e ter de enfrentar o pior desafio militar desde 1945. A agravar esta situação, creio que temos de ter presente que deste lado do Atlântico há países com situações orçamentais e económicas extremamente difíceis como a França, Alemanha, Reino Unido e Itália que nos colocam algumas interrogações. Não falo, obviamente, da situação do nosso país.
No entanto, gostaria de referir que talvez hoje a liberdade de ação com que Putin vive, apesar das anunciadas sanções ocidentais, parece ser a prova de que a sua aposta no regresso de Trump tinha alguma razão de ser.
Perante estes factos, teremos, por certo, de nos colocar questões sobre como enfrentar os desafios tecnológicos e cibernéticos com que hoje nos debatemos. Como combater a cibercriminalidade e as suas facetas? Como implementar uma melhor cibersegurança contra ciberataques, a destruição de informação, distorção e interrupção de processos, *phishing*, etc.? Como melhorar a tecnologia para melhor proteção das organizações e de indivíduos? Como acautelar a segurança pública e privada, a necessidade de melhorar as capacidades de *deterrence* e de cooperação internacional, como o caso que a Senhora Professora referiu anteriormente, das ligações dentro da NATO, da União Europeia e da própria OSCE? Melhor coordenação entre agentes públicos e privados? Obviamente, um ponto importante, é a melhoria da formação e treino dos funcionários para segurança nas redes, criptografia, monitorização, etc. Portanto, antes de me alongar, gostaria de passar então a palavra ao Senhor General.

Major-General Arnaut Moreira

Muito obrigado, senhor Embaixador, pelas suas simpáticas palavras. Gostava de começar por agradecer naturalmente o honroso convite que me foi dirigido pelo Instituto da Defesa Nacional e pela EuroDefense-Portugal e de saudar todos. Eu entro sem autorização nas casas de muitos, mas têm sempre o comando da televisão para mudar se for o caso…

O tema que me foi proposto foi este: "Desafios tecnológicos à Segurança do Século XXI", mas eu vou começar um bocadinho antes. Vou começar em 1767. Durante muitos anos, uma das minhas paixões era os relatos das viagens dos grandes exploradores e um dia adquiri um livro chamado "A Descoberta do Tahiti", que relata esta experiência de 1767, quando Samuel Wallis, que era já um homem com muita experiência de navegação na *Royal Navy*, recebeu uma carta secreta do almirantado para procurar um continente que se entendia que existia algures ali no Pacífico Sul e que ainda não tinha sido descoberto. Foi essa a missão de Samuel Wallis. Ele chegou em junho de 1767 ao Tahiti, no Sul do Pacífico, mas não foi o primeiro a chegar lá, pois a ilha já era conhecida desde Bougainville, pelo menos, um francês que já tinha andado por lá, mas foi a primeira expedição que entrou em contato com uma nova civilização. E este relato é fascinante porque mostra o que acontece quando duas civilizações que nunca se tinham visto se encontram pela primeira vez. O que acontece é que a desconfiança e a insegurança crescem exponencialmente e os habitantes do Tahiti meteram-se nas suas canoas com a tecnologia que possuíam que eram lanças, pedras, etc., e foram atacar a fragata inglesa com essas lanças e com essas pedras.

A fragata inglesa era uma fragata relativamente moderna, com casco revestido a cobre e 24 peças de artilharia naval, mas os ingleses perceberam que aquela tecnologia era desadequada para aquele problema. Podiam ter resolvido o problema com o disparo das suas peças de artilharia naval, mas não. Enfrentaram quase ombro a ombro, contacto a contacto e evitando disparar as peças. A primeira vez que dispararam as peças não produziu efeito nenhum porque havia barulho e havia fogo, mas os habitantes do Tahiti não percebiam qual era o efeito prático das peças da artilharia naval. Depois destes contactos exploratórios, finalmente foi possível estabelecer um contato amigável entre as partes, mas os habitantes do Tahiti nunca se interessaram pela grande tecnologia da fragata que eram as suas peças de artilharia naval, o que lhes interessava eram os pregos que seguravam as madeiras do navio, que estavam agarrados à sua infraestrutura e, então, os pregos tornaram-se de repente a grande moeda de negócio e de troca entre os ingleses e os habitantes do Tahiti.

Correram-se riscos de segurança imensos porque onde havia dois pregos passou a haver só um, ao ponto de os marinheiros aprenderem que aquilo tinha um valor comercial imenso e o capitão arriscou-se a ficar sem barco por causa de uma tecnologia que tinha introduzido no Tahiti que era completamente

desconhecida e revolucionária – os pregos. Portanto, este episodio demonstra várias coisas. Primeiro, o valor da tecnologia não é igual durante todo o tempo nem para toda a gente. Alguns sentem que têm uma determinada tecnologia e essa tecnologia é inútil depois para uma determinada função, sendo, por isso, importante refletirmos sobre tecnologia e sobre segurança.

Esta é a agenda que eu me proponho seguir. Vou começar com ameaças e depois segurança e defesa. Estes são os instrumentos de natureza conceptual com que eu gosto de trabalhar. Não quer dizer que eles sejam clássicos nem universais, mas são aqueles que, na minha perspetiva, são úteis para abordar este problema.

O primeiro [problema] é o da ameaça. A ameaça é uma alteração disruptiva da normalidade. Não é uma alteração qualquer ao normal. É disruptiva. Provoca alterações brutais àquilo que é o funcionamento normal de uma sociedade. Tenho vindo a afastar-me, cada vez mais, daquela noção muito clássica que a ameaça tem a ver com uma intenção e uma capacidade, porque isso atira-nos muito para as ameaças de natureza malévola, onde existe uma intenção de um ator de natureza humana. Ora eu acho que as ameaças, hoje em dia, já extravasaram, largamente, aquelas que têm origem humana. Basta olhar, na primeira imagem, que está do lado esquerdo, para o que aconteceu em Valência, onde o número de mortos é esmagadoramente superior ao que ocorreu nos atentados de 2004, em Atocha. Em Atocha morreram 193 pessoas. Essa foi considerada uma enorme ameaça em Espanha. Pois as cheias de Valência têm capacidade para multiplicar muitas vezes o número de mortos e de feridos e de envolver toda a sociedade. Não envolvem apenas os serviços de proteção civil, mas trouxeram também tudo o que se relaciona com as forças de segurança e, na última contabilidade, havia cerca de 18 mil militares. É um exército inteiro. Dezoito mil militares em Valência, o que significa, do meu ponto de vista, que as ameaças hoje em dia não são apenas de natureza humana. Há ameaças que são catástrofes de natureza natural, que têm implicações sobre aquilo que é a proteção da vida das pessoas, a normalidade da vida das pessoas e a destruição do seu património.

Depois, a segunda questão é a questão da segurança. Eu vejo sempre a segurança como uma questão de perceção. É a perceção. Eu sinto-me seguro quanto tenho a perceção de que disponho de um conjunto de instrumentos, de capacidades, que me permitem fazer face às alterações da normalidade. Portanto, eu não digo que estou protegido delas. Significa que eu tenho a

perceção de que tenho a capacidade de poder enfrentá-las.
E depois a questão da defesa, que é um caso particular da segurança, porque, neste caso, estamos perante uma ameaça de natureza intencional e de natureza externa. Portanto, digamos, estes são os meus instrumentos conceptuais para a minha abordagem.
Há três reflexões que me parecem essenciais sobre segurança para iniciar o nosso debate. O primeiro é: não existe segurança absoluta! Isso é uma miragem. É impossível de prometer e impossível de conseguir. Porquê? Porque desconhecemos muitas das ameaças. Porque é mais fácil de prever quando nós conhecemos as ameaças. Simplesmente, quando introduzimos na equação as catástrofes de natureza natural, muitas delas são imprevisíveis e, portanto, a segurança absoluta é uma questão que não existe. Ou seja, do facto de não existir segurança absoluta, significa naturalmente que existem riscos, porque não há recursos disponíveis para fazer face a todas as ameaças. Compete ao poder político verificar duas coisas: qual é o nível de perigosidade da ameaça e qual é a probabilidade de ela vir a acontecer. E é da conjugação da perigosidade e do risco de acontecer que os riscos têm de ser trabalhados. E depois há a questão da volatilidade. Há quinze dias, o que tínhamos nos telejornais durante todo o dia, era o que se tinha passado nalguns bairros periféricos de Lisboa. Ou seja, de um instante para o outro, alterou-se a nossa perceção de segurança. Neste momento, ela parece ter regressado, outra vez, ao normal. Portanto quando falamos na perceção de segurança, temos de ter ideia desta enorme volatilidade. Porquê? Porque eu defini segurança como uma perceção, e essa perceção vai-se alterando com o tempo.
Olhemos agora para tecnologia e poder. E o meu primeiro slide mostra quais são as quatro empresas mais valiosas em termos de valor de mercado, isto é, o número de ações vezes o valor dessas ações em mercado. Se olharmos para as quatro maiores companhias mundiais por valor de mercado — dados de meados de 2024 —, notamos várias coisas: a primeira delas é que todas elas são tecnológicas. Isto é, a tecnologia é um fator de poder, hoje em dia, pois a tecnologia gera um poder económico tremendo. Segunda questão: são todas americanas. Nestas quatro não há nenhuma que não seja norte-americana, o que significa que, por um lado, geram poder económico e, por outro lado, estão todas debaixo daquilo que é a capacidade norte-americana de gerir a tecnologia também como instrumento de poder.
Segunda reflexão sobre tecnologia e poder, tem a ver como a tecnologia. É um

dos componentes do poder, mas não é o único componente do poder. Nós, no Afeganistão, dominámos tecnologicamente e acabámos por sair. Porquê? Porque, a tecnologia não é sequer o fator decisivo. É um fator importante, mas não é decisivo. Segundo, a sua importância não se altera com o período histórico. Como eu mostrei, já em 1767 os ingleses tinham tecnologia que era importante e fazia a diferença. A tecnologia pode fazer a diferença nos períodos de conflitualidade.

Depois, terceiro ponto: as tecnologias somam-se, não se substituem. De vez em quando, é preciso ir buscar os *pagers*, com fez o Hezbollah. É preciso voltar atrás nas etapas tecnológicas, para ir buscar tecnologias que sejam adequadas a uma determinada situação. Portanto, elas não se apagam à medida que se inventam novas tecnologias. Vamos acrescentando, somando tecnologias às existentes.

Depois, o problema do Ocidente é a vontade, não é a tecnologia. Se isto fosse apenas uma luta de tecnologias, nós estávamos muito avançados e descansados do ponto de vista da gestão do poder. O problema é que falta vontade e, portanto, o que nos sobra em tecnologia falta-nos muitas vezes em vontade. Mais à frente tornarei a falar sobre este tema.

A tecnologia alimenta, hoje em dia, a conflitualidade, também a conflitualidade de natureza económica. Isto tem a ver com um artigo que saiu no *The Guardian* a 10 de agosto de 2023 que tem a ver com esta guerra tecnológica entre os Estados Unidos e a China. E eu coloquei ali quais eram os elementos de conflitualidade. Isto é, os EUA pretendiam evitar que a parte dos semicondutores, da computação quântica e da inteligência artificial pudessem ser dominados pela China. Portanto, uma preocupação norte-americana de controlar o desenvolvimento tecnológico da China. E a China? Bom, a China tem vantagem enorme sobre todos os outros países. É que as terras raras são fundamentais para a construção dos grandes dispositivos tecnológicos, hoje em dia. As terras raras, primeiro, não são raras. Existem em todo o mundo. O que é raro é ter capacidade de as processar, do ponto de vista industrial. E é aí que a vantagem da China é enorme. Cerca de 57% da capacidade industrial de manipular e tratar as terras raras está concentrada na China e não nos outros países.

Vamos falar agora sobre desafios tecnológicos. Naturalmente que não tenho a ambição de referir todos os desafios. Selecionei alguns e durante a fase de discussão podemos eventualmente levantar outros.

O primeiro desafio tecnológico tem a ver com uma questão que é fundamental hoje em dia que é a velocidade. A velocidade vem transformar tudo e vem trazer-

nos novos desafios, absolutamente extraordinários, como vamos ver, com reflexos depois na evolução tecnológica noutros campos. O que temos ali [no slide] é uma arma hipersónica, disparada a partir [de uma aeronave]. Este é o célebre míssil Kinzhal, que tem esta característica extraordinária… atinge Mach 10 de velocidade. É lançado, não de forma balística, mas é lançado a partir de um bombardeiro estratégico e normalmente aproxima-se do alvo abaixo da linha de deteção dos radares. Isto é, quando surge sobre o alvo já está muito perto, o que reduz imensamente o tempo de reação de quem está a ser atacado. Portanto, as armas hipersónicas introduzem aqui um desequilíbrio fundamental, porque nos retiram tempo de resposta. E o que é retirar tempo de resposta? Uma coisa fundamental: retira a decisão humana. Nós não podemos confiar só no nosso tempo de decisão humana para fazer face às nossas armas, temos de entregar à tecnologia a capacidade de detetar e de ser capaz de intercetar estas ameaças. O ser humano já não tem tempo suficiente para o poder fazer com oportunidade.

A segunda questão tem a ver com os mísseis balísticos. Os mísseis balísticos seguem uma trajetória curva e normalmente vão a altitudes acima da atmosfera. Chamava a atenção para algumas das velocidades que estão ali [no slide]. Um míssil balístico hipersónico anda a cerca de 6.125 km/h. Isto é uma brutalidade. Significa que faria a distância entre Madrid e Lisboa em pouco mais de cinco minutos. Vejamos todos os desafios que se colocam quando atores que nós considerávamos de terceira ou de quarta categoria, como os Hutis, que, a certa altura, dispõem de mísseis de natureza balística. Uma vez, num programa, chamei a atenção para o facto de que, se os Hutis recebessem mísseis de natureza balística, o que impediria que o Irão e a Federação Russa forneçam esse armamento à Líbia, onde também existem atores que poderiam gostar de dispor disto? A distância de Trípoli a Roma é de cerca de 1.000 km. Isto é, a partir do momento que se quebrou a regra de os mísseis balísticos estarem apenas na posse de atores de natureza estatal, a Europa passou a estar profundamente ameaçada pela existência desses mísseis. E depois temos também um dado interessante, que é o facto de os mísseis intercontinentais terem, hoje em dia, alcances na ordem dos 5.500 km.

Ligado e muitas vezes disfarçado sob os avanços na tecnologia dos mísseis balísticos, temos o desenvolvimento da tecnologia espacial. Porquê? Porque os foguetes são os mesmos. Isto é, o tipo de propulsão que nós utilizamos no desenvolvimento espacial é o mesmo. Em vez de termos um satélite, temos uma

carga explosiva. E, portanto, a coberto daquilo que é aceite como o percurso tecnológico para o espaço, seguem-se também desenvolvimentos que têm implicações diretas na nossa segurança, porque quem é capaz de lançar um satélite também é capaz de substituir o satélite por uma carga de natureza explosiva. Há aqui alguns dados interessantes. Primeiro, o número de satélites que circundam à volta da Terra: cerca de 9.000. Metade são lixo espacial. Isto é, dos 9.000, metade não funciona. Já ultrapassaram o seu tempo de vida. Estão na órbita da Terra, mas já não funcionam, já não são úteis. Oitenta e quatro por cento estão numa órbita baixa, definida entre 500 e 1.000 km de altitude. Porquê em órbita baixa? Bom, porque os tempos de propagação do sinal são muito mais baixos e é possível ter muito menos interferências de natureza atmosférica nesta faixa e, portanto, como a maioria dos satélites hoje em dia são satélites de comunicação, há uma enorme vantagem em ter estes satélites numa órbita baixa. Se olharmos para ali, uma percentagem muito importante de satélites, hoje em dia, são satélites de comunicações. Já há cerca de 105 países ou organizações com capacidade espacial e estão identificados cerca de 320 satélites de natureza militar.

Outro aspeto tecnologicamente significativo é que privatizámos o espaço. Isto mostra muito o que é a evolução tecnológica. Relembremos que eram as agências como a NASA, que eram agências que dependiam dos contribuintes norte-americanos e, portanto, do financiamento estatal, que contribuíram para o desenvolvimento espacial. Hoje em dia, a NASA já não tem capacidade de ir buscar os seus astronautas, que estão na Estação [Espacial] Internacional. Quem os teve de ir resgatar foram os foguetões de Elon Musk. Mais de metade dos satélites ativos pertencem à Starlink, que, num só lançamento, coloca 20 satélites em órbita.

Tecnologias de destruição: Não tem havido uma evolução significativa naquilo que é o poder explosivo das cargas que nós colocamos, mas pequenas alterações de natureza tecnológica permitiram pegar em arsenais muito antigos e transformá-los em armas de destruição tremenda. O que temos ali [no slide], a fotografia do lado direito, é Vovchansk. Vovchansk não fica longe de Kharkiv, fica junto da fronteira entre a Ucrânia e a Federação Russa e mostra Vovchansk antes e depois [dos ataques]. E o que temos do lado esquerdo é uma bomba. Esta bomba é uma bomba antiga, dos tempos soviéticos, simplesmente foi adaptado um kit que lhe permite planar. E a adaptação, pequena, tecnologicamente pequena, produz resultados de uma devastação tremenda. Foram 3.000 [bombas

deste tipo] lançadas em março de 2024 sobre a Ucrânia. Duzentas foram lançadas sobre a cidade de Vovchansk.
Depois, não podemos deixar de falar dos drones. Tenho a impressão de que mais cedo ou mais tarde, os drones vão ser proibidos. Os drones vão ter que ser proibidos. Estamos aqui num ambiente muito reservado. Nós tínhamos três refinarias em Portugal: Cabo Ruivo, Matosinhos e Sines. Depois, desistimos de Cabo Ruivo e, recentemente, desistimos de Matosinhos. Nós, neste momento, temos uma refinaria, em Portugal. Os drones têm de ser proibidos. Hoje em dia, a militarização de um drone, aquilo que está ali do lado esquerdo [do slide] é um drone de 500 euros, ao qual foi adaptada uma granada convencional; é um elemento de destruição tremendo, que está disponível a quem conseguir meter cargas explosivas. Os drones vão acabar por ser, do meu ponto de vista, proibidos, porque nós não podemos ter as nossas infraestruturas críticas reduzidas àquilo que é a sua expressão mínima, sob o risco de serem atacadas por dispositivos que custam 500 euros e que se compram no mercado. Nós, hoje em dia, com 500 euros, temos observação, orientação de fogos e combate. Já existem drones para os níveis tático, operacional e estratégico. As oficinas são todas "de vão de escada". Isto é, a tendência é militarizar produtos de natureza comercial, porque estão disponíveis e são baratos.
A Ucrânia quer produzir dois milhões de drones em 2024, mas como existe esta ameaça, também, neste jogo de guerra muito antigo, é preciso descobrir como é que o combatemos. Ora, não podemos combater um drone de 500 euros disparando um míssil que custa 5.000 dólares. Temos que encontrar aqui sistemas baratos para destruir aquilo que são drones baratos. Isto [no slide] tem poucos dias, 28 de outubro, é um sistema da ELBIT, que é uma empresa israelita, a quem foi concedido e atribuído um programa para armas de energia dirigida. Cada disparo sai à volta entre três a cinco euros; é quanto custa um disparo de um laser de alta potência. Portanto, o que nós temos é de encontrar, para a ameaça dos drones, sistemas compatíveis. Não podemos estar a utilizar mísseis de 5.000 euros para destruir um drone de 500 euros.
Depois, os drones também evoluíram. É que já não temos apenas drones de natureza aérea, agora temos drones navais. O que está aqui [no slide], United 24, é o drone que está a ser financiado por subscrição pública. Se forem ao site United 24, veem lá quando é que já foi recolhido, cerca de 75 milões de dólares, que as pessoas deram através de contribuições de cinco euros, dez euros, etc. Qualquer um pode contribuir para os drones navais ucranianos. Bom, estes

drones já afundaram 30% da frota do Mar Negro e, hoje em dia, nós podemos financiar a aquisição de equipamento militar para as forças armadas, que é uma coisa que nos parecia impossível, isto era sempre através de programas estatais pois, hoje em dia, nós contribuímos diretamente para o financiamento da aquisição de equipamentos letais em utilização das forças armadas.
Existem, neste momento, cerca de 200 experiências, na Ucrânia, para drones de natureza terrestre. Os drones de natureza terrestre não são como os drones navais nem como os drones aéreos. Porquê? Porque o meio onde se deslocam não é um meio fluido e sem obstáculos. É um meio que está cheio de pedras, de buracos das granadas de artilharia, de troncos de árvores, enfim, a mobilidade de um drone de natureza terrestre é muito mais condicionada que a dos drones navais e dos drones aéreos. Ainda assim, estes são os desafios que existem neste momento. O desafio da mobilidade, o desafio da energia, porque eles têm de ser recarregados, têm de voltar para tornarem a ser recarregados, e o preço, porque as quantidades produzidas são ainda muito pequenas e o preço é muito elevado. O que temos aqui [no slide] é um robô-dog desta brigada ucraniana, utilizada para situações mais complicadas.
E depois há aquilo que é pegar nas tecnologias de natureza militar e ver que essas tecnologias afetam todos. As tecnologias que nós temos, que a Federação Russa tem utilizado para dificultar a utilização de equipamentos GPS, tem também implicações na aviação civil. Depois há um conjunto de tecnologias que foram desenvolvidas para outras áreas, esta [no slide] é a *blockchain* (eu depois vou fornecer os slides). Depois podem ver com maior atenção. O *blockchain*, o que traz de importante aqui é que a tomada de decisão sobre a validação de uma determinada operação é feita por entidades independentes e é preciso haver consenso entre as várias unidades independentes para validar uma determinada operação. E depois há a Internet das Coisas, nós humanos já somos uma minoria na utilização da Internet. Existem 50 mil milhões de objetos conectados. Nós somos pouco mais de 8 mil milhões. Portanto, a grande maioria dos utilizadores da Internet já não são humanos, são coisas. São coisas cada vez mais baratas.
E, naturalmente, se temos estes objetos todos, a forma de os comandar é dar-lhes autonomia. Se nós não dermos autonomia aos objetos, eles não servem para nada, se nós temos que ir lá, cada vez, empurrá-lo para aqui, empurrá-lo para ali; portanto, nós temos que dotar estes objetos de inteligência artificial. Bom, a inteligência artificial está presente, hoje em dia, em muitas coisas, desde os filtros de *spam*, aos nossos robôs caseiros até à condução de viaturas. Há

aqui um problema, que ninguém nos explicou ainda, é que estão a afastar os humanos da tomada de decisão. Muito em breve, os dispositivos do automóvel não nos vão permitir acelerar se, por exemplo estiverem definidos para 60 km/h. Bem podem carregar no acelerador, ninguém vai conseguir ultrapassar aquele limite. Só não foi tomada ainda a decisão, mas os carros, hoje em dia, já todos têm os dispositivos preparados. Portanto, trata-se de afastar os humanos da tomada de decisão.

O reconhecimento da importância da inteligência artificial é também muito recente, 24 de outubro de 2024. O memorando de Biden em que manda que as agências de *inteligência* dos Estados Unidos e as agências ligadas à segurança nacional têm que utilizar a "artificial intelligence" em quantidades industriais, mas preservando direitos civis, privacidade e segurança. Vamos ver mais tarde como isto é difícil e depois há aquilo que são as tecnologias da vontade. Eu já demonstrei, no início, que nós temos muita tecnologia e pouca vontade. Nós, no Ocidente temos muita tecnologia e pouca vontade, e, portanto, a técnica, pelas nações que são hostis às democracias liberais, é influenciar, ao máximo, a nossa vontade. O que nós temos aqui [no slide] é uma coisa extraordinária. Não há muitas fotografias disto. Isto é uma *bot farm*. Uma *bot farm* é aquele conjunto todo de telemóveis que podem ser milhares de telemóveis ligados à Internet. Para quê? Para tornar virais determinadas mensagens que alguém pretende distribuir, para atribuir *likes*, para fazer subir nos *rankings* das redes sociais determinadas mensagens em relação a outras. De colocar *fake news*.

A gestão, hoje em dia, dos processos da nossa vontade, através destas *bot farms*, tem um operador que vai controlando… cada telemóvel daqueles, é, digamos, um utilizador virtual de uma rede social. Portanto, para o utilizador normal, aquilo é uma pessoa que está do lado de lá, mas na verdade não. Isto está tudo a ser controlado por um operador que vai controlando, colocando *likes* e *dislikes*, combatendo informação, etc. Para quê? Para fazer subir no nível das redes sociais as mensagens que interessam em relação a mensagens que não interessam. Em março de 2022, foram destruídas cinco *bot farms*, eliminadas 100 mil falsas contas *online* e apreendidos 10 mil cartões, que depois eram utilizados nestas *bot farms*. Os números são verdadeiramente impressionantes.

Depois, como nós não podemos deixar de estar ligados em todo lado, temos de evoluir naturalmente para o 5G e para o Starlink. O Starlink está a preços baratíssimos, quase concorrenciais, com o 5G. Aquele equipamento que está ali [no slide] custa trezentos e tal euros, e depois a assinatura custa para aí 40 EUR

por mês. Ou seja, neste momento, o Starlink tem capacidade de chegar a áreas onde a montagem de uma infraestrutura tecnológica 5G é muito dispendiosa ou demora muito tempo.
Depois, a computação quântica. Finalmente temos disponível o primeiro sistema operacional desenvolvido pela IBM. Não pode ser vendido, mas pode ser utilizado. Isto é, a sua utilização é alugada e disponibilizada na *cloud* da IBM. Portanto, já podemos utilizar a computação quântica subscrevendo os serviços da IBM. A computação quântica traz-nos problemas de segurança muito grandes. Primeiro, as nossas *passwords* são descobertas em muito pouco tempo. Mas, por outro lado, certamente, também oferecerá novas oportunidades de fazer a encriptação dos nossos segredos e isto, (estou quase a terminar) implica fiabilidade e vulnerabilidades. Este número é, para mim, impressionante e eu próprio fiquei admirado com a dimensão deste número: nós, os programadores, escrevemos, por ano, 111 mil milhões de linhas de código de *software*, ou seja, é impossível verificar se há *bugs*, se há problemas nestas linhas de código. Porquê? Não é humanamente possível. Nós produzimos muito mais linhas de código do que aquilo que é a nossa capacidade de saber se há ali problemas ou não há problemas de vulnerabilidade, o que depois, naturalmente, pode ser utilizado em todas as operações no ciberespaço através de *hackers* e de especialistas na exploração das vulnerabilidades. Nós somos as cobaias, nós é que descobrimos que há *bugs*, através da nossa utilização diária, e é por isso que todos os dias há atualizações de *software,* porque escrevem 111 mil milhões de linhas de código. Não há capacidade de verificar se há *bugs* ou não há *bugs* no sistema.
E vou concluir com o espaço da liberdade. Há duas áreas que me preocupam especialmente. A primeira tem a ver com a resposta a esta pergunta: quem fabricou o produto? Nós, antigamente, quando comprávamos - ainda se lembram - havia uns telemóveis Ericsson, nós sabíamos que aquilo tinha sido fabricado na Suécia, desenvolvido por engenheiros suecos, fabricado na Suécia e que os componentes eram certamente todos testados, etc. Alguém já conseguiu responder a quem fabricou os *pagers* para o Hezbollah? Ninguém conseguiu. É impossível saber, porque a cadeia de produção de um equipamento tecnologicamente moderno, hoje em dia, envolve tantas entidades, algumas das quais só dão o nome, mas há tanta gente envolvida na cadeia de produção que é difícil dizer quem construiu e qual a entidade.
Os norte-americanos tinham instalado na entrada das suas agências de

intelligence e da segurança nacional um conjunto de câmaras. Depois, descobriram que as câmaras eram chinesas, mandaram retirar as câmaras chinesas, ficaram só com as câmaras americanas, e depois quando tiraram a carapaça das câmaras americanas, descobriram que, por dentro, eram chinesas. Isto é, nós compramos um produto, compramos um produto e sabemos que o produto faz aquelas coisas, o que nós não sabemos é o que o produto faz para além das coisas que diz que faz e isso é que é o grande problema. Portanto, isto é um problema tremendo porque debaixo das carcaças, por mais que a gente desmonte coisas, encontramos sempre uma mão chinesa que fez qualquer coisa ali naquele produto.

E, para terminar, talvez o mais preocupante dos cenários. Isto que está aqui [no slide] é uma demonstração feita na China sobre as capacidades de reconhecimento das pessoas. Todas estas pessoas que estão ali já têm um número atribuído. Têm o número de identificação do cartão de cidadão da pessoa ou o seu nome. Simplesmente, o que está ali demonstrado não é apenas que aquelas pessoas estão todas identificadas e já têm um número de seguimento. É o número de vezes que já foram vistas, por que câmaras foram vistas e onde foram vistas e a que hora foram vistas. Isto é, o sistema seguiu estas pessoas no seu percurso. Isto era um percurso dentro de uma feira, mas todas elas foram seguidas, identificadas pelas várias câmaras, relacionadas, colocado um número de seguimento e tem toda a informação disponível sobre o que aquelas pessoas fizeram. Isto é, nós, hoje em dia, estamos a correr aqui um risco, que é um risco de a segurança acabar por interferir naquilo que são os aspetos mais normais da nossa liberdade de ação, mesmo quando estamos em espaços de natureza pública. Esse é um problema muito complicado porquê? Por causa do valor que nós damos à segurança. Nós damos muito valor à segurança e sempre que há um problema, dizemos, "mas porque é que não há uma câmara de segurança ali?". Ou seja, sobre esta pressão da segurança, nós vamos instalar câmaras em todos os lados. Ora, depois de instalarmos as câmaras, alguém vai lembrar-se sobre uma outra questão de segurança que o que era importante talvez era dar um alarme à polícia de que determinada pessoa com determinadas características está naquela área e, portanto, de seguida, nós vamos deixar cair mais uma barreira da nossa liberdade e vamos permitir que quem controla as câmaras também controle o acesso de determinadas pessoas. E a certa altura, a nossa vida está completamente seguida e catalogada, a que horas, em que local estivemos. Portanto, há aspetos de natureza tecnológica que ajudam à

segurança, mas que são feitos contra aquilo que são as nossas liberdades de permanecermos anónimos, onde quer que estejamos.
E eu (este é o último slide) gostaria de lembrar aquilo que disse Benjamin Franklin: "Todos aqueles que estão disponíveis para prescindir de um pouco de liberdade para ganhar uma segurança temporária, não merecem, nem terão nem segurança nem liberdade". Quando estamos dispostos, em favor da tecnologia e da segurança, a abdicar da nossa liberdade, vamos acabar por perder ambos.
Esta apresentação está no meu *blog*. É muito fácil lá chegar. Basta escrever "Blog Arnaut", no Google, entram na minha quinta. Em quinta, é só entrar e clicar em "Geopolítica". Estão lá todas as minhas conferências e discursos e, portanto, é fácil recolher esta ou outra qualquer, podem fazer o *download*.
E, só para terminar, Senhor Embaixador, o que é que aconteceu com os pregos? Porque a história repete-se no ano seguinte. O famoso explorador James Cook, a bordo do "Endeavour", foi enviado de novo para Pacífico Sul, e foi ao Tahiti também um ano depois, e nas suas ordens específicas à tripulação, dizia "muita atenção, todos os pregos e todos os artigos em ferro só podem, exclusivamente, ser trocados por mantimentos". Lições aprendidas, muito obrigado pela vossa atenção.

Embaixador Joaquim Ferreira Marques

Muito obrigado, Senhor General. A sua exposição foi excelente, mas coloca-nos imensas preocupações porque toca em pontos que fazem sobressair a nossa ignorância do que é o presente e, sobretudo, o que é o futuro. Um dos pontos que referiu, quando disse que apostava, no fundo, no fim dos drones, isso pode acontecer, creio eu, porque, por exemplo, é um ponto que o Direito Internacional Humanitário nunca abordou. Ou antes, abordou, mas há conceções diferentes e os três grandes países desta área, portanto, os Estados Unidos, a Rússia e China, não estão interessados em desenvolverem ações preventivas que os possam levar a questões, como por exemplo, na questão dos drones, eu, se me permite, eu questionaria. Há um ponto do direito internacional humanitário que levanta que é este: no caso de haver danos colaterais, quem é o responsável? É o operador do drone? É o fabricante do drone? São pontos a que nós temos de nos referir e, até hoje, não conseguimos.
Outro ponto importante que referiu é, no fundo, eu diria, o poder dos bilionários nesta ação porque, hoje em dia, o poder das nossas vidas foi transferido do

Estado para poderes individuais, não controlados pelo Estado, não controlados por nós. Como é que nós nos podemos orientar no meio desta falta de regulação? O outro ponto que eu gostaria também de referir, que abordou, embora, muito especificamente, muito devagarinho, foi o que eu posso chamar de astro-política. Hoje em dia, como falava, mais de metade do lixo no espaço já está inutilizado, mas nós temos de contar também que há outro lixo que anda no espaço e que tem objetivos não declarados. Ou seja, ter estruturas espaciais que estão no Gespaço para poder destruir outras estruturas espaciais. Ou seja, podemos estar a caminhar para um ponto de guerras, guerras espaciais, não do cinema, mas na realidade. Portanto, não sei. Lembro-me, também, destas guerras cibernéticas que nós temos. Falou-se aqui nos *pagers* e nos *walkie-talkies* e eu não sei se nós não teremos de vir a considerar a inserção de sistemas em, por exemplo, tanques, em aviões, em lançadores de mísseis, que nós julgamos serem muito fiáveis e, no fundo, eles já estarem a ser controlados por terceiros, quartos ou quintos e já não são sequer os Estados que estão a controlar essas atividades, mas indivíduos que ultrapassam os "*malwares*", os "*ransomwares*", essa gente toda que controla isso tudo. Os "*hackers*" já estão ultrapassados por outros indivíduos que até podem não ser já de carne e osso, serem de inteligência quântica, que estão muito mais avançados que a nossa própria inteligência. Eu creio que a inteligência humana ainda consegue colocar questões e hipóteses, mas com o avançar do quântico, estaremos, muito em breve, com essa realidade e teremos de enfrentar essa inteligência [artificial]. Gostaria de passar a palavra ao professor João Rucha Pereira.

Professor João Rucha Pereira

Queria cumprimentar a senhora professora diretora do IDN pela sua excelente intervenção e também por nos acolher nesta sua casa, cumprimentar também o senhor General Valença Pinto por esta iniciativa da EuroDefense-Portugal, a quem tenho a honra de também pertencer. Neste momento estou a coordenar o Grupo de Estudo sobre cibersegurança e proteção de infraestruturas críticas. Queria felicitar o Senhor Embaixador, o Senhor General Arnaut Moreira pela sua excelente conferência. Estamos sempre a aprender consigo, não só na televisão, mas também com estas conferências que faz, e queria-lhe pôr uma questão: qual é a sua perceção quanto à proteção que nós temos das nossas infraestruturas críticas, que muitas delas, enfim, têm uma proteção deficiente, na minha opinião,

e também muitas vezes falta de redundância a nível de segurança. Por outro lado, embora em todas as conferências se fale no ser humano e nas suas falhas, porque na realidade a questão da engenharia social, embora já muito desenvolvida e com muitas recomendações, a verdade é que nós, seres humanos, continuamos a falhar nessa área e, muitas vezes, até o clicar num link que não devíamos clicar, enfim, todas essas situações que o senhor General conhece, queria saber também a sua opinião sobre o que é que podemos fazer para melhorar a falta de literacia nessa área, e se podemos contar com seres humanos muito mais competentes a nível da segurança? Muito obrigado.

Major-General Arnaut Moreira

Muito obrigado. Só uma referência muito rápida às preocupações levantadas aqui pelo senhor Embaixador. Eu gostaria de chamar à atenção para a questão dos drones. Os drones transformaram-se em equipamentos militares de valor insubstituível. Nós, neste momento, não temos capacidades para fazer face àquilo que são as produções imensas de drones que estão a ocorrer nas guerras e não vemos nenhum sinal de que a nossa capacidade de resposta, em termos de defesa perante essas ameaças, que esteja em tempo de corrigir este enorme potencial destrutivo dos drones.

O que nos faltava agora era que um conjunto de organizações disruptivas, que existem em todas as nossas sociedades e que já tem acesso aos drones, que os podem mandar vir anonimamente, que serão entregues nas suas próprias casas, que tivessem agora capacidade de os militarizar e de os utilizar contra a sociedade. Os drones oferecem capacidades únicas de sobrevoo, de identificação, de reconhecimento, de pegar e de largar objetos onde muito bem lhes interessa e lhes apetece e, portanto, nós como sociedade, vamos ter de considerar os drones como instrumento de natureza militar. Nós não vamos poder ter uma única refinaria, quando há drones a 500 euros que podem dar cabo da única refinaria que temos.

Isto vai também um bocadinho em relação à questão que é a proteção das infraestruturas críticas. Eu, sobre a proteção das infraestruturas críticas, sempre achei o seguinte: tem que haver, do ponto de vista da defesa, uma preocupação acrescida sobre as infraestruturas de natureza crítica, desde logo pela sua localização. A localização não é indiferente. Um aeroporto a Sul do Tejo não é, do ponto de vista da defesa militar, a mesma coisa que um aeroporto a Norte do

Tejo. Simplesmente, nós entrámos numa era de facilitismo e de paz garantida que nos impede de trazer reflexões sobre o que é que está em causa. Está em causa uma infraestrutura de natureza crítica ou uma infraestrutura de natureza comercial. Isto é, uma coisa que garante muito dinheiro, mas que nos custa pouco a pagar ou é uma infraestrutura crítica que é essencial para o funcionamento do país, em tempos de crise e que tem de ser protegida. Isto é, como eu disse, a ameaça balística sobre a Europa está à distância de uma pequena decisão: é o Irão interessar-se pela Líbia. Se o Irão se interessar pela Líbia, nós vamos ter um problema europeu tremendo, porque os alcances dos mísseis balísticos iranianos, se se disparar de Trípoli para Lisboa não chegam a Lisboa, mas chegam a Alcochete, um bocadinho antes. Agora. Daqui a alguns tempos será certamente diferente. Isto é, nós andamos a dormir, também, um bocadinho, nestas questões da necessidade de repensar do ponto de vista da defesa, a localização das nossas infraestruturas críticas. Onde é que devem estar as refinarias, onde é que deve estar o abastecimento de água? Quais são as medidas alternativas que temos no caso de Castelo de Bode ficar indisponível, por qualquer razão? Nós tomámos por certo que vivemos na paz eterna, e, portanto, descurámos naquilo que é o pensamento estratégico sobre aquilo que é importante defender. Esquecemo-nos de colocar as questões de defesa, e essa é para mim a grande preocupação. Como é que se defende uma refinaria contra drones? Não é muito difícil, são precisos 10.000 drones que levantem voo simultaneamente para formar uma cúpula defensiva sobre a refinaria. É preciso pensar nas infraestruturas críticas como coisas que temos de proteger.

Os ataques que vão ser feitos sobre a Europa, não serão feitos sobre as suas Forças Armadas, serão feitos sobre as suas infraestruturas críticas. E o posicionamento das forças armadas será menos, do meu ponto de vista, pelo menos na Europa do Sul, sobre as suas fronteiras e mais na proteção destas infraestruturas contra um novo tipo de ameaças. Portanto, as ameaças de natureza híbrida vieram para ficar. Nós multiplicámos exponencialmente o número de atores não controláveis e não estatais. Nós estamos cada vez mais dependentes de decisões que não pertencem aos Estados, como referia o Senhor Embaixador, mas pertencem a entidades de natureza privada, com os seus interesses de gestão absolutamente própria e eu termino só dizendo esta coisa absolutamente extraordinária que é isto: no outro dia, sobre Kharkiv foi abatido um drone Shahed 136, que tinha dentro uma antena Starlink. Starlink não funciona na Federação Russa, mas os russos sabem que o Starlink funciona no

território ucraniano, e, portanto, trazendo o drone para dentro do território ucraniano já é possível ativar o Starlink. E o Shahed 136, com aquilo que é a largura de banda que o Starlink vem trazer, pode fazer coisas imensas e não ser apenas um objeto disparado de um sítio para ir para outro sítio já pré-programado. O Starlink não depende de nós. O Starlink depende de uma entidade. É essa entidade comercial que define qual é a área onde o Starlink está ativo e define se aquele terminal pode estar ligado ou não. Elon Musk pode decidir que terminais estão ligados ou desligados. Isto coloca realmente um conjunto de desafios muito grandes. Para terminar: é preciso, sobre as infraestruturas críticas ter uma visão de defesa, não apenas uma questão de natureza económica.

Rui Ribeiro

Bom dia. O meu nome é Rui Ribeiro. Sou membro do recente Observatório dos Ecossistemas e das Infraestruturas Digitais e faço uma pergunta ao senhor general, já agora, permita-me começar com humor. Com esta transferência que há de a decisão humana passar para as coisas, vai ser uma desgraça para os radares de velocidade, que vão deixar de faturar milhões. A minha questão é essa e corrija-me se estiver errado: durante muitos séculos, o poder régio, o poder clerical e o poder imperial condicionaram e fizeram a agenda da evolução tecnológica, no caso até da Inquisição, que desenvolveu e apurou instrumentos de tortura, juntando o conhecimento médico que havia na altura, e a partir, sobretudo, do século XIX, século XX, mas a partir da Segunda Guerra Mundial deu-se uma evolução tecnológica muito grande e a noção que eu tenho ou a perceção que eu tenho, é que o poder tradicional, aquele que nós democraticamente assumimos, ficou aquém daquilo que se passou nos séculos anteriores, e a pergunta que eu faço é como é que se faz esse balanço e onde é que está hoje o poder tradicional. Muito obrigado.

Major-General Arnaut Moreira

Muito bem. O poder tradicional está em erosão, em primeiro lugar porque nós, Estados, perdemos o monopólio das relações internacionais. As relações internacionais, hoje em dia, ganharam um conjunto muito grande de atores sobre os quais não há regulação. O que é que eu quero dizer com isso? Nós, quando

reconhecemos um Estado nas Nações Unidas, ele obrigava-se a um conjunto de obrigações, nomeadamente, assinava a Carta das Nações Unidas, ou seja, ele assumia perante a comunidade internacional que era uma entidade respeitável, que obedecia a um conjunto de princípios e valores que estavam escritos e eram reconhecidos e públicos, e que, por outro lado, podia ser objeto de sanções. Esta coisa de ter direitos só faz sentido se houver deveres. E havendo deveres, também os deveres só fazem sentido se houver sanções. Se nós não recebemos em casa a multa do trânsito, nós andamos à velocidade que quisermos. Isto é, não é apenas regular, depois tem de haver sanções sobre isso.

O que acontece é que a sociedade internacional evoluiu para lá dos Estados e criou um conjunto muito grande de entidades que se sentem cheias de direitos, mas sobre deveres não têm nada, absolutamente, a dizer, e nós não temos instrumentos ao nível daquilo que são as instituições multilaterais, onde quem tem acesso são sobretudo os Estados, para exercer pressão sobre estas entidades. Conclusão: os Estados agora descobriram uma forma fantástica: em vez de eu ser sancionado, vou inventar uma organização qualquer que vai fazer o meu trabalho sujo, para que me retire de tudo aquilo que é o lixo que vai ser produzido e sobre mim não venham a incidir aquilo que são as sanções que resultam de uma ordem internacional. Portanto, o que é que nós temos hoje em dia: uma multiplicação exagerada de atores, muitos deles já não são Estados, alguns dos que não são Estados ainda são políticos e portanto são controláveis relativamente aos seus objetivos, mas já temos um conjunto de atores que já nem políticos são, são apenas criminais, atores criminosos que estão disponíveis para o mais rapidamente possível obter todos os proveitos possíveis e imaginários, e portanto, o nosso desafio aqui é este e em resumo: o sistema internacional, a partir do momento em que evoluiu de um sistema baseado em estados para um sistema baseado em atores, que já não são Estados, perdeu também o controlo sobre as sanções que pode impor a esses atores e esses atores gozam de liberdade de ação estratégica muito superior àquilo que são as limitações que os Estados têm nas instituições multilaterais e em relação ao direito internacional. Portanto, enfim. Como é que isto vai acontecer? Bom, o que isto vai acontecer é que… habituemo-nos…

Embaixador Joaquim Ferreira Marques

Senhor General, muito obrigado pela sua excelente exposição que nos deixou iluminados, mas ao mesmo tempo, mas, de certeza muito preocupados, mas é a vida. Muito obrigado por tudo.

3.3 – Painel 1 – Tecnologias Disruptivas em Portugal

Assistente do Seminário

Segue-se o primeiro painel dedicado às "Tecnologias Disruptivas em Portugal", pelo que se solicita aos oradores convidados que tomem os seus lugares. A moderação do painel estará a cargo do Coronel António Eugénio, Assessor de Estudos do IDN, membro do Conselho Consultivo do EuroDefense Portugal e coordenador do Grupo de Estudos EuroDefense Portugal nº 4, dedicado à transformação digital e inovação.

Coronel António Eugénio

Exma. Senhora Professora Isabel Ferreira Nunes, meu General Valença Pinto, é uma honra para mim poder moderar este painel e assistir às brilhantes intervenções do Senhor General Arnaut Moreira, moderado pelo Senhor Embaixador. Estes temas são extremamente apaixonantes e, como tal, o tempo que nós levamos a discuti-los serve para nos alertar que temos de aprofundar estes temas noutros *fora* e noutras ocasiões. Este painel tem uma grande relevância para a segurança e soberania nacional. O impacto das tecnologias disruptivas, como vimos, no contexto das ameaças híbridas, em Portugal, é marcado pelas rápidas mudanças tecnológicas e também de intensificação de conflitos que vão muito para lá do domínio físico, como vimos na apresentação anterior.
Hoje, as chamadas "tecnologias disruptivas" – que incluem desde a inteligência artificial e a computação quântica até à robótica e biotecnologia – transformam profundamente a forma como os conflitos são travados e como a segurança nacional é concebida. Estas tecnologias, além de criarem novas vulnerabilidades, oferecem oportunidades significativas para reforçar as nossas defesas. No entanto, apresentam também desafios ao nível da soberania tecnológica de países como Portugal, que precisam equilibrar o desenvolvimento interno com a

dependência de capacidades externas, muitas vezes fornecidas, como vimos, por empresas e plataformas sediadas até fora da Europa. Trata-se afinal de uma mudança de paradigma!
Neste contexto de ameaças híbridas, o papel de Portugal, enquanto membro da União Europeia e da NATO, é crucial. Cabe-nos encontrar um equilíbrio entre a adaptação a esta nova realidade tecnológica e a proteção dos nossos interesses estratégicos. Por isso, hoje, neste painel, queremos refletir sobre as seguintes questões centrais: como podemos usar estas tecnologias para reforçar a nossa resiliência? De que forma podemos integrá-las numa estratégia de defesa que proteja tanto os espaços físicos como os virtuais e os informacionais? E, acima de tudo, como Portugal pode fortalecer a sua soberania num cenário de ameaças que é, cada vez mais, global e interligado, proporcionando acesso a agentes maliciosos remotos?
Espero que a discussão que se segue seja inspiradora e rica, como foi a anterior, ajudando-nos a encontrar respostas para estes desafios complexos e, simultaneamente, a identificar caminhos concretos para fortalecer a segurança de Portugal e dos portugueses.
Contamos, para isso, com um competentíssimo painel de oradores, que cumprimento, solicitando-lhes que profiram a sua comunicação em 10 minutos, o que é um período extraordinário, é quase um ritmo televisivo, para que tenhamos tempo depois para alguma discussão com o público. Eu vou abster-me de fazer as apresentações longas, uma vez que depois, posteriormente, poderemos, num relatório, incluir as notas biográficas de cada um dos oradores, dizendo que todos eles são competentíssimos e, como tal, eu passaria, desde já, a palavra ao Senhor Professor Armando Nolasco Pinto, que é professor catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro. Sem mais delongas, Senhor Professor, tem a palavra.

Professor Armando Nolasco Pinto

Muito obrigado a todos. É um prazer estar aqui. Uma saudação muito especial à Prof.. Ferreira Nunes, Diretora do Instituto de Defesa Nacional e também para o General Valença Pinto, Presidente do EuroDefense Portugal. Quero agradecer muito o convite ao Senhor Coronel. É um prazer estar aqui neste painel.
De facto, eu confesso que quando me foi feito o convite, eu não tinha a perceção exata do desafio que me era colocado. Porque não é tanto falar de tecnologias

quânticas. É falar a seguir ao Major-general Arnaut Moreira. Isso é que eu não sabia. E, portanto, eu vou tentar fazer o meu melhor, mas com algum receio.
Antes de mais, eu quero dizer-vos que aquilo que vou dizer obviamente não é trabalho meu. É trabalho do grupo que coordeno na Universidade de Aveiro, no Instituto de Telecomunicações, que é um grupo relativamente grande que se dedica às tecnologias quânticas. Para já, vou falar sobre aquilo que nós fazemos. É a primeira coisa que eu aqui queria deixar bem claro. Nós desenvolvemos tecnologias que procuram explorar e extrair recursos: o princípio da não clonagem, o princípio da sobreposição e o princípio do entrelaçamento. E o que eu gostaria de deixar claro: as tecnologias não são a computação quântica. A computação quântica é apenas uma instanciação particular. As tecnologias são um conjunto de recursos que a partir deste momento ou a partir de alguns anos temos a possibilidade de manipular. Para nós, um sistema quântico é um impulso de luz, que tem poucas partículas de luz. Normalmente, usam-se impulsos de luz na Internet e nas fibras óticas, com muitas partículas de luz, mas nós trabalhamos com impulsos de luz com poucas partículas de luz, de tal forma que a natureza quântica seja visível.
O que nós procuramos explorar é exatamente a não clonagem, a sobreposição e o entrelaçamento. O que é que é isso da não clonagem? Basicamente, o que nós aprendemos é que se nós colocarmos informação num sistema quântico, se alguém a ler, essa informação deixa um rasto. E isso é algo fundamental. É algo que não podemos evitar, o rasto que é deixado. A outra coisa é o princípio da sobreposição. Quando nós temos uma partícula de luz, ela não tem que fazer aquilo que nós temos de fazer na vida real. Chegamos a um cruzamento, temos de decidir se vamos para a esquerda ou para a direita. Não. Ela consegue ir por dois caminhos ao mesmo tempo. Outra coisa é o entrelaçamento. Nós pegamos, de facto, em duas partículas de luz, conseguimos combiná-las de tal forma que elas continuam a ser duas partículas de luz, nós mandamos uma para a esquerda e outra para a direita, mas elas passam a comportar-se como se fossem verdadeiramente apenas uma partícula. Portanto, de facto, isto, o princípio da não clonagem, o princípio da sobreposição e do entrelaçamento são recursos que nós podemos manipular e podemos construir tecnologia, podemos tentar resolver problemas usando estes recursos.
Reparem, eu não vos posso aqui dizer o que vai ser o futuro. Porque esta coisa de prever o futuro… prever é muito difícil, então, principalmente, o futuro, é terrível. E eu aqui concordo com aquele jogador que dizia que prognósticos só

no final do jogo. Portanto, não esperem de mim que vos vá aqui dizer o futuro. Agora, nós podemos olhar um pouco para trás e ver o que a história nos tem para ensinar. E, de facto, se olharem dois séculos para trás e virem o trabalho de Michael Faraday, quando ele descobriu a energia eletromagnética, ele não tinha ideia de que aquilo iria estar na base da sociedade que temos hoje. E demorou tempo, cerca de 50 anos, até Alexander Bell propor o telefone, e quando Alexandre Bell propôs o telefone, na patente do telefone, ele vê que uma das utilizações fosse que, no fundo, a classe nobre pudesse ouvir a ópera através do telefone sem sair de casa. Reparem, não é nada disso que hoje em dia fazemos com o telefone. Fazemos imensas outras coisas. Para chegarmos aos sistemas de comunicações que nós temos hoje, e o Senhor Major-general falou na largura de banda, que está em grande parte relacionado com aquilo que foi o trabalho durante a Segunda Guerra Mundial e depois da Segunda Guerra Mundial, de Claude Shannon. Foram precisos quase 100 anos. Portanto, a tecnologia demora tempo e, no fundo, foi um recurso que foi explorado, que depois deu origem à Internet e à sociedade de informação, mas foram cerca de 200 anos que se passaram. Quando nós falamos em tecnologias quânticas, nós estamos a falar de algo idêntico, no sentido que temos recursos, que estamos à procura deles. De facto, há uma frase muito interessante de Theodore Maiman quando ele descobriu o laser ou quando ele inventou o laser e ele disse: "O laser é uma solução à procura de problemas" e nós de facto encontrámos montes de problemas que podemos resolver com um laser. E um deles ainda hoje aqui o Senhor Major-general Arnaut Moreira referiu aquele exemplo daquele sistema de abater drones ou de poder usar a energia como uma arma, usar o laser como uma arma. De facto, quando nós falamos de tecnologia quântica, nós falamos de recursos que podem ser usados para resolver problemas. Claro que eu me coloco aqui um bocadinho no outro… eu percebo que aqui a grande preocupação é a preocupação da segurança. Mau eu desenvolvo tecnologia partindo do princípio de que a tecnologia vai servir a humanidade. Portanto, a minha perspetiva aqui é um pouco a do outro lado, mas tenho consciência dos problemas da segurança e obviamente que aquilo que o Senhor Major-general aqui falou, obviamente, que são coisas que nós temos que ter essa consciência, portanto nós também não podemos ser ingénuos neste mundo.

Mas para avançar e não vos demorar muito tempo, obviamente que o computador quântico é uma ameaça grave. E porque é que é uma ameaça grave? É uma ameaça grave nesta altura, porque, de facto, a nossa segurança, dos nossos

sistemas de informação, baseia-se em complexidade computacional e, de facto, o computador quântico é uma máquina capaz de resolver problemas que nós hoje não podemos resolver com um computador clássico. Significa que ele pode quebrar a nossa segurança da nossa informação, e nós temos de arranjar forma de combater isso. Isso é um problema conhecido e, de facto, os EUA, num memorando de 2022, definiram rapidamente o que é que eles queriam fazer. Eles queriam ter a supremacia no que diz respeito a esta tecnologia queriam tomar um conjunto de ações que levassem à mitigação dos riscos. E, para isso, incumbiram o NIST [National Institute of Standards and Technology] de desenvolver um conjunto de *standards* que publicaram em 2024 e a partir daí começaram um processo de transição, que já iniciaram. Nós temos, também, um movimento análogo na Europa, ou, pelo menos, a Europa também tem seguido estes passos, nomeadamente um conjunto de agências de diferentes países que têm colocado normas e diretivas sobre isto. Também ao nível da União Europeia, no início deste ano saiu uma diretiva no sentido de propor ou recomendar aos Estados que avancem neste processo de transição.

E porque eu não tenho muito tempo, quais é que são os sistemas que verdadeiramente nós estamos a desenvolver em Aveiro? Nós estamos a desenvolver, por exempo, geradores de números aleatórios. Isto é uma coisa que nós… nomeadamente no âmbito do Gabinete de Segurança Nacional, geramos, utilizado o ruído quântico para gerar aleatoriedade. Sistemas para distribuir chaves quânticas, portanto sistemas em que nós codificamos informação apenas num fotão, neste caso na polarização, e conseguimos distribuir informação do ponto A para o ponto B. A grande vantagem destes sistemas é que nós conseguimos quantificar exatamente qual é que é a quantidade de informação que foi extraída do canal de comunicação. Nós não conseguimos é eliminar um agente que esteja no meio do oceano. Agora, nós conseguimos é saber exatamente que quantidade de informação é que ele foi capaz de retirar do sistema. E, portanto, nós temos estes sistemas de troca de chaves criptográficas, usando fotões únicos. Temos, depois, os outros sistemas análogos. O outro usava codificação da polarização, este aqui utiliza codificação na amplitude. E, de facto, temos vindo a usar estes sistemas no âmbito de muitos projetos. Estes são os projetos que atualmente estamos a trabalhar no grupo. O primeiro, em que nós pretendemos, de facto, fornecer este gerador de números aleatórios à comunidade, e se alguém quiser usar estes números, ele está disponível. Nós tivemos, por exemplo, ainda o ano passado, um aluno da Guatemala, de uma

Universidade da Guatemala, a tentar atacar o nosso gerador, utilizando inteligência artificial. Temos depois um outro projeto, que é um projeto europeu, no âmbito do Discretion, que envolve a defesa nacional, a espanhola, a austríaca e a italiana, também, no sentido de desenvolver esta tecnologia para cenários militares. Estamos envolvidos, também, no PTQCI. E o PTQCI é o quê? No fundo, é um projeto que está integrado num projeto europeu que é o EuroQCI, cujo objetivo é começar a criar as redes quânticas nos diferentes Estados e nós vamos instalar, no início do próximo ano, três nós aqui em Lisboa, no âmbito do que será o embrião da rede quântica nacional. Temos também um projeto NATO, no âmbito do projeto *Science for Peace*, que tem um pouco a ver com aquilo que o Senhor Major-general Arnaut falou no que diz respeito aos satélites. E, de facto, nós hoje temos um conjunto enorme de lixo espacial, de satélites que nós não sabemos de quem são e nem controlamos e há um conjunto de agências que fazem monitorização sobre esses satélites. Mas, de facto, elas querem partilhar informação e este projeto, no fundo, visa utilizar as tecnologias quânticas para que as diferentes agências, mesmo sendo aliadas, possam partilhar informação, mas reservando a privacidade. Ou seja, possam colaborar, mas sem revelar todos os dados que detêm. Basicamente, se quiserem, de uma forma simples, é como calcularmos a média da idade das pessoas que estão aqui nesta sala sem que nenhum de nós precise de dizer a nossa idade. No fundo, conseguimos preservar os nossos dados, mas conseguimos colaborar. Isto é importante, nomeadamente, na área da defesa e também na área da medicina genómica, que é uma área que em que nós também trabalhamos. O genoma, como sabem, é algo também muito importante, porque diz muito sobre nós, não só sobre nós, mas também sobre os nossos filhos e sobre os nossos netos, mesmo que a gente ainda não tenha netos. Portanto, é importante preservar essa informação, porque as empresas estão sujeitas, por um lado, à competição comercial e, portanto, por isso, a informação também tem valor, mas também a um conjunto de regulações relativamente rígida que as obriga a que a informação seja preservada. E depois temos este outro projeto que é o projeto QuantaGENOMICS, em que nós participamos com um conjunto de entidades a nível europeu, e depois, também, um outro projeto também relativamente largo em que nós desenvolvemos, no fundo, esta parte da *secure multi party computation*, utilizando tecnologias quânticas.

Mas só para concluir, esta é a parte da rede quântica nacional que nós estamos a concluir, em que nós estamos envolvidos. Portanto, vai haver (ali a vermelho

no slide), temos um círculo que vai ser um conjunto de nós que vão ser instalados em Lisboa e depois irá haver uma segunda fase. A ideia é interligar as diferentes redes quânticas que estão a ser criadas no espaço europeu, interligá-las entre si. Obviamente que Portugal tem interesse quanto à interligação a Espanha, é o nosso vizinho e, portanto, a ligação a Vigo e a Madrid. Mas é importante para nós, também, que a rede tenha uma cobertura nacional, não só em Portugal continental e por isso a tecnologia dos satélites é importante, porque uma das limitações da tecnologia quântica é o alcance e nós não conseguimos chegar à Madeira e aos Açores usando fibra ótica e por isso aparece ali [no slide] a parte dos satélites.

E agora, muito rapidamente, alguns sistemas práticos. Nós fizemos aqui, em 2021, uma primeira demonstração do sistema quântico, entre o Estado-Maior-General das Forças Armadas e o Comando Aéreo da Força Aérea. Depois, isto foi uma experiência que fizemos na rede quântica de Madrid. Em Madrid existe já uma rede quântica, bastante avançada e nós corremos lá uma experiência com os nossos protocolos de *secure multi party computation* no âmbito da medicina genómica. Isto foi com o Exército. Fizemos uma demonstração, também, no âmbito do ARTEX, em Santa Margarida, em 2023, e fizemos também com a Marinha, neste caso foi uma transferência de chaves criptográficas para uma fragata, que quando chega ao porto há um cabo que é ligado e são transferidas as chaves utilizando estes sistemas. Agora, mais recentemente, e num cenário mais complexo no âmbito do REPMUS e também no âmbito de um exercício da NATO, fizemos um cenário em que há um sistema criptográfico e depois as chaves chegam já a um conjunto de aplicações, ou seja, um conjunto máquinas de *chyfer machines*, de máquinas de encriptação e um conjunto de rádios no âmbito de um cenário militar.

Eu não me irei alargar muito mais. Só dar nota aqui que, neste momento, estamos também a participar em três grupos NATO relativos às tecnologias quânticas, um que tem a ver com aquilo que se designa por Internet quântica, outro que tem a ver com as vulnerabilidades da tecnologia quântica e outro que tem a ver com a parte dos *use cases*, que é um grupo que nós lideramos e que neste cenário poderá ser relevante para a discussão. E eu ficaria por aqui para não me alongar muito.

Coronel António Eugénio

Muito obrigado, Senhor Professor, especialmente por ter essa capacidade dual de nos transmitir informação preciosa e também de se circunscrever ao tempo de apresentação. E este é um dos pontos que eu acho que é fundamental nós percebermos que o nosso país por vezes nos causa algumas surpresas, e que estas surpresas tecnológicas nos devem alimentar o espírito para aprofundarmos e divulgarmos todo um conjunto de avanços tecnológicos que existem e residem nas universidades portuguesas, como é o caso da Universidade de Aveiro. Mas que também tem a componente de ligação às Forças Armadas, como bem exemplificou e que eu saúdo e que nos mostra que, de facto, é preciso focarmo-nos na experimentação prática e também com o envolvimento das Forças Armadas nestes setores de ponta tecnológicos.
Passamos, sem mais delongas, para a intervenção número dois, que tem a ver com cyber e peço ao orador, Senhor Engenheiro Paulo Moniz, que tem uma relação com o Eurodefense e com outras empresas, nomeadamente a Edinfor, e a quem eu passo a palavra.

Engenheiro Paulo Moniz

Olá, muito bom dia a todos. Antes de mais, agradecer à Professora Isabel Nunes e ao IDN, com quem eu gosto muito de colaborar, o convite. Obviamente ao General Luís Valença Pinto, que é o meu líder na Eurodefense PT, que é um prazer e um privilégio, e também a todos vós por proporcionarem a disponibilidade de poder adicionar valor nesta conferência e nas vossas vidas. Portanto, vou fazer o meu melhor. Se o meu desafio de falar depois do General Arnaut já era difícil, sem slides então e depois da magia quântica, ainda será mais. Ainda mais porque eu queria correr quatro tópicos, em dez minutos, o que me dá cerca de dois minutos por cada um, porque, entretanto, eu já falei não sei quantos segundos.
Eu queria falar convosco sobre a caracterização da tecnologia e da nossa sociedade e a sua dependência, os aspetos do ciberpoder, como é que o poder se projeta no ciberespaço, as ameaças e depois uma mensagem de esperança, ou seja, aquilo que podemos fazer para que as coisas corram melhor.
Bom, então, para o primeiro tema, eu tenho duas palavras: dependência e complexidade. Dependência porquê? Porque, por muito que eu chegue a todos vós e vos pergunte se nós dependemos muito da tecnologia, todos vão dizer que sim e que sabem, mas não. A dependência é profunda e eu, neste ponto,

gosto sempre de dar aqui um exemplo do setor primário, que é, portanto, uma quinta de vinhos, que produz um produto do qual eu sou um apreciador, e acho que fazemos aqui com muita qualidade. Essa quinta fica na zona Oeste, uma quinta pequena. Tenho um amigo que lá trabalha e que há coisa de três anos me ligou, um bocadinho aflito, porque estavam parados. E estavam parados porquê? Porque não tinham computadores e eu comecei a pensar um bocadinho, obviamente depois mais tarde, depois de o ajudar, pensei quando, nos tempos do meu avô eu ia, pisava as uvas, apanhávamos as uvas, trazíamos no carro com os bois, na altura, e depois fazíamos o vinho, mas agora a quinta não faz nada sem computadores. Literalmente nada. Eles estiveram três dias parados porque tiveram um ataque *ransomware* e, portanto, fizeram com que o setor mais primário que nós podemos ter na nossa sociedade, fosse completamente imobilizado porque eles não sabiam o que colher, onde colher, como registar no computador. A dependência é profunda e podia alarga-me aqui noutros temas.

Falamos de um sistema complexo. É aquele que nós efetivamente não conseguimos prever quando há uma ligeira alteração de algumas das suas variáveis e, portanto, é um sistema emergente, um sistema com um comportamento imprevisível. Lembramo-nos da meteorologia. É muito difícil de fazer uma previsão a muitos dias e, como sabemos, às vezes até de um dia para o outro falha. Também existe esta coisa nos sistemas. Quando aqui o General, se calhar é engenheiro, General Arnaut falou dos milhões de linhas código, não sei se sabem quantos milhões de linhas de código tem o vosso carro. Cem milhões de linhas de código. Por isso é que quando ele deixar de funcionar, o melhor que vocês têm que fazer, é desligar e voltar a ligar. Pode ir a duzentas ou mais. Portanto, a complexidade é brutal. É como se eu tirasse o esparguete, porque é assim, um fiozinho e atrás vem uma série de coisas que foram sendo construídas ao longo dos anos. Os sistemas ainda dependem - o Windows - daquilo que foi feito há vinte anos no *core*, onde não sabemos se o *developer* está vivo, atualmente, ou se não está vivo. Isto é tudo um emaranhado. Mas depois isto projeta-se na sociedade. Reparem que há cerca de três semanas tivemos um caso que tem alguma ironia, que é o caso da CrowdStrike. E porque é que eu digo que tem uma ironia? Porque vamos pensar assim: aquelas máquinas foram todas abaixo, e pensaram, a maior parte das pessoas, porque não estavam com segurança. Errado. Foram os que investiram mais em segurança. Aquele software é um software de topo para proteger o nosso

endpoint e, ainda assim, uma atualização automática – reparem nisto que eu digo da dependência da complexidade, como estão intimamente ligadas – ainda assim, uma atualização automática meteu milhares ou talvez milhões de máquinas em baixo, afetando serviços. Se vocês vissem o Flightradar, onde vêm os aviões todos no espaço aéreo, no período em que estavam as empresas afetadas veem que o espaço aéreo ficou vazio. Imaginem o impacto que isto é! É esta ideia de complexidade que eu vos queria deixar e eu adorava continuar aqui, mas vou ter que passar para o segundo tema.

O segundo tema é: porque é que o ciberespaço é tão bom para a projeção de poder? Muito bom, muito simples, poucas barreiras à entrada. Não consigo comprar um carro de combate, um míssil, obviamente, mas eu com um computador, se eu tiver uma infraestrutura crítica que está desprotegida, eu posso provocar, há uma simetria. Simetria não é idêntico a equidade. Portanto, simetria, os agentes que têm mais poder, com mais recursos, continuam a ser, eles próprios, aqueles que podem projetar ainda mais poder no ciberespaço. Mas há uma assimetria, ou seja, há poucas barreiras à entrada e isso é uma característica fundamental que faz com que o ciberespaço se torne um elemento, portanto, um espaço único. O outro elemento é nós podermos esconder a nossa identidade; também é muito fácil dar-vos exemplos, mas por questões de tempo, vou passar ao terceiro, que é a plasticidade da geografia. Ou seja, enquanto no mundo convencional, que eu não gosto de chamar mundo físico e mundo virtual, porque o ciberespaço também é físico, mesmo na quântica, portanto, acabamos por ter, também, a parte física. Portanto, eu gosto de chamar o mundo convencional e o ciberespaço. E reparem uma coisa. Enquanto no mundo convencional consigo caracterizar a minha geografia como as montanhas, os rios, os vales e mover as minhas forças, no ciberespaço, eu posso estar a ver aqui a minha infraestrutura a ser atacada, agora, e estou a identificar uma origem que é de um Estado pária, num outro hemisfério, imaginem, no outro lado do mundo, e na verdade, o indivíduo pode estar ali fora, num jardim, a fazer esse ataque. É muito complexa a atribuição no ciberespaço. E isso, depois, tem implicações nas fronteiras e naquilo que se pode dizer, o que poderia ser uma declaração de guerra que também me parece um desafio muito grande só no ciberespaço.

Passando aqui ao terceiro ponto, a parte dos atores e do tipo de ataques. Não sei se vocês se recordam dos filmes de Hollywood, em que normalmente quem atacava os sistemas eram aqueles jovens com muito acne na cara, fechados em

quartos escuros, pouco sociáveis e que tinham os computadores por todo o lado, a comer pizzas e a beber Coca-Cola. Bom, esses continuam a existir, mas eles agora são mais sofisticados e não precisam de saber tanto de computadores como era suposto, porque as ferramentas estão mais acessíveis aos atacantes. Nós podemos, efetivamente, adquirir ferramentas ou fazer parte de redes com uma facilidade brutal para podermos perpetuar outros atos noutras entidades e organizações.

Depois temos o terrorismo. Eu acho que o terrorismo - só isso, poderia dar aqui uma intervenção inteira de uma hora - não tem propriamente um apetite pelo ciberespaço e pela cibersegurança no sentido direto. Porquê? Porque não proporciona a espetacularidade. Portanto, as torres que caem, etc. No entanto, proporciona várias coisas, como, por exemplo, a angariação de fundos, propaganda, treino à distância, ou seja, em que há menos risco de serem apanhados nas transações e nas viagens que fazem. O terrorismo faz um ótimo, um excelente uso do ciberespaço, portanto isto podia ser muito mais desenvolvido.

Depois temos ainda os *insights*, portanto, as ameaças internas, as ameaças internas que nós podemos ter, dentro da organização, motivadas financeiramente e essas existem amiúde. Aliás, todos estes crimes que eu vos falei, o exemplo que eu dei, o da quinta dos vinhos, acaba por ter uma motivação puramente financeira e temos os geopolíticos ou mais derivados, portanto, das relações entre Estados e estes sim tocam também aqui o aspeto da guerra híbrida. Porquê? Porque eu não creio, da minha perspetiva, que o ciberespaço, em si, acabe ou a cibersegurança acabe por ser o mote central, pelo menos para já, da guerra, mas sim, como um elemento potenciador e coordenador de outras atividades que podem esgotar-se entre o mundo convencional e o mundo do ciberespaço. Vou só dar só um exemplo muito rápido. Todos nós tivemos ataques [cibernéticos], e a minha própria empresa teve, em 2020, em pleno Covid, um ataque cibernético. Mas depois tivemos [ataques cibernéticos] em companhias de comunicações, no retalho, e nos media. Se vocês imaginarem, todos esses dias tivemos um bocadinho de perturbação. Ah, foi numa empresa de retalho… ah, não vou a este, vou ao outro. Eu não tenho um operador de comunicações, mas tenho outro. Tudo bem. Quer dizer, foi-se vivendo. Houve prejuízos, houve danos, houve, se calhar, até mais do que aqueles que nós podemos ter documentados, mas acabámos por ser resilientes. Agora imaginem que há um ator que coordena todas estas teclas e que as toca todas ao mesmo tempo. Pois,

isto é um pouco aquilo que é o receio, que eu penso que pode ser uma ameaça e que pode juntar-se a meios convencionais no terreno.
Passando ao último ponto, para fechar. O último tema era este: o que é que nós podemos fazer? Ora bem, uma coisa é fundamental, a regulação. A regulação não é uma coisa, como dizia um treinador, uma faca de dois legumes, mas é parecido, porque a regulação é fundamental. Porquê? Porque ela atua nas falhas do mercado, nas falhas do interesse e da motivação, porque nem todas as empresas poderão ter esta consciência, e não podemos esquecer que há infraestruturas críticas geridas por operadores privados. Portanto, a regulação é fundamental. Ela tem que atuar porque pode haver uma falha de mercado e os incentivos podem não estar alinhados. A regulação é fundamental. Qual é o perigo da regulação? É ser fragmentada, é ser partilhada, é ser ou demasiado genérica, que não tem efeito nenhum, ou demasiado pormenorizada que cai em obsolescência com muita facilidade, portanto, não é fácil. Mais ainda, no contexto europeu - alguém, no início, fez a alusão ao *day after* -, era bom que ela não fosse uma coisa em Portugal, outra em Espanha, outra em França, porque empresas e outras organizações que operam nestes sítios todos acabam por duplicar esforços, meios, e com efeitos que são mais reduzidos.
A cooperação é fundamental, porque há organizações que não têm meios. Não têm meios para ter capacidade de defesa. Todas estas empresas, esta quinta que eu falei, e outras noventa e nove vírgula qualquer coisa - não sei qual é a percentagem de pequenas e médias empresas em Portugal - poderão não ter os meios para conseguir fazer face ao cibercrime. Há aqui uma outra palavra que é importante nos dias de hoje, que é a competição, ou seja, nós podemos competir de uma forma saudável. É muito bom mudar este *mindset*, que eu acho que ainda temos e fazer um esforço durante as nossas vidas, para que isso aconteça.
Eu queria terminar com a *awareness* e treino, ou seja, ter a ideia do que é um risco. Eu sei o risco de chegar ao pé de um indivíduo que tenha dois metros e seja muito musculado e se calhar, começar a provocá-lo. Eu sei que eu tenho aqui um risco. Se eu atravessar a estrada, ninguém precisa de explicar isto. O ciber-risco, eu tenho muita dificuldade em poder explicar aos meus pais porque é que eles têm que mudar a *password* do *router* para ir ao *homebanking*. Porquê? Não é uma coisa inata. Portanto, muito *awareness*, muito treino para criarmos talento, não é? Necessitamos de muito talento. E no aspeto do talento, vou fechar com aquilo que não podia deixar de ser, que era pecado hoje em dia, sem falar de inteligência artificial. Ainda que eu já tenha programado inteligência artificial

há trinta anos no Instituto Superior Técnico. Esta nova inteligência artificial é potenciada pela quantidade de dados e pela capacidade de processamento. É assim: a inteligência artificial tem, mais uma vez, os dois lados, não é? Não vou usar outra vez a piada da faca, mas tem os dois lados. Ela tanto serve, obviamente, para potenciar o lado mau da força, por assim dizer, mas nós podemos fazer dela algo muito bom, como por exemplo, se calhar, dominar esta complexidade que eu falei. Falava o General e muito bem - parabéns pela intervenção, já agora - que nós não conseguimos dominar isto. Se calhar nós não conseguimos, mas, quem sabe, podemos utilizar a inteligência artificial? Eu adoro o tema da complexidade e acho que a inteligência artificial pode ter um papel muito preponderante nisto. Depois, também, na falta de talento e colmatar essa falta de talento. Depois vão dizer… ah, está a preconizar que as pessoas não têm mais papel na sociedade. Não. Têm de certeza. Nós sempre nos soubemos adaptar e eu tenho a certeza absoluta de que nós vamos encontrar novas formas de sermos úteis para a sociedade, mas ela pode ser muito importante na parte da defesa da cibersegurança. E, por último, nas próprias ferramentas. Aí vai ser sempre o jogo do gato e do rato, mas as próprias ferramentas podem evoluir para que, efetivamente, nós possamos estar um bocadinho mais seguros nesta sociedade. Portanto, meus amigos, é um tema fundamental, no contexto das ameaças híbridas. E eu acho, que devemos estar todos conscientes, com esta consciência aberta, e acreditar que o futuro será sempre melhor.
Obrigado e bom dia.

Coronel António Eugénio

Muito obrigado ao Senhor Engenheiro Paulo Moniz pela clareza e pelo foco que nos trouxe, uma vez que nos abstraímos de olhar para os slides e concentrámo-nos em si. Muito obrigado pela intervenção e fez uma excelente ponte para a próxima apresentação do João Montenegro que é um *designer* premiado, com trabalho em vários setores incluindo o aeroespacial, o automóvel e a impressão 3D e é, também, o CEO de uma companhia com o nome Darkmetter e, como tal, representa, aqui, o espírito empresarial. Tem a palavra.

João Montenegro

Bom dia a todos. Queria, primeiramente, agradecer à Professora Doutora Isabel Nunes pelo convite, ao Coronel António Eugénio, também pelo convite, e é um prazer estar aqui à frente de tanta gente muitíssimo importante no país. De facto, a linguagem é preciosa e usar palavras tão ambiciosas como estas em dez minutos é difícil. Portanto, em vez de uma reunião, vamos fazer uma interseção dos dois temas: Inteligência Artificial e Espaço, já que é uma das áreas de foco principal da Darkmatter.

Para começar, vou só garantir aqui um problema, um problema básico. Usamos muito a palavra "inteligência artificial" e sempre que estamos envolvidos em alguma invocação com os nossos clientes, temos este problema principal na segunda palavra. A segunda palavra, "artificial", não há grandes dúvidas, não é? Na primeira palavra há muitas dúvidas. O que é que é "inteligência"? O que é que isto quer dizer? Quem já tem muito tempo na indústria, sabe perfeitamente que esta palavra foi usada para 30.000 coisas diferentes. E hoje em dia estamos, de facto, a falar de um tema ou de um ângulo diferente. Não é nada de novo na inteligência artificial, que esse sim tem tomado conta, se bem que os anteriores continuem a ser válidos. Então, só para desambiguar, aqui, um bocadinho. Inteligência, não é? Eu vou estar mais a falar sobre uma perspetiva de inteligência geral, das novas tecnologias gerais, sendo que as ferramentas anteriores, de tecnologias que têm capacidade de fazer previsões, têm capacidade de aprender, continuam a ser tão válidas hoje como sempre e ainda mais, não é?

Mas vamos então começar. Sou o CEO da Darkmatter. Nós trabalhamos com inteligência artificial em áreas difíceis. Gostamos de nos meter em problemas, basicamente. Nos últimos meses, neste último *quarter*, foram 24 biliões de dólares investidos em novas empresas de inteligência artificial, no mundo. A maior parte delas estão a fazer trabalhos muito semelhantes. Estão todas a trabalhar para criar mais conteúdos de redes, criar mais *bots*, criar mais sistemas automatizados. O que acontece é que nós vimos que havia oportunidades em alguns setores difíceis e um setor difícil era o setor em que nós temos bastante interesse, que era o setor aeroespacial, que se alastra, não é? Temos alguns clientes já nesta área, a pilotar algumas tecnologias, que vou falar um bocado, rapidamente, sobre isto tudo. Sim, alguns projetos em que eu, pessoalmente, e a Darkmatter estamos envolvidos, que vão desde utilizar inteligência artificial no desenho, utilizar inteligência artificial na operação e utilizar inteligência artificial na decisão. Ou seja, diferentes ângulos. Vamos ver se conseguimos explicar

todos estes ângulos em dez minutos.
Portanto, *design*, não é? Eu estou aqui, na parte do *design*, a incluir a manufaturabilidade, a cadeia do valor, essa coisa muito complicada que acontece desde a ideia até à realidade, que é ambicioso. Depois a operação, a dificuldade de nós conseguirmos mostrar como funciona, todo um sistema na cabeça de pessoas muito inteligentes, mas, que mesmo assim, já estamos a chegar um bocado ao limite, e depois as decisões. Os seres humanos não decidem bem com muita informação. Entramos numa coisa chamada "*analysis paralysis"*, não é? Começamos a analisar, a analisar, a analisar e depois não conseguimos tomar uma decisão e adiamos ou eventualmente decidimos à força.
Começando pelo *design*, isto é uma área em que nós trabalhamos. O que nós vimos é que há uma oportunidade muito grande, principalmente nos nossos sistemas grandes de espaço, para mudar como é que se desenham arquiteturas. Os sistemas do espaço são desenhados, cada vez mais, com um modelo mais ou menos semelhante entre as várias grandes empresas, que é o *modelway systems engineering*, em que centenas de engenheiros escrevem requisitos para esse sistema, que, basicamente, são frases sobre como o sistema deve funcionar. Uma delas diz, por exemplo, que os satélites têm que ter uma massa não maior do x, a largura de banda, no terminal do cliente, não pode ser maior que y. Isto pode expandir-se até 10.000 requisitos de sistema, por exemplo, para um dos nossos clientes. Nenhuma das pessoas dentro de uma empresa destas tem na sua cabeça os 10.000 requisitos. Ora isto é um problema. Vem um cliente e diz: o meu navio tem um diferente tipo de mecanismo ou um diferente tipo de antena ou um diferente tipo de terminal. Esse tipo de perguntas dá cabo da equipa. Porque a equipa vai ter de pegar em toda a gente que está envolvida, em todos os requisitos que são afetados por aquela pergunta, fazer uma análise de impacto. Isso poderá demorar três meses, quatro meses. Para uma empresa de vários milhões anuais, centenas de milhões, neste caso, é algo muito custoso, não é? Não estamos aqui a falar da substituição do trabalho humano, mas estamos a falar do aumento do trabalho humano. Pegámos nas ideias que nós já conhecemos, ideias profundamente enraizadas na nossa indústria, como é que se montam coisas, como é que se desenham coisas, como é que se juntam cadeias de valor, e a pôr a inteligência artificial, no fundo, a controlar os vários mecanismos de baixo nível. Isto é o que nós estamos a ver de mais interessante. Atenção, para desambiguar, outra vez aqui. A inteligência é uma coisa muito difícil. Mesmo estes sistemas são altamente falíveis, se não forem usados

corretamente. Uma coisa que nós garantimos aqui e que eu acho que é uma coisa que eu queria passar, acima de tudo, é que o conhecimento de domínio é muito importante e estes sistemas de inteligências gerais são muito bons em generalidades, mas quando estamos a afunilar sobre uma determinada vertical, caímos rapidamente no problema de precisão. E tal como nós, como eu aqui, se estiver a falar de coisas muito interessantes, ainda bem que os dez minutos estão a ser limitadores, eventualmente, começamos a juntar buracos que temos na nossa cabeça, usando palavras que não são, necessariamente, as mais adequadas, que nesta indústria se chamam alucinações. Portanto, o que nós fazemos é dar ferramentas para os sistemas de inteligência artificial, para que eles tenham de usá-las para as suas conclusões, tal como nós usamos calculadoras, tal como nós usamos os computadores? Nós somos inteligentes, mas não somos assim tão precisos. Temos o mesmo tipo de problemas e neste caso estamos a falar de coisas semelhantes. Uma das áreas interessantes que nós estamos a ver, principalmente, tem a ver como é que se desenham estes sistemas grandes, em iterações mais rápidas. Enquanto nós fazemos as nossas análises de engenharia, nós não conseguimos fazer as análises de concorrência. Nós não conseguimos estar a trabalhar nas duas coisas ao mesmo tempo. E agora estamos a querer fazer as duas coisas, porque, de repente, nós podemos estar a decidir sobre se vamos utilizar um determinado subsistema, não só porque o cliente pediu, mas porque a concorrência está a implementar uma outra solução. Ou seja, estamos a elevar o potencial humano. Esta é atualmente a nossa ambição.

Operações: só um bocadinho de contexto. O Major-general já deu aqui muitíssimo contexto sobre a indústria. Eu não vou estar aqui a ir muito mais longe no contexto da indústria. O nosso mundo está a mudar em alguns assuntos chave. Tem a ver com duas tecnologias-chave, à partida. Não são propriamente tecnologias novas. Uma delas tem a ver com esta capacidade que a Space-X está a ter, cada vez mais, de lançar massa para a órbita baixa, a preços cada vez menores e em quantidades cada vez maiores, durante o ano. A Space-X já é responsável por 80 % de todos os lançamentos durante o ano e vai continuar a aumentar, provavelmente, mesmo que nós europeus tentemos lançar estas novas *start-ups* que estão já a conseguir fazer alguns lançamentos, nomeadamente a TDL Space e a HyImpulse; temos dificuldade em competir e vamos ter, provavelmente, durante não sei quanto tempo. Muito tempo. Portanto, neste momento, vemos um futuro em que vamos conseguir lançar cerca de 150

toneladas por foguetão, para a órbita baixa. Se fizermos mil lançamentos por ano, que é o Elon Musk quer fazer, façam as contas. Estamos a falar de insfraestrutura pesada. Também já ouviram falar sobre estas redes novas. A Starlink é a mais conhecida. Não é a única. Obviamente, esta é a nova insfraestrutura. Não estamos a falar só de Internet. Estamos a falar de todo o tipo de comunicação. Os cabos marítimos continuam a existir, claro. Mas imaginemos que há cada vez mais interesse nas novas forças políticas a participarem na infraestrutura nova, em conseguirem fazer uma espécie de *bypass* às várias limitações das infraestruturas atuais e, no fundo, aliarem-se a estas tecnologias. Estas redes estão a ser lideradas por empresas, neste momento. Empresas, uma delas, uma grande, a Eutelsat, que adquiriu a defunta Oneweb, que está a competir no espaço da Starlink. Outras, como a Eutelsat, que estão a competir, também, com as suas próprias constelações, com propósitos diferentes. Vamos ver cada vez mais disto. Estamos a falar de mais ou menos 7.000 satélites, neste momento, em novembro. No próximo ano, se conseguirmos ter a Starship a funcionar, provavelmente este número pode duplicar, vamos ver se eles conseguem.

Portanto, estamos a falar realmente de uma infraestrutura completamente desconectada, não é? A operação de uma infraestrutura assim é um bocado caótica. Este slide aqui é de propósito para confundir. Não tentem ler, nem eu, se calhar, daqui, consigo ver muito bem. Isto é mesmo só para percebermos o quão complicado estas ameaças híbridas podem ser. Isto é neste momento. A complexidade vai aumentar ainda mais. E, acima de tudo, vamos estar a ver que estes diferentes pontos, cada um deles, no fundo, é um *chip*, é um GPUzinho, eventualmente, capaz de correr o modelo localmente. Aqui, estamos a falar de um modelo de inteligência artificial a fazer as suas próprias decisões ou apresentar as suas próprias decisões, caso o ser humano ainda se mantenha no *loop*. Será que na ameaça, como já foi falado, será que vamos ter o tempo para que o ser humano decida? E, realmente, quando as coisas são apertadas, a decisão pelo ser humano o pode ser um problema.

Trouxe aqui alguns exemplos de *dual-use* que são interessantes. Os satélites estão a ser desenvolvidos em massa, claro, comercialmente, mas muitos deles têm esse *dual-use*. Em particular, foram desenvolvidos sistemas para mitigar o tal lixo espacial que já foi falado aqui, mas que tem um outro interesse, claro, esse menos comercial ou, digamos, para o bem comum, que tem a ver com os satélites passarem a ter a capacidade de agarrarem-se a outro satélite, desorbitarem-no, literalmente, tomarem conta dele, fazerem esse tipo de coisas,

não é? Tal como os drones cá na terra ou os barcos em alto mar, mas isto no espaço. Um exemplo prático e real. Isto é um satélite em órbita geo. É gigante, não é? É um satélite russo. A Slingshot, que é uma empresa americana que faz o *tracking* de vários corpos no espaço, reparou que ele estava a sair do sítio. Estava a sair da sua posição registada na órbita de geo e estava a mover-se à frente de outros satélites que estão ali, a pagar bastante para terem aquela posição. Claro que o satélite não toma decisões sozinho, ainda são os seres humanos. Mas estamos a ver o que é que pode acontecer se, de repente, os satélites começarem a fazer estas decisões sozinhos. Além disso, como já falámos aqui, existe uma série de outras capacidades que os satélites já tem.
Vou falar agora mais sobre esta parte das decisões. Não só a inteligência artificial criou um novo paradigma, que é este paradigma: já devem ter ouvido falar da palavra *transformers*, é o T no GPT. É basicamente, uma maneira de conseguirmos fazer um modelo que consegue relacionar coisas. É assim uma boa analogia. É uma arquitetura muito específica e o que se faz, regra geral, na computação, é quando uma arquitetura funciona muito bem, alguém eventualmente, arranja maneira de fazer um *chip* que corre aquela arquitetura melhor. E é o que estamos a ver, cada vez mais. Há novas propostas, cada vez mais potentes, de ter sistemas dedicados a estas arquiteturas, estas inteligências todas correrem, praticamente, instantaneamente, e a custo zero. Isto faz com que em vez de precisarmos de um *data center* para correr um Chat GPT, podemos ter uma coisa tão pequena como um telefone. Isto já acontece. Já temos modelos desses. Não são assim tão bons, mas é possível e é altamente credível que nos próximos anos isso deixe de ser verdade. Portanto, miniaturização total e a maturação destes *chips*, vai fazer com que, não só estejam em todas as coisas cá na Terra, mas também no próprio espaço. Portanto, teremos mini Chat GPT em todo o lado, e isso já está a ser projetado. Temos aqui empresas como a Lumen Orbit e a Planet que estão envolvidas com a Nvidia, a fazer uma grande *trend* que é "*data centers* no espaço". Vamos ver se funciona, mas a ideia é simples: para processar infomação no espaço, normalmente, faz-se um *trade-off*, faz-se aqui um compromisso, em que o processamento ainda está feito no chão, não é? Isso faz com que dependemos de território, dependemos de antenas que estejam no chão, em determinados países, etc. Portanto, depende de quem são os nossos aliados, os nossos satélites, etc. Mas isso é uma coisa que carece de ser mudada. Tal como, de repente, temos a Internet no espaço, no futuro também vamos ter os *data centers* no espaço. Vamos ter, provavelmente, uma série de

infraestruras que nós normalmente associamos a *real estate* terrestre, vamos tê-lo lá em cima e tudo o que seja possível pormos dentro de um satélite vai estar lá em cima e, neste caso, a Lumen Orbit apresenta uma solução que usa painéis solares para, basicamente, ter energia de graça e não pagar renda, que é uma das coisas problemáticas de quando se quer ter um grande *data center*. Vamos ver se economicamente é viável. Eles já reuniram fundos bastante grandes para fazer isso.

O que é que se faz com esta potência toda, com esta capacidade toda? Bem, para já, o que está planeado é aumentar a capacidade de os satélites conseguirem… primeiro, comunicarem, é uma coisa importante, claro. Isto é a primeira tecnologia que foi, no fundo, usada para o espaço comercialmente e é a maior de todas a que está no espaço em termos comerciais, se não incluirmos coisas como o GPS. Mas uma segunda, que é muito interessante, é termos "olhos" fantásticos no espaço. Digamos que uma grande parte das imagens que são recebidas no chão são só oceano azul, sem interesse. É um dilema clássico da observação terrestre. Um dos paradigmas que está a ser mudado é que os satélites, de repente, não respondem só com uma imagem do oceano azul, mas só quando detetam o objeto que estamos à procura. E só respondem aí. E porque é que isso é importante? Porque quer dizer que o satélite não tem que estar a perder tempo de processamento e energia a fazer tudo o resto, tudo o resto que são "toneladas" de bytes, que são gigabytes e muita energia e muito tempo perdido, principalmente, para a questão de resposta. Se queremos responder rapidamente, temos de tentar alguma coisa… estes sistemas vão responder com o produto, digamos, não com *data*.

Isto é só uma visão como o segmento do espaço está relacionado com todos os outros segmentos. Tal como nós estamos a fazer um sistema de desenho para uma constelação, todas as outras áreas estão ligadas ao desenho dessa constelação e a todas as outras empresas que estão, também, interessadas em participar nesse sistema. E há aqui um detalhe que acho interessante, tal como estivemos a falar agora, ou seja, a infraestrutura. A própria infraestrutura de GPS está a receber concorrência, não é? Digamos que, tal como estamos a ver a miniaturização da tecnologia dos drones, tal como o Major-general falou, fazer um drone-míssil-bomba, enfim, arma, é cada vez mais barato. Fazer satélites é cada vez mais barato. Já vimos que pôr um satélite na Starship vai ser cada vez mais barato. Vai estar acessível a cada vez mais empresas, pessoas com dinheiro, para porem satélites em órbita e fazerem a sua própria rede de

infraestrura, seja ela uma competidora com qualquer uma das organizações que tradicionalmente eram governamentais, como o GPS. O GPS decide, ou melhor, o sistema é decidido por, neste caso, os Estados Unidos, que fez com que certos países tivessem de desenvolver o seu próprio sistema, aliás, como a Galileu e como a China. Mas, no futuro, isso não vai ser necessariamente verdade. Uma empresa pode ter o seu próprio sistema de posicionamento sem prestar contas a ninguém.
E, pronto, aqui a proposta é muito simples. É que num futuro próximo não vamos estar a falar de substituição do trabalho humano. Não é isso. Os seres humanos continuam a ter, no fundo, a proposta de valor. Mas é a ideia de que os sistemas muito complexos, já como foi falado aqui até agora, hão-de ser cada vez mais geridos por seres humanos a trabalhar com inteligências. Inteligências que têm de ser desenvolvidas, idealmente, pelos agentes que têm interesse em ter esses sistemas. Isto porquê? Acho que a McKinsey fez um *report*, revelando que, em Portugal, tivemos um aumento de 57% de adoção de inteligência artificial em empresas. Isso parece ótimo. Mas nenhuma daquelas empresas, exceto uma minoria, está de facto a usar, software europeu. O software é quase 100% ou da Open AI ou, se tiver alguns pedidos de privacidade, provavelmente da Meta, que faz os modelos *open source*. Portanto, nós não estamos na cadeia de valor. Nós estamos na cadeia de consumo. E isso é um dos grandes problemas ainda muito verde e que nós que estamos a atacar, um bocado ambiciosamente, que é o dos sistemas complexos. Obrigado.

Coronel António Eugénio

Muito obrigado, João Montenegro, por trazer-nos aqui um admirável mundo novo, para esta discussão. Para finalizar este painel, tenho a honra de apresentar o senhor Coronel Penha Gonçalves, que tem uma carreira militar de relevo e também científica. Portanto, o tema é a Biotecnologia e vamos ver que, de vez em quando, há momentos da História em que há co-evolução de diversos setores tecnológicos e que, provavelmente, estaremos num momento desses.

Coronel Penha Gonçalves

Muito obrigado. Muito bom dia a todos. Eu gostaria de começar por agradecer à Professora Isabel Ferreira Nunes, Diretora do IDN o convite para aqui estar e

também ao Senhor General Valença Pinto, também, este convite. É sempre com muito agrado que venho ao Instituto da Defesa Nacional e vou falar sobre Biotecnologia. Por esse motivo, eu vou começar por mostrar um slide que mostrei nesta mesma sala há 12 anos. E o slide é este. O argumento que eu queira fazer na altura era que no Século XIX, quando foi começada a descrição das ligações químicas e da natureza química de muitas dessas ligações, esse conhecimento passou à indústria e cerca de 50 anos depois nós assistimos à utilização de agentes químicos em cenários de guerra. O Século XIX foi chamado o Século da Química.

No princípio do Século XX, começaram a distinguir-se os primeiros modelos e a propor os primeiros modelos da formação dos núcleos das substâncias, dos protões, dos neutrões, etc. Cerca de cinquenta anos depois disso ter acontecido, a energia atómica foi usada em cenários de guerra. Foi mais ou menos há 50 anos que se descobriu o código genético e a estrutura do DNA. E, nessa altura, há 12 anos, quando eu fiz esta comunicação aqui no IDN, este senhor que se chama Craig Venter [no slide], tinha feito, pela primeira vez, um organismo completamente sintético. Sintetisou o DNA e a partir daí criou uma bactéria e, por isso, a mensagem que eu queria transmitir na altura era esta que está aqui e que agora é uma citação de um ex-comandante de um regimento NBQ da Grã-Bretanha que diz que o século XXI vai ser o século da Biologia e das ameaças biológicas.

O que é que aconteceu há umas semanas? O Prémio Nobel da Química foi dado a estes três investigadores [no slide]. Dois deles, o Demis Hassabis e o John Jumper vêm do University College of London, formaram uma empresa que se chama DeepMind e esta empresa queria utilizar inteligência artificial para definir a estrutura tridimensional de proteínas. Nós sabemos, desde há muito tempo, do código genético, como é que do DNA passamos para uma proteína. Mas o que faz a função das proteínas é a sua estrutura tridimensional e as regras por que isso se cria não são conhecidas. Normalmente, demoraria, há meia dúzia de anos, muitos meses num laboratório de cristalografia de raios X para determinar a estrutura de uma proteína. O software que estes senhores desenvolveram, baseado em inteligência artificial e não vou entrar na semântica da inteligência artificial, que se chama AlphaFold, que agora vai na sua terceira versão, determina a estrutura de uma proteína em segundos. E, neste momento, todas as proteínas que são conhecidas nos seres vivos, todos, que foram estudados até agora, que são cerca de 220.000, este software já determinou a estrutura

tridimensional de todas essas proteínas. O David Baker, que vem da Universidade de Washington, o que ele fez foi uma coisa interessante. Quis usar inteligência artificial para produzir proteínas artificiais, que façam coisas que as proteínas normalmente não fazem e que a gente pode querer que elas façam. E, portanto, as consequências de produzir novas proteínas para conseguirmos degradar poluentes ambientais, criar novos medicamentos, é imensa. As consequências desta tecnologia são quase inimagináveis. Mas uma coisa é certa e está ali escrita, é que isto é tudo *open source*. Qualquer pessoa, no mundo, hoje em dia, pode desenhar uma proteína nova com funções e propriedades que nós não conhecemos.

Este é um estudo ou uma análise que foi feita sobre a indústria biotecnológica, sobretudo nos Estados Unidos. Analisou mais de 4.000 *startups* e empresas emergentes. E o que é que eles tentaram perceber? O que é que estas empresas andam a fazer? E focaram-se ou convergiram em dez tendências: inteligência artificial, *big data analysis*, *gene editing*, emfim, uma série delas e eu pus aqui num círculo a Biologia Sintética, porque é aquela que do ponto de vista da segurança, no sentido do que o Senhor Major-general nos disse há pouco, de uma perceção de que nos podemos sentir seguros, nos provoca mais problemas. Então, o que é que é isto da Biologia Sintética? O ciclo é muito simples, começamos com um computador a desenhar o organismo que queremos fazer, construímos esse organismo na base de um organismo que nós chamamos *chassi*, testa-se se ele realmente faz aquilo que a gente quer ou não, analisa-se os resultados e depois volta-se ao ciclo. E fazendo esse ciclo vamos gerar cada vez mais componentes que são sintéticos do ponto de vista biológico. E o mercado, nos Estados Unidos, está a crescer desta maneira. E eu quero chamar a atenção para este gráfico para esta parte roxa do gráfico que diz respeito aos organismos que vão estar disponíveis por empresas, comercialmente, e que podem receber DNA estranho e modificar e criar micro-organismos e organismos com propriedades que nós desconhecemos. Como é que estas empresas estão distribuídas? Estão distribuídas, sobretudo, na costa oeste e na costa leste dos Estados Unidos e, também, de alguma maneira, na Europa. Cria um problema. São 4.000. E há um problema das autoridades em tentarem rastrear o que é que estas empresas andam a fazer. Porque elas vendem-se umas às outras, alguém as compra, alguém as vende e não se percebe bem o que é que elas andam a fazer. E isto cria um problema às autoridades. Mas há outras abordagens a este tema. A China, durante os últimos 20 anos, decidiu ser um líder na área da

Biologia Sintética. Estes são os departamentos de universidades que são financiados pelo Estado chinês e que desenvolvem atividades na área da Biologia Sintética [no slide]. Só que, ao contrário do que acontece no Oeste, isto não é *open source* e eles já têm regulamentos internos para proibirem a exportação ou restringirem a exportação das tecnologias que eles desenvolvem e, portanto, nós ficamos sem saber, realmente, o que aquilo é. Isto é só uma fotografia de um destes institutos que ficou muito famoso durante a pandemia, que é o Wuhan Istitute [no slide]. Então, o que é que se está a passar? O mercado SynBio, ou da Biologia Sintética, em 2000 era dominado pelos Estados Unidos. Em 2019, a China já tinha um *share* maior do mercado global do que o dos Estados Unidos. Na China, a jusante daqueles departamentos estatais que eu há bocado mostrei, existiam, em 2023, 925 empresas de média e grande dimensão. Já não estamos a falar de *startups*. Muitas delas com financiamento inicial do Estado. O que é que eles produzem? Aquilo que se chamam *tools*, que são os tijolos iniciais, vou-lhe chamar assim, para se conseguir fazer Biologia Sintética e depois estão muitos focados em gerar produtos para vender no mercado. Portanto, o que é que nós temos aqui? Temos uma situação em que, por um lado, no Ocidente temos uma certa dificuldade em mapear o que está a acontecer e, por outro lado, noutras regiões do mundo, temos uma certa opacidade sobre o que está a acontecer. E, portanto, temos de desenvolver mecanismos para controlar, de alguma maneira, estes riscos, por parte das autoridades.

A propósito e para terminar, quero deixa aqui dois pontos. O primeiro ponto é este: a única maneira que nós temos para lidar com um organismo de que não conhecemos as características são os chamados laboratórios de contenção máxima. E eu quero que vocês notem que até ao ano 2000 existiam no mundo meia dúzia destes laboratórios. Nos últimos 20 anos aconteceu isto: eram mais de quarenta. Eles estão aqui mapeados, estes quarenta e tal laboratórios [no slide]. O que se passa neste momento é que já há, para além destes quarenta, há, neste momento, cinquenta e um laboratórios BCL-4, portanto, são estes de contenção máxima, de nível quatro, operacionais no mundo. Há três em construção e há quinze que estão planeados. Já vinte e sete países têm estes laboratórios. Portugal ainda não tem nenhum, como vêem naquele mapa. A Espanha já tem, apesar de ainda não estar ali mapeado. E eu quero só aqui fazer uma pequena reflexão. E eu vou dizer isto muito claramente, porque as coisas são o que são; com o impulso do Senhor General Valença Pinto, em 2006 foi tomada a decisão de fazer um laboratório BCL-3 em Portugal, no Exército. Na

altura em que isso foi feito, havia um laboratório ou dois no Ricardo Jorge parecido com BCL-3, mas que realmente não davam as mesmas garantias que o laboratório que foi construído no Exército. Uma dúzia de anos depois disso, em 2019, esse laboratório do Exército era dos únicos sítios em Portugal onde se conseguia fazer um PCR para a Covid-19. E esse laboratório fez coisas que são conhecidas e coisas que, se calhar, são menos divulgadas, que foram muito importantes nessas primeiras semanas e meses, porque essas primeiras semanas e meses são as semanas em que ninguém sabe nada e toda a gente tem medo de tudo. E é isso que é crucial, termos capacidade de atuar. O Exército tem um plano para fazer um laboratório BCL-4. Os papéis andam para cima e para baixo. A decisão não se toma. E a pergunta que eu deixo é esta e é muito simples: se num período de tempo futuro, mais longínquo ou menos longínquo, Portugal tiver necessidade de ter um laboratório destes, de contenção máxima, e não tiver, o que é que as autoridades vão dizer aos portugueses? Que acharam que não era preciso? Que havia outras prioridades? Uma coisa não podem dizer: é que não sabem quais são os riscos e quais são as ameaças. Isso não podem dizer, porque toda a gente sabe quais são.

Eu quero deixar um último ponto. E vou acabar com um slide que também mostrei aqui há doze anos. É este slide sobre a autoridade estatal. Existe uma Convenção das Armas Biológicas que, de alguma maneira, em termos internacionais, dá uma cobertura legal àquilo que são as atividades na área da Biossegurança que os Estados podem ou não podem fazer e o modo como as têm de controlar. Há cento e tal países que já assinaram esta convenção, alguns ainda não assinaram, mas isso é irrelevante para o meu ponto. O ponto é que esta convenção estimula os Estados a fazerem controlo de Biossegurança no seu território. Eu vou tentar dizer isto com cuidado. Neste momento, existem em Portugal, depois daquele período desde 2006, mais de trinta laboratórios de segurança biológica de nível três, que, mais ou menos, se auto-regulam. O Estado não tem nenhuma supervisão sobre aquilo. O Exército tomou a iniciativa, em 2007, 2008, 2009, eu não consigo precisar bem, de propor a implementação de uma Autoridade Nacional de Defesa Biológica. É um processo complexo, eu compreendo. Inclui o Ministério dos Negócios Estrangeiros que, aliás, está a pilotar o assunto, o Ministério da Defesa, o Ministério da Saúde, o Ministério da Ciência e Tecnologia. São muitos parceiros que têm de estar em conjunto para tomarem esta decisão. Passaram quinze anos e nós ainda não temos um documento legal para a implementação desta Autoridade Nacional, que também

é importante para outros regulamentos internacionais, nomeadamente o Regulamento Internacional Sanitário que obriga os países a terem controlo sobre aquilo que se está a passar no seu território. Passaram quinze anos e ainda não há nada. Se passarem vinte anos e nós não tivermos uma Autoridade Nacional de Defesa Biológica eu vou começar a pensar que o processo está a ir um bocado devagar.
Muito obrigado.

Coronel António Eugénio

Muito obrigado, Senhor Coronel Penha Gonçalves pela excelente apresentação e também pelos alertas que lançou que, ao fim e ao cabo, também são partilhados pelas outras áreas setoriais. Se quisermos identificar uma linha comum às intervenções deste painel é exatamente a característica citentífico-tecnológica que estas matérias trazem e também a necessidade dos responsáveis tratarem destas áreas, de investigação científica, a própria divulgação e o alerta a quem decide. Portanto, isso transforma-se, ao fim e ao cabo, num problema comunicacional da comunidade científica para a parte política e também quem utiliza os diversos setores que, de facto, temos pela frente e veremos isso, também, depois, na parte do segundo painel. De facto, a comunicação estratégica e a decisão estratégica é fundamental nos tempos que correm. E eu abriria agora o período de debate, já estamos um bocadinho atrasados, mas ainda há tempo para duas ou três questões. Peço que se identifiquem e que sejam breves.

Comandante António Mourinha

Bom dia. Sou o Comandante António Mourinha, até há pouco tempo, o Diretor do Centro de Experimentação Operacional da Marinha e principal responsável do Exercício REPMUS. Neste momento, sou assessor de inovação do Senhor Chefe de Estado-Maior da Armada. Agradeço esta excelente conferência e toda a informação que tem sido aqui passada e gostaria de lançar aqui uma questão a todos os painelistas e que tem a ver com o seguinte: considerando algo que já foi levantado aqui, que a tecnologia altera as relações de poder, trazendo assimetria para o poder; considerando, também, que o poder é o produto da vontade e da capacidade, que também foi aqui referido; considerando que as

tecnologias e designadamente a inteligência artificial têm uma capacidade enorme de alterar a vontade, incluindo coisas tão simples, como, por exemplo, o Tik Tok, que pode ser perfeitamente utilizado até junto das crianças, talvez aqueles que são mais frágeis, neste âmbito, e moldando-lhe a vontade e a capacidade de pensar; e considerando ainda a necessidade de os países, em termos de capacidade, desenvolverem soberania tecnológica, que é algo que é fundamental. Não se falou ainda muito, mas existe uma guerra de chips. Portanto, sem chips nós não conseguimos desenvolver muita coisa e quem diz chips, diz outras áreas. E tudo isto são problemas e ameaças, mas eu julgo que este fator assimétrico que a tecnologia traz poderá beneficiar Portugal, por Portugal considerando o nosso tamanho e, enfim, a população, poderá beneficiar desta nova onda tecnológica. Portanto, a questão que eu coloco é o seguinte: já se falou muito de ameaças, quais são, nas vossas opiniões, as forças e as oportunidades que o país tem para podermos avançar e desenvolvermo-nos neste âmbito. Obrigado.

Professor Bruno Oliveira Martins

Bom dia. O meu nome é Bruno Oliveira Martins. Sou investigador no Peace Research Institute Oslo, na Noruega, mas também aqui no Instituto da Defesa Nacional. Gostava de lhe perguntar em relação à questão da Biotecnologia, a área da Biotecnologia é uma das áreas onde historicamente e ao longo das últimas décadas se assistiu a mais debates acerca de como regular o desenvolvimento tecnológico, tentar saber onde é que se podem traçar as linhas vermelhas. O modelo de Asilomar de autorregulação foi suficiente num período, mas, de certa forma, não corresponde aos desafios atuais. Já referiu a questão de como a inteligência artificial vem alterar as regras do jogo. No fim da sua apresentação, de forma muito interessante, falou dos problemas de regulação que existem neste momento, focou-se no caso de Portugal, muito importante, mas, a nível internacional, o que é que nos pode dizer mais acerca de onde é que se podem colocar barreiras, como é que se podem colocar barreiras, se se devem colocar barreiras, etc. Obrigado.

Coronel António Eugénio

Eu penso que podemos começar por esta questão, uma vez que lhe é dirigida.

Senhor Coronel Penha Gonçalves.

Coronel Penha Gonçalves

Muito obrigado pela questão. A questão é interessante. Tem vários ângulos. Eu vou começar pelo ângulo mais difícil, que é este. A regulação nesta área começou no tempo do presidente Obama, por gerar um instrumento que pudesse controlar acidentes biológicos naturais. Nós estamos a falar de Biologia Sintética, mas acidentes biológicos naturais que viessem a acontecer no mundo, inclusivamente pandemias, como mais tarde se veio a verificar que realmente aconteceu. Esse instrumento foi muito importante e Portugal até foi um dos poucos países que no início esteve nesse processo. Eu estive também envolvido nesse processo. Mais uma vez, quem pilotava isto era o Ministério dos Negócios Estrangeiros, para mapear quais eram as capacidades de resposta aos países que têm ameaças biológicas. No fundo, era isso que se pretendia fazer. O projeto cresceu ao longo de alguns anos e foi transferido para as Nações Unidas e agora chama-se o Instrumento, chama-se mesmo assim, Instrumento do Secretário-Geral das Nações Unidas para estas Situações Biológicas e Portugal tem uma parte muito ativa nesse instrumento. Com as novas evoluções, digamos assim, das forças e dos jogos de força das relações internacionais, como foi aqui referido pelo nosso Major-general Arnaut Moreira, nós ficamos sem saber se agora as Nações Unidas têm capacidade suficiente para se imporem aos países. Isto é uma parte da questão. Outra parte da questão é um bocadinho mais centrada naquilo que disse. Eu sou, ao mesmo tempo, um académico e um militar e, portanto, tenho esta duplicidade de considerar que a instituição deve ser livre, deve ter o mínimo de barreiras possível, para poder ser inovadora e trazer mais soluções para a nossa sociedade, mas tenho também a componente militar que me diz que as coisas têm de ser feitas numa certa área de perceção de segurança, certo? Não é muito fácil resolver esta equação em nenhum domínio e em Biologia ainda muito menos. Quando nós estamos a restringir alguma coisa na área da Biologia, podemos estar a dizer que não estamos a conseguir desenvolver medicamentos, não é? Que não estamos a encontrar curas para doenças. Portanto, é um território muito difícil e muito fino. Mas há uma coisa que nós podemos fazer, é ter, realmente, supervisão. Não proibir nada, mas ter supervisão sobre o que está a acontecer. Os Estados têm de ter uma visão, uma visibilidade, digamos assim, sobre aquilo que está a acontecer e sobre aquilo que

está a nascer e naquelas áreas que acharem que é precisamente necessário regular e eu vou dar o exemplo da clonagem humana: regula-se. Mas, para isso, temos de perceber se estão a clonar humanos ou não, portanto, temos de ter visibilidade sobre o sistema. Isto quer dizer visibilidade sobre o que está a acontecer nas universidades, visibilidade sobre o que está a acontecer nas empresas e a visibilidade possível que os outros países nos quiserem dar sobre aquilo que estão a fazer. Eu não me vou alongar muito mais.

Coronel António Eugénio

Muito obrigado, meu Coronel. E agora para responder, de uma forma abreviada, uma vez que já ultrapassámos largamente o nosso tempo, à primeira questão, do Senhor Comandante António Mourinha eu passo a palavra ao Senhor Professor Armando Pinto.

Professor Armando Nolasco Pinto

Muito obrigado pela questão. Eu gostaria de responder porque, de facto, nós temos, durante este painel, salientado aqui muitas questões, muitas ameaças que a tecnologia traz. E eu acho que, no caso das tecnologias quânticas, há também muitos ganhos que a tecnologia traz. Ou seja, a grande motivação por trás do desenvolvimento, por exemplo, do computador quântico, não é, propriamente, para quebrar os sistemas criptográficos atuais. É para resolver problemas que nós temos, que são irresolúveis usando computadores clássicos, e isso pode trazer muitos ganhos. Mas quando nós falamos, na primeira apresentação do senhor General por exemplo, naquela questão dos dispositivos, quando a gente compra um dispositivo, não sabe, exatamente, se ele faz só aquilo que é suposto fazer. Por exemplo, essa é uma área da criptografia quântica que o quantum também pode trazer que é nós passarmos a ter dispositivos em que os pressupostos de segurança são mínimos, ou seja, nós pegamos no nosso dispositivo, não interessa o que está dentro da caixa, desde que eu consiga fazer um conjunto de coisas mínimas e, portanto, nós conseguimos isto com, por exemplo, o entrelaçamento, eu sei que aquele dispositivo é seguro. Ou seja, a tecnologia pode ser também uma ameaça, mas também serve para nos protegermos. Agora, uma questão que eu acho que é a mais crítica de todas, e tem um pouco a ver, também, com esta questão da

regulação; de facto, hoje, a tecnologia está disponível em todo o lado e está disponível a preços muito acessíveis. Eu vou fazer aqui uma inconfidência; eu acho que a minha mulher não se vai importar. Ela é vereadora numa câmara municipal e está responsável pela área social e pela área da educação. Só para vocês verem os problemas que isto levanta num caso que não tem nada a ver. Eles organizam na área de educação, agora, no Halloween, concursos de bonecos relativos ao Halloween e depois põem no Facebook e fazem uma votação. E depois, também há pouco tempo, nos lares, organizaram um concurso de fotografias e puseram no Facebook para fazerem uma votação. Em ambos os casos, foram contratadas empresas estes *botfarms*, para falsearem as votações. Reparem que nós estamos a falar de uma coisa que não há motivação nenhuma. Só que está tão disponível ali, que as pessoas fazem isto e, depois, obviamente, que aparecem mil coisas de um fenómeno esquisito. Só para termos a ideia de quão disponíveis as coisas estão. E, de facto, esta questão da regulação é muito complexa e eu, de facto, não me quero alargar muito, porque não tenho uma resposta cabal para isso, porque eu acho que é demasiado complexa, para nós sabermos até que ponto é que a regulação restringe o avanço da própria ciência, mas até que ponto é que a regulação é necessária para garantir a própria sobrevivência da espécie humana. Eu acho que é bastante complexo.

Coronel António Eugénio

Muito obrigado, Professor Armando Pinto. E, de facto, este é um tema que mereceria um painel muito mais longo, mas temos de cumprir o horário que está previsto, até porque o próximo painel vai ser ainda mais interessante e, como tal eu dou por concluído e agradeço aos oradores deste painel e convidava a audiência a contribuir com uma salva de palmas.

3.4 – Painel 2 – Dissuasão e Resiliência às Ameaças Híbridas

Retomamos o com o segundo painel que tratará da dissuasão e resiliência às ameaças híbridas. O painel será moderado pelo Coronel Agostinho Paiva da Cunha, Secretário-Geral do Eurodefense Portugal.

Coronel Agostinho Cunha

Bom dia a toda a gente. É um prazer estar aqui a coordenar este painel com entidades que vão falar de várias áreas sociais e partilhar as suas perspetivas relativas à dissuasão e resiliência às ameaças híbridas. Eu vou fazer a apresentação de cada um dos oradores, quando for a sua parte de oração, mas, para já, ficam a saber que temos connosco a Senhora Juíza Conselheira Maria Helena Fazenda, temos connosco o Coronel Navegador António Beja Eugénio, que já tiveram a apresentação, temos também o Senhor Jornalista João Carlos Barradas e o Dr. Filipe Santos Costa, investigador do IPRI. Obrigado a todos por aceitarem o convite e por tentarem conduzir a vossa intervenção em apenas quinze minutos e se puderem poupar dois ou três minutos, nós agradecemos. No final, temos ainda um tempo de perguntas e respostas, que espero possamos levar avante com o tempo que vai ser tomado por cada um dos oradores. Eu começaria, então, pelo Senhor Coronel António Beja Eugénio. Não vou fazer a apresentação que já foi feita, mas posso realçar que a sua capacidade em termos académicos, ele também teve uma experiência operacional na área dos P-3 Orion, em exercícios e atividades da NATO.

Coronel António Eugénio

Muito obrigado, mais uma vez, Senhor Professora Isabel Ferreira Nunes, meu General e restante audiência, é um prazer estar perante vós e eu vou tratar de um tema que é um bocado o complemento daquilo que foi tratado atrás, em termos de ameaças tecnológicas e se é possível ou não, eu não tenho uma resposta concreta relativamente a isso, dissuadir agentes maliciosos da utilização de alguns destes métodos.
Parece haver algum consenso sobre qual foi o mecanismo principal que manteve a paz entre as duas grandes superpotências, como então se designava, no período da Guerra Fria e esses mecanismos não foram mais do que a dissuasão nuclear e clássica que funcionou e susteve o confronto direto entre os Estados Unidos da América e a União Soviética.
Depois, na transição para o novo século, o estudo da dissuasão, resumia-se a um exercício essencialmente especulativo sobre a sua aplicação no contexto das guerras irregulares e do terrorismo internacional. Porém, olhando retrospectivamente, podemos interpretar a postura revisionista da Rússia, das últimas duas décadas, como um fracasso da dissuasão clássica e, quiçá, este

seu *modus operandi* como uma resposta híbrida àquilo que percecionou, pelo seu lado, como uma ameaça também ela híbrida ocidental, protagonizada pelas revoluções coloridas e por um alegado expansionismo.

Com a emergência da China e de outros atores políticos de relevo, nomeadamente a Coreia do Norte e o Irão, deu-se um aumento da instabilidade potencial de um sistema que antes só continha dois blocos e onde a dissuasão funcionava.

Confrontados com o alargamento e aprofundamento das questões de segurança, como vimos atrás, com a instrumentalização de setores não convencionais da sociedade e ainda com o desenvolvimento de tecnologias não triviais, como a computação quântica, a inteligência artificial e a biotecnologia, por potências revisionistas e emergentes, os teóricos da dissuasão retomam a sua abordagem na esperança que sirva de guia aos decisores dos diferentes níveis e setores da sociedade. Apesar de toda a colaboração em sede das organizações internacionais, este tema é particularmente sensível pelo facto de as respostas às ameaças híbridas serem essencialmente de responsabilidade nacional.

Numa aliança ou numa união, a vulnerabilidade do todo não é mais do que a vulnerabilidade do seu elo mais fraco, pelo que esta discussão tem toda a atualidade no âmbito nacional, é nós não queremos ser o elo mais fraco.

As ameaças híbridas não são novidade nenhuma. O que é realmente novo é o conjunto de tecnologias e técnicas utilizadas para alcançar os mesmos objetivos de sempre, poder e influência.

Para compreendermos melhor o desafio que temos pela frente, utilizámos aqui o modelo desenvolvido pelo Centro Europeu de Excelência para Combate às Ameaças Híbridas. É uma organização internacional a que Portugal aderiu no final de 2019, para ilustrar as nuances principais da nossa discussão. Este organismo resultou de uma iniciativa do governo da Finlândia, um dos países da linha da frente híbrida, e é apoiado pela União Europeia e pela NATO.

O Hybrid COE considera quatro pilares para compreendermos o panorama das ameaças híbridas. Os atores e os seus objetivos estratégicos, essencialmente estatais e não estatais, os 40 instrumentos aplicados pelos atores, um espectro alargado que inclui as operações de influência, exploração de dependências económicas, ciberespionagem e outros, os 13 domínios que não devem ser tomados isoladamente, mas antes como um todo e que incluem os tradicionais do poder nacional, mas também novos, como o espaço e o ciberespaço, as fases, incluindo o tipo de atividades observadas em cada fase, e a elas voltaremos mais

tarde.
O grande objetivo dos atores que misturam este tipo de instrumentos é adulterar a capacidade de decisão individual e coletiva de uma sociedade ou Estado-alvo. A dissuasão é um jogo psicológico, gerado em torno de perceções. Mais do que um algoritmo de decisão baseado em informação precisa ou capacidades concretas, destina-se a convencer um potencial agressor que os custos e as consequências dos seus atos ultrapassarão largamente os seus ganhos potenciais.
Como gerar então um estado de consciência desencorajador na mente dos decisores que planeiam as suas ações de forma integrada e com intenções hostis, se eles limitam propositadamente os seus atos, primeiro, para não serem notados e, segundo, para serem de difícil atribuição, até ao momento em que tenham poder suficiente para coagir os decisões políticos de um Estado ou sociedade vítima?
Dos pilares que vimos atrás, o fazeamento é aquele que é mais relevante em termos de dissuasão, porquanto nos permite obter uma perspectiva cambiante da atuação de um agente hostil, que inicialmente poderá parecer neutral e assim permitir uma detecção antecipada, favorecendo uma ação dissuasora mais flexível.
As fases das ameaças híbridas desenvolvem-se num *continuum*, que podem ser designadas de preparação, destabilização e coerção. A preparação começa com os esforços de interferência e influência, de maneira a moldar, pré-condicionar e obscurecer as ações subsequentes. A destabilização envolve as operações ou campanhas para influenciar e alcançar objetivos relativos à informação obtida e aos efeitos produzidos na fase anterior. A coerção concentra-se nas operações e campanhas de destabilização propriamente ditas, com a inclusão de ameaças militares, coercivas ou incursões pontuais.
O cruzamento entre o nível de funcionamento de um Estado-alvo, na linha amarela, no gráfico da esquerda, e a detecção da interferência e influência, linha vermelha, dá origem àquilo que se convencionou chamar a zona cinzenta, entre o comportamento aceitável e inaceitável, entre o legal e o ilegal.
A prevalência dos meios híbridos para demonstrar a hostilidade dos atores estatais indica que as posturas dissuasoras não tenham sido suficientemente convincentes. Porque? Porque as ameaças híbridas minam os fundamentos tradicionais da dissuasão, nomeadamente a comunicação, a capacidade e a credibilidade. A comunicação é afetada pela ambiguidade e subjetividade das

narrativas. A capacidade é desafiada pela abrangência e novidade dos meios híbridos, em especial os que envolvem tecnologias emergentes, como aquelas que vimos no painel anterior, e a credibilidade, posta em dúvida pelos limiares da deteção e resposta.

Como um agente agressor utiliza múltiplos meios e vetores em diversos domínios, que podem evadir a deteção e a atribuição, em que poderá consistir a dissuasão de ameaças híbridas? Entre outras características, a dissuasão apresenta dois mecanismos essenciais, a negação e punição. A negação pode ser alcançada através da proteção, por exemplo, das designadas infraestruturas críticas, mas também da resiliência, conceito este que recentemente concentrou todas as atenções relativas a um conjunto de ameaças, protagonizadas por pessoas, mas também riscos com origem na natureza, indo ao encontro das preocupações do nosso General Arnaut Moreira, que pode ser considerado um elemento dissuasor proativo.

Porém, para que alcance um efeito suficientemente dissuasor, a função de punição tem de ser equacionada. Levar o agente malicioso a pensar nas consequências da resposta perante uma incursão num domínio, por exemplo, ciber, e a resposta noutro, por exemplo, diplomático ou comercial, e é aqui que a responsabilidade nacional é mais evidente e não pode ser subalternizada, uma vez que cada Estado que pretenda dissuadir um agressor deverá identificar os seus limiares de reação, baseados na avaliação dos riscos e das ameaças que sobre si impendem, e nas suas vulnerabilidades sistémicas.

Da conjunção das duas forças, negação e punição, deverá resultar uma diminuição da liberdade de atuação do agente hostil.

O triângulo verde [no slide] representa as atividades que são difíceis de prevenir ou que limitam a capacidade de resposta de um Estado, necessitando do desenvolvimento de novas políticas e instrumentos de dissuasão.

As principais propostas de dissuasão de ameaças híbridas provêm, por enquanto, de duas origens: Estados Unidos da América e países nórdicos.

Os Estados Unidos, que avançaram com o conceito de dissuasão integrada na sua Estratégia de Defesa Nacional de 2022, definida como uma aproximação holística, através de domínios, regiões, espetro de conflito, setores governamentais e com aliados e parceiros, e com a noção de *campaigning*, que mais não é do que a atuação das forças armadas de uma lógica abaixo do patamar da guerra, aquilo que em Portugal se chama o apoio militar a emergências civis, por exemplo.

Este conceito é seguido no Reino Unido através da designação Integrated Operating Concept e, em resumo, é a inclusão das operações militares no contexto de competição geopolítica em favor da dissuasão articuladas com outros elementos do Poder Nacional.
Os países nórdicos apresentam um conjunto de boas práticas herdadas do seu conceito de Defesa Total e avançam com o conceito de segurança societal, onde as preocupações dos diversos setores são equacionadas através de uma articulação colaborativa, em especial devido à confiança mútua e institucional, o que é, desde logo, um fator de coesão e, como tal, bastante desencorajador para um agente com intenções hostis. Propõem um Conceito Nacional de Resiliência, baseado numa aproximação intergovernamental de todos os setores da sociedade e dirigido a todos os riscos e ameaças.
Estes conceitos fazem parte do relatório Niinistö, apresentado na semana passada, e poderão ajudar a União Europeia a estabelecer as equipas de resposta rápida e híbrida previstas na Bússola Estratégica de 2022.
No entanto, os desafios tecnológicos não param com a adoção de conceitos de resiliência integrada. O que é mais importante é a alteração do paradigma dominante. A crescente utilização de sistemas dotados de inteligência artificial poderá agravar substancialmente as tensões provocadas pelas perceções induzidas nos decisores, devido a fenómenos ainda pouco estudados, como foi o caso do ataque a Israel pelo Hamas, bem como a resposta protagonizada pelo sistema israelita Lavender, que seleciona dezenas de milhares de alvos e os prioriza. Por tudo isto, a dissuasão de ameaças híbridas merece ser estudada e os seus mecanismos relacionados com as tecnologias mais bem compreendidas para futura inclusão num conceito de defesa, de segurança ou até mesmo de resiliência nacional.
Muito obrigado pela atencão.

Coronel Agostinho Cunha

Depois desta excelente introdução, que enquadrou o nosso tema deste painel, dissuasão e resiliência às ameaças híbridas, vamos passar agora a outra área sectorial.
E para isso temos o Dr. João Carlos Barradas, que é licenciado em História e cuja atividade profissional é jornalismo, desde 1982. Desempenhou diversas funções de repórter, coordenador, editor e comentador em empresas de rádio,

televisão, jornais, revistas e na própria Agência Lusa. O Dr. João Barradas é colaborador atualmente da revista Sábado e vai focar a sua atenção nas redes sociais e na informação pública.

Dr. João Carlos Barradas[2]

JOURNAUX Ne pouvoir s'en passer mais tonner contre. Gustave Flaubert, Dictionnaire des idées reçues

Vou tentar cingir-me quanto possível aos riscos que possam apresentar para Estados democráticos as tecnologias digitais em conflitos aquém do limiar do confronto armado. Neste quadro limitar-me-ei, conforme pedido, ao universo redes sociais e informação pública. No caso de redes sociais tenho em vista plataformas digitais de acesso livre ou restrito para publicação e partilha de imagens, sons e textos em tempo real ou diferido, com exposição efémera ou permanente.

Qualquer análise implica, em primeiro lugar, classificar o teor das mensagens, identificar os emissores de materiais noticiosos ou doutrinários, propagandísticos, publicitários, de entretenimento, académicos, empresariais, institucionais, partidários ou confessionais presentes em redes sociais. É essencial, também, apurar se está em causa fito comercial ou não, se se trata de conteúdos lícitos ou ilícitos, graciosos ou pagos na totalidade ou parcialmente.

Os meios de transmissão de mensagens — serviços de mensagens curtas, *newsletters*, correio electrónico, etc. —, bem como modelos de financiamento dos emissores e das plataformas que utilizem – publicitário, via dotações públicas ou privadas, v.g. – devem, também, ser tidos em linha de conta. Importa, igualmente, apurar o que representam e quanto pesam as redes sociais no sistema global de entidades com existência legalmente reconhecida a par de emissores individuais ou grupais informais.

As condições de receção e tratamento efectivo dessas mensagens e os

[2] Por solicitação do orador, o texto reproduzido não corresponde à transcrição *ipsis verbis* da comunicação durante o Seminário, mas sim a um artigo de sua autoria, com o mesmo título, enviado propositadamente para o efeito. Bibliografia no final do Relatório. Texto escrito segundo o Acordo Ortográfico de 1945

fenómenos de retroação são, além disso, fenómenos a ter em conta.[3]
Quanto à informação pública limito-me a defini-la como toda e qualquer mensagem, no sentido lato de conjunto de signos, em circulação de acesso livre, deixando de lado materiais restritos, ou seja, segredos de Estado[4], propriedade intelectual conferida pelo segredo comercial, dados pessoais, etc.
Dada a sua especificidade terei de omitir análises à utilização para fins

[3] Trata-se essencialmente do modelo definido por *The Mathematical Theory of Communication* (Urbana, 1949), de Claude Shannon e Waren Weaver, ampliado por análises de circularidade de acção desenvolvidas a partir dos estudos de Nobert Wiener sobre mecanismos autorregulados em *Cybernetics: Or Control and Communication in the Animal and the Machine* (Paris/Cambridge, Ma, 1948). Outra vertente de análise deriva das investigações sociológicas que Paul Lazarsfeld e Herta Herzog levaram a cabo a partir dos anos de 1930 nos Estados Unidos. Os seus estudos empíricos sobre comunicação — um dos frutos da emigração transatlântica vienense — contribuíram para ultrapassar a «*psychologie des hommes en foule*» popularizada por Gabriel Tarde, *L'Opinion et la Foule*, Paris, 1901, e Gustave Le Bon, em especial com *Psychologie des Foules*, Paris, 1895. As teses sobre «*la nature féminine des foules*» (Bon), o papel da «*contagiation mentale*» e da acção dos «*meneurs*» — «*la foule ne saurait se passer de maître*» (Tarde) —, do poder da «*fascination véritablement magnétique*» (Bon) de raros grandes líderes, como Napoleão, continuam, no entanto, bem presentes no imaginário social. Refiro estas matrizes de estudo pelo facto de serem frequentemente ignoradas nas publicações académicas ou ensaísticas sobre a matéria.

[4] Deve aqui considerar-se um amplo domínio, inclusivamente em regimes democráticos, de não-direito, o «vazio jurídico», cuja existência é particularmente propícia a poderes interessados em escapar a constrangimentos legais ou em negar direitos a outrem. A inexistência de regulação jurídica onde deveria estar presente de acordo com a sua função dogmática pode assumir múltiplas formas e levar a outras formas diversas de regulação social, conforme teorizou o jurista francês Jean Carbonnier. Frequentemente, é mesmo uma derrogação de regras jurídicas e morais fundada na clássica definição com que o jesuíta italiano Giovanni Botero abriu a sua Della Ragion di Stato (1589): «*Ragione di Stato si è notitia di mezi atti a ondare, conservare et ampliare un dominio.*»

notoriamente ilegais da *Darkweb* ou de plataformas facilmente acessíveis em que é comum o tráfego de dados ilícitos ou contrários a convenções sociais.[5]
Ora, em matéria de ameaças, descartando outro género de conflitos, atentemos de imediato na sua manifestação violenta pela guerra, tendo em conta a conjuntura internacional. É essencial atermo-nos a esta forma de violência organizada porque, em última análise, mesmo restritos aqui a um contexto informativo, as redes sociais levaram a algo que na expressão cínica e acertada do romancista Michel Houellebecq se pode denominar como a extensão do domínio da luta. Na genérica definição de Carl von Clausewitz guerra é «acto de violência destinado a forçar o adversário a submeter-se à nossa vontade» (Da Guerra, Cap. I, § 2). Outras tradições como as ancestrais reflexões chinesas ou indianas sempre destacaram igualmente esta característica de imposição de vontade, de uso de força, para submissão ou extermínio total ou parcial do inimigo.[6]

---

[5] Veja-se, por exemplo, a reportagem «Entrámos no grupo de Telegram português onde 70 mil pessoas devassam a intimidade de mulheres» de Mariana Durão, José Alves e Catarina Póvoa, *Público*, 20 de Outubro de 2024.

[6] Este aspecto é essencial e explica a razão pela qual a mutação de situação pré-bélica em confronto aberto é um processo em que diversas fases se imbricam e cuja escalada pode ser orquestrada por um contendor que pretenda criar as melhores condições possíveis para desencadear as hostilidades. Boa parte das análises correntes de propaganda, contra-informação e guerra híbrida claudica por ignorar este traço essencial, patente, por exemplo, na doutrinação militar da Rússia putinista que, sem deixar de levar em conta a especificidade da condução de operações bélicas e níveis destrutivos, visa abarcar a totalidade das modalidades do confronto com inimigos existenciais ou circunstanciais.
As teses apresentadas pelo chefe-de-estado-maior Valerii Gerassimov numa intervenção na Academia de Ciências Militares, sintetizadas num artigo escrito para o semanário *Correio Militar e Industrial*, de Moscovo (O valor da ciência na previsão), por exemplo, não representam qualquer novidade doutrinária, incidindo antes sobre a importância do estudo do «aumento do papel de meios não-militares para alcançar fins políticos e estratégicos cuja eficácia em determinados casos superaram significativamente a força das armas» registado

na chamada Primavera Árabe. Muito mais relevante é a questão de unidade ideológica da nação, uma obsessão de Putin — um sucinto estudo de Nicolas Werth é boa introdução ao seu excepcionalismo étnico-nacionalista —, que os tratados tradicionais chineses debatem amiúde e cuja influência sobre as doutrinas militares soviéticas legadas ao putinismo não pode ser subestimada.

O mais influente dos grandes clássicos *A Arte da Guerra*, de Sun Tzu, estabelece a Lei Moral (a Via) como a primeira das cinco condições -- além da estação do ano, do território em vista, da liderança militar e da estrutura organizativa, comando e recursos -- a considerar nos Cálculos Preliminares. No primeiro de treze capítulos a Via é, assim, definida como a situação na qual «o pensamento do povo é idêntico ao pensamento do soberano, quando o povo está disposto a morrer com ele, pronto a viver com ele, quando ignora quer o medo, quer a discórdia» Capítulo I, 3 (Da tradução de Nikolai Konrad, constante do volume *Sinologia*, das Obras Escolhidas, p. 26).

O académico russo destacou a importância da coesão moral ou ideológica nos tratados reunidos nos Sete Clássicos Militares, a denominação pela qual passaram a ser conhecidos a partir do século XI na dinastia Song. Konrad assinalou, por exemplo, como a segunda obra mais relevante, Tratado sobre a Arte Militar, de Wu Qi, igualmente datado do século V a.c., apresenta logo no Capítulo I, 3, a seguinte premissa: «o soberano, conhecedor da Via que pretenda levantar o seu povo em armas, estabelece antes do mais a concórdia e só depois se lança à grande obra». (p. 318, idem, ibidem.)

De sublinhar, também, que o conflito entre a ideia de incontornável incerteza, associada às noções taoístas de fluxo natural a que o ser humano deve adaptar-se (*wuwei*), e o mérito de imposição pelo soberano da lei ideal expressa pelas doutrinas legalistas a partir do século V a.c., é outra constante do universo chinês que chega até aos nossos dias, perpassando nas polémicas comunistas do período maoísta e após 1976.

É significativo que as traduções e comentários de Konrad tenham sido realizados durante um período de detenção. Preso em Leningrado em julho de 1938, condenado a cinco anos por «traição à pátria», foi enviado, em dezembro de 1939, para um campo de trabalhos forçados na região de Krasnoiarsk, na Sibéria Central, sendo libertado em setembro de 1941, dois meses após o início da

invasão nazi. Durante o período de detenção, Konrad, reputado especialista em cultura japonesa e chinesa, gozou intermitentemente de condições invulgares para trabalho intelectual a que não foi alheio o conflito fronteiriço entre a União Soviética e o Japão (os combates de Khalkhin Gol, na República Popular da Mongólia, tiveram lugar entre Maio e Setembro de 1939) e a fase final vaga da Iejovshina que se saldou por cerca de 800 mil execuções e mais de 1 milhão de condenações a pena de 10 anos de trabalhos forças. Nikolai Iejov, o comissário à frente do NKVD entre Setembro de 1936 e Dezembro de 1938, foi executado em Fevereiro de 1940. A tradução de Sun Tzu foi publicada em 1950 e a de Wu Qi oito anos mais tarde. O tomo das *Obras Escolhidas - Sinologia*, publicado em 1977, sete anos depois da sua morte, integra estas duas traduções. No pós-guerra Konrad elaboraria o conceito de Renascimento como «período histórico da cultura mundial», em que o humanismo assume papel crucial, destacando uma «Renascença Oriental» iniciada na China, entre os séculos VII e X, passando pela Ásia Central nos séculos XI e XIII, e Europa Ocidental nos séculos XIII e XVI (Ocidente e Oriente, 1966), tese que discutiu em correspondência com o historiador inglês Arnold Toynbee.

É igualmente relevante que o confuciano Xunzi no século III a.c., na era dos Estados Combatentes (séculos V-III a.c.), no Debate sobre os Princípios da Guerra aborde três métodos de ampliação de domínios e conquista de populações: a virtude (de), a força bruta e a sedução pela riqueza. Xunzi conclui que só «aquele que incorpora populações através da virtude (de) é um verdadeiro soberano» capaz de «impor a sua autoridade austera e severa sem ter de a brandir e de proclamar punições em ter de as aplicar». (*Xunzi: A Translation and Study of the Complete Works*, Volume II: Books 7–16, p. 233.) A especificidade destas tradições chinesas e seu impacto são destacadas na investigação especializada, como por exemplo, em estudos de Yü Ying-shih, Jao Tsung-i, ou, mais recentemente, Ge Zahoguang.

As polémicas chinesas sobre ontologia política geraram uma síntese única taoista-confuciana-budista extremamente influente e demarcam-se notoriamente de doutrinas clássicas indianas, expressas, por exemplo, no Arthashastra, atribuído a Kautilya, séculos IV-III a.c.

Atente-se, ainda, que o prussiano considera estarmos ante «uma trindade em que se encontra primeiro que tudo, a violência original do seu elemento, o ódio e a animosidade que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso que fazem dela uma livre actividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura». (Cap. I, § 28). O ódio e a animosidade têm sobretudo a ver com o povo assinala von Clausewitz, nos escritos compilados pela viúva Marie Sophie entre 1832-35.[7]

É, pois, a vertente de mobilização, um dos domínios da luta, quer antes, quer após a abertura de hostilidades, e estamos, assim, de volta às redes sociais que podem ser vistas como antecâmara ideológica da guerra. Um risco muito real até porque também neste domínio não se pode ignorar, conforme indica uma conhecida passagem do Livro II de Clausewitz, ao abordar A Teoria da Guerra,

---

O tratado pode ser visto um caso de «maquiavelismo, verdadeiramente radical no sentido popular do termo», conforme afirmou Max Weber na sua conferência de Janeiro de 1919, em Munique, ante a União dos Estudantes Livres. O «Príncipe, de Maquiavel é inofensivo» comparado a Kautilya, no entender de Weber. «*Der wirklich radikale, Macchiavellismus, im populären Sinndieses Wortes ist in der indischen Literatur im Kautaliya Arthasastra*, (*lange vorchristlich, angeblich aus Tschandva-guptas Zeit), klassisch vertreten;· dagegen ist Macchiavellis, Príncipe, harmlos*.»

Para Kautilya política é o saber que propicia «a aquisição do que não se possui, a preservação do que obteve, o aumento do que se detém e a sua justa distribuição a quem o merece» e a enumeração dos passos a seguir na condução da guerra baseia-se na ideia de «força superior» de um soberano indiscutível (tradução de Patrick Olivelle e excertos em *Sources of Indian Tradition*, pp. 244 ss.).

Os ensinamentos de Kautylia não tiveram continuidade comparável à dos clássicos chineses, tendo, ademais, florescido na Índia a ideia de *ahiṃsā* (não-violência) muito marcante no jainismo e no budismo (Cf. Romila Thapar, p. 868).

[7] Nada indica que Clausewitz tenha lido a primeira tradução de Sun Tzu na Europa publicada pelo jesuíta Jean Joseph Marie Amiot: *Art militaire des Chinois*, ou, R*ecueil d'anciens traités sur la guerre: composés avant l'ere chrétienne, par différents généraux chinois*. Paris, 1772.

que «toda a acção se realiza, por assim dizer, numa espécie de crepúsculo que, por vezes, confere às coisas um aspecto nebuloso ou lunar, uma dimensão exagerada, um cariz grotesco.»[8] Clima, tensão e exaltação necessárias ao esforço de guerra e temor ao que possa escapar às formas tradicionais de produção, omissão e circulação de informação transparecem precisamente quando se questiona o que possa ser o risco disruptivo das redes sociais.

Cinjo-me à difusão de informação falsa ou inexacta e à expressão de opiniões puníveis por ofenderem interesses constitucionalmente protegidos, como, por exemplo, injúrias e incitamentos à violência étnica ou religiosa. Tais casos integram-se frequentemente em acções de propaganda, enquadradas em actos de guerra híbrida, visando influenciar a opinião pública, quer sejam ou não assumidos pelos agentes emissores.[9]

---

[8] Clausewitz é particularmente feliz nas metáforas e imagens desta passagem: «(…) *alles Handeln gewissermaßen in einem bloßen Dämmerlicht verrichtet wird, was noch dazu nicht selten wie eine Nebel — oder Mondschein beleuchtung den Dingen einen übertriebenen Umfang, ein groteskes Ansehen gibt.*»

[9] Em rigor guerra híbrida deveria designar exclusivamente a combinação de subversão ideológica, espionagem e sabotagem, associada à preparação ou condução de acções de confronto bélicas. Seria assim entendida, quanto ao tema que nos interessa, como cúmulo de actos persistentes visando minar a confiança e ou adesão de determinados grupos da população a princípios constitucionais democráticos, propagandeando ou não valores alternativos. Estas acções podem ser dissimuladas (caso de campanhas de desinformação promovidas por Estados ou seitas religiosas) ou abertamente reivindicadas (como é frequente da parte de grupos terroristas. Cf. por exemplo, Khosrokhavar, 2018).

O conflito russo-ucraniano, em que desde 2014 se ultrapassou o limitar da guerra, é fértil em exemplos do uso tendencioso de informação oficial e oficiosa, além da veiculada pelas fontes mais diversas, em que é frequentemente dificílima a destrinça entre censura, propaganda, boatos, rumores, descrições e relatos de eventos e situações sem testemunhos identificáveis e credíveis, além de desinformação coordenada a nível estatal. Nesta guerra deparamo-nos, portanto, com informações controladas pelo Estado em que os canais sem vínculo oficial servem para propósitos de desinformação ou veiculam dados à revelia da

propaganda oficial. Dois exemplos. O alegado uso pelas forças armadas da Rússia de crematórios móveis para incinerar baixas mortais, denunciado pelo ministério da defesa do Reino Unido, em 2024, retomando, aliás, notícias não confirmadas difundidas a partir de 2015. «Um efeito secundário extremamente arrepiante do modo como os russos encaram as suas forças», considerou o ministro da defesa do Reino Unido, Bem Wallace, em declarações destacadas no jornal londrino *The Daily Telegraph* na véspera da ofensiva russa de Fevereiro de 2024. No blog Ribar (O Pescador), rybar.ru, dinamizado por Mikhail Zvintchuk, ex-militar russo, que no Telegram reivindica 1,3 milhões de seguidores, surgem com frequência informações à revelia e em contradição com os relatos oficiais das operações militares, mas os materiais disponibilizados, passíveis de censura e em caso algum pondo em causa a legitimidade da guerra, são parte ínfima no sistema de informação formal e informal controlado pelo Kremlin. A produção industrial de *trolls* típica da Agência de Investigação da Internet, fundada por Ievgenii Prigojin, em São Petersburgo, em Julho de 2013, mas já posta em prática na década anterior, é outra face da utilização de redes sociais para fins de destabilização, conforme demonstraram inquéritos pioneiros dos jornalistas Ilia Barabanov e Denis Korotkov. Prigojin reivindicou publicamente a sua interferência nas eleições norte-americanas de 2016 num *post* colocado na página do seu grupo empresarial Concord na rede VKontakte, a 7 de Novembro de 2022. O empresário num comunicado de imprensa do Concord, datado de 14 de Fevereiro de 2023 — seis meses antes de ser assassinado —, revelou, por fim, ser o fundador da Agência de São Petersburgo. Abordei as limitações dos esforços de contrapropaganda da União Europeia face à Rússia em artigo para a revista *Sábado* colocado online a 28 de Maio de 2024 https://www.sabado.pt/mundo/detalhe/a-violacao-das-massas-pela-propaganda e chamo a atenção para a análise de Maxime Audinet e Colin Gérard (2024) acerca das recentes mutações do «*dispositif proteiforme d'influence informationnelle*» de Moscovo. As redes sociais sedeadas na Ucrânia, na Rússia e no estrangeiro são, também, veículos privilegiados para mensagens pessoais de grande relevância política, posteriormente ampliadas por outros meios de comunicação. Na Ucrânia são de citar as reacções à morte, a 7 de Janeiro de 2024, na frente de Kharkiiv, do poeta Maksim Krivtsov. Na sua última entrada no

Facebook na véspera de morrer lembrava tristemente que «90% dos poemas aqui são sobre a morte». Na mesma rede, a derradeira declaração de amor de Aleksei Navalnii à mulher Iulia em que, dois dias antes da morte, ocorrida a 16 de Fevereiro de 2024, evocava a memória do enamoramento a partir da prisão de máxima segurança Lobo Polar, em Kharp, nos confins árticos dos Urais e da Sibéria Ocidental. Referi estes dois casos no comentário publicado a 24 de Fevereiro de 2024 na edição digital da revista *Sábado*. (https://www.sabado.pt/opiniao/convidados/joao-carlos-barradas/detalhe/da-nossa-guerra-com-amor) Por fim, deixando de lado confrontos bélicos de guerrilha, guerras civis, conflitos independentistas, podemos referir situações em que organizações criminosas assumem controlo territorial persistente, privando o Estado da soberania. É possível identificar nestes casos muitos traços de guerra híbrida. Os cartéis mexicanos representam, actualmente, um exemplo, em crescendo desde a década de 1980, de controlo de espaços de soberanias adversos a um Estado, que, aliás, infiltram e subvertem, conforme argumenta o antropólogo Claudio Lomnitz. A ruína ideológica do Estado nacional mexicano é patente na incapacidade de obstar à promoção de valores culturais característicos de bandos e organizações criminosas – os cultos de São Judas Tadeu ou do bandoleiro Jesús Malverde, o consumo ostentatório, a estética feminina das buchonas, etc. Estes valores alternativos e afrontosos, só em parte excluídos do espaço comunicacional reconhecido legalmente, são potenciadas por redes sociais. É, todavia, um fenómeno de cultura popular muito abrangente, evidente, por exemplo, na ampla divulgação do narcocorrido, um dos veículos, tal como os mausoléus funerários, de idealização de uma vida que um popularíssimo corrido retrata bem:

Nacido en Sinaloa
Donde se aprende a matar
Traigo sangre de combate
Y la orden de ejecutar
Como una fiera salvaje
El terreno hay que cuidar

(El abogado del diablo, do álbum El Katch, 2009, de José Alfredo Ríos Meza, El Komander – Fonovisa Records https://www.youtube.com/watch?v=McD0ykbmpJQ)

Neste particular é corrente falar-se do condicionamento da opinião pública, outro conceito controverso. Vou ater-me a uma ideia veiculada por Walter Lippmann nos anos de 1920 devido à influência que exerceu e exerce nos estudos sobre condicionamento mediático. Para o nova iorquino vive-se num mundo opaco e o conhecimento indirecto que dele se absorve, necessariamente impreciso e parcial, gera-se a partir de estereótipos: «na maior parte dos casos não começamos por ver e depois definir, mas definimos primeiro e vemos depois.»[10]

[10] « Speed, Words, and Clearness», cp. V da segunda parte, abre com «*The unseen environment is reported to us chiefly by words*» e na terceira parte do livro ao abordar os estereótipos, cp. VI, Lippmann escreve: «*For the most part we do not first see, and then define, we define first and then see*.» Sobre o contexto da publicação de Public Opinion, em 1922, e a evolução do pensamento de Lippmann. Cf. o estudo de Tom Arnold-Forster (2023). Um dos aspectos menos explorados das configurações ideológicas dos estudos sobre pressupostos filosóficos e políticos de condicionamento social de que são exemplos o biologismo pavloviano do clássico antinazi de Sergei Tchakhotin, *Le Viol des Foules par la Propagande Politique* (Paris, 1939), ou o racional universo fictício da «esfera pública» (*Öffentlichkeit*) teorizado por Jürgen Habermas a partir dos anos 1960, é a sua desconexão com a economia neoclássica, caso do biólogo russo e também de Lippmann, ou a sua homologia, como sucede com o filósofo alemão, e as implicações que tal acarreta para a definição de um sistema liberal-democrático.

Os estudos de propaganda, são por vezes, erroneamente dissociados da censura, essencial a qualquer regime ditatorial, e das regulamentações e jurisprudências muito variadas de estados democráticos. O Secretariado de Propaganda Nacional, criado pelo decreto-lei n.º 23:054, de 25 de Setembro de 1933, visava, por exemplo, nos termos do artigo 2º, «evidenciar no País e no estrangeiro, o espírito de unidade que preside à obra realizada e a realizar pelo Estado Português.» Na alínea f) do art. 4º estipulava-se a tarefa de «combater a penetração no nosso país de quaisquer ideias perturbadoras e dissolventes da unidade e interesse nacional». O Secretariado de António Ferro surge, institucionalmente, associado à Censura na lógica expressa no art. 20º da Constituição de 1933: «A opinião pública é elemento fundamental da política e

Podemos seguir esta linha de raciocínio com um exemplo norte- americano da II Guerra Mundial particularmente interessante. Três meses após o ataque japonês a Pearl Harbour, de Dezembro de 1941, o diário Boston Herald lançou uma Rumor Clinic, dinamizada pelo psicólogo Robert Knapp para denunciar e refutar a doença dos boatos que afectava o esforço de guerra. Outros jornais norte-americanos e canadianos, além de revistas de grande tiragem como *Life*, passaram a publicar clínicas de boatos baseadas no modelo do Boston Herald.[11]
O Office of War Information partiria inicialmente, por sua vez, do pressuposto de que boatos se espalham no vazio noticioso, fazendo sentido, portanto, a divulgação de «notícias o mais possível precisas, atempadas e integrais». Esta ideia, tal como é referido num dos livros essenciais de análise do esforço de contrapropaganda norte-americano, seria apenas «parcialmente correcta». Em *The Psychology of Rumor*, publicado em 1947, por Gordon Allport e Leo Postman, da Universidade de Harvard, boato é definido como «uma proposição específica (ou tópica) de convicção (*belief*), transmitida de pessoa a pessoa, geralmente boca a boca, sem apresentar critérios de prova seguros». Allport e Postman identificaram, ainda, na propagação de boatos três momentos essenciais, a saber: a nivelação, levando à supressão de pormenores, a acentuação, destacando determinados detalhes na transmissão, e a assimilação, resultando na distorção da informação recebida em resultado de motivações subconscientes. Sublinharam, igualmente, que o rumor deve incidir sobre algo que se revista de «alguma importância para o emissor e o ouvinte», devendo «os factos verdadeiros estar envolvidos em alguma espécie de ambiguidade».
Já quanto à eficácia das campanhas durante a guerra para contraditar boatos os autores concluíram ser difícil mensurar o seu impacto, aventando que, aparentemente, terão criado uma maior «consciência quanto a boatos» e certa «imunidade ao boato».
É importante destacar que as investigações sobre o papel desempenhado por boatos no estímulo e reforço de preconceitos levaram Allport a apresentar teses inovadoras sobre a intensidade de contactos grupais e étnicos para a génese e

administração do País, incumbindo ao Estado defendê-la de todos os factores que a desorientem contra a verdade, a justiça, a boa administração e o bem comum.»

[11] Pascal Froissart (2024).

escalada de locuções e actos preconceituosos — afirmações depreciativas indirectas, discriminação, agressão física, etc. — ao publicar em 1954 *The Nature of Prejudice*.

Estas referências bastariam para precavermo-nos contra uma abordagem das redes sociais sem considerar a sua integração nos sistemas mediáticos. Uns quantos estudos abalam ideias-feitas sobre a questão e nem entraremos na discussão fulcral do modo como a internet levou a uma eventual «invasão dos idiotas», na expressão de Umberto Eco, ou da estratégia propagandística de difusão do maior número possível de informações, falsas ou deturpadas.[12]

---

[12] «*I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel. È l'invasione degli imbecilli.*» Eco fez esta afirmação aos jornalistas na Aula Magna della Cavallerizza Reale, após ter recibido, a 10 de Junho de 2015, o título de *doutor honoris causa* em "Comunicazione e Cultura dei media" pela Universidade de Turim. Cf. La Stampa, 11 de Junho de 2015.

«*The democrats don´t matter. The real opposition is the media and the way to deal with them is to flood the zone with shit*.» Esta fórmula de Steve Bannon consta de uma entrevista a Michael Lewis publicada a 9 de Fevereiro de 2018 pela Bloomberg com o título "Has Anyone Seen the President?".

A estratégia de descredibilização dos media era já identificável na campanha presidencial do republicano Barry Goldwater contra Lyndon Johnson, em 1964, conforme sublinhou, entre outros, o professor de jornalismo da Universidade de Nova Iorque Jay Rosen: "Why Trump Is Winning and the Press Is Losing" (*The New York Review of Books*, 25 de Abril de 2018).

«Had a very good and interesting meeting at the White House with A.G. Sulzberger, Publisher of the New York Times. Spent much time talking about the vast amounts of Fake News being put out by the media & how that Fake News has morphed into phrase, "Enemy of the People." Sad!», lia-se num tweet de Trump de 29 de Julho de 2018.

Dos muitos comentários sobre a campanha trumpista vide, por exemplo, "Trump vs. the Times: Inside an Off-the-Record Meeting", David Remnick, na revista *New Yorker* de 30 de Julho de 2018.

O recurso ao instituto jurídico do dolo é aqui essencial para distinguir entre má-fé, como intento de prejudicar, iludir ou enganar outrem, e situações em que primam a imprudência, a negligência, a imperícia, a ignorância e, tanta vez, a incivilidade que justifica a expressão «chafurdar nas redes sociais».

Comecemos assim: o contacto directo com os cidadãos e a informação veiculada pelos media tradicionais podem ser classificadas como as fontes mais úteis para políticos eleitos aferirem o pulsar da opinião pública, superando as redes sociais e as sondagens. Tal apurou um inquérito, realizado em 2018, envolvendo 898 representantes eleitos em países com sistemas eleitorais diferentes: Canadá, Países Baixos, Bélgica, Alemanha e Suíça.[13]

O então presidente gabar-se-ia em entrevista ao programa do pastor baptista e antigo governador do Arkansas Michael Huckabee na Trinity Broadcasting Network a 7 de Outubro de 2017: «The media is — really, the word, I think one of the greatest of all terms I've come up with is "fake"; Trump said. I guess other people have used it, perhaps, over the years, but I've never noticed it.» (Mike Huckabee on TBN | Huckabee.TV)

A regra da confusão para pôr em causa os princípios de rigor e objectividade, mais genericamente o conceito de verdade comprovável, é, igualmente, marcante no pensamento mágico da era putinista. Cf. por exemplo, o estudo de Peter Pomerantsev (2014).

[13] Walgrave, S., e Soontjens, K. (2023). Noutras áreas, como num estudo de 2019 sobre desinformação

(maliciosa e errónea sem dolo) em assuntos de saúde nas redes sociais, os investigadores concluíram que «*misinformation is highly prevalent on social media and tends to be more popular than accurate information, while its narrative often induces fear, anxiety and mistrust in institutions. The severity and the deleterious effects it may pose on the society is hardly quantifiable, but evidence abounds that we need more research on the identification of susceptible populations, and on the understanding of socio-demographic and ideological asymmetries in the intention to spread misinformation. Finally, since the persistence of misinformation owes both to the psychological responses and to the social contexts under which misinformation spread, potential interventions should target both fronts.*» Yuxi Wang, Martin McKee, Aleksandra Torbica, David

Prossigamos. Num contexto de acesso a múltiplas fontes de informação Andrea Part, da Universidade de Columbia, e Patrick Kennedy, de Berkeley, admitem ser possível apurar o peso relativo de cada uma em função do tempo de atenção despendido Este conceito de «*media power*» levou-os, por exemplo, a identificar SIC, TVI e RTP, como os grupos de media mais relevantes em Portugal, utilizando dados de um inquérito a 72 mil pessoas em 36 países para o Reuters Institute for the Study of Journalism, realizado em 2017 pelo YouGov.[14]

Exercício semelhante efectuado em França, recorrendo a dados de 2017 e 2022, refere que o grupo estatal que integra France Télévision e Radio France, concentra a maior atenção dos consumidores de informação (19,8%), seguido do Meta (10,1%) e da TF1 (9,9%), do consórcio Bouygues.[15]

Apesar de limitações de amostras deste género de inquéritos abrem-se algumas pistas. Contamos com bastantes indícios de que em Portugal prevalece um consumo noticioso concentrado em meios de comunicação com registo legal, pertencentes a grandes grupos de comunicação, predominando o contacto via televisão e rádio dada a escassa difusão da imprensa escrita (passe a redundância). É reduzida a relevância das redes sociais alheias a essas

---

Stuckler (2019). A pandemia COVID-19 deixou, todavia, a claro o papel preponderante da comunicação e censura institucionais e dos media tradicionais na disseminação e ocultação de informação sanitária e o desempenho secundário de redes sociais, independentemente da penetração dos meios digitais. Já o estudo "Analysis of the Impact of Disinformation on Political, Economic, Social and Security Issues, Governance Models and Good Practices: The cases of Spain and Portugal (2023)" admite que ao analisar desinformação «*concentrating on social media makes sense*» dado serem «*all built and conceived with the final goal of capturing data from users and selling ads. The algorithms propose content to keep users within their platform for the longest time possible. These algorithms not only participate in the problem of echo chambers but can amplify some disinformation by recommending content that is deemed false*.» Os autores sublinham, ainda, que «*another potential reason to explain the focus on social media is the data collection*.» (p. 22).

[14] Patrick J. Kennedy, Andre Prat (2019).

[15] Sylvain Dejean, Marianne Lumeau, Stéphanie Peltier (2023).

entidades.[16]

[16] Em Portugal, um inquérito da Havas Media Network assinala que os canais de televisão abertos eram tidos como o meio noticioso mais credível em 2023 por 75% dos inquiridos (72% no ano anterior), seguindo-se jornais, 64%, rádio, 59%, motores de busca, 39%, e canais televisivos por subscrição, 14%. O estudo "Meaningful Media" (consulta paga), baseado em 600 entrevistas, realizadas em Outubro de 2023, a residentes em Portugal Continental, com idades entre os 15 e os 64 anos, constata nesta sua quarta edição, padrões de consumo liderados, no entanto, pelos motores de busca, 59% (54% em 2022), seguidos de canais televisivos em sinal aberto, 56%, rádio, 43%, redes sociais, 36%, e jornais, 26%. O inquérito da agência de meios refere, também, que a relevância dos canais de televisão abertos é maior a partir dos 45 anos e a de redes sociais e motores de busca entre os 15 e 35 anos. De acordo com os dados de 2024 do Bareme Internet, produzido pela Marktest, 84,4% dos cidadãos com mais de 15 anos e residentes em Portugal Continental assume o hábito de ligar-se à Internet, seja por trabalho ou por lazer, sobretudo através de telemóvel. Outro estudo desta empresa "Os Portugueses e as Redes Sociais 2024" (consulta paga) indica que, com 97 minutos de tempo médio dedicado às redes sociais pelos utilizadores, Instagram é a plataforma a que os inquiridos acedem mais frequentemente (34,2%), seguida de WhatsApp (27,2%) e Facebook (20,9%). Num universo estimado em 5,432 milhões de indivíduos, os utilizadores mantêm contas no Facebook (90%), WhatsApp (88,3%) e Instagram (82,1%). Facebook é, por fim, a rede com maior notoriedade espontânea *top of mind*, ou seja, é a primeira nomeada por 59,4% dos 803 entrevistados online com idades compreendidas entre os 15 e os 64 anos. A Associação Portuguesa para o Controlo de Tiragem e Circulação contabilizava, por sua vez, circulação paga impressa de 38 650 exemplares e 2 680 para circulação paga digital no caso do *Correio da Manhã*, 36 878/ 48 719 *Expresso*, 17 721/ 4 073 *Jornal de Notícias*, 10 058/ 52 656 *Público*, 4 976/1 532 *Diário de Notícias da Madeira*, 1 124/1 175 para o *Diário de Notícias*, 15 478/ 5 049 para *Sábado*. No segmento de desportivos o *Record* vendia 13 582/4 416, a *Maria* 26 736/ 22 e o *Jornal de Negócios* 1 656/ 5 466. No conjunto a circulação impressa paga de órgãos de informação geral cifrava-se em 2 051701 exemplares e a respectiva circulação digital paga atingia 1 395 068.

O consumo de rádio, segundo o Bareme Rádio, em inquérito efectuado entre 2 de Maio e 23 de Setembro de 2024, apurava que 83,4% dos residentes no Continente com 15 anos ou mais ouviu rádio pelo menos uma vez por semana e 59,6% na véspera. Rádio Comercial, M80, Cidade FM, Smooth FM e Batida FM, do
Grupo Bauer Media Audio Portugal, somaram 42,3% de share de audiência, 52,8% de reach semanal (percentagem de ouvintes de uma estação de rádio, no período sete dias, independentemente do tempo despendido) e 30,1% de audiência acumulada de véspera. O Grupo Renascença Multimédia registou 27,8% de share de audiência, 50,6% de reach semanal e 24,1% de audiência acumulada de véspera, enquanto as estações do Grupo RTP se quedaram por 7,3% de share de audiência, reach semanal de 15,3% e 6,9% de audiência acumulada de véspera. A estação mais ouvida é a Rádio Comercial, 25,7% de share, seguida pela RFM, 17,1%, e a M80 com 10,1%. Note-se, ainda, cerca de 3,5 milhões de pessoas afirmam escutar rádio pela internet e 2,4 milhões ouvem *podcasts*.
Finalmente, a televisão. A Autoridade Nacional de Comunicações recenseava no final do primeiro semestre deste ano 4,6 milhões de assinantes de serviços de TV paga, entre os quais 65,2% com acesso via fibra ótica.
(FTTH/B). No segmento residencial a penetração de aparelhos de TV atingiu 96 por 100 famílias. A maioria, 58,7%, visiona televisão via canais de cabo e plataformas de *streaming*, cabendo aos canais generalistas 41,3% dos espectadores. A média de visionamento televisivo foi de 5h 23m por dia em 2023 e, para referir dados de setembro último, basta indicar que os programas de maior audiência do mês foram os jogos de Portugal para a Liga das Nações (Portugal x Escócia e Portugal x Croácia). Os jogos, transmitidos pela RTP1 foram vistos em média por mais de 2 milhões e 70 mil telespetadores, equivalente a um share de 42,4%. O *reality show* da TVI "Secret Story – O Regresso" foi o terceiro programa com audiência média de 1 milhão e 95 mil telespetadores, representando um share de 29,2%.
A Entidade Reguladora para a Comunicação Social, na ausência de estudos de acesso público, disponibiliza «recursos educativos dirigidos aos cidadãos e órgãos de comunicação social», a saber: cartazes, "Não dê Voz a Estereótipos e

É certo que as funções comunicacionais não se esgotam na esfera da informação noticiosa. A função fática do estou aqui! (O «Tou xim? É pr'a mim?», do anúncio, de 1995, da empresa de telecomunicações Telecel, actual Vodafone), a função emotiva das interjeições, a função apelativa e imperativa, estão muito presentes na linguagem utilizada nas redes sociais. Todas elas integram actos de comunicação que podem assumir relevância política.

O modo como se fala e escreve, o tom, a gesticulação, o vocabulário, as formas de tratamento variam consoantes os meios e os interlocutores. Os estudiosos,

---

Preconceitos!" e "Protege-te da Desinformação!", além de *posts* para redes sociais, "Proteja-se da Desinformação" e "Usa o Teu Sentido Crítico contra a desinformação". Cardoso, G., Paisana, M. e Pinto-Martinho, A. (2024) *Digital News Report 2020 Portugal*. Ober Com — Reuters Institute for the Study of Journalism no nono relatório anual da série constatam que 66% dos inquiridos tem por bom/muito bom o trabalho dos media ao disponibilizar notícias que os mantêm a par da actualidade. 65% concordam com a afirmação de que os media lhe permitem melhor compreensão da actualidade, ainda que apenas 51% se declarem interessados por notícias, 36% manifestam interesse neutro e 10% se digam não-interessados.

Quanto a fontes de acesso principal a notícias entre os 18 e 24 anos vinga a internet (incluindo redes sociais), para 58%, seguindo-se a televisão (31%). A internet é, aliás, a principal fonte de acesso a notícias até aos 44 anos, assumindo esse papel a televisão para as faixas etárias mais velhas. Importa sublinhar que só 16% dos acessos online são feitos ao site de marcas das notícias.

A incongruência destes dados parcelares na ausência de estudos abarcando a totalidade do sistema informativo/comunicacional em Portugal nota-se ainda mais ao constatar-se, Magallón-Rosa, R., Paisana, M et al., (2024), que, em 2023, o contacto noticioso de última semana revelava 82% para televisão, 50% websites noticiosos, 41% redes sociais e blogs e 34% rádio. O nível de confiança na televisão e rádio públicas cifrava-se em 65% (média europeia 48%), na imprensa escrita, incluindo as suas plataformas online, atingia 54%, para televisões e rádios privadas era de 53%, surgindo pessoas, grupos e amigos seguidos nas redes sociais com 11%. Acresce que 66% se diziam confiantes/muito confiantes em reconhecer desinformação, segundo dados de 2022, idênticos, aliás, aos registados na média dos 27 Estados da União Europeia.

utilizadores de língua culta por definição, são particularmente sensíveis a linguagem por vezes desbragada corrente em certos meios informais das redes sociais e também ao cunho fugaz e inconstante da retórica.[17]

Já a perversão e contaminação política da linguagem passam mais frequentemente em claro, sobretudo quando se revestem de laivos tecnocráticos e anglicismos: o *player* focalizado no *target*. E não foi por acaso que o verbo *vernichten*, aniquilar, ou o adjectivo *fanatisch*, marcaram o tom da linguagem nazi que Viktor Kamplerer analisou detalhadamente na *Lingua Tertii Imperii: Notizbuch eines Philologen*, publicado em 1947 e nos diários editados em 1955, tal como a Newspeak de George Orwell, em 1949, fazia sentido e, muito antes dele, o relevo dado à corrupção da língua russa no tumulto revolucionário pós 1917 por Mikhail Bulgakov na novela *Coração de Cão* de 1925. Isto conta na

[17] O cunho fugaz e autocentrado da novidade «instante a instante» do «telégrafo eléctrico» foi sagazmente antecipado por um cronista anónimo que a 25 de Fevereiro de 1868 se interrogava no *Jornal do Comércio*, diário lisboeta nascido em 1853 e que encerrou em 1983, sobre o que será o jornalismo em 2 000?: «Daqui a 50 anos, os jornais publicarão uma folha, inteiramente nova, de hora a hora, e, daqui a 100 anos, de minuto a minuto, de instante a instante. Será um moto contínuo e ainda não satisfará a curiosidade pública. Cada cidadão fará um jornal: o artigo de fundo constará sempre das notícias da sua vida pública e íntima. Cada um informará o respeitável público das horas a que se levanta da cama, tendo previamente declarado como passou a noite; noticiará a que horas almoça e o que almoçou; referirá, minuciosamente, o seu jantar e as pessoas com quem jantou; dirá se o jantar estava bem cozinhado; contará se o seu gato miou, se o cão ladrou, se o papagaio está incomodado; narrará todas as miudezas da sua casa, não escapará à publicidade a mínima dor de cabeça ou de estômago; se estiver doente, publicará um boletim.
das moléstias, não só a seu respeito, mas de toda a sua família; enfim, todas as circunstâncias da vida caseira, as mais íntimas, serão contadas no jornal, acomodando o estilo aos factos. Deste modo, haverá um grande progresso, porque se dispensarão os curiosos de espreitar o que se passa na casa de cada um, para ouvirem dizer ao público: o cidadão contará, de instante a instante, a sua vida, e, deste modo, fica completamente satisfeita a curiosidade geral.» (In *Crónica Jornalística*. Século XIX).

análise de redes sociais e do sistema comunicacional de toda uma sociedade.
É provável que o cunho não-regulado por entidades públicas estatais nacionais e supranacionais dos primórdios da internet na década de 1990 ainda condicione as orientações teóricas de análise de redes sociais. Haverá, talvez, tendência a considerá-las disruptivas no sentido popularizado pelo estudioso norte-americano de gestão Clayton Christensen. Os computadores pessoais, telemóveis, fotografia digital foram citados por Christensen como exemplos de «tecnologias disruptivas» (1995) por criarem mercados e consumidores ao implantarem invenções e explorarem técnicas existentes para modelos de negócio inéditos.
Posteriormente, optou pela expressão «inovação disruptiva» para sublinhar que na maior parte dos casos não eram as tecnologias disruptivas, nem os meros aperfeiçoamentos técnicos *per se*, a gerarem inovação, mas sim a utilização empresarial que lhes era dada (2003). Em qualquer dos casos, independentemente da validade da teoria de Christensen sobre os tipos de inovação e o impacto económico da sua gestão empresarial, o termo vingou, deixando na sombra reflexões bem mais ricas que na tradição ocidental datam da Política de Aristóteles (as considerações sobre instrumentos inanimados e animados do Livro I) e que, em Portugal, interessaram investigadores como Hermínio Martins.
Na análise política ou na abordagem do sistema comunicacional o adjectivo disruptivo é, estou em crer, essencialmente tido como elemento desestabilizador, potencialmente nocivo, em especial quanto se aborda as redes sociais, presumivelmente omipresentes.
Se considerarmos os Estados Unidos, país para o qual existe maior número de dados e estudos, chega-se, contudo, à conclusão de que a maior parte do tempo de acesso aos media não tem a ver com material noticioso que se cifraria em apenas 14,2% da duração média de contacto diário. O consumo de notícias por televisão é, por sua vez, cinco vezes superior ao registado via internet, sendo estimada uma exposição diária muito baixa de apenas 0,15% a notícias falsas. É, no entanto, possível que o consumo noticioso *online* tenha maior impacto por minuto ou que notícias falsas de teor malicioso possam alcançar influência superior à de noticiário fidedigno, sendo, ademais, de considerar níveis díspares

de sentido crítico e de preconceitos consoante diversos grupos sociais.[18]

A baixa exposição a notícias falsas tinha, por sinal, sido constada numa investigação anterior circunscrita ao Twitter. Na campanha presidencial de 2016 a exposição e partilha de notícias falsas maliciosas por eleitores registados foi muito concentrada numa rede que contava com 313 milhões de utilizadores e em que 27% dos norte-americanos tinha conta aberta. Assim, 1% dos eleitores registados — um painel de 16 442 indivíduos, equivalente a 3,7% do total de contas de eleitores com contas no Twitter — era responsável por 80% dos contactos com notícias falsas e 0,1% gerava cerca de 80% das notícias falsas partilhadas. O perfil político apontava para a orientação conservadora destes utilizadores que, tal como demais indivíduos presentes no Twitter, consumiam sobretudo notícias emanadas de media tradicionais.[19]

Outro estudo publicado este ano comprova que a exposição a informação falsa maliciosa se restringe a um segmento reduzido e altamente motivado dos utilizadores de redes sociais.[20]

Nas audiências realizadas ante o Comité Judicial do Senado de Washington, em 2017, Facebook revelou ter identificado 120 páginas de notícias falsas, criadas por órgãos de desinformação da Rússia, responsáveis por 80 000 posts na campanha presidencial de 2016 a que acederam 126 milhões de norte-americanos. Tal correspondeu a 0,004% do material disponível nesta rede social. O maior acesso e partilha de notícias falsas maliciosas é, igualmente, detectado entre minorias militantes com elevada motivação ideológica.

O efeito de afunilamento de algoritmos, por outro lado, resulta, em redes como YouTube, pelo menos a partir de 2019, essencialmente da procura, mas o acesso

---

[18] Jennifer Allen, Baird Howland, Markus Mobius, David Rothschild e Duncan J. Watts (2020).

[19] Grinberg N, Joseph K, Friedland L, Swire-Thompson B, Lazer D. (2019). No ciclo eleitoral presidencial de 2020, McCabe, S.D., Ferrari, D., Green, J. et al. (2024) analisaram o tráfego de 550 000 contas — nesse ano contavam-se 347,6 milhões de utilizadores em todo o mundo e 21% dos norte-americanos teriam conta aberta —, concluindo que somente 7,5% tinham partilhado uma ou mais notícias falsas maliciosas.

[20] Budak, C., Nyhan, B., Rothschild, D.M. et al. Misunderstanding the harms of online misinformation. Nature 630, 45–53 (2024).

a dados de redes sociais e plataformas digitais é insuficiente para permitir generalizações sobre as alterações a algoritmos e seus efeitos.[21]

É importante, aliás, ter em conta que à pergunta sobre se confia e acredita no noticiário veiculado pela imprensa, rádios e televisões, cada vez mais norte-americanos tendem a responder pela negativa. Este ano, 36% afirmam não ter qualquer confiança, e 33% reveem-se na opção «escassa confiança e credibilidade», de acordo com um inquérito da Gallup efectuado entre 3 e 15 de Setembro. Caiu para 31% a percentagem de inquiridos a assumirem «muita ou razoável» confiança nos media, o valor mais baixo desde que a empresa iniciou estudos sobre a questão em 1972. Pessoas que se identificam como democratas revelam maior confiança nos media: 54%, mas apenas 31% dos inquiridos desta orientação política entre os 18 e 29 anos partilham tal opinião, percentagem que ascende aos 74% a partir dos 65 anos. Entre independentes a percentagem de alta ou média confiança nos media queda-se pelo 27% dos questionados e para republicanos desce aos 12%. Este grau de desconfiança coloca os media abaixo de qualquer instituição cívica ou política, incluindo entidades legislativas, executivas e judiciais, considerada nos inquéritos da Gallup.

Aos órgãos de administração local é atribuído o nível mais alto, manifestando os inquiridos «muita ou razoável» confiança (67%) na sua actividade.

A polarização partidária leva 82% dos democratas a declararem «muita ou razoável» confiança no poder executivo, contra apenas 32% dos independentes e 9% dos republicanos, registando-se sempre valores mais baixos entre inquiridos menores de 29 anos quando confrontados com questões relativas a instituições políticas e judiciais.

O poder judicial, em contrapartida, merece apreciação positiva a 71% dos republicanos, 49% dos independentes e a apenas 24% dos democratas.

A derrocada na confiança e fiabilidade dos media é devastadora num país em que até meados dos anos 1970 a esmagadora maioria da população fazia fé na imprensa e rádios de referência locais e estaduais, associadas ou não às cadeias de radiodifusão nacionais. Valia o mesmo para as subsidiárias das três cadeias de televisão, NBC, ABC e CBS, com Walter Cronkite, o apresentador das CBS Evening News, considerado invariavelmente, nos inquéritos de opinião dos anos

[21] Homa Hosseinmardi, Amir Ghasemian et al. (2021) e Homa Hosseinmardi, Amir Gahsemian, Miguel Rivera-Lanas, Ducan Watts (2024).

60 e 70, como «o homem mais confiável na América». A confiança começou a decair após o escândalo Watergate, que levou Richard Nixon a abandonar a Casa Branca, em 1974, mas só no início deste século os estudos de opinião passaram a registar respostas em que mais de metade dos inquiridos expressava desconfiança em relação aos media.

À medida que diminui a confiança quanto a informações emanadas de organizações de media nacionais e locais, aumenta a fiabilidade atribuída a redes sociais. Assim, 37% dos inquiridos pelo Pew Research Center, entre 16 e 22 de Setembro, conferiam «muita ou razoável confiança» a notícias colhidas em redes sociais — 1/3 em acessos a Facebook e YouTube —, subindo para 52% na faixa entre 18 e 29 anos. Ainda que comparativamente mais alta, a confiança em «organizações de informação» locais, 74%, e nacionais, 59%, esta percentagem tem vindo a reduzir-se desde 2016 quando se cifrava em 82% e 76%, respectivamente, indicam os estudos do Pew Research Center.[22]

Face a estes dados importa sublinhar, uma vez mais, que se, nos Estados Unidos, é cada maior o volume de informação e desinformação disseminadas através de redes sociais, incluindo a emanada por media tradicionais, o seu consumo é inferior ao da veiculada por órgãos de rádio, televisão e imprensa locais e nacionais. O impacto é variável consoante faixas etárias, convicções políticas e religiosas, níveis educacionais e de rendimentos, além da frequência e exclusividade de consumo.

Informação verdadeira disseminada através de redes sociais, bem como falsidades ou alegações tendenciosas expressas por má-fé, só ganham, no entanto, impacto relevante a partir do momento em que entram no cardápio de oferta dos media institucionais que asseguram a maior difusão nacional possível. Donald Trump aproveitou a sua conta no Twitter, aberta em Maio de 2009, para o lançamento da candidatura presidencial seis anos depois quando @realDonaldTrump contava com 2,98 milhões de seguidores. O candidato alargou com recurso às redes sociais a base de apoiantes, mas nessa estratégia

---

22 https://news.gallup.com/poll/651977/americans-trust-media-remains-trend-low.aspx https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/
https://www.pewresearch.org/short-reads/2024/10/31/americans-top-sources-of-political-news-ahead-of-the-2024-election/ John White (2024).

contou ainda mais a opção da Fox News de Rupert Murdoch — líder do mercado noticioso por cabo à frente da CNN e MSNBC — em promover Trump que assim se tornou presença incontornável nos serviços informativos da NBC, CBS e ABC, os maiores canais comerciais em sinal aberto. Na Casa Branca @realDonaldTrump serviu para, dispensado meios de comunicação institucionais, veicular todo o tipo de informação e desinformação. Em Janeiro de 2021, quando a plataforma Twitter suspendeu a conta, @realDonaldTrump apresentava 88,9 milhões de seguidores e convertera-se em fonte obrigatória de citação por agências de notícias e toda a panóplia de media.

Sobrestima-se a penetração de informações — falsas, tendenciosas, parcelares ou suficientemente exaustivas, verdadeiras, incoerentes ou infundadas, de fonte identificada ou fidedigna — por via de redes sociais, ao ignorar que, presentemente, e, em especial, nos Estados Unidos, o seu impacto passa pela mediação dos media.

Uma conclusão: em regimes democráticos são os media, como guardiões no sistema informativo do universo comunicacional, a definir critérios de publicação em função de veracidade, relevância genérica ou para público-alvo, de oportunidade. Independentemente do seu viés sobrepõem-se a outras formas de produção e difusão de notícias para a maioria da população. A evolução deste sistema é uma incógnita, mas, de momento, a maior ameaça num regime democrático, em que a liberdade de expressão conta, é a degradação de qualidade, a diminuição da penetração e do impacto dos chamados media tradicionais.

BIBLIOGRAFIA

- Allport, Gordon e Posntman, Leo. The Psychology of Rumor, Henry Holt & Company, New York, 1948.
- Allport, Gordon. The nature of prejudice. Addison-Wesley, Reading, Ma., 1954.
- Arnold-Forster, Tom. Walter Lippmann and Public Opinion, American Journalism, 40:1, 51-79, 2023.
- Audinet, Maxime e Colin, Gérard. Crise, recomposition et clandestinisation du dispositif d'influence informationnelle de la Russie après l'invasion de l'Ukraine In Diplomatie numérique et stratégies d'influence politique. Réseaux 2024/3 N° 245, La Découvert, Paris.
- Badillo-Matos, A., Baldi, V., Arteaga, F., Paisana, M., Crespo, M., Cardoso, G.,

Rementería, M.J., Philippe, O., Calvo, B., Buslón, N., Hernández-Escayola, P., Gómez-Romero, J., Molina-Solana, M. Analysis of the Impact of Disinformation on Political, Economic, Social and Security Issues, Governance Models and Good Practices: The cases of Spain and Portugal. Pamplona: IBERIFIER, Pamplona, 2023.

- Barabanov, Ilia, e Korotkov, Denis. Nash Biznes — Smert, Meduza Riga, 2024 (Trad. portuguesa, O Nosso Ofício é a Morte. A História do Grupo Wagner. Ed. Zigurate, Lisboa, 2024).
- Botero, Giovanni. Della Ragion di Stato, Ed. a cura di Pierre Benedittini e Romain Descendre, Einaudi, Torino, 2016.
- Budak, C., Nyhan, B., Rothschild, D.M. et al. Misunderstanding the harms of online misinformation. Nature 630, 45–53, 2024.
- Bulgakov, Mikhail. Sabatchie Serdtze / Coração de Cão (1925), Eksmo, Moscovo, 2019.
- Carbonnier, Jean. Flexible droit. Textes pour une sociologie du droit sans rigueur, LGDJ, Paris, 2001.
- Christensen, Clayton e Bower, Joseph. Disruptive Technologies: Catching the Wave, Harvard Business Review 73, no. 1 (January–February), 1995.
- Christensen, Clayton e Raynor, Michael. The Innovator's Solution, Harvard Business School Press, Cambridge, Ma., 2003
- Clausewitz, Carl von. Vom Kriege. Mit einem Nachwort von Fredmund Malik, Insel Verlag, Frankfurt am Main – Leipzig, 2016 (Da Guerra, tradução de Teresa Pinto Barroso, Perspectivas & Realidades, Lisboa, 1976).
- Cockett, Richard. Vienna: How the City of Ideas Created the Modern World, Yale University Press. New Haven – London, 2023.
- Froissart, Pascal. L' Invention Du Fact-Checking: Enquête Sur La Clinique Des Rumeurs, Boston, 1942-1943, Presses Universitaires de France, Paris 2024.
- Ge Zhaoguang. What is China? Harvad University Press, Cambridge, Ma / London, 2018
- Gerassimov, Valerii. Tsennost Nauki v Prividenii / O Valor da Ciência na Previsão, Voennoe-Promishlennii Kurrier, Nº 8, (476), Moscovo, 27/02/2013.
- Grinberg N, Joseph K, Friedland L, Swire-Thompson B, Lazer D. Fake news on Twitter during the 2016 U.S. presidential election. Science. 2019 Jan 25; 363(6425):374-378.

- Homa Hosseinmardi, Amir Ghasemian et al. Examining the consumption of radical content on YouTube. Proceedings of the National Academy of Sciences Vol. 118 | No. 32, August 10, 2021.
- Homa Hosseinmardi, Amir Gahsemian, Miguel Rivera-Lanas, Ducan Watts, Causally estimating the effect of YouTube's commender system using counterfactual bots https://doi.org/10.1073/pnas.2313377121 .
- Houellebecq, Michel. Extension du domaine de la lutte, Éditions Maurice Nadeau, Paris, 1994
- Jao Tsung-I. Space, Time, Myth, and Morals: A Selection of Jao Tsung-i's Studies on Cosmological Thought in Early China and Beyond, Brill, Leiden, 2022.
- J. Allen, B. Howland, M. Mobius, D. Rothschild, D. J. Watts. Evaluating the fake news problem at the scale of the information ecosystem. Sci. Adv. 6, eaay3539 (2020).
- Kennedy, Patrick J. e Prat, Andre. Were do People get their news? Economic Policy, January 2019-
- Khosrokhavar, Farad. Le Nouveau Jihad en Occident, Robert Laffont, Paris, 2018.
- Klemperer; Victor. Elke Fröhlich (ed.). LTI — Lingua Tertii Imperii: Notizbuch eines Philologen, Reclam, Stuttgart, 2010.
- Knoblock, John trans., Xunzi: A Translation and Study of the Complete Works, Volume II: Books 7–16, Stanford University Press, Stanford, 1990.
- Konrad, Nikolai. Izbrannie Trudi – Sinologia / Obras Escolhidas – Sinologia, Nauka, Moscovo, 1977.
- Konrad, Nikolai. Zapad i Vostok. Statii / Ocidente e Oriente. Artigos, Nauka, Moscovo, 1966.
- Lippmann, Walter. Public Opinion (1922), Dover Publications Mineola, NY, 2004
- Lomnitz, Claudio. El tejido social rasgado. Ediciones Era, Ciudad de México, 2022
- Lomnitz, Claudio. Para una teología política del crimen organizado. Ediciones Era, Ciudad de México, 2023.
- Magallón-Rosa, R., Paisana, M et al. Disinformation consumption patterns in Spain and Portugal, Pamplona: IBERIFIER, Pamplona, 2004.
- Martinho Hermínio, Experimentum Humanum – civilização tecnológica e

condição humana, Relógio D'Água, Lisboa, 2011.
- McCabe, S.D., Ferrari, D., Green, J. et al. Post-January 6th deplatforming reduced the reach of misinformation on Twitter. Nature 630, 132–140, 2024.
- Olivelle, Patrick. King, Governance, and Law in Ancient India: Kautilya's Arthaśāstra, Oxford University Press, Oxford, 2013.
- Pomerantsev, Peter. Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia, Public Affairs New York 2014.
- Rodrigues, Ernesto. Crónica Jornalística. Século XIX. Círculo de Leitores, Lisboa, 2004.
- Sorokina, Marina. Nikolai Konrad: jizn mejdu Zapadom e Vostokom // Tragitchkie sudbi: repressirovannie utchonie Akademii nauk SSSR / Nikolai Konrad: Uma vida entre o Ocidente e o Oriente // Destinos trágicos: cientistas vítimas de repressão da Academia de Ciências da RSSS, Nauka, Moscovo, 1995.
- Sylvain Dejean, Marianne Lumeau, Stéphanie Peltier. Une analyse de la concentration de l'attention par les groupes médiatiques en France. Document de travail, 2023. hal-04124447 https://hal.science/hal-04124447v1
- Tchakhotine, Serge, Le Viol des foules par la propagande politique, Gallimard, Paris,1939.
- Thapar, Romila. Cultural Pasts, Oxford University Press, New Delhi, 2000.
- Walgrave, S. e Soontjens, K. How politicians learn about public opinion. Research & Politics, 10 (3), 2023.
- Weber, Max. Politik als Beruf (1919), Duncker & Humblot, Berlin, 2010. (Trad. de Helena Toppa, A Ciência e a Política como Ofício e Vocação, Relógio D' Água, Lisboa, 2017)
- Werth, Nicolas. Poutine, Historien en chef, Gallimard, Paris, 2022.
- White, John Kenneth. Grand Old Unraveling. The Republican Party, Donald Trump, and the Rise of Authoritarianism, University Press of Kansas, Lawrence, 2024.
- Wm. Theodore de Bary, Stephen Hay, Royal Weiler, Andrew Yarrow. Sources of Indian Tradition. Motilal Banarsidass, New Delhi/ Patna / Varanasi, 1988 = Sources of Indian Tradition, Columbia University Press, New York, 1958.
- Ying-shih Yü. Chinese History and Culture. Sixth century B.C.E. to seventeenth century. Columbia University Press, New York, 2016.
- Ying-shih Yü. Chinese History and Culture. Seventeenth century through

twentieth century. Columbia University Press, New York, 2017.
- Yuxi Wang, Martin McKee, Aleksandra Torbica, David Stuckler. Systematic Literature Review on the Spread of Health-related Misinformation on Social Media, Social Science & Medicine Volume 240, November 2019, 112552 Elsevier, Amsterdam.

Coronel Agostinho Cunha

Depois desta área que dava lugar quase a uma conferência específica e porque pode utilizar instrumentos que são importantes em termos de pública, nomeadamente as redes sociais, vamos passar a outra área setorial e vamos ver a segurança económica e energética. E para isso temos connosco o Dr. Filipe Santos Costa, que é investigador do IPRI e foi já presidente da AICEP e foi cônsul económico e comercial de Portugal nos consulados gerais em São Francisco e em Xangai. Foi também encarregado da estrutura de missão para a gestão dos fundos comunitários no Ministério da Administração Interna e chefe de gabinete do Ministro da Justiça. Atualmente, o Dr. Filipe Santos Costa é vice-presidente do Conselho Portugueˆs do Movimento Europeu e vogal do Conselho Fiscal da Comissão Portuguesa do Atlaˆntico.

Dr. Filipe Santos Costa

Muito obrigado e muito obrigado à Senhora Professora Isabel Ferreira Nunes pelo convite e ao General Valença Pinto. É um gosto estar aqui.
Também não vim equipado com slides, até porque tinha ficado com o conceito de que se tratava de uma mesa-redonda de debate e para ser fiel a essa minha própria interpretação, vou pegar, por exemplo, na referêˆncia que o João Carlos Barradas fez a Pearl Harbour.
Esta audieˆncia sabe muito melhor que eu que grande parte da justificação do ataque japoneˆs a Pearl Harbour foi o embargo dos Estados Unidos a produtos petrolíferos. O Japão importava 80% do petróleo dos Estados Unidos, era essencial para a sua máquina de guerra, interpretou este ato como um ato de agressão económica e, de qualquer maneira, também era preciso, peço desculpa pelo simplismo, era preciso, a bem do tempo, simplificar para ser sucinto, e também precisava da abertura desse conflito para poder progredir pelas colónias francesas, e,nomeadamente, pelas holandesas, fontes de petróleo, de recursos.

Este erro, juntamente com o erro da Alemanha, que também na sua precipitação na Operação Barbarossa, em 1941, se precipitou para o Cáucaso. Estes dois erros, dois em 1941, contribuíram muito para o desfecho feliz da Segunda Guerra Mundial, mas mostram, de facto, a importância dos recursos económicos, neste caso energéticos, para a guerra e também a circunstância da guerra por recursos económicos e energéticos. E também mostram que a disrupção tecnológica, com as tecnologias disruptivas, é essencial para o progresso económico e energético. Isto era verdade na altura.

Isto aconteceu porque, na Primeira Guerra Mundial, houve a mecanização dos conflitos e, com consumos pouco otimizados, deva-se dizer. Desde os blindados às aeronaves, aos navios, enfim, eu sei que muita gente nesta sala saberá detalhes que eu agora não posso estar a referir, como os tratados de limitação marítimo anglo-alemão e os navios a carvão, navios a petróleo, etc., mas era notório que o *oil and gas* teve um papel essencial aqui. E o *oil and gas* tem um papel essencial também numa análise que, se quisermos fazer, do ponto de vista económico e energético, da Guerra da Ucrânia.

Vejamos duas valências completamente diferentes. Por um lado, a guerra na Ucrânia, ou a invasão da Ucrânia pela Rússia, mostrou uma Europa Oriental e Central completamente dependente do gás russo. O gás russo vem pelo gasoduto, ou seja, é um *seller's market*. Se vem pelo gasoduto, só vem de um sítio, só se compra a esse sítio.

Portugal não teve este problema, porque obviamente Portugal, até pela sua posição geográfica e, em parte, por ter a França pelo meio, entre si e o resto da Europa, não tem gasodutos que liguem à Europa, muito menos à Europa de leste e, portanto, recebe o seu gás por terminais de gás natural e liquefeito.

Aliás, metade da capacidade de receção, não é exatamente metade, é 48,5% da capacidade de receção e de gasificação de gás natural da Europa está na Península Ibérica, apesar de haver agora alguns esforços, para desenvolver infraestruturas em Wilhelmhaven e outros sítios na Alemanha. Mas tirando nós e a Grécia, que nunca se colocou nessa situação, de depender de gasodutos que viessem, por exemplo, da Turquia ou do Azerbaijão, temos esta dependência exclusiva.

Do outro lado da Rússia, o Japão não teve o mesmo problema que a Alemanha. Ninguém aqui nesta sala está a ver o Japão a colocar-se na situação de ter o seu fornecimento energético dependente de um par de gasodutos vindos da Rússia. Não. O Japão tem trinta e seis terminais de gás natural liquefeito. Nós, na

Península Ibérica, temos metade da capacidade europeia e temos cinco a funcionar, um em Portugal e quatro em Espanha. Portanto, estas questões têm, obviamente, a sua importância.

Também não é por acaso que o Japão é o primeiro país a ter um terminal de receção e regaseificação de hidrogénio liquefeito. Portanto, a tecnologia que se tem falado tanto em Portugal, e em várias perspetivas, do hidrogénio, seja gasificado, seja liquefeito, já é uma realidade no Japão. O Japão já arranjou maneira de produzir, neste caso na Austrália, mas é com tecnologia japonesa, tecnologia disruptiva, produzir hidrogénio na Austrália com um processo de captura e sequestro de carbono feito a partir de carvão castanho, que é menos pretendido, de o liquefazer. O desafio é que o gás natural tem um ponto de ebulição em torno dos, para simplificar, 160 graus negativos e o hidrogénio são 260. Mais ou menos isto, não él? E, portanto, é uma dificuldade, mas é uma dificuldade em que há um grande investimento em tecnologia para, no caso do Japão, que é um país que tem sempre esta preocupação, superar a sua dependência do exterior.

E é um bocadinho disto que falamos quando falamos no problema do fornecimento de gás natural da Rússia à Alemanha no contexto da Guerra da Ucrânia. Rapidamente, a evolução e a aposta na disrupção tecnológica, na evolução tecnológica da produção de energia, teve um salto ao nível das instituições europeias. A União Europeia produziu, de repente, medidas de legislação, a começar no "*Fit for 55*", depois o "*Repower EU*", depois o "Quadro Temporário de Transição e Crise 2023", que deram origem a uma série de iniciativas de criação de terminais de gás natural liquefeito, que passou a ser considerada uma energia verde de transição, para diminuir a dependência do petróleo e para facilitar a sua aceitação na Europa, uma vez que agora vem a um custo mais caro e que requer grandes investimentos. Portanto, teve que se abandonar um pouco aquelas teorias de não vamos investir, porque é uma energia que produz carbono, vamos antes dizer que é uma energia que produz baixo carbono e que relativamente ao petróleo é uma boa opção, e vamos classificá-la como energia verde de transição, porque vamos ter que fazer investimentos massivos para passar a importar mais dos Estados Unidos, da África Ocidental e do Médio Oriente, por via marítima.

O gás natural liquefeito, com as tecnologias atuais, é antieconómico liquefazê-lo para menos de 5.000 km de percurso. Vamos apostar no nuclear, vamos considerar o nuclear como verde. Vamos dar razão aos protestantes

adolescentes suecos e vamos dizer que o nuclear é verde e vamos apostar no nuclear. Vamos inverter completamente a nossa ideia de abandonar o nuclear na Alemanha, na Holanda, nos Países Baixos, e vamos começar a fazer centrais nucleares.

Aqui há um processo de evolução tecnológica que tem sido descrito ao longo desta manhã que implica enormes quantidades de energia. Então estas ideias de que reduzir o consumo, otimizar o consumo, reduzir o consumo lá em casa, ter uma bomba de calor em vez de ter ar condicionado, são ótimas medidas de poupança, mas não têm impacto na dinâmica de brutal consumo de eletricidade. Esse brutal consumo de eletricidade vem de dois fatores. E quais são os dois fatores? O desenvolvimento. Portanto, nós ouvimos aqui algumas intervenções e, por exemplo, a intervenção de João Montenegro quando fala em *data centers*. *Data centers* no espaço, não sei, mas imagino que tenham zero humidade e uma ótima temperatura. Mas nada nunca consumiu tanta eletricidade como *data centers*. Nunca se construíram tantos *data centers* tão complexos. É uma coisa de multiplicação exponencial como agora para as tecnologias, por exemplo, da inteligência artificial. Portanto, estamos a falar num aumento brutal do consumo de energia a par de uma eletrificação de tudo. Tudo, porque a maneira de descarbonizar é eletrificar. Eletrificar diretamente, por exemplo, à aposta da atual administração americana, as ações da Tesla subiram ontem 14%, por motivos vários que agora não vale a pena comentar. Já foram há bocado falados acerca do Starlink, mas também porque há uma clara opção pelos veículos elétricos em detrimento de veículos a gases renováveis. E depois outras implicações geopolíticas, sendo os Estados Unidos um país que agora basicamente controla o comércio internacional de *oil and gas*, não há grande incentivo para substituir por gases renováveis. E as ações de tudo o que é hidrogénio e gases renováveis nos Estados Unidos caíram a pique. Portanto, as relacionadas com a eletrificação direta subiram 15%. As relacionadas com os gases renováveis como uma intermédia de eletrificação, porque, lá está, para produzir hidrogénio verde, para produzir amoníaco verde, estamos a falar na eletrólise, estamos a falar na aplicação de eletricidade à água, estamos a falar de mais eletricidade, mais eletricidade de fontes renováveis. É uma coisa brutal. Essas caíram 15%, 16%, 20%. Mas a Europa aposta nelas, porque a Europa, ao contrário dos Estados Unidos, não é excedentária em petróleo e gás. E, portanto, nós temos uma grande aposta nos instrumentos europeus, no "*RepowerEU*", no "*Fit for 55*", e na produção de gases renováveis para a indústria. Isto é eletrificação. O crescimento

do setor das tecnologias de informação e comunicação, que foi tão falado hoje, é mais eletrificação. Eletrificação daquilo que ainda não foi eletrificado, os transportes. É mais eletrificação. Portanto, há aqui uma soma brutal do consumo de eletricidade.

Aliás, aludindo, também, aqui, às minhas anteriores funções de Presidente da AICEP, nós tínhamos um problema, que agora até posso referir um bocadinho mais à vontade, é que no Plano de Desenvolvimento da Infraestrutura da Rede Nacional de Transmissão Elétrica, o palavrão que tem o acrónimo DIRT-E, que é aprovado pela Assembleia da República por proposta da entidade reguladora do setor energético, por proposta da Direção-Geral de Energia, e é transmitido à REN e à E-REDES, como empresas privadas, mas 100% reguladas, previa-se 50% de *terawatts* de consumo em Portugal, com um crescimento ali à volta de 7% a 14%. A estimativa que há com os *pipelines* de investimentos em *data centers*, eletrificação dos veículos, construção e eletrificação, como, há pouco, Arnaut Moreira falava da refinaria de Sines. Vou usar isso como exemplo. Só isto significa que as necessidades de consumo elétrico não crescem no período de análise até 2031, entre 7% a 14%, mas sim cerca de 100%, entre 100% e 200%, conforme o nosso sucesso na transição e na atração de alguns destes projetos, que, aliás, projetos que Portugal conseguirá atrair, projetos químicos, H2, NH3, *data centers*, etc., se tiver disponibilidade de eletricidade verde. Se não tiver, não tem. Portanto, se correr bem, o nosso consumo elétrico triplica. Se correr mal economicamente, duplica. Agora, crescer 7% a 14%, só em caso, de facto, de vir aí o diabo, como em tempos se dizia, e acho que eram precisos vir vários.

O segundo aspecto, que também foi aqui falado é a importância da energia na Guerra da Ucrânia. A infraestrutura energética é um alvo. Portanto, muito do que foi aqui falado, da utilização de drones, da utilização de mísseis balísticos hipersónicos, não sei se já são usados, mas todos os outros que são usados são muito direcionados à infraestrutura energética, porque, obviamente, a energia é absolutamente essencial para a soberania, para a autonomia, para a capacidade de operação de um país. Temos exemplos extremos de segurança, de procura de segurança económica e energética, melhor sintetizados nas teorias Juche da Coreia do Norte, que é de facto um país que funciona melhor em autarcia do que nós. Nós não funcionávamos, se amanhã tivéssemos que nos fechar, como a Coreia do Norte se fecha, queríamos isso? Provavelmente não.

Mas também não vale a pena dramatizarmos, porque a taxa de dependência do mundo ocidental em relação ao resto do mundo é relativamente mais pequena

do que aquilo que pensamos. Nós falamos, eu vou aqui fazer uns apontamentos hipersónicos. Nós, aqui falamos na nossa dependência do exterior. Portugal, se considerarmos só o comércio extracomunitário, tem uma taxa de abertura da economia de 25%. É a mesma dos Estados Unidos. Portanto, nós, como membros da União Europeia, temos uma taxa de abertura da economia igual à dos Estados Unidos. Sendo que o nosso maior fluxo da União Europeia é precisamente com os Estados Unidos e dos Estados Unidos connosco. A China é ligeiramente maior fornecedor que os Estados Unidos, mas depois de somarmos a energia e somarmos os produtos, o investimento, aí a desproporção é brutal. Só para dar um número, o investimento direto acumulado europeu, de empresas europeias na América do Norte, nos Estados Unidos e no Canadá, é mais de dez vezes o acumulado das empresas da União Europeia na China e na Índia. O *stock* de investimento. Portanto, a relação bilateral aqui é muito forte. A dependência não é tão grande quanto se pensa. Mas, escolhendo aqui um último apontamento para fazer, além da questão energética, que eu já tentei referir, nós temos um grande sucesso em Portugal na transição energética. E isso reflete-se na nossa segurança económica. Porquê? Porque dependemos menos de energia importada e dependemos de uma maior diversidade de fontes energéticas, algumas das quais autóctones. Isto tem uma expressão tão grande, que eu vou dar-vos só um número. Hoje não tenho slides e, portanto, vou só dar apenas um número. Nós, em 2023, importámos menos 6 mil milhões de euros de *oil and gas* do que no ano anterior. E tivemos um superávit comercial de 3,3 mil milhões de euros. Portanto, só a quebra que tivemos na importação de *oil and gas* mais que justifica ou justifica o dobro da nossa passagem de déficit para superávit. Não justifica totalmente, porque o déficit era de 4 mil milhões, mas é praticamente isso. Isto é o quê? Já não temos centrais a carvão, não usamos centrais a diesel, são as centrais de ciclo combinado a gás. O gás é importado, mas a funcionar é menos, porque temos mais hídrico, mais eólico, mais solar. Portanto, isto reduz a nossa dependência do exterior. Também ajuda o facto de, em vez de termos um *pipeline* para a Rússia, podermos decidir se amanhã a Nigéria, por algum motivo, não nos vender gás natural, como já aconteceu, podemos comprar aos Estados Unidos ou podemos comprar ao Qatar, como já aconteceu.

Último apontamento: este era o desengajamento da Europa em relação à Rússia em termos de energia. Desengajamento tecnológico, que eu gostava de falar que também foi aqui muito referido. Só para dar um apontamento final: números

daquilo que alguns participantes já referiram, Estados Unidos da América. Falando aqui nos *chips*, nessa questão crítica, os *chips* são críticos por quê? Porque vêm maioritariamente de Taiwan, muitos deles são produzidos na China, mas obviamente há uma enorme necessidade de diversificar o risco em relação a Taiwan. E o que é que se faz? Faz-se aquilo que os chineses fizeram aos europeus e aos americanos, que é o que é inteligente fazer. Atraiem—se as empresas que têm a tecnologia e obriga-se essas empresas a investir nos nossos países. Estados Unidos: *Chips Act* e *Science Act* de 2022 mobilizam 53 mil milhões de dólares para incentivos ao fabrico de semicondutores. A Taiwan Semiconductor Manufacturing Company, a famosa TSMC, já recebeu 6,6 mil milhões de euros para instalar produção nos Estados Unidos. Produção nos Estados Unidos para garantir que há *chips*, nos Estados Unidos, para quando é preciso construir automóveis ou outra coisa qualquer, e é sempre preciso construir automóveis e frigoríficos e tudo e mais alguma coisa, e linhas de produção de vinho que não funcionam se não tiverem *chips*. E diversificar o risco em relação a Taiwan, porque atualmente a produção de semicondutores está quase exclusivamente concentrada em Taiwan e na Coreia do Sul. A SK Hynix da Coreia do Sul recebeu 450 milhões de dólares por uma pequena unidade.

A Europa a mesma coisa. O *European Chips Act* 2023 mobiliza 43 mil milhões de euros. Na Alemanha, a mesma TSMC, aí numa parceria com a Bosch e com a Infineon, etc., tem um projeto de uma fábrica de *microchips* de 10 mil milhões de euros de investimento em Brandenburg, não, perdão, em Dresden. Em Brandenburg é a outra que eu gostava de referir, mas… metade é incentivo alemão aprovado precisamente ao abrigo do quadro temporário de transição e crise no qual o nosso atual orçamento de Estado, portanto, resulta da Resolução do Conselho de Ministros 74 de 2023, de março, tem também uma verba de mil milhões de euros. E essa verba de mil milhões de euros está prevista ser investida em quê? Num projeto de refinação de lítio, incentivos para um projeto de refinação de lítio, incentivos para um projeto de construção de baterias de lítio para veículos elétricos e um projeto para fabrico de cobre e níquel para baterias elétricas. Um projeto sueco, um projeto chinês, um projeto belga, todos com parceiros portugueses. E projetos, claro, de hidrogénio verde, NH3 e combustíveis alternativos.

Última frase: para os *hard to abate sectors* da eletrificação, transporte aéreo, transporte marítimo e transporte rodoviário pesado, estou a falar de *sustainable aviation fuel*, *alcohol-to-jet fuel*, tudo coisas a ser feitas na refinaria de Sintes,

onde, só para substituir os 600 megawatts de potência do hidrogénio cinzento que lá atualmente é produzido, que é o *cracking* do metano, CH4, é preciso substituir isso por hidrogénio verde. Para substituir esses 600 megawatts de potência da refinaria de Sines de hidrogénio cinzento, que é uma pequena parte da refinaria, por hidrogénio verde, é preciso gastar cinco a seis terawatts/hora/ano de eletricidade. Ou seja, o equivalente a 10% ou 12% do nosso atual consumo elétrico nacional.

Coronel Agostinho Cunha

Obrigado. Sem mais demoras, vamos passar aqui à nossa última oradora, a Sra. Dra. Juíza Conselheira Helena Fazenda, que se especializou na área criminal e na área das informações e foi Diretora Nacional Adjunta da Polícia Judiciária, foi Membro da Unidade dos Magistrados do Organismo de Luta Antifraude, foi Diretora Adjunta do SEF e do Centro de Estudos Judiciários e foi Secretária-Geral do Sistema de Segurança Interna e Juíza Conselheira do Supremo Tribunal de Justiça.

Juíza Conselheira Helena Fazenda

Muito obrigada, Senhor Coronel. Muito boa tarde a todos. Eu prometo restringir a minha intervenção o máximo possível. Muito obrigado Senhora Professora Isabel Ferreira Nunes e também ao Senhor General Valença Pinto por esta oportunidade e pelo regresso a esta casa, onde fui muito feliz. Começou, precisamente, há um ano, fez ontem um ano, que iniciei o Curso de Defesa Nacional, onde tive a honra de ser auditora e, de facto, passámos momentos inesquecíveis.
Bom, toda a manhã, de facto, se falou de um conjunto de inovações tecnológicas e desenvolvimento tecnológico acelerado, capazes de corresponderem e darem resposta a situações boas, mas também a situações disruptivas e criarem e serem potenciais criadores das ameaças híbridas. E penso que é esse o tema central aqui do nosso painel, ligado à questão das informações. E a ameaça híbrida é isso, é um tipo de perigo que combina diferentes formas de ataque ou táticas, para alcançar objetivos específicos, geralmente envolvendo contextos civis e ou militares.
O agente da ameaça pode utilizar uma combinação de táticas convencionais e

não convencionais, ataques cibernéticos, desinformação, espionagem e manobras políticas e económicas subversivas. Enfim, de tudo se tem falado esta manhã e também outras estratégias para desestabilizar o alvo ou alcançar objetivos determinados. Pode ser utilizado por Estados ou por grupos não estatais e geralmente busca explorar as vulnerabilidades do alvo em diversas frentes, dificultando resposta eficaz.

Portanto, a ameaça híbrida exige uma abordagem multifacetada, encurtando aqui razões, na defesa e nas políticas de segurança, dado que envolve ou implica contextos militares, proteção de redes de informação, comunicação, integridade e segurança da sociedade civil. Esta abordagem multifacetada refere-se à necessidade de envolver um conjunto diversificado de estratégias e ferramentas para enfrentar a ameaça. Por isso, a dissuasão de ameaças híbridas requer um entendimento profundo do contexto e dos respetivos agentes, além de uma preparação para responder de forma ágil e coordenada a uma gama variada de cenários e táticas, com foco na importância da informação correta e no fortalecimento da resiliência social e institucional.

Daí eu identificar a importância da transparência e da comunicação clara por parte das autoridades junto das populações, de forma a construir confiança e minimizar o espaço para a desinformação. Da educação e da consciencialização, a literacia é, de facto, fundamental também aqui, em capacitar as pessoas em como reconhecer e reagir às desinformações e ameaças híbridas é vital, por isso os programas educativos a este respeito são essenciais. Monitorização e análise de informações, através do uso de tecnologias de análise de dados e através da inteligência artificial, que aqui, de facto, estará do lado do bem, na deteção de padrões e de ameaças e na cooperação internacional, já que também este tipo de ameaças, frequentemente, senão sempre, ultrapassam fronteiras e aqui a cooperação é absolutamente incontornável.

Também, a resiliência das infraestruturas críticas, de que se falou bastante e acaba de se falar, críticas ou sensíveis, de acordo com a nova designação do Regulamento da União Europeia. É que proteger as infraestruturas críticas de ciberataques, por exemplo, e garantir que haja planos de contingência e recuperação atualizados e sobretudo testados é absolutamente incontornável para manter a operacionalidade normal, em situação de crise. Do envolvimento da sociedade civil em toda esta panóplia de ações de dissuasão, através da participação de organizações, incluindo os media, organizações da sociedade civil, porque aumenta a consciencialização e a resiliência da população. Também

políticas de resposta e contenção, ou protocolos que suportem a disseminação de informações corretivas e a contenção de narrativas prejudiciais, para além de, naturalmente aqui, ter de haver um equilíbrio com a proteção da liberdade de expressão, sendo essencial, encontrar aqui a proporcionalidade entre a luta contra a desinformação e a proteção da liberdade de expressão.

Olhando um pouco mais para dentro, e de acordo com o RASI, em 2023, diversos instrumentos foram utilizados persistentemente contra interesses nacionais e da Aliança Atlântica, salientando-se de entre as diversas ameaças híbridas, a propaganda e as operações de informação e desinformação em ambiente digital, que visam afetar a coesão sociopolítica das sociedades, a capacidade de decisão das instituições e dos alicerces do Estado de direito democrático. Indivíduos e movimentos que subscrevem ideários extremistas, violentos ou conspirativos adaptaram as suas ações de desinformação aos novos acontecimentos internacionais.

A desinformação em plataformas digitais mais sofisticadas e com significativa integração de ferramentas de inteligência artificial continua a ser fortemente disseminada e a visar diversos tipos de audiências no espaço euro-atlântico, abrangendo não só as duas questões supracitadas, mas também questões migratórias e de igualdade de género. Isto refere o RASI de 2023 e na parte referente às ameaças.

No contexto da dissuasão de ameaças híbridas, sublinha-se o papel importante dos serviços de informações. Considerando o tema do painel e, enfim, o ponto que me foi proposto, gostaria de notar que quando falamos de informações, tal deve ser entendido no sentido anglo-saxónico do termo, isto é, *intelligence*, falamos de conhecimento de informações que contribuem para diminuir a incerteza do decisor político, no âmbito da segurança, defesa nacional e política externa, melhorando, dessa forma, a tomada de decisão. Distingue-se, portanto, de informação no sentido do órgão de comunicação social, ou de informações criminais, ou de informações policiais, ou de *competitive intelligence*, ou ainda de informações produzidas por empresas privadas. A intervenção das informações diria ser marcada por oito momentos cruciais e que entram, de facto, num quadro clássico, mas também as ameaças híbridas têm a componente convencional e não convencional. Daí que, parece-me, se mantêm atuais estes momentos de produção de informações. Tem a ver com a recolha sistemática de dados relevantes e aqui, de facto, as fontes são fundamentais. Tem a ver com a análise de dados recolhidos para identificar padrões, tendências e ameaças e portando

transformar dados brutos em informações úteis. Tem a ver com a produção de relatórios que se pretende que possam ser utilizados para planear ações estratégicas e, sobretudo, lidos pelos respetivos destinatários, nomeadamente no plano político, é fundamental que isso aconteça. Disseminação da informação, ela é crucial. Os serviços de informações devem garantir que as informações e os relatórios chegam às pessoas e às instituições certas, em tempo útil, possibilitando uma decisão informada. A monitorização permanente, com vista à deteção de potenciais mudanças. O desenvolvimento de capacidades e é muito importante que aqui, de facto, os serviços de informações consigam beber e captar para o seu quotidiano, enfim, todo este desenvolvimento tecnológico a que assistimos, que, de facto, pode comprometer a segurança, mas também pode e deve ser utilizado no combate à ameaça. A integração de dados, também é fundamental que seja feita de forma a garantir uma visão transversal e de conjunto da situação da ameaça e a proteção de dados sensíveis que tem de ser salvaguardada, de acordo com os regulamentos em vigor que eu me dispenso de referenciar.

Têm, assim, os serviços de informações, na minha modesta opinião, um papel catalisador na transformação de dados em conhecimento útil, essencial para a avaliação da ameaça à segurança e para a tomada da decisão bem informada, sem prejuízo, naturalmente, das medidas de segurança que as instituições e cada um de nós deve tomar na utilização das tecnologias.

Por seu turno, a complexidade da abordagem destinada à deteção e combate às ameaças no atual contexto, implica intervenção, também, dos serviços de informações em diversos patamares e, desde logo, na cooperação internacional. E aqui, de facto, a circunstância de pertencermos à União Europeia e à NATO facilita, naturalmente, esta colaboração. A capacidade de monitorização, designadamente, por parte dos dois serviços de informações, em ligação, também, estrita com os serviços militares. A desinformação em cibersegurança que requer um esforço conjunto com outras instituições, designadamente com todas as forças e serviços de segurança, serviços militares e com o Centro Nacional de Cibersegurança e também uma política de legislação assertiva que não se cruze e não se oponha entre si e que permita que, de facto, a agilidade nestes mecanismos dissuasores, seja uma realidade.

Devem, portanto, os serviços de informações de segurança vislumbrar os efeitos das dissonâncias, das fragmentações e polarização da opinião pública, na capacidade de resistência aos efeitos das guerras, detetar eventuais avanços de

projetos anti democráticos, avaliar os efeitos da desinformação e das *fake news*, na deslegitimação política e das instituições.

A segurança interna em Portugal é uma componente da segurança interna europeia e de um espaço comum de liberdade, segurança e justiça, com objetivos consagrados na Bússola Estratégica, recentemente aprovada para reforçar, na próxima década, a segurança e a defesa da União Europeia, tal como o Senhor Coronel também já referiu. Trata-se de um projeto ambicioso que envolve os 27 Estados-membros e a segurança de 450 milhões de cidadãos europeus, não deixando lugar para dúvidas quanto ao papel que cada um dos Estados-membros desta União tem nos planos nacional e europeu.

As exigências da era moderna, considerados os tipos de ameaça, cuja antecipação assenta, indiscutivelmente, na intervenção das informações, competindo, aliás, aos serviços de informação de segurança, a avaliação permanente das ameaças à segurança interna, acreditando que a simplificação de estruturas, meios e procedimentos constituem, potencialmente, eficácia, para além do Estado de direito democrático é tanto mais forte quanto melhor for a qualidade dos seus serviços de informações e toda a estrutura que têm de os suportar, colocam-se hoje algumas interrogações que frontalmente aqui deixo expressas.

Na prática, está assegurada, eficazmente, a cooperação entre serviços de informações que integram o Sistema de Segurança Interna e as informações militares? Haverá necessidade de repensar a arquitetura, ou simplesmente agilizar estruturalmente o funcionamento das instituições de prevenção e de reação? Estarão os serviços apetrechados dos meios tecnológicos adequados para fazer face a toda esta panóplia, todo este desenvolvimento acelerado, designadamente das tecnologias disruptivas? É a regulação em vigor e falo aqui no edifício legislativo tão fragmentado e tão parcelado e, por vezes, contraditório, suficiente?

Sem prejuízo de todos os esforços desenvolvidos junto das instituições públicas e privadas, por parte dos serviços de informações, justificar-se-ia, sob escrutínio judicial e democrático, o alargamento do acesso a fontes classificadas? Eu penso que sim. Até porque a avaliação da ameaça é uma coisa muito séria que deve estar sempre presente na tomada da decisão estratégica, designadamente, ou da reação à ameaça iminente e, portanto, quando faço esta pergunta a mim própria, naturalmente, estou a pensar nas restrições impostas pelo Tribunal Constitucional ao acesso a metadados por parte dos serviços de informações.

Metadados não revelam o conteúdo das comunicações, mas podem revelar-se essenciais na antecipação e na avaliação da ameaça. Não deveriam as autoridades que agem com base nas informações transmitidas pelos serviços de informações dar retorno dos resultados dessa mesma comunicação? É que os serviços de informações se queixam, este é o termo correto, e muito bem, que, de facto, não têm retorno do trabalho que produzem. E isto é essencial para ir acumulando informação, para ir tratando informação, para proceder a nova análise e manter atualizado o controlo da situação. Por fim e embora integre órgãos do Sistema de Segurança Interna, como o Conselho de Segurança Interna e o Gabinete Coordenador de Segurança, não traria benefícios à segurança interna, à recolha de dados e à produção de informações, a circunstância do Centro Nacional de Cibersegurança, atualmente no Gabinete Nacional de Segurança, estivesse a par de outras unidades, integrado, sob coordenação do Secretário-Geral do Sistema de Segurança Interno? Eu ponho esta questão a mim própria e partilho-a aqui, desta forma, assim, muito aberta, porque o Centro Nacional de Cibersegurança está representado no Conselho Superior de Segurança Interna, mas, por seu turno, tem um outro Conselho Superior. Muitas vezes esta sobreposição de conselhos, de órgãos, de estruturas, de uma panóplia imensa de legislação a par de estruturas que se vão autonomizando, naturalmente prejudicam a centralidade e a centralização dos dados que produzem informações e que são incontornáveis na resposta, na identificação prévia, na avaliação e na resposta à ameaça.
Muito obrigado.

Coronel Agostinho Cunha

Muito obrigado, Senhora Doutora Juíza. Antes de terminarmos, e não teremos muito tempo para perguntas e respostas, e eu, por isso, vou dar apenas lugar a uma pergunta.
Gostaria só de deixar aqui uma nota. Nós temos estado a abordar esta questão das ameaças híbridas abaixo do patamar do conflito armado. No entanto, todas estas manifestações se passam também ao nível do conflito armado, com dois grandes problemas. O primeiro é que é desenvolvido por entidades que são estatais e não estatais. Por outro lado, é que estas ameaças, em ambientes de conflito armado, poderão ser menos limitadas do que serão, normalmente, abaixo desse patamar, mesmo que possam existir regulamentos para tal, como, por

exemplo, o Direito Internacional Humanitário, que estabelece as suas regras, mas, em termos de conflito, os contendores tendem a não observar essas regras. Portanto, é importante perceber que as ameaças híbridas, em termos de conflito armado, produzem um novo paradigma em termos de guerra. Vão usar um misto de armas convencionais, de táticas irregulares, de terrorismo, criminalidade disruptiva e usando picos diferentes de conflitualidade e desestabilização do adversário. Isto implica que as Forças Armadas desenvolvam uma estratégica militar que misture, não só, no mesmo momento e conflito, aquilo que é a guerra convencional, a guerra irregular, guerra de informação, guerra cibernética, tudo isso para conseguir conter um adversário que pode usar todos os meios que tenha ao dispor no momento que entender para levar avante as suas ações.
Então, para terminar, vou dar palavra a uma pergunta da audiência.

Perguntas e Respostas

Professor João Rucha Pereira

Boa tarde. João Rucha Pereira. Também pertenço ao EuroDefense Portugal. Queria felicitar todos os oradores pelas suas excelentes intervenções, mas queria colocar uma questão à Senhora Dra. Helena Fazenda. Qual é a sua percepção e a sua ideia sobre este problema dos metadatos que tem sido motivo de muita discussão, com opiniões diversas, desde a Polícia Judiciária, enfim, até outras entidades? Como é que vê que se possa resolver esse problema, o que seria muito importante, não só para as questões de investigação, mas também de prevenção?
Muito obrigado.

Juíza Conselheira Helena Fazenda

Muito obrigada.
Eu sou uma defensora de que os serviços de informações deviam ter acesso, pelo menos nos termos em que estava antes do último acórdão do Tribunal Constitucional, aos metadados.
E às vezes acho que isto é uma questão honestamente tão básica para discutirmos num tempo… tão básica, neste sentido, entenda-se. Como é que uma sociedade em pleno século XXI, e nomeadamente o órgão de soberania que

tem a ver com o poder judicial, não entende que é absolutamente necessário, nomeadamente aos serviços de informações, que procedem à avaliação constante da ameaça, que a comunicam ao decisor político, que a comunicam às forças e aos serviços de segurança e a outras entidades, que têm depois a autoridade para reagir à ameaça, não lhes restringir o acesso?
E restringir o acesso quando já estava a ser ensaiado um modelo, legitimado pelo Supremo Tribunal de Justiça, que nem de perto nem de longe, em minha modesta opinião, punha em causa os direitos, liberdades e garantias fundamentais.
Portanto, qual é a minha opinião? A minha opinião é que o acesso devia ser mais alargado. E se, perante todos estes desafios, todas estas ameaças, ainda andamos a discutir o acesso dos serviços de informações a metadados, que só dizem onde é que eu estive, nem dizem com quem é que eu estive, que dizem que eu liguei aqui ao Senhor Doutor, mas que podem trazer uma série de informações que conjugadas com outros dados, podem indicar, e através da análise da informação, efetivamente, material necessário à reação contra a ameaça, interrogo-me se estamos no bom caminho. Hoje, os serviços de informações têm acesso com restrições muito grandes. E estas restrições também se estenderam aos órgãos de polícia criminal, relativamente às investigações criminais, porque foi encurtado o tempo em que os dados podem ser mantidos, guardados. E também trouxe outros problemas acrescidos, como foi a anulação de muitos julgamentos, nomeadamente de decisões que ainda não tinham transitado em julgado, com base nesta decisão. Isto é altamente disruptivo, desculpem a expressão, porque nem causa segurança, nem a montante dá aos serviços que têm que ter a informação para a poderem trabalhar na nossa segurança coletiva, aquilo que deviam ter. E a montante, com a reação de muitos tribunais que acabaram por anular julgamentos com decisões que já tinham sido proferidas, naturalmente, criou uma situação de insegurança jurídica muito, muito grande. Houve outros tribunais que assim não entenderam, felizmente, e sobretudo entendeu-se que decisões transitadas em julgado, como é óbvio, e respeitando o respetivo princípio, não podem ser tocadas.

Coronel Agostinho Cunha

Eu agradeço aos oradores e peço à audiência uma salva de palmas.

3.5 – Encerramento – General Valença Pinto

Eu nunca fui escuteiro, mas prometo que vou ser breve. Bom. O EuroDefense-Portugal congratula-se pela realização deste seminário sobre tecnologias disruptivas num contexto de ameaças híbridas. É-nos muito grato que tenha sido possível organizá-lo em parceria com o Instituto da Defesa Nacional. Estamos agradecidos por isso, tomando as parecerias IDN-EuroDefense-Portugal como algo absolutamente natural.

O tema que aqui hoje trabalhámos dificilmente podia ter maior atualidade. Estas tecnologias existem, porventura não as conhecemos suficientemente bem, nem na sua natureza nem nas suas implicações e consequências, mas sabemos que têm um potencial para alterarem de modo, muitas vezes surpreendente, paradigmas estabelecidos. É por isso que as classificamos como disruptivas. E é também verdade que as ameaças, e por extensão os conflitos do futuro, serão sempre híbridos, numa gama ampla de hibridismo que irá destas fantásticas novíssimas tecnologias à desinformação ou à insurgência. E também com a certeza que nenhuma guerra híbrida será igual a outra guerra híbrida. Cruzam-se assim dois caminhos cuja previsibilidade nos escapa muito significativamente. Neste seminário discutiram-se essas duas dimensões e o seu inevitável cruzamento. Ninguém prescreveu caminhos de sentido obrigatório ou enunciou receitas. Ainda bem. Nem isso seria possível e se alguém tivesse a presunção oposta estaria a iludir-se e a iludir-nos. Para fazer este caminho tem que se adorar a complexidade, como disse o *keynote speaker,* hoje e saber que a realidade faz parte dessa complexidade e saber também que a extraordinária acessibilidade e a facilidade como que tudo isto é movimentado, é parte dessa complexidade.

Eu cumprimento todas as senhoras e senhores que intervieram como conferencistas e como moderadores. O critério intelectual que adotaram de nos proporcionarem informação e de nos fazerem pensar era exatamente o que ambicionávamos. Trouxeram para o seminário o vosso saber, a vossa reflexão, a vossa curiosidade e o vosso interesse. Além disso questionaram-se e questionaram-nos. Em nome do IDN e do EuroDefense- Portugal expresso-vos o nosso agradecimento. Saímos daqui realmente enriquecidos, mesmo que com mais inquietações. Desde logo, as múltiplas inquietações ligadas às diversas tecnologias, para continuar com a inquietação básica que se projeta certamente na dicotomia entre a segurança e liberdade. Ficámos curiosos. A curiosidade é um caminho fundamental para o progresso intelectual. Quero também agradecer

a todos os participantes os vossos contributos estando presentes, questionando e debatendo, em muito valorizaram este evento. Finalmente é devido uma palavra de especial reconhecimento ao senhor Coronel Beja Eugénio, que de modo tao disponível, criterioso e cuidadoso foi a pessoa central na organização do seminário. Muito obrigado, meu Coronel. Minhas senhoras e meus senhores, crendo termos beneficiado de um evento muito pertinente e útil e permitindo falar em nome do IDN e do Eurodefense-Portugal dou por encerrado este seminário com a convicção que as matérias que ele versou e as interrogações que ele nos colocou permanecerão vivas nos nossos espíritos.
Muito obrigado.