CONFERÊNCIA

RESILIÊNCIA DIGITAL DE UM ESTADO DEMOCRÁTICO

CONFERENCE

DIGITAL RESILIENCE OF A DEMOCRATIC STATE

8 de maio de 2018 | Sala do Senado | Assembleia da República

8 May 2018 | Senate Room | Assembly of the Republic

Colóquios e Conferências Parlamentares

ASSEMBLEIA DA REPÚBLICA

CONFERÊNCIAS de LISBOA
DA ASSEMBLEIA PARLAMENTAR DA OSCE

ÍNDICE | CONTENTS

ABREVIATURAS E SIGLAS

APOSCE	Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa
CEO	Diretor Executivo
CNCS	Centro Nacional da Cibersegurança
COPS	Comité Político e de Segurança da União Europeia
EMGFA	Estado-Maior-General das Forças Armadas
ENISA	Agência da UE para a Segurança das Redes e da Informação
EUA	Estados Unidos da América
FIDESZ	União Cívica Húngara (Partido nacional conservador de direita da Hungria)
GIFCT	Fórum Mundial da Internet contra o Terrorismo
I&D	Investigação e Desenvolvimento
IA	Inteligência Artificial
IFES	Fundação Internacional de Sistemas Eleitorais
MGC	Medidas Geradoras de Confiança
NATO	Organização do Tratado do Atlântico Norte
ONU	Organização das Nações Unidas
OSCE	Organização para a Segurança e Cooperação na Europa
PE	Parlamento Europeu
PT	Portugal Telecom
R&D	Pesquisa e Desenvolvimento
SIRP	Sistema de Informações da República Portuguesa
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia

ABBREVIATIONS

AI	Artificial Intelligence
CBM	Confidence Building Measure
CEO	Chief Executive Officer
CNCS	National Cybersecurity Center Portugal
COPS	EU Political and Security Centre Portugal
EMGFA	Armed Forces General Staff
ENISA	EU Network and Information Security Agency
EP	European Parliament
EU	European Union
FIDESZ	Hungarian Civic Alliance (National conservative right-wing political party in Hungary)
GIFCT	Global Internet Forum to Counter Terrorism
I&D	Investigation and Development
ICT	Information and Communication Technology
IFES	International Foundation for Electoral Systems
IT	Information Technology
MP	Member of Parliament
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security and Co-operation in Europe
OSCEPA	Organization for Security and Co-operation in Europe Parliamentary Assembly
PT	Portugal Telecom
R&D	Research and Development
SIRP	Portuguese Intelligence System
UN	United Nations
USA	United States of America

Da esquerda para a direita: George Tsereteli, Jorge Lacão e Isabel Santos
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04866/2018
From left to right: George Tsereteli, Jorge Lacão and Isabel Santos
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04866/2018

ABERTURA
OPENING SESSION

JORGE LACÃO

A Resiliência Digital de um Estado Democrático é o tema que hoje aqui nos junta. Um tema da maior atualidade.

A Internet tem sido um fator de promoção da liberdade de expressão e de divulgação de ideias. Tem aproximado pessoas e culturas.

É também impressionante o contributo da Internet para a economia, quer ao nível da inovação dos produtos, quer ao nível da facilitação do comércio e das transações financeiras.

No entanto, convém não esquecer que estas oportunidades vêm acompanhadas de riscos e ameaças.

Vários acontecimentos, mais ou menos recentes, têm contribuído para que passássemos do discurso otimista para o discurso realista em relação à Internet.

Quero, pois, saudar a Assembleia Parlamentar da OSCE por esta iniciativa.

A Segurança do Ciberespaço é hoje em dia um dos pilares de qualquer estratégia nacional digna desse nome.

E esta Conferência de Lisboa é mais um contributo para o desenvolvimento de uma verdadeira cultura da Cibersegurança em Portugal e no seio da OSCE.

O processo de globalização transformou as sociedades desenvolvidas em sociedades da informação.

Neste tipo de sociedades, o potencial estratégico de cada Estado está muito relacionado com o conhecimento e a inovação.

A Internet tornou-se palco de disputa global pelo poder e pelo conhecimento.

Por isso, a Cibersegurança é hoje um ramo da estratégia de segurança e defesa, como são os ramos tradicionais das forças armadas.

À segurança dos territórios, das águas, do espaço aéreo e do espaço exterior, temos agora de juntar a segurança do Ciberespaço.

Hoje praticamente todo o mundo está *online*.

O Ciberespaço está, portanto, aberto a qualquer um, o que comporta ameaças evidentes.

Note-se que a Internet é também a base na qual assentam os sistemas de comunicações entre governos, forças armadas, serviços de informações e de segurança.

Temos, portanto, as ameaças dos *hackers*, as ações de propaganda extremistas e antidemocráticas, o crime organizado, e até o apoio a ataques terroristas a passar por ações *online*.

Surgem mesmo suspeitas de interferências estatais ou paraestatais em processos eleitorais através de meios digitais.

Os dados pessoais já não parecem estar em segurança, com os escândalos que envolvem grandes empresas ao setor digital.

Toda esta nova realidade obriga a União Europeia, a NATO, a OSCE e os Estados Nacionais a prepararem-se cada vez melhor para enfrentar esta ameaça.

Infelizmente, as ameaças avançam mais depressa do que a capacidade de respostas dos Estados de direito democráticos e das suas organizações internacionais.

Exige-se mais cooperação internacional e uma promoção mais eficaz de uma cultura de Cibersegurança entre os utilizadores da Internet, e, em particular, entre as entidades responsáveis pela gestão de infraestruturas críticas.

Esta Conferência destina-se a contribuir para essa nova cultura de segurança.

Aqui teremos, na Assembleia da República, especialistas internacionais e responsáveis políticos, judiciais e militares.

Estou certo que se reunirmos estas competências, se mobilizarmos estes recursos nacionais e internacionais, seremos capazes de enfrentar com sucesso estas ameaças, atingindo o objetivo da resiliência digital das democracias.

Resiliência que, na sociedade digital, não pode também esquecer a vertente fundamental da proteção de dados, em particular dos dados pessoais inerentes ao respeito devido à nossa vida privada. Sem respeito pela autonomia das pessoas não há sociedades aberta e sem sociedade aberta não há democracia, liberdade e segurança.

Tais princípios continuam, por isso, a ser os fundamentos do nosso desafio. Bom trabalho a todos na reflexão que se nos impõe.

A todos o meu muito obrigado.

JORGE LACÃO

The Digital Resilience of a Democratic State is the theme that brings us together here today. A theme that is extremely topical.

The internet has been a factor in promoting freedom of expression and the spread of ideas. It has brought people and cultures closer together.

The internet's contribution to the economy in terms of innovation of products and facilitating trade and financial transactions is also impressive.

But it is important not to forget that these opportunities come hand-in-hand with risks and threats.

Several events, some more recent than others, have led us to shift from an optimistic discourse to a realist discourse about the internet.

I would therefore like to congratulate the OSCE Parliamentary Assembly on this initiative.

The security of cyberspace is today one of the pillars of any national strategy worthy of that name.

And this Lisbon Conference is another contribution to the development of a true cyberspace culture in Portugal and in the OSCE.

The globalisation process has transformed developed societies into information societies.

In these types of societies, the strategic potential of each state is heavily linked to knowledge and innovation.

The internet has become the stage for the global dispute for power and knowledge.

That is why cybersecurity today is a branch of security and defence strategy, like the traditional branches of the armed forces.

We now have to add the security of cyberspace to the security of territories, waters, airspace and outer space.

Today, practically the whole world is online.

Cyberspace is, therefore, open to anyone, which involves clear risks.

The internet is also the base on which communications systems between governments, armed forces, and intelligence and security services are founded.

We therefore have threats from hackers, extremist and antidemocratic propaganda actions, organised crime, and even support for terrorist attacks happening in online acts.

Suspicions even emerge of state or parastate interference in electoral processes using digital means.

Personal data no longer appear to be safe, with the scandals involving large companies in the digital sector.

All of this new reality compels the European Union, NATO, OSCE and nation states to increasingly prepare themselves to confront this threat.

Unfortunately, the threats are advancing faster than the responses of democratic states based on the rule of law and international organisations.

More international cooperation is required, along with more effective encouragement of a culture of cybersecurity among internet users and, in particular, among the organisations responsible for managing critical infrastructure.

This conference is intended to contribute to that new security culture.

Here, at the Assembly of the Republic, we will have international specialists and political, judicial and military leaders.

I am certain that if we bring together these skills, if we mobilise national and international resources, we will be able to successfully face up to these threats, achieving the goal of digital resilience in democracies.

Resilience that, in the digital society, must also remember the fundamental aspect of data protection, particularly for the personal data inherent to due respect for our private lives. Without respect for people's autonomy, there cannot be open societies, and without open societies, there is no democracy, freedom or security.

These principles are therefore still the foundations of our challenge. I wish you all a successful day working on the reflection incumbent upon us.

Thank you all very much.

GEORGE TSERETELI

Em primeiro lugar, gostaria de agradecer à Assembleia da República de Portugal por ter organizado esta conferência, que é, simultaneamente, oportuna e importante.

Nesta era dominada por debates sobre notícias falsas, cibersegurança, radicalização na Internet e proteção de dados, é essencial que nos juntemos para discutir estas questões.

Na Assembleia Parlamentar da OSCE, na última década, temos vindo a dedicar cada vez mais atenção à cibersegurança. Adotámos a nossa primeira resolução sobre este tema em 2008, identificando as ciberameaças como um dos maiores desafios de segurança do nosso tempo. Nos últimos dez anos, estes desafios não pararam de crescer.

Os nossos deputados recordar-se-ão que, durante a nossa reunião de outono em Andorra, discutimos a forma como as ciberameaças podem pôr em causa o modo de vida das sociedades modernas e de toda a civilização.

No nosso mundo cada vez mais digital, os conflitos armados não são o único foco de ameaças contra os governos e os cidadãos. No ciberespaço, vemos surgir novos desafios e assistimos à evolução dos desafios existentes.

Em questões como a exploração sexual de crianças, o recrutamento de terroristas ou crimes como a usurpação de identidade e a fraude, a Internet oferece novas oportunidades a criminosos e extremistas. Temos de responder com eficácia e garantir que a resposta é proporcionada.

Atualmente, os Estados Unidos e a União Europeia estão a seguir políticas de enfraquecimento das regras internacionais em matéria de investigação transnacional da cibercriminalidade pelas autoridades de aplicação da lei. Embora estas alterações nas regras possam ser bem intencionadas, o que menos desejamos é um nivelamento por baixo das formas de proteção da vida privada a nível mundial.

Por outras palavras, quando abordamos estes problemas, temos sempre de defender as normas mais rigorosas de respeito das liberdades fundamentais.

Reconhecendo o papel essencial da cooperação entre governos para fazer face aos riscos de segurança atuais, devemos rever os quadros jurídicos existentes e harmonizar a legislação aplicável para que a cooperação internacional seja mais eficaz e eficiente. Todos os intervenientes e partes interessadas devem procurar, de boa-fé, soluções assentes no direito internacional, de uma forma que não atente contra a liberdade de informação ou a privacidade individual.

Embora os governos tendam a encarar a cibercriminalidade na perspetiva das ameaças à segurança do Estado – olhando para a proteção das infraestruturas digitais ou para a garantia da proteção dos segredos de Estado –, os nossos cidadãos não são menos vulneráveis ao cibercrime e às violações de dados pessoais. Vimos recentemente os danos resultantes da violação de dados cometida pela Cambridge Analytica, que afetou milhões de utilizadores do Facebook.

Os dados das pessoas visadas foram recolhidos e ilegitimamente vendidos a políticos para fazer avançar as suas agendas políticas e as suas carreiras. Este escândalo suscitou importantes questões legais e éticas sobre a natureza da privacidade numa era digital. Por exemplo, o que significa para a democracia que operacionais da política possam utilizar dados pessoais altamente pormenorizados para influenciar a opinião pública?

Apesar de as atenções se terem centrado no Facebook, esta recolha de dados em grande escala é um problema em todo o ciberespaço. Coloca-se, pois, a questão fundamental de saber se os utilizadores da Internet podem contar com qualquer tipo de proteção da privacidade.

Afinal, a tecnologia não é boa ou má em si mesma. Tudo depende das pessoas que a utilizam.

Quando é possível obter um conhecimento profundo e detalhado das opiniões dos cidadãos e vendê-lo a quem apresenta a melhor oferta, os cidadãos tornam-se alvos preferenciais das campanhas de notícias falsas e da propaganda. Esta situação pode, por sua vez, ter consequências desastrosas para o funcionamento da democracia.

Tem havido muitas alegações de que atos eleitorais recentes também foram alvo de ciberataques. Pode discutir-se se os resultados eleitorais foram ou não influenciados, mas é inegável que essa possibilidade é inquietante. E, mesmo que as eleições passadas tenham sido seguras, não se pode presumir que as eleições futuras o serão, pelo que devemos envidar todos os esforços para proteger os nossos sistemas eleitorais contra a pirataria.

Espero que neste fórum possamos partilhar boas práticas, desenvolver medidas de reforço da confiança e encontrar formas mais eficazes de construir democracias resilientes que nos protejam das ciberameaças e, ao mesmo tempo, salvaguardem a liberdade de informação e a privacidade pessoal.

A romancista britânica Phyllis Bottome disse que existem duas formas de enfrentar as dificuldades: mudar as dificuldades ou mudar-nos a nós mesmos para as encarar.

Penso que todos concordamos que a tecnologia trouxe grandes vantagens à nossa civilização. Ajudou a conectar o mundo, partilhar conhecimento, promover o comércio e incentivar o desenvolvimento democrático.

Veja-se, por exemplo, a nossa Assembleia Parlamentar, em que todos estamos conectados através dos nossos *smartphones* e todos podemos partilhar e recolher informação a uma velocidade sem precedentes. Nesta era da diplomacia digital, devemos perceber que a Internet também pode ajudar a resolver problemas de política externa.

Caros colegas e amigos, o que nos cabe fazer agora é assegurar que esta tecnologia é segura, para que os desafios da era digital sejam geridos de uma forma que garanta simultaneamente a segurança e a liberdade.

É nossa responsabilidade zelar por que a tecnologia moderna continue a ser útil sob o nosso controlo e não perigosamente controladora.

Agradeço uma vez mais à Assembleia da República por ter organizado esta importante conferência e aguardo com expectativa a análise mais aprofundada destes temas com todos os presentes.

Obrigado.

GEORGE TSERETELI

First of all, I'd like to thank the Assembly of the Republic of Portugal for organizing this conference, which is both timely and important.

In this era dominated by debates about fake news, cybersecurity, online radicalization, and data protection, it is essential that we come together to discuss these issues.

In the OSCE Parliamentary Assembly, we have been increasingly focused on cybersecurity for the past decade. We adopted our first resolution on the topic in 2008, identifying cyber threats as some of the most serious security challenges of our time. Over the past ten years, these challenges have only grown.

Our Members will recall that during our latest Autumn Meeting in Andorra, we discussed how cyber threats can jeopardize the way of life of modern societies and the whole of civilization.

In our increasingly digital world, armed conflicts are not the only breeding ground for threats against governments and citizens. In cyberspace, we see new challenges emerging and old challenges evolving.

Whether the issue is child sexual exploitation, terrorist recruitment, or crimes such as identity theft and fraud, the internet offers new opportunities for criminals and extremists. We must respond effectively and ensure that the response is proportionate.

Currently, there are policies being pursued by the United States and European Union to relax international rules for cross-border law enforcement investigations of cybercrime. While these rule changes might be well-intentioned, what we don't want is a race to the bottom of weaker privacy protections around the globe.

While addressing these problems, in other words, we must always uphold the highest standards of respect for fundamental freedoms.

Recognizing the essential role of co-operation between governments to cope with modern security risks, we should revise existing legal frameworks and harmonize relevant legislation to make international co-operation more effective and efficient. All actors and stakeholders must search, in good faith, for solutions based on international law in a way that does not infringe on freedom of information or individual privacy.

Although governments often see cybercrime through the lens of threats to state security – whether the protection of digital infrastructure or ensuring the protection of state secrets – our citizens are no less vulnerable to cybercrime and breaches of their personal data. We saw recently the damage done by the Cambridge Analytica data breach, which affected millions of Facebook users.

These people had their personal data collected and inappropriately sold to politicians to advance political agendas and careers. The scandal raised important legal and ethical questions about the nature of privacy in a digital age. For example, what are the implications for democracy when extremely detailed personal data can be used by skilled political operatives to influence public opinion?

While Facebook has been in the spotlight, this sweeping data collection is an issue throughout cyberspace. This raises the fundamental question of whether internet users should expect any privacy protections at all.

After all, technology is not good or bad in and of itself. It all depends on the people who use it.

When intimate and detailed knowledge of citizens' views can be collected and sold to the highest bidder, citizens become prime targets for fake news campaigns and propaganda. This, in turn, can have dire consequences for the functioning of democracy.

There has been much speculation that recent elections have also been the target of cyberattacks. Whether electoral outcomes have been affected or not is a matter of debate, but what is not a matter of debate is that this possibility is troubling. And even if past elections have been secure, there is no reason to assume that future elections will remain secure, so we must make every effort in protecting our electoral systems from hacking.

I hope that in this forum, we can exchange best practices, develop confidence-building measures, and find the most effective ways to build resilient democracies that protect against cyber threats while also protecting freedom of information and personal privacy.

British novelist Phyllis Bottome once said: "There are two ways of meeting difficulties: you alter the difficulties, or you alter yourself to meet them."

I think we can all agree that technology has offered great advances for our civilization. It has helped to connect the world, share knowledge, promote commerce, and to advance democratic development.

Take for example our own Parliamentary Assembly, where we are now all connected through our smartphones, and able to share and gather information as fast as ever. In this era of digital diplomacy, we should realize that the internet can also help solve foreign policy problems.

Dear colleagues and friends, what we now must do is make sure that this technology is secure so that the challenges of the digital age are managed in a way that ensures both security and liberty.

It is up to us to make sure that modern technology remains a useful servant and not a dangerous master.

I once again thank the Assembly of Portugal for organizing this important conference, and I look forward to exploring these topics in greater detail with you all.

Thank you.

ISABEL SANTOS

Exmo. senhor vice-presidente da Assembleia da República, deputado Jorge Lacão

Exmo. senhor presidente da Assembleia Parlamentar da OSCE, George Tseretelli

Exmo. senhor secretário-geral da Assembleia Parlamentar da OSCE, Roberto Montella

Excelências

Caros convidados, caras convidadas

Caros colegas, caras colegas

É para todos nós motivo de grande satisfação e alegria dar-vos as boas vindas à primeira das Conferências de Lisboa da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa (AP OSCE).

Um dos grandes desafios com que as Organizações Parlamentares Internacionais se confrontam reside na necessidade de se criar uma maior proximidade entre a sua abordagem dos diferentes temas e o debate realizado nos parlamentos e nas sociedades dos seus Estados-parte.

Em resposta a este incitamento, a Delegação da Assembleia da República à Assembleia Parlamentar da OSCE decidiu lançar as Conferências de Lisboa da Assembleia Parlamentar da OSCE. Uma iniciativa que, de dois em dois anos, procurará reunir, na Assembleia da República, elementos de diversas delegações dos 57 Estados-parte, especialistas, investigadores, jornalistas, estudantes e organizações da sociedade civil, para abordar temas que ocupam o topo da nossa agenda.

É isso que hoje aqui vai acontecer, com a participação de intervenientes com saberes e visões diversas e com proveniências culturais e geograficamente distintas que se estendem do Quirguistão aos Estados Unidos, na abordagem de questões ligadas à segurança do ciberespaço, enquadradas pelo título "Resiliência Digital de um Estado Democrático".

Se tivéssemos dúvidas sobre a pertinência desta conferência, os múltiplos casos vindos a público, já depois da escolha do tema – de utilizações perversas do ciberespaço, colocando em causa direitos fundamentais dos cidadãos, a segurança e qualidade das democracias e inquinando o diálogo entre Estados – teriam feito soçobrar qualquer questionamento.

Vivemos um tempo marcado por um notável progresso tecnológico, em que as Tecnologias da Informação e da Comunicação são cada vez mais presentes nos mais pequenos gestos quotidianos.

Usar um *smartphone* ou um computador e a partir deles, com um simples clique, ter acesso a notícias de todo o mundo, gerir contactos pessoais ou de negócios, aceder à conta bancária, comprar um livro, é algo absolutamente banal para um número crescente de nós.

De uma forma ou de outra, todos estamos presentes numa qualquer plataforma informática ou base de dados.

Contudo, toda a face tem o seu reverso e a par dos múltiplos benefícios e vantagens da conectividade, as novas tecnologias trouxeram, também, uma onda de incertezas e ambiguidades.

Como bem assinalou Henry Kissinger, "A omnipresença das redes de comunicação nos setores social, financeiro, industrial e militar tem aspetos muitíssimo benéficos; mas também revolucionou as vulnerabilidades."(...)"Um computador portátil pode ter repercussões mundiais." Um ator solitário com os devidos reconhecimentos e recursos pode incapacitar e destruir infraestruturas fundamentais a coberto de um quase anonimato.

Os ciberataques representam uma séria ameaça à segurança em toda a esfera social, afetando os governos e os setores público e privado.

Numa era em que muitos dos antagonismos geopolíticos tendem, cada vez mais, a transferir-se para o espaço virtual, num complexo xadrez de intrusões em redes, processamento de dados, e manipulações de toda a espécie – vejam-se os mais recentes casos com repercussões eleitorais –, a ambiguidade em torno do desenvolvimento do ciberespaço tem servido para alimentar a desconfiança e as tensões à escala global, de um modo que faz com que este assunto não possa ser ignorado ou subestimado.

Diante deste quadro-de-fundo, a Organização para a Segurança e Cooperação na Europa tem vindo a assumir-se como plataforma de diálogo e desenvolvimento de *Confidence Building Measures*, procurando reduzir os riscos provenientes do uso das Tecnologias da Comunicação e da Informação ao assegurar maior previsibilidade ao ciberespaço; oferecer ferramentas e mecanismos concretos para evitar equívocos; facilitar o diálogo; promover a partilha das melhores práticas, visando gerar maior proteção contra as ciberameaças e manter o ciberespaço aberto, livre e seguro.

Paralelamente, a OSCE e as suas instituições estão focadas em fazer face às ciberameaças provenientes de atores não estatais, como as que têm origem no mundo do crime organizado e do terrorismo.

Ao longo dos anos, a Assembleia Parlamentar da OSCE tem produzido diversas resoluções e recomendações, abordando a cibersegurança e o cibercrime, que sublinham o risco das modernas violações da segurança.

Um dado bem ilustrativo da importância deste tema no quadro do debate promovido no seio da AP OSCE é o número de textos aprovados desde 2008, um total de 12.

Logo em 2008, na Declaração de Astana, sublinhamos que os conflitos armados não são a única ameaça à nossa segurança regional – o despontar do ciberespaço criou um novo palco para os conflitos. E, ao mesmo tempo, incitamos os parlamentares e os Estados-parte a juntar esforços para combater o abuso das tecnologias da comunicação e informação para fins criminais e de terrorismo.

As declarações produzidas pela AP OSCE nos anos seguintes, entre as quais sublinho a de Oslo, em 2010, e a de Istambul, em 2013, são a prova da grande importância devotada ao combate às violações da cibersegurança e ao cibercrime e à salvaguarda da troca de informação online.

Ninguém é ingénuo ao ponto de pensar ser possível tornar o ciberespaço inviolável a qualquer utilização malévola, mas torná-lo cada vez mais resiliente é tornar as democracias mais resilientes e constitui dever de todos nós, especialistas, políticos, cidadãos.

Estou certa de que as conclusões dos diversos debates que ocorrerão ao longo deste dia terão eco na declaração a produzir em julho, na Reunião da AP OSCE, em Berlim, e serão fator de enriquecimento da mesma.

Resta-me, assim, agradecer:

- ao senhor presidente da Assembleia da República, na pessoa do senhor vice-presidente Jorge Lacão, pelo constante estímulo à atividade da Delegação da Assembleia da República à Assembleia Parlamentar da OSCE e pela forma como acolheu esta iniciativa;
- ao presidente da AP OSCE, George Tseretelli, ao secretário-geral, Roberto Montella, e a todos os membros do secretariado internacional, pelo seu incansável contributo, em todos os momentos;
- ao vasto leque de oradores, aos moderadores, aos relatores e a todos os participantes, que fazendo convergir em Lisboa a força desta grande plataforma Euro-Atlântica para a cooperação, segurança, democracia e desenvolvimento, nos honram com a sua presença;
- a todos os que, diariamente, nos diferentes serviços da Assembleia da República, asseguram a retaguarda do funcionamento desta casa e sem os quais este evento não seria possível.

Desejo a todos e a todas uma proveitosa sessão de trabalho.

Muito obrigada!

ISABEL SANTOS

Mr Vice-President of the Assembly of the Republic, Jorge Lacão MP
Mr President of the OSCE Parliamentary Assembly, George Tsereteli
Mr Secretary General of the OSCE Parliamentary Assembly, Roberto Montella
Your Excellencies
Dear invited guests
Dear colleagues

It is a source of great satisfaction and joy for all of us to welcome you to the first of the Lisbon Conferences of the Organisation for Security and Co-operation in Europe Parliamentary Assembly (OSCE PA).

One of the major challenges facing international parliamentary organisations lies in the need to create a closer relationship between its approaches to different topics and the debates held in the parliaments and societies of their Participating States.

In response to this, the delegation of the Assembly of the Republic to the OSCE Parliamentary Assembly decided to launch the Lisbon Conferences of the OSCE Parliamentary Assembly. It is an initiative that will seek to bring together members of the various delegations of the 57 Participating States, specialists, researchers, journalists, students and civil society organisations at the Assembly of the Republic every two years to discuss topics at the top of our agenda.

That is what will be happening here today, with the participation of speakers who have different knowledge and visions from different cultural and geographical backgrounds that range from Kyrgyzstan to the United States to discuss issues connected to the security of cyberspace framed under the title "Digital Resilience of a Democratic State".

If we had any doubts about the relevance of this conference, the many cases that have been uncovered even after the topic was chosen – of perverse uses of cyberspace, calling into question citizens' fundamental rights, the security and quality of democracies and poisoning dialogue between states – would have dispelled any questions.

We live at a time marked by impressive technological progress, when information and communication technologies are increasingly present in the smallest of our everyday actions.

Using a smartphone or a computer to, with just a click, see news from the whole world, manage personal or business contacts, access bank accounts or buy a book is something completely ordinary for a growing number of us.

One way or another, we are all present in some computerised platform or database.

However, there is a flipside to every coin and, alongside the many benefits and advantages of connectivity, new technologies have also brought a wave of uncertainties and ambiguities.

As Henry Kissinger so rightly pointed out, "The ubiquity of communication networks in the social, financial, industrial and military sectors has highly beneficial features; but it has also revolutionised vulnerabilities. (...) A laptop computer may have worldwide repercussions". A single actor, with the due recognition and resources, may incapacitate and destroy fundamental infrastructure under the cover of almost anonymity.

Cyberattacks represent a serious threat to security throughout the social sphere, affecting governments and the public and private sectors.

At a time when many geopolitical conflicts are increasingly shifting into the virtual space – in a complex chess game of hacking into networks, data processing and manipulations of all kinds – look at the most recent cases with repercussions on elections – the ambiguity surrounding the evolution of cyberspace has bolstered mistrust and tensions at global level in such as way that this matter cannot be ignored or underestimated.

Against this backdrop, the Organisation for Security and Co-operation in Europe has been establishing itself as a platform for dialogue and the development of confidence-building measures, seeking to reduce the risks arising from the use of information and communication technologies by providing cyberspace with greater predictability, offering concrete tools and mechanisms to avoid mistakes, promoting dialogue, encouraging the sharing of best practices with a view to generating greater protection against cyberthreats and keeping cyberspace open, free and safe.

Alongside this, the OSCE and its institutions are focused on facing up to cyberthreats from non-state actors, such as those originating in the world of organised crime and terrorism.

Over the years, the OSCE Parliamentary Assembly has produced several resolutions and recommendations dealing with cybersecurity and cybercrime that underline the risk of modern security violations.

One piece of data that illustrates the importance of this theme in the debate framework developed within the OSCE PA is the number of texts approved since 2008, a total of 12.

Even in 2008, in the Astana Declaration, we underlined that armed conflicts are not the only threat to our regional security – the emergence of cyberspace had created a new stage for conflicts. At the same time, we called on parliamentarians and Participating States to join forces to fight the abuse of information and communication technologies for criminal ends and terrorism.

The declarations produced by the OSCE PA in following years, and I would particularly highlight the 2010 Oslo Declaration and the 2013 Istanbul Declaration, are proof of the great importance devoted to fighting violations of cybersecurity and cybercrime and safeguarding online information exchange.

Nobody is naive to the point of believing that cyberspace could be made inviolable, but making it more and more resilient means making democracies more and more resilient and this is a duty for all of us: specialists, politicians and citizens.

I am sure that the conclusions from the different debates that will be taking place today will find resonance in the declaration to be produced in July at the OSCE PA meeting in Berlin and will enrich it.

All that remains is for me to thank:

- The President of the AR, represented by the Vice-President Jorge Lacão, for the constant encouragement for the activities of the Assembly of the Republic's delegation to the OSCE Parliamentary Assembly and for the way in which he welcomed this initiative;
- The President of the OSCE PA, George Tsereteli, the Secretary General, Roberto Montella, and all the members of the International Secretariat, for their untiring contributions at all times;
- All the many speakers, moderators and rapporteurs and all the participants, who honour us with their presence by gathering in Lisbon the strength of this great Euro-Atlantic platform for co-operation, security, democracy and development;
- All those who, in the different services of the Assembly of the Republic, provide the backstage work for the running of this organisation, without whom this event would not have been possible.

I wish you all a very successful session.

Thank you!

Da esquerda para a direita: João Fernando Ramos, Anatoly Smirnov , Susana Amador, Ignacio Sanchez Amor e William Sweeney
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04884/2018
From left to right: João Fernando Ramos, Anatoly Smirnov , Susana Amador, Ignacio Sanchez Amor and William Sweeney
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04884/2018

CIBERSEGURANÇA & DEMOCRACIA: CONFIDENCE BUILDING MEASURES

CYBERSECURITY & DEMOCRACY: CONFIDENCE BUILDING MEASURES

JULIAN KING

Saúdo os presentes e agradeço, antes de mais, a oportunidade de intervir através de uma mensagem por vídeo – lamento não poder estar convosco pessoalmente.

O tema que estão a debater hoje é fundamental – as ameaças no ciberespaço ou possibilitadas pelo ciberespaço figuram entre os desafios mais significativos que se colocam à nossa segurança. Tal deve-se, em parte, ao facto de dependermos hoje mais do que nunca da tecnologia nas nossas vidas quotidianas – para as notícias que lemos, para nos mantermos em contacto uns com os outros, para fazermos compras e utilizarmos serviços bancários, enfim, para todos os tipos de atividades diárias. A Internet trouxe-nos oportunidades extraordinárias, mas torna-se cada vez mais evidente que tem um outro lado, um lado mais negro.

Os ciberataques são cada vez mais frequentes e têm um impacto cada vez mais nefasto. São fáceis de cometer e difíceis de rastrear e imputar, enquanto a lista de potenciais alvos é tão extensa que, na verdade, qualquer cibercriminoso tem um sem-número de opções. A motivação subjacente a esses ataques é muitas vezes financeira, mas também já assistimos a ataques com fins políticos e estratégicos. O seu objetivo é perturbar as nossas instituições democráticas e interferir nas nossas eleições.

Em resposta, continuamos a trabalhar para reduzir o espaço de quem nos tenta atingir, o que inclui cibercriminosos, terroristas e, na verdade, intervenientes estatais e não estatais.

Tal como noutros domínios da segurança, são os governos e os poderes públicos que estão na linha da frente. Todavia, dada a natureza transnacional das ciberameaças, a cooperação é mais importante do que nunca, e a UE tem um claro papel a desempenhar no apoio aos esforços desenvolvidos a nível nacional e internacional.

Por esse motivo, a Comissão propôs um pacote de medidas, em setembro último, para reforçar a nossa ciber-resiliência, garantir uma dissuasão eficaz e ajudar a concretizar uma ciberdefesa e uma cooperação internacional credíveis.

Reforçar a resiliência implica tornar-nos mais difíceis de atacar e manter sistemas, estruturas e procedimentos que nos permitam reagir rapidamente e de forma coordenada quando ocorre um ataque de grandes proporções. Tal implica, em primeiro lugar, uma aplicação eficaz da Diretiva sobre a Cibersegurança – cujo prazo de transposição termina, aliás, amanhã –, que deve assegurar uma melhor proteção de setores fundamentais em toda a Europa e uma cooperação mais eficiente entre os Estados-Membros. Para complementar estes importantes primeiros passos, propusemos a definição de um plano com orientações para responder a incidentes em grande escala, bem como a ampliação do mandato da atual Agência da UE para a Segurança das Redes e da Informação, ENISA, para a transformar numa verdadeira e eficaz Agência da UE para a Cibersegurança.

Tendo em conta que deverão entrar no mercado milhares de milhões de novos dispositivos conectados, é igualmente crítico reforçar as normas de cibersegurança e promover a "segurança desde a conceção". É por isso que a nossa proposta inclui um quadro de certificação para produtos e serviços.

Estamos também a investir em competências para além da ciber-higiene básica, assim como em investigação para nos mantermos à frente de quem nos pretende atacar e provocar danos.

O setor privado também tem de assumir o seu papel, passando de consumidor de segurança a prestador de segurança e encarando a segurança não como um custo, mas como um fator de vantagem concorrencial.

Além de nos tornarmos mais resilientes, temos também de garantir uma dissuasão eficaz – assegurando, nomeadamente, que o cibercrime não compensa. Tal implica facilitar a deteção e a repressão da cibercriminalidade.

Nesse sentido, demos um passo significativo no mês passado, apresentando propostas destinadas a facilitar o acesso a meios de prova eletrónicos – onde quer que estejam –, bem como a melhorar a capacidade das autoridades de aplicação da lei para investigar e levar a tribunal delitos como o terrorismo e os cibercrimes, cujas provas estão muitas vezes em formato digital e são guardadas, cada vez mais, em países diferentes.

O nosso trabalho inclui a luta contra a utilização de meios cibernéticos para a difusão de propaganda e desinformação ou para o incitamento ao terrorismo. A fim de combater estes fenómenos, a Comissão apresentou, há duas semanas, um conjunto de medidas contra a desinformação e as notícias falsas na Internet. Esta iniciativa envia um sinal claro e firme a plataformas da Internet – Facebook, Twitter e outras – que, importa dizê-lo, ganham muito dinheiro com as nossas vidas *online*. Têm um papel fundamental a desempenhar no nosso combate à desinformação, e esperamos ver progressos significativos nos próximos meses.

Não lhes estamos a pedir que avaliem o que é ou não verdadeiro ou que, de alguma forma, censurem conteúdos. O que pretendemos é mais transparência, rastreabilidade e responsabilização na Internet, e as plataformas têm de nos ajudar a consegui-lo.

Os nossos *feeds* de notícias têm de indicar-nos com clareza quais os conteúdos que foram pagos, e por quem, se foram difundidos por *bots* e não por outros utilizadores e por que motivo nos são apresentados determinados conteúdos específicos.

Além disso, vamos reforçar o trabalho desenvolvido por "verificadores de factos", apoiar o jornalismo de qualidade e promover a literacia mediática e o pensamento crítico.

Trata-se de uma questão urgente, sobretudo no contexto dos atos eleitorais que se avizinham, nomeadamente as eleições de maio próximo, em toda a Europa, para o Parlamento Europeu (PE). Já vimos como algumas eleições, nos EUA e em França, por exemplo, foram alvos de intervenientes mal-intencionados no passado.

Em alguns casos, estas tentativas de interferência envolviam partes estrangeiras. Temos de ser claros: essa interferência externa, baseada na desinformação e na manipulação, não é aceitável.

Também tomámos medidas para combater os conteúdos terroristas na Internet. Ao contrário do que acontece na desinformação, em que predominam a manipulação e a coação, no caso dos conteúdos terroristas existe uma clara linha divisória – estes últimos são ilegais, na Internet ou fora dela. Não vos seria permitido estar no centro de Lisboa a distribuir panfletos terroristas e, como tal, também não pode ser permitido distribuir esse tipo de material na Internet.

Neste âmbito, estamos também a exercer uma forte pressão sobre as grandes plataformas da Internet para que intensifiquem e acelerem o seu trabalho. Em março, a Comissão apresentou um conjunto de recomendações operacionais, segundo as quais, por exemplo, os conteúdos terroristas devem ser removidos no prazo de uma hora após a sua sinalização pelas autoridades de aplicação da lei e as plataformas devem usar ferramentas automatizadas para detetar estes conteúdos e impedir que sejam reinseridos. Preferimos que as plataformas trabalhem connosco voluntariamente, mas estamos preparados para rever as disposições normativas ou legislativas se não obtivermos os progressos rápidos que pretendemos.

Esta é uma descrição geral do nosso trabalho a nível europeu para aumentar a resiliência digital e para reforçar a confiança dos nossos cidadãos em vidas *online* mais seguras. Estamos determinados a realizar progressos, mas este é um trabalho que não tem um prazo definido. Teremos de prosseguir os nossos esforços e reforçar a cooperação para fazer face às ciberameaças crescentes e em evolução.

Obrigado. Agradeço a prioridade que atribuem a esta questão. É muito importante.

JULIAN KING

Hello, and thank you first of all for the opportunity to address you via video message – I am sorry I cannot be there with you in person.

The topic you are discussing today is a key one – cyber threats and cyber enabled threats are among the most significant challenges to our security. That is partly because we now rely on technology in our everyday lives to an unparalleled extent – for the news we read, for staying in touch with each other, for shopping and banking, all sorts of everyday activities. The internet has provided us with incredible opportunities – but it is becoming increasingly apparent that it also has a flip and darker side.

Cyber-attacks are becoming more frequent and more damaging in their impact. They are easy to perpetrate and hard to trace and attribute, while the list of potential targets is so long that any would-be cyber attacker is, frankly, spoiled for choice. The motives behind such attacks are often financial, but we have also seen attacks driven by political and strategic ends. They are aimed at disrupting our democratic institutions, and interfering with our elections.

In response, we are continuing our work to close down the space for all those who seek to harm us, whether they are cybercriminals, terrorists or indeed non-state and state actors.

As in other areas of security, it is national governments and public authorities that are on the frontline. But the cross-border nature of the cyber threat means that cooperation has never been more important, and the EU has a clear role to play in helping, assisting efforts both at home and internationally.

That is why the Commission proposed a package of measures last September to strengthen our cyber resilience, build effective deterrence and help deliver credible cyber defence and international cooperation.

Strengthening resilience means making ourselves both harder to attack and having the systems, structures and procedures in place to enable us to react rapidly and in a coordinated way when there is a major attack. This first means an effective implementation of the NIS Directive, for which the deadline is tomorrow, by the way, and which should ensure key sectors are better protected across Europe, and that Member States cooperate more effectively. To complement these important first steps, we have proposed the definition of a game plan on how to respond to large-scale incidents, and to expand the mandate of the existing EU Network and Information Security Agency, ENISA, into a genuine, effective EU Cybersecurity Agency.

With billions of new connected devices set to come to the market it is also critical to raise cyber security standards and promote 'security by design'. This is why our proposal includes a certification framework for products and services.

We are also investing in skills beyond basic cyber hygiene, as well as in research to stay ahead of those who are looking to attack us and to cause us harm.

The private sector needs to play its role too, and switch from being a security consumer to a security provider, and from seeing security not as a cost but as a factor of competitive advantage.

Aside from becoming more resilient, we also need to build effective deterrence – we need to make sure, for example, that cyber-crime does not pay. That means making it easier to detect and to prosecute.

To this end, we took a significant step last month with proposals to make access to electronic evidence – wherever it is – easier, to improve the ability of law enforcement to investigate and prosecute offences including terrorism and cybercrime – the evidence for which is often digital and increasingly stored in different countries.

Our work also includes countering the use of cyber means to spread propaganda and disinformation or to incite terrorism. To combat this, the Commission brought forward a range of measures a couple of weeks ago against disinformation and fake news online. In doing so we sent a very clear and strong message to internet platforms – Facebook, Twitter and others – who make, frankly, so much money from our online lives. They have a key role to play in helping us to counter disinformation, and we hope to see significant progress in the next few months.

What we are not doing is asking them to judge what is true or not, or in any way to censor content. But we do want more transparency, traceability and accountability online, and platforms need to help deliver this.

Our newsfeeds should tell us clearly when content has been paid for and by whom, when it has been distributed via bots rather than other users and why we are being shown certain, particular content.

In addition, we will strengthen the work done by 'fact checkers', we will support quality journalism and we will promote media literacy and critical thinking.

It is an urgent issue, especially in the context of upcoming elections such as those across Europe for the EP next May. We have already seen how some elections, in the US and in France, for example, have been targeted by malicious actors in the past.

Some of this attempted interference involves foreign actors. We need to be clear, such outside interference through disinformation and manipulation, is not acceptable.

We have also taken action to combat terrorist content online. Unlike the challenge of disinformation, where manipulation and coercion are the order of the day, with terrorist content there is a clear dividing line – terrorist content is illegal, whether it's online or offline. You wouldn't be allowed to go round the centre of Lisbon handing out terrorist pamphlets, and you shouldn't be allowed to spread that material on the internet, either.

Here we are also putting real pressure on the big internet platforms to step up and speed up their work. In March, the Commission tabled a set of operational recommendations, including that terrorist content should be removed within one hour after being flagged by law enforcement and that platforms should use automated tools to detect this content and prevent it from being re-uploaded. We prefer to work with the platforms on a voluntary basis, but we are ready to look again at regulation or legislation if we don't get the rapid progress we need.

This is a brief overview of our work at European level to increase our digital resilience and to build confidence amongst our citizens that their online lives are more secure. We are determined to make progress, but this is not a work that has an end date. We are going to need to maintain our efforts and reinforce our cooperation in the face of a growing and evolving cyber threat.

Thank you. Thanks for your focus on this issue. It is really important.

ANATOLY SMIRNOV

Muito obrigado! Gostaria de agradecer a todas as autoridades portuguesas que me convidaram a participar nesta conferência. Falarei em russo, embora os meus diapositivos sejam apresentados em língua inglesa.

Além de tudo o resto, o que mais me preocupa é o que Georges Tsetereli acabou de referir ... temos de pôr termo à guerra nas nossas próprias mentes. Só então conseguiremos alcançar os objetivos, para podemos viver em paz. E, hoje, a Europa celebra 73 anos da vitória contra a Alemanha Nazi, e é este o símbolo que trago na lapela, é este o símbolo da vitória na

Segunda Guerra Mundial. Hoje, os espaços da Internet são críticos, e tal não se aplica apenas à Rússia. Sabemos que existem muitos outros países que permitem mais do que a criação de condições difíceis ... contra outros países.

Por exemplo, a Rússia e outros países podem perguntar em que se baseia a justificação desta ameaça. O que têm em mente? E, na verdade, este é o ponto de viragem para entendermos o que está a acontecer em termos de ciberespaço, os problemas relacionados com... representados pelo ciberespaço.

Neste sentido, a Rússia elaborou vários documentos, documentos estratégicos, todos eles com o objetivo de desenvolver a sociedade da informação e, por outro lado, de nos mostrar como nos devemos defender no ciberespaço, que também comporta uma série de riscos, ameaças e problemas. A Rússia, através da sua política externa, declarou com clareza que... a Rússia interveio perante a ONU e pediu-lhe que abordasse este problema do combate às ameaças que os meios tecnológicos estão a criar em todo o ciberespaço.

A ideia proposta pela Rússia não foi bem acolhida, tendo alguns países, inclusivamente, criticado a Rússia por esta ideia. E, durante este período, verificou-se que perdemos a noção do tempo. Assim, limitámo-nos a perder tempo, e o que constatamos hoje nas tecnologias da informação é que estas estão cada vez mais sofisticadas. Criam um medo crescente, e foi referido que os terroristas podem usar o ciberespaço para os seus fins, para cumprir os seus intentos.

Estes são os registos das bases de dados relativos a 2017, e pode ver-se como o ciberespaço se torna cada vez mais complexo, muito mais sofisticado e difícil de gerir de forma positiva para podermos combater a criminalidade no ciberespaço. Os crimes que utilizam as TIC demonstram que estas tecnologias estão a evoluir, sendo desenvolvidas por vezes pelos próprios criminosos. E, enquanto sociedade, entendemos que a prioridade é, ou pelo menos deveria ser, o desenvolvimento de um dispositivo universal, um módulo universal, para que todos possamos combater este problema.

Esta nossa conferência incide sobre o Ciberespaço, mas vejamos este diapositivo. Segurança da informação: é esta a relação entre informação e cibersegurança. Como tal, no que se refere à Rússia, esta tem uma excelente compreensão deste domínio. Contudo, analisam apenas a parte "ciber" e esta é apenas uma pequena parte do conjunto, o conjunto inserido na informação e na segurança da informação.

Este facto está relacionado com a perceção do conceito e da ideia, e nós queremos também salientar que a tendência é a seguinte: a Rússia criou uma associação para a segurança da informação, de cariz internacional, e a organização de Moscovo juntou-se a outras universidades que também participaram nesta associação.

O líder desta associação é, na verdade, uma pessoa que conhecemos muito bem, o Sr. Chestuk, que é diretor-geral e também faz parte do *praesidium*, que é constituído por peritos no domínio da informação e também da segurança da informação.

Existe, contudo, um problema. As ameaças que observamos e o efeito que constatamos torna, muito importante garantirmos este tipo de segurança. Este aspeto é importante para nós, em vez da regulação de conflitos, no seio da OSCE; por vezes, assume-se um papel passivo. Uma atividade passiva face ao que acontece no mundo digital. E isto é chocante.

Uma prova disto mesmo é o caso da Cambridge Analytica, que ameaçará Cambridge, não Moscovo, mas suscita críticas contra a Rússia, não contra o Reino Unido. Em Chipre, por exemplo, todos os documentos do Wikileaks foram expostos através dos EUA e sabíamos que os EUA possuíam informações segundo as quais países terceiros podiam ser atacados. Tal aconteceria sob a bandeira de outros países, e isto tem de ser revelado: quem tem utilizado a bandeira de outro país para atacar? É algo de que devemos ter conhecimento.

O político da UE Antonio Tajani perguntou o seguinte: o que está a acontecer neste domínio? A OSCE, após a decisão de 10 de março de 2016, tomou muitas decisões, e decisões eficazes, que revelam um conjunto de situações, mas em concreto, no que respeita às áreas internacionais da informação, não houve medidas.

E este é um aspeto que devemos lembrar, sobretudo tendo em conta as palavras do vencedor do Prémio Nobel, quando diz o seguinte: "a quarta revolução da informação trará mais ameaças, porque são revoluções que ocorrem no quotidiano e que não conseguimos localizar".

E, neste sentido, a Rússia tem uma vasta experiência na criação e no reforço da confiança. Por exemplo, nas ideias que nos foram apresentadas em 16 propostas relativas à confiança nestas matérias, que dizem respeito a todos nós, percebemos que esta atividade é muito estreita e que, por conseguinte, na nossa ação não estamos a reconhecer o valor real desta organização. Não estamos a aumentar o seu valor. Só apresentaremos estas propostas para que outras organizações trabalhem no ciberespaço, mas estas trabalham separadamente, não em conjunto, rumo ao mesmo objetivo.

Além disso, não existe transparência em termos de tomada de decisões. O que devemos fazer? Devemos revitalizar a Assembleia Parlamentar para lhe dar mais ímpeto e transparência, para que todos possam atuar de forma mais enérgica e transparente.

Na Rússia, foi adotado um plano. O Sr. Shlavort mencionou o facto de este ser um ciberplano para a OSCE. Um dos eventos relacionados com o papel da gestão da paz nos territórios em conflito deve ser realizado sob a alçada da OSCE, e de uma forma mais abrangente, e, por isso, reconhecemos que a conferência de hoje em Lisboa é muito importante e que devemos criar um grupo de especialistas que trabalhe apenas no domínio da segurança do ciberespaço.

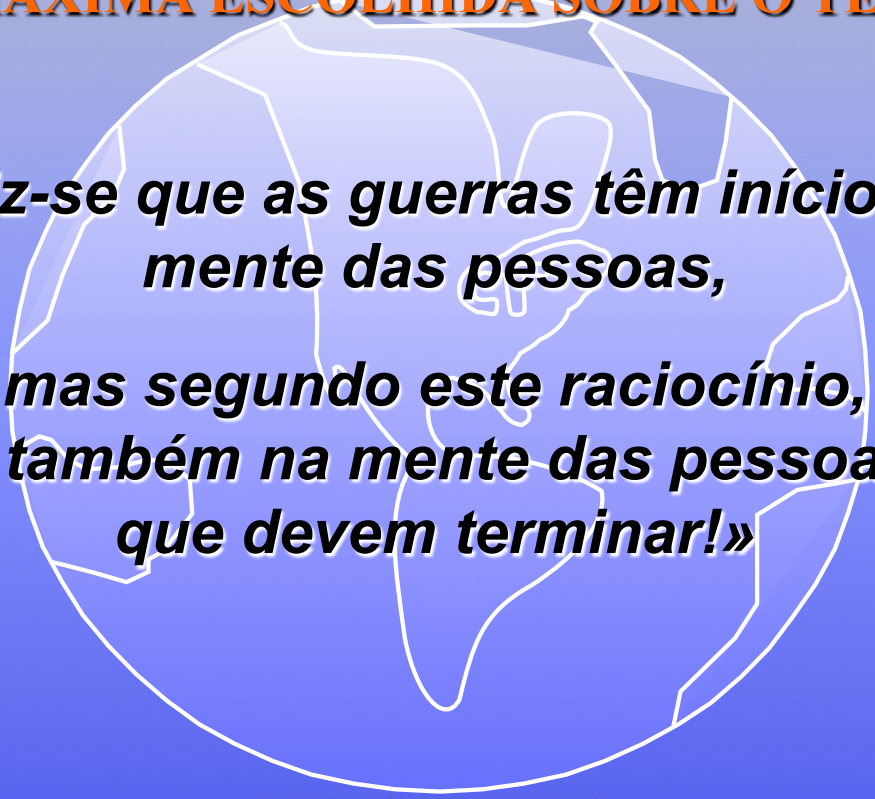
A OSCE organiza duas conferências, e outros pontos do plano ainda não foram abordados. Em dezembro de 2017, como é sabido, a OSCE envidou esforços para reduzir os riscos no que respeita aos conflitos e divergências, tendo sido proposta uma reestruturação do trabalho da OSCE para otimizar a sua participação, além da iniciativa do nosso colega italiano, tendo em vista a realização de uma reunião separada da Comissão em Viena.

Assim, esperamos que este ano comecemos efetivamente a debater o papel da OSCE no domínio da cibersegurança e do combate à cibercriminalidade.

Além disso, o nosso presidente Putin assinou ontem um decreto-lei destinado a promover progressos no país até 2024, no qual se descreve tudo o que deve ser feito em termos de cibersegurança e de combate à cibercriminalidade. Todas estas questões estão no texto de um diapositivo, creio que os intérpretes não o conseguem ver à distância, mas o que pretendemos é garantir a segurança no ciberespaço e lutar contra a criminalidade no ciberespaço.

Por fim, quero agradecer o convite e expressar a minha gratidão por poder estar aqui convosco.

MÁXIMA ESCOLHIDA SOBRE O TEMA



«Diz-se que as guerras têm início na mente das pessoas,

mas segundo este raciocínio, é também na mente das pessoas que devem terminar!»

Смирнов_инф_аспекты_гибрид_войн

2

CONCEITO DE POLÍTICA EXTERNA DA FEDERAÇÃO DA RÚSSIA

Aprovado por V. Putin 30.11.2016

28. A Rússia toma as medidas necessárias para garantir a cibersegurança nacional e internacional, combater ameaças à segurança social, económica e do Estado provenientes do ciberespaço, combater o terrorismo e outras ameaças criminosas relacionadas com a utilização das tecnologias da informação e comunicação;
    - Impede a sua utilização para fins militares e políticos contrários ao direito internacional, designadamente ações destinadas a interferir nos assuntos internos dos Estados ou que representem uma ameaça para a estabilidade, a segurança e a paz internacional;
    - Visa conceber, sob os auspícios da ONU, normas universais de comportamento responsável no que respeita à cibersegurança internacional, nomeadamente no tocante à concretização de uma governação mais internacional da Internet de forma equitativa.

ISO/IEC 27032:2012 Tecnologias da informação -- Técnicas de segurança -Diretrizes para a cibersegurança

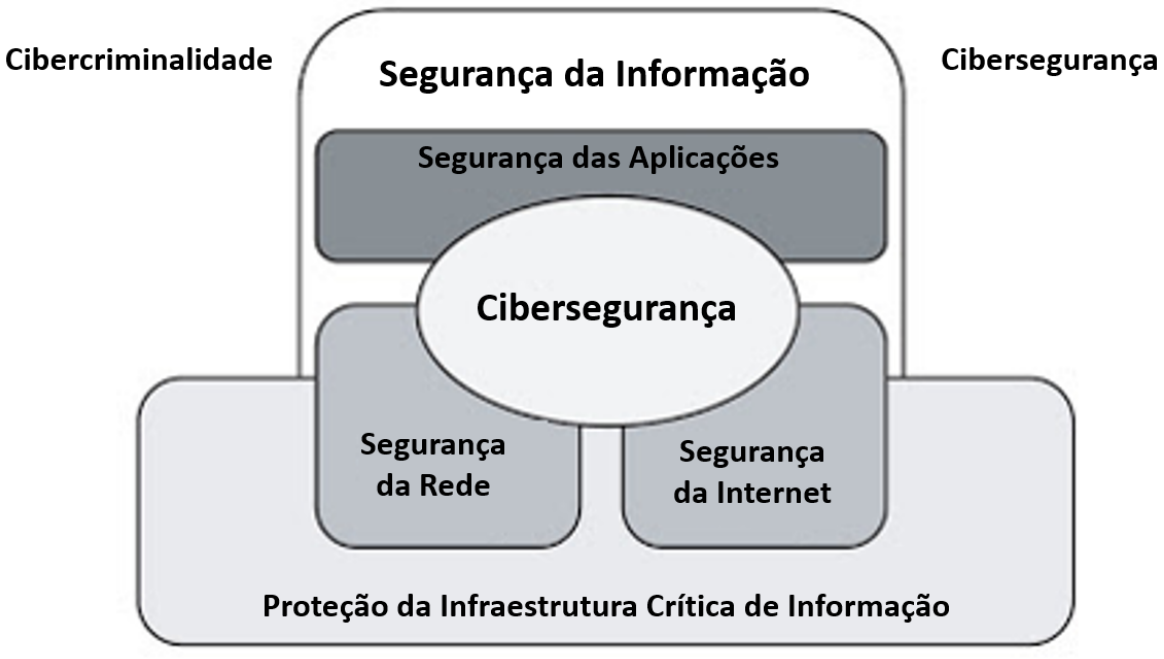


Figura 1 – Relação entre a Cibersegurança e outros domínios de segurança

SMIRNOV_DSI

1. «As alegações de utilização indevida de dados dos utilizadores do Facebook constituem uma violação inaceitável dos direitos dos nossos cidadãos à vida privada. O Parlamento Europeu procederá a uma investigação exaustiva, responsabilizando as plataformas digitais».

OSCE

Organização para a Segurança e a Cooperação na Europa
Conselho Permanente

PC.DEC/1202
10 de março de 2016

Original: INGLÊS

1092.ª Reunião Plenária
Jornal Oficial n.º 1092 do CP, ponto 1 da ordem de trabalhos

DECISÃO N.º 1202
MEDIDAS DA OSCE PARA A GERAÇÃO DE CONFIANÇA DESTINADAS A REDUZIR OS RISCOS DE CONFLITO DECORRENTES DA UTILIZAÇÃO DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Na decisão n.º 1039 do Conselho Permanente (26 de abril de 2012), os Estados participantes na OSCE decidiram intensificar os esforços individuais e coletivos no sentido de abordar a questão da segurança nas tecnologias da informação e comunicação (TIC) e na respetiva utilização de forma abrangente e transversal, em conformidade com os compromissos assumidos pela OSCE e em cooperação com as organizações internacionais pertinentes, doravante designada «segurança das TIC e na respetiva utilização». Ademais, decidiram elaborar um conjunto de projetos de medidas de geração de confiança (CBM, do inglês *confidence building measures*) tendo em vista aumentar a cooperação, a transparência, a previsibilidade e a estabilidade interestatais, bem como reduzir os riscos de erros de perceção, agravamento e conflitos que podem decorrer da utilização das TIC.

Os Estados participantes na OSCE, recordando o papel da OSCE enquanto acordo regional nos termos do capítulo VIII da Carta das Nações Unidas, confirmam que as CBM elaboradas no âmbito da OSCE complementam os esforços envidados pelas Nações Unidas no sentido de promover as CBM no domínio da segurança das TIC e na respetiva utilização. Os esforços envidados pelos Estados participantes na OSCE no sentido da aplicação das medidas de geração de confiança no domínio da segurança das TIC e na respetiva utilização serão consonantes com o direito internacional, nomeadamente com a Carta das Nações Unidas e o Pacto Internacional sobre os Direitos Civis e Políticos, bem como com a Ata Final de Helsínquia e as respetivas responsabilidades no tocante ao respeito dos direitos humanos e liberdades fundamentais.

As seguintes CBM foram adotadas pela primeira vez através da Decisão n.º 1106 de 3 de dezembro de 2013 do Conselho Permanente:

INCYDER

OSCE reafirma que um ciberataque pode ser equivalente a um ato de agressão

A Assembleia Parlamentar da OSCE (AP OSCE) adotou a Declaração de Minsk de 2017 centrada em recomendações em matéria de paz e prosperidade destinadas aos governos nacionais, aos parlamentos e à comunidade internacional, tendo em vista contribuir para a definição de políticas nos domínios dos assuntos políticos, da segurança, da economia, do ambiente e dos direitos humanos. A reunião deste ano foi realizada em Minsk entre 5 e 9 de julho de 2017.

Esta reunião da Assembleia Parlamentar incidiu claramente nas questões emergentes no domínio dos assuntos políticos e da segurança em geral, e não só em questões cibernéticas emergentes, tendo abrangido vários aspetos cibernéticos. No âmbito da declaração, salienta com preocupação os desafios contínuos em matéria de segurança em toda a região da OSCE, designadamente as ameaças à cibersegurança, mas o documento carece de dados pormenorizados sobre as atuais ameaças. Insta à tomada de medidas destinadas a aumentar a cibersegurança entre Estados, a fim de prevenir tensões e conflitos decorrentes da utilização das tecnologias da informação e comunicação e proteger infraestruturas críticas de ameaças cibernéticas, nomeadamente através do reforço da aplicação das medidas de geração de confiança da OSCE no domínio da cibersegurança, e da facilitação de cooperação entre os órgãos nacionais e as forças de segurança competentes.

CYBER ARMAGEDDON ?

A HISTÓRIA DAS GUERRAS É UMA HISTÓRIA DOS AVANÇOS TECNOLÓGICOS...

Não podemos esperar que a casa seja roubada para pôr trancas à porta.

http://www.stantonchase.com/wp-content/uploads/2016/09/Leadership-in-Fourth-Industrial-Revolution.pdf

O Presidente da Federação da Rússia assinou o Decreto relativo a «Metas de desenvolvimento e objetivos estratégicos nacionais da Federação da Rússia para o período até 2024» de 7 de maio de 2018.

11. O Governo da Federação da Rússia, no âmbito da implementação do programa nacional «Economia Digital da Federação da Rússia», deve garantir em 2024:

- A triplicação, no mínimo, da despesa interna para o desenvolvimento da economia digital proveniente de todas as fontes (proporção em função do PIB) até 2017;
- A criação de infraestruturas de informação e telecomunicações sustentáveis, seguras e acessíveis para todos para a transmissão a alta velocidade, o processamento e o armazenamento de grandes volumes de dados;
- A criação de um sistema de regulação jurídica da economia digital com base numa abordagem flexível em cada domínio, bem como a introdução de tráfego civil com base em tecnologias digitais;
- Garantias da segurança da informação com base nos progressos nacionais em matéria de transferência, processamento e armazenamento de dados, assegurando a proteção dos interesses relacionados com a identidade, as empresas e o Estado;
- A criação de um sistema de financiamento integrado para projetos de desenvolvimento e/ou implementação de tecnologias digitais e soluções de plataformas, designadamente instituições de financiamento de risco e outras instituições de desenvolvimento.

SMIRNOV_MGIMO 10

CONFERÊNCIAS de LISBOA DA ASSEMBLEIA PARLAMENTAR DA OSCE
LISBON CONFERENCES OF THE OSCE PARLIAMENTARY ASSEMBLY
8 May 2018 | Assembly of the Republic | Portugal
Digital Resilience of a Democratic State

МГИМО УНИВЕРСИТЕТ

Obrigado!

http://niiglob.ru aismirnov@niiglob.ru

ANATOLY SMIRNOV

Thank you very much, I would like to thank all the Portuguese authorities who have invited me to be a part of this conference. I will be addressing you in Russian, although my slides will be presented in the English language.

Despite anything else, what concerns me the most is what Georges Tsetereli has just mentioned ... we have to put an end to war in our own heads. Only then can we reach the goals, so that we can live in peace. And today Europe is celebrating 73 years of victory against the Nazi Germans, and this is the symbol I bring in my coat, this is the symbol of the victory over the 2nd World War, so nowadays the internet areas are very critical ones and this does not mean only Russia. We know that there are many other countries which allow not only the creation of difficult conditions, when it comes to... vis-à-vis other countries.

For instance, Russia and other countries may claim what is the basis around the reason behind this threat. What is on their minds? And actually this is the turning point for us to understand what is happening in terms of cyberspace, the problems related to... represented by cyberspace.

And along these lines, Russia has created a number of documents, strategic documents, and all of them are aimed at the development of the information society and on the other hand they aim at how should we defend ourselves around the cyberspace, which is also bringing about a number of risks, threats and problems. Russia, through its external policy, has clearly declared that... Russia has addressed the UN and asked them to address this problem of the fight against threats that the technological means are bringing about around the cyberspace.

And the idea that has been proposed by Russia was not well accepted and some countries have even criticized Russia due to this idea. And during this time, what happens is that we have lost track of time. So, we simply lost time and what we have seen today in information technology is that are there and they are more and more sophisticated. They are creating more and more this fear and they mentioned so that terrorist may use the cyberspace for their intentions, in order to carry out their intentions.

These are the database records for the year 2017 and you can see how this cyberspace is becoming more and more complex, far more sophisticated in order to be managed, in a positively way, so that we can fight criminality over the cyberspace. The criminals who are using the ICTs show that these technologies are developing, even the criminals are the ones who are developing them. And, as a society, we believe that the priority is this, or, at least, should be that of drafting a universal device, a universal module, so that all of us could fight against this problem.

Our conference is in the name of Cyberspace, but look at this slide. Information security, and this is the relation between information and cybersecurity. So, in terms of Russia, Russia has a very great understanding on this domain. But they only look at “cyber” and “cyber” is only a small part of the whole, of the whole that is part of information and information security. And this has to do with the perception of the concept and the idea, and we also want to highlight that the trend is that Russia has created an association for information security and this is of an international nature, and the Moscow organization together with other universities have also participated in this association, and the President of this association is indeed someone who is very well known to us, Mr Chestuk, who is the general director, and also a part of the presidium, who is made of experts in the field of information and also in the field of information security.

But there is an issue. The threats that we are witnessing and the effect that we see very important board is to ensure this type of security. What is important for us, instead of regulating conflicts, inside this OSCE, sometimes they have a passive role. A passive activity vis-à-vis what happens in the digital world.

And this is a scandal. And a witness thereof is the Cambridge Analytica and this is not something that will endanger Cambridge, but Moscow, but they are criticizing Russia, and not the UK. In Cyprus, for instance, all the Wikileaks documents have exposed via the US and we knew that the US had information whereby third countries could be attacked. And under the flag of other countries and this should be revealed: who has been using the flag of another country to attack and this is something we should raise our awareness to.

The Europolitics Antonio Tajani stated the following: what is happening in this field? The OSCE, after the decision of 2016, March 10th, many of the decisions have been taken, and these have been effective decisions, are showing a number of situations but concretely, in terms of the international areas of information, this hasn't been tackled.

And this is something we ought to be a remind, especially when it comes to the expression by the Nobel Prize when he states the following: “the forth information revolution will bring about more threats, because this is about revolutions that happen on an everyday and which we cannot trace”.

And therefore Russia has a very rich experience in creating, raising trust. For instance, the ideas that have been presented through 16 proposals in terms of trust concerning these matters that concerns us all, we have realized that this activity is very narrow and, therefore, in so doing we are not acknowledging the real value of this organization. We are not enhancing its value. We only will show these proposals just so that other organizations are working over the cyberspace, but they work separately, and not together, for one single goal.

And there's no transparency, in terms of decision-making. And what shall we do? We should revive the Parliamentary Assembly to give more life and transparency so that they can act more lively and more transparence, and in Russia a plan has been adopted. Mr. Shlavort referred to the fact that this is a cyberplan for the OSCE. One of the events which has to do with the role for the regulation of peace around conflict territories, this should be done under the flag of the OSCE, and this should be done under a more encompassing manner, and this is why we acknowledge today's conference in Lisbon, something very important, and we should create a group of specialists that should work strictly in the field of cyberspace security.

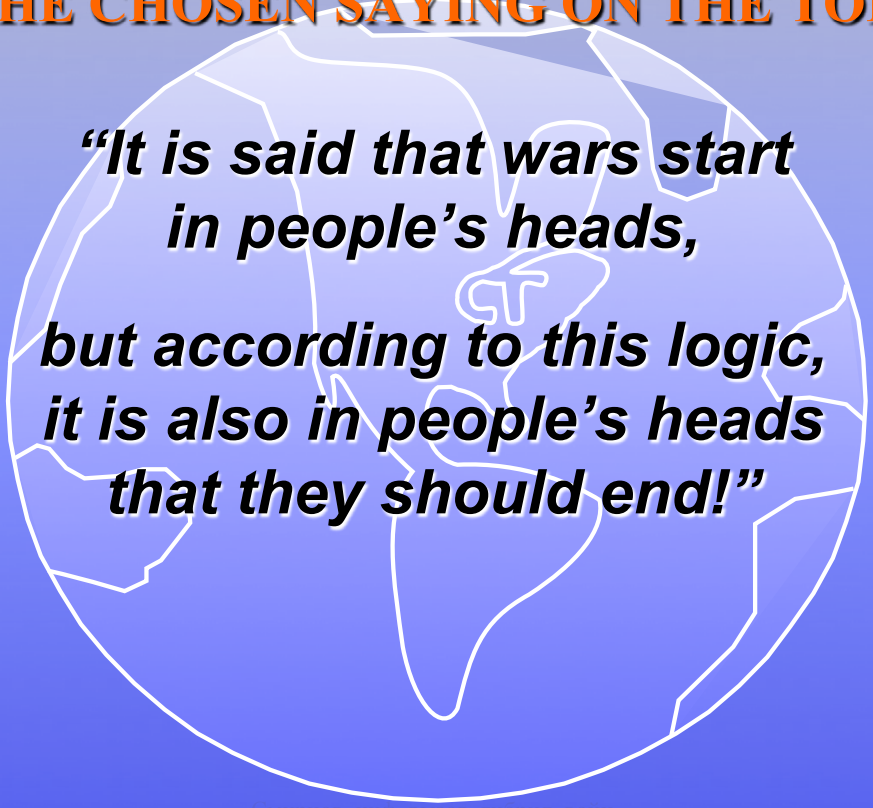
The OSCE organizes two conferences and other points of the plan have not yet been tackled. In December 2017, as you know, efforts by the OSCE were made in order to reduce risks when it comes to conflict and discussion and the restructuring of the OSCE work was proposed in order to optimize their participation and the initiative of our Italian colleague, in order to carry out a separate meeting of the Committee in Vienna.

So, we expect that this year we will truly start to discuss the role of the OSCE in the field of the fight against cybercrime and cybersecurity.

And our President Putin signed yesterday a decree, law, to develop the country until the year 2024, where he states everything that ought to be done in terms of cybersecurity and the fight against cybercrime. And all these issues are written in a slide, surely the interpreters cannot look at it, at the distance, but what we want to do is to ensure the security in the cyberspace, and fighting against crime over the cyberspace.

And finally my words are those of thanking for the invitation and to express my gratitude in being here with you.

THE CHOSEN SAYING ON THE TOPIC



"It is said that wars start in people's heads,

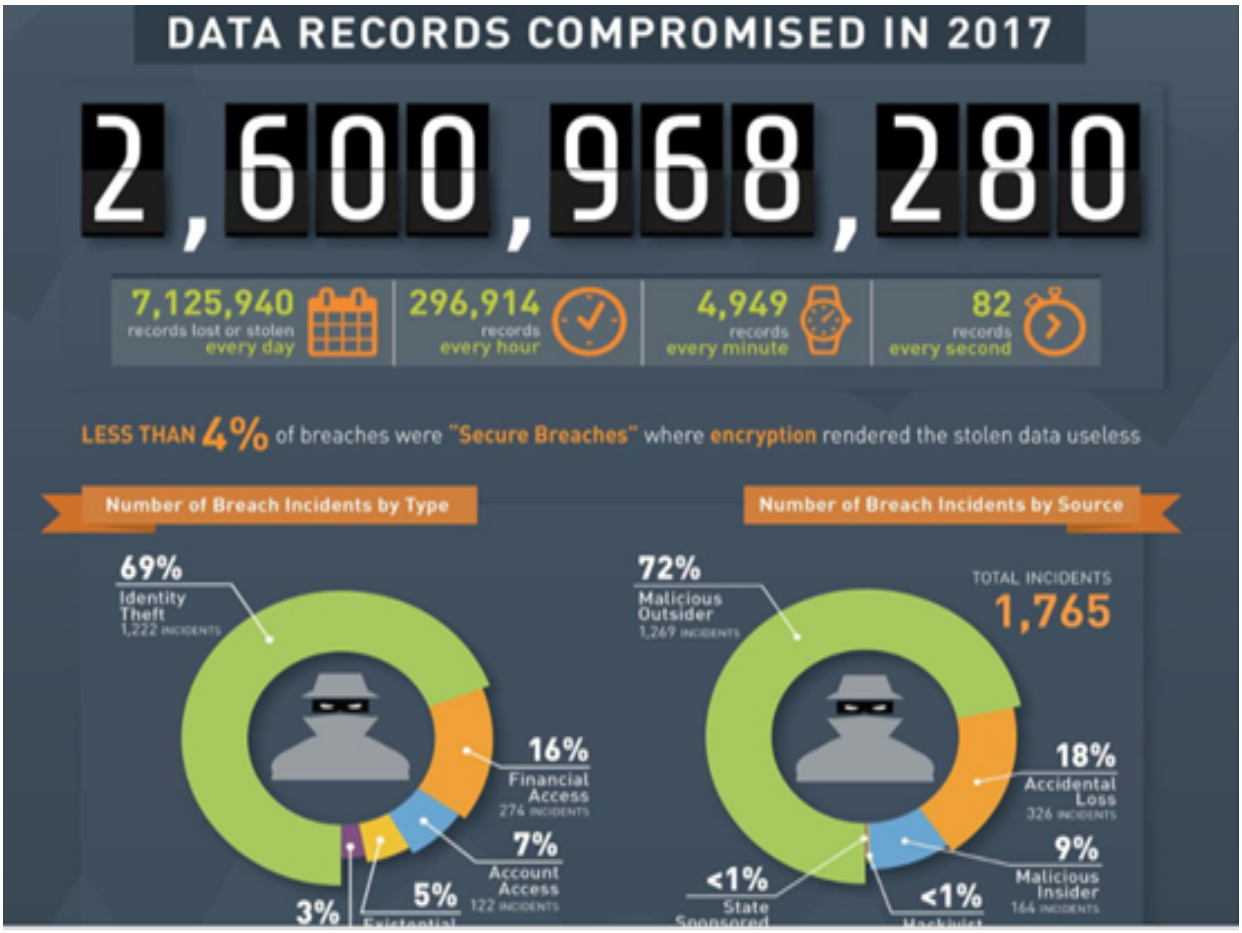
but according to this logic, it is also in people's heads that they should end!"

FOREIGN POLICY CONCEPT OF THE RUSSIAN FEDERATION

Approved by V. Putin 30.11 2016

28. Russia takes necessary measures to ensure national and international cyber security, counter threats to State, economic and social security emanating from cyberspace, combat terrorism and other criminal threats involving the use of information and communication technology;

- deters their use for military-political aims that run counter to international law, including actions aimed at interfering in the domestic affairs of States or posing a threat to international peace, security and stability;
- and seeks to devise, under the UN auspices, universal rules of responsible behaviour with respect to international cyber security, including by rendering the internet governance more international in a fair manner.



ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity

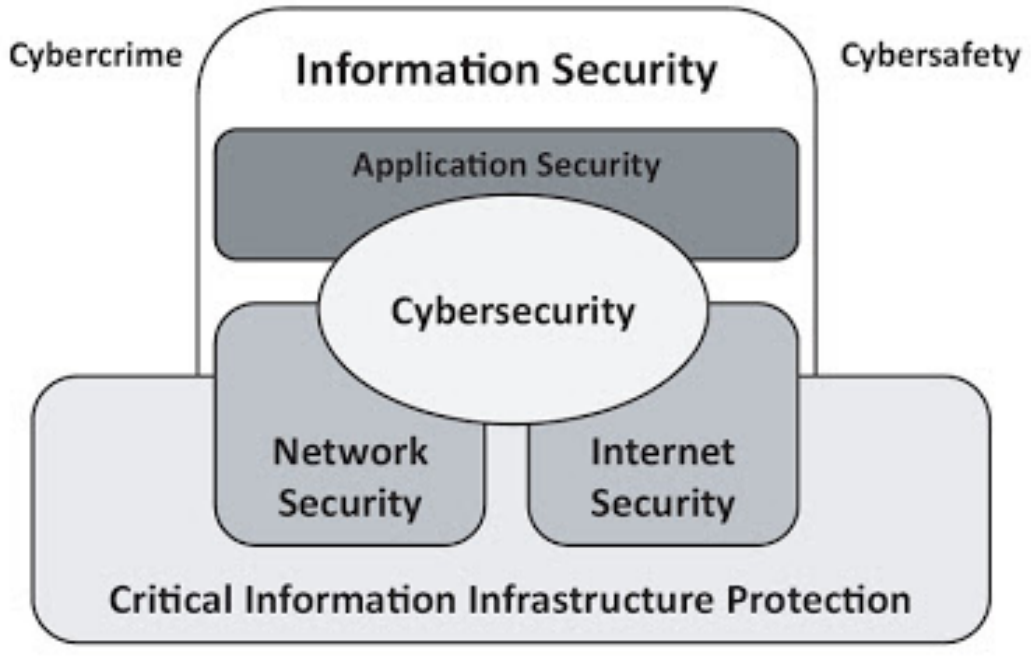


Figure 1 — Relationship between Cybersecurity and other security domains

SMIRNOV_DSI

Antonio Tajani
@EP_President

Читать

Allegations of misuse of Facebook user data is an unacceptable violation of our citizens' privacy rights. The European Parliament will investigate fully, calling digital platforms to account. #CambridgeAnalytics #CambridgeAnalyticaFiles

---

OSCE

Organization for Security and Co-operation in Europe
Permanent Council

PC.DEC/1202
10 March 2016

Original: ENGLISH

1092nd Plenary Meeting
PC Journal No. 1092, Agenda item 1

DECISION No. 1202
OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The OSCE participating States in Permanent Council Decision No. 1039 (26 April 2012) decided to step up individual and collective efforts to address security of and in the use of information and communication technologies (ICTs) in a comprehensive and cross-dimensional manner in accordance with OSCE commitments and in co-operation with relevant international organizations, hereinafter referred to as "security of and in the use of ICTs." They further decided to elaborate a set of draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, *inter alia*, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.

The following CBMs were first adopted through Permanent Council Decision No. 1106 on 3 December 2013:

Resources > INCYDER database Subscribe

OSCE Reaffirms that Cyberattack May Be Equivalent to an Act of Aggression

The OSCE Parliamentary Assembly (OSCE PA) adopted the 2017 Minsk Declaration with a focus on recommendations for peace and prosperity to national governments, parliaments and the international community to help shape policies in the fields of political affairs, security, economics, the environment, and human rights. This year's meeting was held in Minsk from 5 to 9 July 2017.

The emphasis of this meeting of the Parliamentary Assembly was clearly on emerging issues within the field of political affairs and security in general, and not only on emerging cyber issues, but it covered several cyber aspects. Within the declaration, it notes with concern the ongoing security challenges throughout the OSCE region, including cybersecurity threats, but the document lacks thorough detail on current threats. It urges that measures be taken to enhance cybersecurity between states, to prevent tension and conflict stemming from the use of information and communication technologies, and to protect critical infrastructure from cyber threats, including by strengthening the implementation of the OSCE's confidence-building measures in the area of cyber security, and facilitating co-operation among the competent national bodies and law enforcement agencies.

CYBER ARMAGEDDON ?

THE HISTORY OF WARS IS A HISTORY OF TECHNOLOGICAL BREAKTHROUGHS…

You cannot wait until a house burns down to buy fire insurance on it.

http://www.stantonchase.com/wp-content/uploads/2016/09/Leadership-in-Fourth-Industrial-Revolution.pdf

The President of the Russian Federation signed the Decree “On national development targets and strategic objectives of the Russian Federation for the period up to 2024” of 7 May 2018.

From paragraph 11. The Government of the Russian Federation, within the scope of implementing the “Russian Federation’s Digital Economy” national programme, should guarantee in 2024:

- An increase in internal spending for the development of the digital economy drawn from all sources (proportions in relation to GDP) by at least three times by 2017;
- The creation of information and telecommunications infrastructure that is sustainable, secure and accessible to all for the high-speed transmission, processing and storage of large amounts of data.
- The creation of a legal regulation system for the digital economy based on a flexible approach in each area, as well as the introduction of civil traffic based on digital technologies;
- Guarantees of the security of information based on national developments in data transfer, processing and storage, ensuring the protection of interests regarding identity, business and the state;
- The creation of an integrated funding system for projects to develop and/or implement digital technologies and platform solutions, including risk financing and other development institutions;

SMIRNOV_MGIMO 10

CONFERÊNCIAS de LISBOA DA ASSEMBLEIA PARLAMENTAR DA OSCE
LISBON CONFERENCES OF THE OSCE PARLIAMENTARY ASSEMBLY
8 May 2018 | Assembly of the Republic | Portugal
Digital Resilience of a Democratic State

МГИМО УНИВЕРСИТЕТ

Thank You!

http://niiglob.ru aismirnov@niiglob.ru

WILLIAM SWEENEY

Caros amigos!

É um prazer estar com tantos colegas e amigos da política e da ação política ao longo das últimas décadas.

Recebo membros das equipas de observação de eleições legislativas da OSCE nos Estados Unidos, na minha qualidade de Presidente da Fundação Internacional de Sistemas Eleitorais (IFES) desde 2010, e aguardo com expectativa a minha próxima participação no vosso programa, em novembro de 2018, em Washington. O tempo que passamos juntos a promover eleições democráticas atravessa já algumas décadas.

A IFES está a celebrar o seu 31.º aniversário. A fundação tem programas em 24 dos 57 países da OSCE desde 1987. Juntos todos celebramos o progresso das nossas sociedades na realização dos ambiciosos objetivos do artigo 21.º da Declaração Universal dos Direitos do Homem, segundo o qual "toda a pessoa tem o direito de tomar parte na direção dos negócios públicos do seu país, quer diretamente, quer por intermédio de representantes livremente escolhidos" e "toda a pessoa tem direito de acesso (...) às funções públicas do seu país".

Fui observador eleitoral acreditado em eleições na Geórgia, na Ucrânia e até nas eleições de 1994 para a Duma, na Rússia!

Fui membro da equipa internacional que aconselhou os partidos húngaros na preparação para as primeiras eleições, em 1990, quando o Muro de Berlim ainda continuava de pé e o partido FIDESZ tinha um limite de idade de 35 anos.

Em 1991, a IFES organizou a reunião constitutiva das Associações Responsáveis Eleitorais da Europa Oriental, que apoiamos desde a sua fundação. Será um prazer representar de novo a IFES este ano, em 7 de setembro, em Vilnius.

Durante a minha carreira, trabalhei de forma estreita com o Congresso dos EUA. O vosso amigo e colega Roger Wicker e os demais membros do Congresso lamentam não poderem estar presentes aqui em Lisboa. Como sabem, o Congresso dos EUA está em período de sessão e os seus membros não puderam viajar para Portugal e participar nesta importante conferência.

Fui encarregado de transmitir aos membros do Congresso informações sobre esta importante reunião. A democracia é um valor a que todos aspiramos. Os desafios colocados pela cibersegurança e pelo terrorismo ao nosso objetivo partilhado de confiança no processo democrático são substanciais. A missão declarada da IFES é assegurar que cada voz seja ouvida e tida em consideração, e este objetivo é hoje mais complexo do que nunca.

A minha apresentação de hoje pretende demonstrar que o papel das comissões eleitorais está a mudar profundamente devido ao que aconteceu nos últimos anos.

Na política nunca podemos ser meros espectadores. Todas as partes envolvidas estão plenamente empenhadas no processo e nos resultados. Os líderes políticos que têm a responsabilidade de selecionar e apoiar as ações dos organismos de gestão eleitoral têm de mudar a sua perspetiva e reconhecer as novas funções e responsabilidades de um organismo dessa natureza.

Todos os empregos começam com uma descrição de funções, e a descrição de funções dos elementos das comissões eleitorais – presidentes e membros – está a mudar substancialmente em resultados das lições retiradas em 2015, 2016 e 2017.

A primeira função de um responsável eleitoral é administrar de forma justa e transparente o processo eleitoral em conformidade com a lei. Esta tarefa parece simples, mas aqueles que, como eu, trabalham na realização de eleições compreendem que é um trabalho complexo, particularmente nas sociedades em que a prestação do serviço público representa um desafio.

Após as experiências dos últimos anos, a descrição de funções de um responsável eleitoral começa pelo primeiro dia.

Quais são os novos papéis e responsabilidades?

Imaginemos uma situação em que a janela da nossa casa tem impressões digitais e pegadas de botas lamacentas. Alguém esteve de pé à janela a olhar para o interior da casa. Não sabemos se a casa foi assaltada ou se um estranho estava simplesmente a olhar/vigiar. Temos de presumir que havia "intenção", mas o crime em si continua, de algum modo, indefinido. Imaginemos também que os nossos vizinhos sabem que tal aconteceu e estão agora preocupados com a segurança da zona.

Quando discutem a cibersegurança em eleições, sobretudo no contexto de experiências dos últimos anos, as comissões eleitorais veem-se confrontadas com este possível local de crime. Um acontecimento é conhecido por todos na vizinhança política e proliferam os rumores.

O papel e a responsabilidade dos organismos de gestão eleitoral mudaram profundamente devido ao confronto com a realidade da administração eleitoral no mundo digital, a nova Internet das coisas, e exemplos sucessivos de governos estrangeiros e de intervenientes sectários no seu país que procuram tirar partido da perturbação e/ou enfraquecimento da credibilidade/integridade do processo eleitoral.

O dia de eleições já não é um evento, mas um ciclo. Talvez mais até do que um ciclo, se o objetivo for a perturbação das eleições. Nos ciberataques, 90% do tempo é dedicado a planear o ataque e menos de 10% ao ataque ou "ato de pirataria" concreto.

A maioria dos atos eleitorais está a tornar-se mais dependente da informação digital. Os sistemas de identificação biométrica, a melhor utilização de imagens fotográficas e os códigos de barras baseiam-se em informações digitais, o que significa que os cartões de identificação dos eleitores são de leitura automática, com as listas em papel como opção de recurso.

A maior interconexão dos sistemas cria riscos para a segurança. Equipamentos como impressoras e telemóveis tornaram-se oportunidades para piratear ou perturbar um sistema, sobretudo quando as máquinas são instaladas em todo o país no dia de eleições. Os sistemas enfrentam vulnerabilidades adicionais quando os membros das mesas tentam carregar as baterias dos seus telemóveis e portáteis, ligando-os de forma inadequada a outras redes.

Por último, os ensinamentos retirados nos Estados Unidos em 2016, e no Quénia e na Libéria em 2017, bem como as experiências no Afeganistão, na Geórgia, Indonésia e Ucrânia testemunhadas pela IFES sugerem que um organismo de gestão eleitoral não pode desvalorizar o risco de um ambiente sectário com uso de armas em que todas as decisões – relativas a pessoas, políticas ou contratos públicos – de uma comissão eleitoral são contestadas por forças internas que tentam descredibilizar o processo de negociação de um acordo pós-eleitoral ou a possibilidade de interferência deliberada patrocinada por um Estado estrangeiro.

Enquanto parlamentares da OSCE, quais são os novos desafios a ter em conta no plano legislativo?

Em primeiro lugar, os organismos de gestão eleitoral devem passar a ter um estatuto e um orçamento de infraestrutura crítica nacional, quer enquanto parceiros das entidades governamentais pertinentes (serviços de informações, polícia, forças armadas, Ministério dos Negócios Estrangeiros), quer como geradores de produtos (registos de eleitores; declarações de interesses públicas dos candidatos; registos de financiamento das campanhas).

Os EUA estabeleceram este estatuto em 2017, mas os respetivos pormenores e orçamentos ainda não são conhecidos. Esta conferência em Portugal é um exemplo perfeito. Estamos a debater a cibersegurança em eleições sem a participação da Comissão Nacional de Eleições. Esta omissão não é invulgar.

Por vezes, as comissões de eleições não estão articuladas com as forças de segurança do seu país por razões históricas e também culturais. Em todos os países, o planeamento de uma relação de confiança entre o organismo de gestão eleitoral e as forças militares e policiais para assegurar apoio logístico e a segurança física dos eleitores, dos membros das mesas e das urnas sem intimidação deveria ser uma componente do plano estratégico para qualquer ato eleitoral. Expandir esta relação de modo a incluir a cibersegurança implica parcerias com os ministérios responsáveis pelos serviços de informações e pelas telecomunicações. A IFES desenvolveu uma sequência de boas práticas para a segurança das eleições.

Em segundo lugar, grande parte das informações sobre ataques e proteções de cibersegurança são informações classificadas em todos os países. Em 2016, nenhum responsável eleitoral dos Estados Unidos obteve o estatuto necessário para receber dados dos serviços de informações, forças armadas ou forças de segurança dos EUA sobre os ciberataques russos. Na alteração do papel dos organismos de gestão eleitoral, tem de haver um investimento que proporcione o nível adequado de autorização de segurança a funcionários públicos designados responsáveis pelo ato eleitoral.

Em terceiro lugar, a informação só é útil se puder ser partilhada e dar lugar a medidas. Devem ser desenvolvidos protocolos de informação entre os organismos de gestão eleitoral e as fontes dos serviços de informações em matéria de ciberataques para ser possível atuar em tempo real sem pôr em causa a privacidade e as informações de identificação pessoal. Se o sistema de uma empresa ou de uma instituição financeira estiver a ser alvo de um ataque, haverá uma resposta em tempo real. Sem protocolos de informação adequados em vigor, uma comissão eleitoral disporá apenas dos seus próprios sistemas de defesa, que normalmente são inadequados porque o investimento em cibersegurança não é robusto. Foi por isso que o seu sistema foi violado.

Em quarto lugar, é necessário aumentar a escala das capacidades e dos orçamentos de comunicação das comissões de gestão eleitoral para dar resposta às ameaças à sua integridade. A ascensão das redes sociais como uma força autónoma na maior parte das sociedades, bem como a possibilidade de utilização abusiva destas plataformas por todos os intervenientes partidários, incluindo empresas de consultoria política mundiais e interesses estrangeiros, transforma as comissões eleitorais na primeira linha de defesa das eleições e da democracia nos respetivos países.

A maioria das comissões eleitorais é culturalmente avessa à participação em debates públicos. Não creem que afirmar e defender publicamente a integridade do sistema eleitoral – cada decisão relativa a pessoas, políticas e contratos públicos – faça parte das suas responsabilidades. Existe o receio de que uma presença constante no diálogo político possa manchar a sua imagem e lesar a sua credibilidade na gestão das regras. De um modo geral, temem ser rotulados como "partidários" e preferem evitar discussões que possam desequilibrar a balança.

A minha experiência diz-me que os líderes políticos nacionais preferem geralmente nomear para as comissões eleitorais pessoas menos propensas a participar em debates públicos. Privilegiam pessoas que são bons administradores e seguem fielmente as disposições da legislação eleitoral, mas evitam as funções de comunicação.

Esta situação tem de mudar.

A afirmação e defesa do processo democrático de uma nação é agora parte integrante da descrição de funções. A comunicação representa um conjunto de competências. Pode ser aprendida.

Em quinto lugar, a corrupção nos contratos públicos é um cancro para um governo e o seu apoio público. Ignorar o cancro só diminui o tempo de vida. A corrupção nos contratos públicos de materiais eleitorais sensíveis, por exemplo urnas e tinta, bem como de tecnologias eleitorais, resulta necessariamente em contestação jurídica das decisões tomadas pela comissão eleitoral.

Em muitos países onde a IFES trabalha, a realidade da corrupção é uma ferida aberta que só vem reforçar a narrativa de qualquer parte interessada ou potência estrangeira que procure desacreditar a integridade do processo político, as eleições, os resultados e a capacidade do país para se autogovernar no futuro.

Quando os elementos das comissões eleitorais são parte do problema da corrupção pública e não da solução para o seu país, comprometem a base da esperança num processo e em eleições credíveis. São conspiradores no caminho de enfraquecimento da democracia.

Em sexto lugar, a dependência crescente da tecnologia implica normalmente que o primeiro teste de credibilidade da comissão eleitoral e, na verdade, de todo o processo político deve ocorrer quando são elaborados os cadernos de encargos dos contratos públicos para tecnologia eleitoral e materiais eleitorais, no quadro de um esforço holístico para transformar a urna "negra" numa urna transparente. A elaboração dos cadernos de encargos para os contratos públicos deve assentar num diálogo aberto.

A primeira utilização de comités de ligação aos partidos e à sociedade civil deve acontecer quando se tomam decisões sobre a tecnologia a utilizar e sobre a solução de problemas de eleições anteriores. Este diálogo e esta explicação técnica devem ocorrer no início dos preparativos para o ato eleitoral seguinte e não, seguramente, no ano das eleições, quando o calendário político é intenso e apertado. Esta atitude exige que os partidos políticos estejam preparados para compromissos em domínios técnicos logo no início do ciclo, normalmente vários anos antes do ato eleitoral.

Infelizmente, muitas comissões eleitorais são alvo de pressão política para que introduzam demasiadas tecnologias numa fase avançada do calendário eleitoral, o que geralmente redunda em contratos públicos com falhas e um intervalo temporal inadequado para testes, formação e implantação. Estas más decisões limitam o futuro das comissões eleitorais. A IFES testemunhou situações em que comissões eleitorais entregaram a fornecedores os seus direitos legais sobre os cadernos eleitorais e o *software* eleitoral.

Em sétimo lugar, a administração pública é fundamental na prestação de todos os serviços públicos. Os líderes públicos devem investir na criação e manutenção de um grupo profissional de funcionários públicos com experiência e conhecimento especializado nos domínios pertinentes. Em demasiados países, as comissões eleitorais são designadas pontualmente, sem as proteções concedidas aos demais funcionários públicos nem um compromisso público de excelência sustentada. É necessário passar a incluir na descrição de funções destas comissões uma abordagem de gestão, tendo em vista os desafios futuros, para que os serviços sejam prestados por uma equipa profissional capaz de interagir com as inovações nas tecnologias e nas ameaças.

Acredito que a promoção e proteção dos valores democráticos é um desporto coletivo que deve tornar-se uma responsabilidade partilhada por todos os líderes políticos interessados na resolução pacífica dos problemas através do voto. A democracia, em todos os países, necessita de um coro, grupos de instrumentos, uma orquestra sinfónica – não de solistas.

WILLIAM SWEENEY

My Friends:

It is a pleasure to be with so many colleagues and friends from policy and politics over the last few decades.

I have welcomed members of the OSCE Parliamentary election observation teams to the United States in my role as IFES President since 2010 and I look forward to being part of your program again in November 2018 in Washington, D.C. Our time together to promote democratic elections goes back a few decades.

IFES is now celebrating our 31st year. IFES has had programs in 24 of the 57 OSCE countries since 1987. Together, we all celebrate the progress of our societies towards the aspirational goals of Article 21 of the Universal Human Rights Declaration, of "Everyone having the right to take part in the government of his country, directly or through freely chosen representatives, and everyone having the right to have access to public service in his country."

I have been an accredited election observer for elections in Georgia, Ukraine and even the 1994 Russian Duma elections!

I was a member of the international team advising Hungarian parties in preparation for the first election in 1990 when the Berlin Wall was standing and FIDESZ was a party with an age limit of 35.

In 1991, IFES convened the organizational meeting of the ACEEEO which we have supported since its founding. I look forward to again representing IFES this year on September 7th in Vilnius.

During my career, I have worked closely with the U.S. Congress. Your friend and colleague, Roger Wicker and the other Members of Congress, regret that they are not in attendance here in Lisbon. As you know, the U.S. Congress is currently in session and Members are unable to travel to this important meeting in Portugal.

I have been tasked to report to the Members of Congress on this important meeting. Democracy is a value we all aspire to. The challenges of cybersecurity and terrorism to our mutual goal of trust in a democratic process are substantial. IFES mission statement is every voice heard and counted and that goal is more challenging now than ever before.

My presentation today is to argue that the role of election commissions is fundamentally changing due to what's happened over the last few years.

Politics has never been a spectator sport. All parties in the game are fully engaged in both the process and the outcome. Political leaders who have a responsibility for selecting and endorsing the actions of election management bodies need to change the optics and recognize the new roles and responsibilities of an election management body.

All jobs start with a job description and the job descriptions of election commissioners – chairs and members – are fundamentally being changed as a result of the lessons of 2015, 2016 and 2017.

The initial task for an election official is to fairly and transparently administer the election process in accord with the law. That assignment sounds simple but those of us who work in the election delivery business understand it is a complex undertaking, particularly in societies where delivery of public service is a challenge.

After the experiences of the last few years, the job description of an election official starts on day one.

What are the new roles and responsibilities?

Let's imagine a situation where the window on your porch has both fingerprints and muddy boot prints. Someone was standing at that window looking into your home. We don't know if the house was burgled or if a stranger was simply looking/stalking. We must assume there was "intent" but the exact crime remains somewhat undefined. Let's also acknowledge that your neighbors know this happened and are now worried about the safety of the neighborhood.

When we discuss cybersecurity in elections, particularly in experiences over the last few years, election commissions find themselves confronting this possible crime scene. An event is known by everyone in the political neighborhood and rumors abound.

The role and responsibility of election management bodies have fundamentally changed due to confronting the reality of election administration in the digital world; the new internet of things; and, repeated examples of foreign governments and partisans within their country seeking advantage from disrupting and/or undermining the credibility/integrity of the election process.

Election Day is no longer an event but a cycle. Perhaps even longer than a cycle if the goal is disruption of the election. Cyberattacks invest 90% of their time in planning the attack and invest less than 10% in the actual attack or "hack".

Most elections are becoming more dependent on digital information. Biometric identification systems, better photographic imagery, bar coding rely on digital information which means voter identification cards are machine readable with a paper list backup.

The greater interconnectivity of systems raises risks to security. Equipment such as printers and cell phones have become opportunities for hacking or disrupting a system, particularly when the machines are deployed across the country on election day. Systems confront added vulnerabilities when election workers try to recharge their batteries for their cell phones and laptops by adding them improperly to networks.

Finally, the lessons learned from the United States in 2016, Kenya and Liberia in 2017 as well as experiences in Afghanistan, Georgia, Indonesia and Ukraine witnessed by IFES suggest an election management body cannot dismiss the potential for either a weaponized partisan environment where every decision – people, policy, procurement -- by an election commission is challenged by domestic forces trying to undermine the credibility of the process to negotiate a post-election arrangement or the possibility of deliberate foreign state sponsored interference.

As OSCE Parliamentarians, what are the new challenges for legislative consideration?

First, election management bodies must become designated and budgeted as national critical infrastructure as both a partner of the other relevant government agencies (intelligence, police, military, foreign ministry) as well as a product (voter registration files; public disclosures by candidates; campaign finance records).

The U.S. made this designation in 2017 but the details and budgets are still unknown. This conference in Portugal is a perfect illustration. We're talking about cybersecurity in elections without the participation of the Comissão Nacional de Eleições (Election Commission of Portugal). Such an oversight is not unusual.

Election commissions are sometimes not aligned with the security apparatus of their country due to history as well as culture. In all countries, planning a trusting relationship between the election management body and the military and police forces to provide logistical support and physical safety to the voters, election poll workers and the ballots without intimidation should be a component of the strategic plan for every election. Expanding this relationship to include cybersecurity involves partnerships with intelligence and telecommunications ministries. IFES has developed a discipline of best practices for election security.

Second, much of the information about cybersecurity assaults and protections is classified by every country. In 2016, there was no election official in the United States with the proper classification status to receive information on the Russian cyberattacks from U.S. intelligence, military or law enforcement. In reviewing the changed role of the election management bodies, there must be an investment in providing the appropriate level of security clearance to designated public servants responsible for the election.

Third, information is only valuable if it can be shared and acted upon. Information protocols must be developed between election management bodies and the sources of intelligence concerning cyberattacks so the information can be acted upon in real time without compromising privacy and personally identifiable information. If a company or financial institution system was under assault, there would be a real-time response. Without appropriate information protocols in place, an election commission will only have its own defensive systems which are usually inadequate because the cyber security investment is not robust. That's why their system got penetrated.

Fourth, the communications capabilities and budgets of election management commissions must scale to match the challenges to their integrity. The rise of social media as a force within most societies as well as the potential for abuse of these platforms by both partisan forces, including global political consultants, as well as foreign interests transforms election commissions into the first line of advocacy and defense of the election and democracy in the country.

Most election commissions are culturally averse to engagement in public debates. They do not believe advocacy and defense of the integrity of the election system – each personnel, policy and procurement decision – is embedded in their responsibility. There's a fear that a constant presence in a political dialogue may tarnish their image and damage the credibility to administer the rules. Generally, there's a fear of being labelled "partisan" and they prefer to avoid encounters which may tilt the balance.

In my experience, domestic political leaders seem to prefer individuals for appointments to election commission who are reluctant to engage in public debates. There's a preference for people who are decent administrators attuned to the legalities of the election law but who eschew the communications role.

This must change.

Advocacy and defense of a nation's democratic process is now part of the job description. Communications is a skill set. It can be learned.

Fifth, corruption in public procurement is a terminal cancer to a government and its public support. Ignoring the cancer only shortens life. Corruption in the public procurements of both sensitive election materials, i.e., ballots and ink, as well as election technology guarantees political and legal challenge to the decisions by the election commission.

In many countries where IFES works the reality of corruption is an open wound which conveniently reinforces the narrative of any effort by any stakeholder or foreign power to discredit the integrity of the political process, the election, the results and the ability of the nation to govern itself in the future.

When election commissioners are part of the problem of public corruption rather than the solution for their country, they fundamentally compromise the hope for a credible process and election. They are conspirators in the process to undermine democracy.

Sixth, the increasing reliance on technology usually means the first test of credibility for the election commission and indeed the entire political process should take place when the specifications are being developed for public procurements of election technology and election materials as part of a holistic effort to transform the "black box" into a glass box. Development of the specifications for the procurement should be an open dialogue.

The first utilization of party liaison committees and civil society outreach should be when the decisions about which technology to address and which issues in past elections are underway. This dialogue and technical explanation should occur at the beginning of the preparations for the next election and certainly not in the year of the election when the political calendar is intense and compressed. This attitude demands the political parties be ready for engagement in technical areas very early in the cycle, usually years ahead of the election.

Unfortunately, many election commissions become subject to political pressure to introduce too many technologies late in the election calendar which usually means flawed procurements and inadequate time for testing, training and deployment. Such poor decisions offer handcuff election commissions' futures. IFES has witnessed situations where election commissions have surrendered their legal rights on voter registries and software to vendors.

Seventh, public administration is a discipline in providing every public service. Public leaders are supposed to invest in creation and maintenance of a professional body of public servants with a career path of expertise in their fields. For too many countries, election commissions are episodic assignments without civil service protections or a public commitment to continued excellence. A management focus with a perspective of emerging challenges to service delivery by a professional staff able to engage with innovations in technology and threat is now needed as part of the job description.

I believe promotion and protection of democratic values is a team sport which should become the shared responsibility by all political leaders who have an interest in the peaceful resolution of issues thru the ballot box. Democracy in every country needs a choir, a chorus, a symphony orchestra – not single voices.

IGNACIO AMOR

Muito obrigado, senhor moderador. Muito obrigado aos colegas portugueses da delegação portuguesa na Assembleia Parlamentar da OSCE, e uma grande saudação aos outros colegas que vejo há muitos anos, o Paulo Pisco, o Jorge Lacão, e outros parlamentares desta Assembleia da República.

Vou tentar falar português, não "portunhol", e sinceramente, se me engasgo, a Susana dá uma ajudinha aqui para ultrapassar a dificuldade.

Eu sou um político generalista. Não posso dizer que seja perito em cibersegurança ou, inclusivamente, em *fake news*. A minha única especialidade é o direito constitucional. Aliás, o direito constitucional português, que estudei há muitos anos aqui na Assembleia da República.

Eu creio que as águas já há alguns anos ficaram turvas e não era fácil distinguir uns fenómenos dos outros. E havia uma sensação de que toda esta nova área da política que tinha que ver com cibersegurança e com as *fake news* era parte de uma mesma atmosfera. Eu creio que hoje as coisas estão a sedimentar-se, e a pasta no meu *iPad*, a que eu chamei há uns anos *ciber and fake* deve ser agora diferenciada, porque uma coisa são as ciberameaças e outra são as *fake news*.

Eu creio que, isso sim, toda esta nova forma de difundir a informação tem que ver com um neo-irracionalismo, um neo-irracionalismo pós-moderno. Assim a ideia dos *alternative facts* é, claramente, um retorno ao irracionalismo, e todos sabemos na História a que tipo de sociedades conduz estas ideias.

As *fake news* são uma ocorrência muito antiga. Não vou falar da propaganda dos reis sumérios, estou a falar de *fake news*, de *news*. Só podemos falar de notícias a partir da invenção da imprensa e, aqui em Lisboa, é oportuno recordar que uma das ocorrências que alcançou mais notoriedade em toda a Europa foi o terramoto de Lisboa de 1755. E o facto de que o terramoto de Lisboa criou um tipo de literatura que eram as "relações de sucessos", que alcançaram toda a Europa. O terramoto alcançou uma notoriedade e foi uma notícia universal, pelo menos no mundo europeu. A universalidade de uma notícia parte do risco que estamos a examinar. Hoje não há "relações de sucessos". Hoje há "notícias virais", nas redes sociais. E o efeito é o mesmo.

Penso que há que distinguir as ameaças cibernéticas das ameaças que utilizam instrumentos cibernéticos para se espalharem pelo mundo, mas que as mesmas não são cibernéticas. Uma notícia falsa não é uma ameaça cibernética. Mas se a notícia falsa se espalhar pelas redes sociais ou outros modos de alcançar uma audiência universal, tem que ver com a cibernética.

Um programa espião, um programa malicioso é uma arma e uma forma de agressão e tem de ser tratado como uma ameaça. O ciber, então, pode ser só o veículo no qual uma notícia falsa ou uma desinformação alcança uma enorme audiência pelo efeito viral e pelas técnicas utilizadas para fazer viral uma notícia qualquer. Mas o ciber, na relação com as *fake news* é puramente instrumental. É apenas o veículo pelo qual as notícias falsas e o conteúdo da desinformação atingem vastíssimas audiências no mundo.

Os *hackers* clássicos, quando conseguiam quebrar a segurança de um sistema, só deixavam uma simples assinatura. Uma assinatura para dizer: "Eu consegui! Eu estive cá, eu tive acesso a esta informação." Isso era tudo. Porém, agora a utilização de ciberameaças e de programas maliciosos serve para extrair ou destruir informação, nem sempre para ocultar informação, mas para revelar informação. Os fenómenos como a *Wikileaks*, ou os fenómenos como os *Panama Papers*, o correio da Sr.ª Clinton são informação real. São informação verídica. Contudo, tinham uma proteção legal que foi quebrada. Pelo que nem sempre estes instrumentos servem para espalhar notícias falsas. Por vezes servem para espalhar informação real e há que ter em conta esta faceta do fenómeno.

Qual é o objetivo da desinformação, o objetivo das *fake news*? É a simples desinformação? A desinformação tem efeitos políticos, que é o objetivo final das agências, dos atores que utilizam este tipo de ameaças. Eu queria falar de alguns dos efeitos políticos da desinformação.

Dantes tínhamos cidadãos desinformados, porque não tinham informação, não tinham acesso aos meios de comunicação. Contudo, agora temos cidadãos desinformados, porque têm acesso a muita informação não hierarquizada, não submetida a filtros profissionais, que chega ao usuário da informação sem um filtro profissional, sem um código ético, no qual um jornalista, como o colega que nos acompanha, fez o seu trabalho de distinguir o que pode ser considerado uma notícia ou não.

E este excesso de informação produz barulho, como acontece nas matemáticas e acontece nas ciências, e creio que é necessário distinguir neste barulho ou neste excesso de informação quais são os objetivos políticos que, por vezes, tratam de ser atingidos.

Há objetivos ingénuos e publicitários de pôr uma notícia espalhafatosa para chamar a atenção, para excitar a curiosidade e para viabilizar uma página com publicidade. É uma fórmula comercial que não tem maior perigo do ponto de vista político. E há que dizer (e vou ligar isto ao que foi dito pelo colega russo), também há teorias da conspiração sobre as teorias da conspiração. E há teorias da conspiração sobre as *fake news*, e há *fake news* sobre as *fake news*. E esta ideia dos *false flag operations*, na qual um agente pode falsificar sinais de que uma intromissão num servidor informático foi feita por outro agente, faz parte de

um jogo no qual teremos de distinguir muito bem o que são *fake news*, o que são *fake news* sobre *fake news*, e qual é o efeito de ambas.

O facto de se criar desinformação tem um efeito político terrível, é a corrosão da legitimidade das instituições democráticas. Os crédulos, que creem em qualquer notícia falsa, são os que não creem nas notícias reais. A psicologia já determinou que, nas *fake news*, a forma de chegar ao usuário é reforçar os próprios preconceitos. Encapsular as ideias pessoais, alimentar as ideias pessoais e não deixar que outras ideias, que podem ser diferentes, ou que podem deter as ideias preconcebidas, tenham efeito.

E nas eleições, como foi dito por William Sweeney, o efeito é esse. O efeito não é trocar os números eleitorais de cinco *counties*, em cinco Estados americanos, que poderia ser decisivo para uma eleição presidencial nos Estados Unidos. O objetivo é criar caos. O objetivo é corroer a legitimidade, a crença e a fiabilidade dos sistemas eleitorais, com o qual é muito mais proveitoso, do ponto de vista político, criar esta deslegitimação do que tentar, por meios cibernéticos, trocar os números numa eleição. Porque se se consegue criar este preconceito, é muito mais duradouro do que o facto de uns números... E pode criar um tipo de eleitorado, encapsulado nos seus preconceitos, e que atua ao ditado, sem o saber, das ideias que lhe são continuamente alimentadas pelos criadores de *fake news*.

Esta tendência, muito perigosa nas democracias menos maduras, de acumular garantias técnicas sobre garantias técnicas, consegue ter um sistema muito mais vulnerável do que o sistema da Holanda, com o papel e a caneta. De tal maneira que as democracias maduras voltam aos sistemas antigos e fiáveis, e as democracias que têm necessidade de aparentar uma grande transparência criam uma multidão de garantias técnicas que vulnerabilizam muito mais os seus sistemas eleitorais. Porque, como dizia William, há muitas mais portas para entrar nesses sistemas.

Para finalizar, queria falar sobre uma ideia: qual é o efeito, na opinião pública, das *fake news* continuamente alimentadas pelas agências de criação das *fake news*? É a completa polarização da sociedade. Se as pessoas alimentam os seus preconceitos, se só leem nas suas redes sociais o que é similar ao que já pensaram disso, ou recebem por Twitter somente ou maioritariamente ideias que vêm confirmar as suas ideias, sem serem submetidas a nenhuma prova em contrário, sem serem submetidas a nenhuma crítica, o efeito é um completo encapsulamento do pensamento e uma completa polarização da sociedade.

Isto tem um efeito político muito importante – o pacto político torna-se mais difícil para os líderes, porque há sempre a sensação de que o pacto é uma traição das ideias. E uma ideologização extrema, uma polarização extrema e ideológica da opinião pública torna o pacto político muito mais difícil do que seria com uma opinião pública muitíssimo mais informada.

A meu ver, estas ameaças são ameaças técnicas e podem ser tratadas tecnicamente. O problema é quando as ameaças técnicas trazem este "oitavo passageiro", que é a desinformação, que cria consequências muito mais duradouras na opinião pública. É muito mais fácil desinstalar um programa malicioso do que um preconceito da cabeça das gentes. Isso não é tão fácil de descobrir e creio que é esse o efeito desse tipo de ideias.

O que fazer neste momento? Devo dizer que encontrei no trabalho de Alina Poliakova, que se chama "*Democratics of Defense Against Desinformation*", uma boa aproximação ao que pode ser feito pelos poderes públicos, pelas empresas privadas e pelos profissionais da informação. Creio que há que adaptar a forma de lutar contra as *fake news*, que há que proceder a um *critical thinking,* como já foi dito aqui pelo comissário, e há que criar regulamentação. O comissário fez uma abordagem muito interessante: há que proceder à regulamentação "*if there's no rapid progress*". Se os atores que disseminam a informação falsa não reagirem, há que proceder à regulamentação.

Para concluir, quero deixar uma ideia que foi introduzida na Constituição Espanhola. Na Constituição Espanhola, o direito de informação é o direito da informação "veraz". Não se traduz como "verdadeira". "Veraz" tem um elemento de fiabilidade, "*it's more truthful than true*". E creio que esta ideia jurídica de proteger a informação "veraz" pode ser uma forma de se abordar o fenómeno do ponto de vista de se proteger os direitos dos consumidores de informação e dos produtores de informação e dos media.

Muito obrigado pelo convite! Foi um grande prazer estar aqui com os senhores.

IGNACIO AMOR

Thank you, moderator. I would like to say thank you very much to the Portuguese colleagues of the Portuguese delegation to the OSCE Parliamentary Assembly and also warmly greet other colleagues I have seen for many years, Paulo Pisco, Jorge Lacão and other Members of this Assembly of the Republic.

I will try to speak Portuguese, not "Portunhol", and, frankly, if I have any trouble, Susana will be able to help get past any difficulties.

Well, I'm a general politician. I can't say that I'm an expert in cybersecurity or even fake news. My only specialist subject is constitutional law. Actually, Portuguese constitutional law, which I have studied for many years here at the Assembly of the Republic.

I believe that the waters have been muddied for several years and it wasn't easy to distinguish some phenomena from others. And there was a feeling that all this new field of politics that dealt with cybersecurity and fake news was part of the same atmosphere. I believe that today things are settling and the folder on my iPad I called "cyber and fake" a few years ago must now be split, because cyber threats are one thing and fake news is another.

What I do believe is that this new way of spreading information has to do with neo-irrationalism, a post-modern neo-irrationalism. So the idea of alternative facts is clearly a return to irrationalism, and we all know from history what type of societies these ideas lead to.

Fake news is a very old occurrence. I'm not going to discuss the propaganda of the Sumerian Kings, I'm talking about fake news, about news, so we can only talk about news since the invention of the press and, here in Lisbon, it is useful to remember that one of the events that gained the most visibility in all of Europe was the 1755 Lisbon earthquake. And the fact that the Lisbon earthquake created a type of literature, '*relações de sucessos*', which reached all of Europe, and that the earthquake became well known, and it was a universal news story, at least in the European world. Because the universality of a piece of news emerges from the risk we are examining. Today, there are no *relações de sucessos*. Today, there are 'viral stories' on social media. And the effect is the same.

I believe that we need to distinguish cyber threats from threats that use cyber instruments to spread throughout the world but are not themselves cyber threats. A piece of fake news is not a cyber threat. But, if the fake news story spreads over social media or other ways of reaching a universal audience, that has something to do with the cyber.

Spyware, malware, is a weapon, it's of a form of aggression and it must be treated as a threat. Cyber, then, can be just a vehicle through which a piece of fake news or disinformation reaches an extremely wide audience, by way of the viral effect and the techniques used to make any news story become viral. But the cyber, in its relationship with fake news, is purely instrumental. It is only the vehicle by which fake news and disinformation content reach extremely wide audiences in the world.

Classic hackers, when they were able to breach a system's security, left a simple signature. A signature to say: "I did it! I was here, I had access to this information". That was all. Now, the use of cyber threats and malware serves to extract or destroy information. Not always to hide information but to reveal information. The WikiLeaks events or events like the Panama Papers, or Mrs Clinton's correspondence, are real information. It is true information. But it had legal protection, which was breached. Therefore, these instruments are not always used to spread fake news. Sometimes they are used to spread real information and we have to bear in mind that side to this phenomenon.

So, what's the goal of disinformation, the goal of fake news? Is it simply disinformation? Disinformation has political effects, and that is the final goal of the agencies, the actors, who use this type of threat. I would like to talk about some of the political effects of disinformation.

In the past we had misinformed citizens because they didn't have information and they didn't have access to media. But now we have misinformed citizens because they have access to a lot of information that is not ranked, it is not filtered by professionals, it reaches the information user without a professional filter, without a code of ethics, in which a journalist, such as the colleague here with us today, has done his or her work to distinguish between what can and cannot be considered a news story.

And this excess of information produces noise, as happens in mathematics and happens in science, and I believe we have to determine, in this noise or excess of information, what the political goals are that, sometimes, are trying to be achieved.

Naive, advertising goals, of launching a lurid news story to get attention, to arouse curiosity and to make a page viable using advertising. This is a commercial formula that is not particularly dangerous from a political standpoint. And, it must be said (and I'm going to connect this to what our Russian colleague said), there are also conspiracy theories about conspiracy theories. And there are conspiracy theories about fake news and there is fake news about fake news. And this notion of false flag operations, where an agent may fake signs that an intrusion into a computer server was carried out by another agent, is part of a game in which we will have to make a clear distinction between what is fake news and what is fake news about fake news, and the effects of both.

The act of creating disinformation has a terrible political effect: corrosion of the legitimacy of democratic institutions. The gullible, who believe any fake news story, are those who do not believe real news. Psychology has already established that, in fake news, the way of reaching users is by strengthening prejudices themselves. Encapsulating personal ideas, feeding personal ideas and not letting other ideas, which may be different or may stop preconceived ideas, having an effect.

And that is the effect for elections, as said by William Sweeney. The effect is not switching electoral numbers in five counties, in five US states. Which may be decisive for a presidential election in the United States. The goal is to create chaos. The goal is to wear down the legitimacy and belief in and reliability of electoral systems, and it is much more advantageous, from a political point of view, to cause this delegitimisation than to try to switch numbers in an election using cyber channels. Because if you can create this prejudice, it is much more long-lasting than the fact that some numbers... And it can create a kind of electorate encapsulated in its preconceptions, which, without realising it, dances to the tune of the ideas it is constantly fed by the creators of fake news.

This very dangerous trend in less mature democracies, of accumulating technical guarantees after technical guarantees, is able to form a system that is much more vulnerable than Holland's system with paper and pen. In such a way that mature democracies are going back to old, reliable systems, and democracies that need to demonstrate great transparency set up a multitude of technical guarantees that make their electoral systems much more vulnerable. Because, as William was saying, there are many doors into these systems.

I wanted to talk about one idea, to finish: what is the effect on public opinion of the fake news continually provided by agencies for creating fake news? It is the total polarisation of society. If people feed their prejudices, if they only read things on their social networks that are similar to what they already thought about something, or if they only receive ideas on Twitter than confirm their ideas, without being exposed to any criticism or evidence otherwise, the effect is total encapsulation of thought and a complete polarisation of society.

This has a very significant political effect: that the political pact becomes more difficult for leaders. Because there's always the feeling that the pact is a betrayal of ideas. And extreme ideologising, extreme ideological polarisation of public opinion, makes the political pact much more difficult than it would be with more informed public opinion.

I believe that these threats are technical threats and can be dealt with technically. The problem is when technical threats carry an eighth passenger – disinformation – which causes much longer lasting consequences for public opinion. Because it is much easier to uninstall malware than it is to remove prejudice from people's minds. That's not that easy to find out and I believe that is the effect of those kinds of ideas.

What can be done right now? I should say that I found a good approach of what can be done by public powers, private companies and information professionals in Alina Polyakova's work *Democratic Defense Against Disinformation*. I believe that the way of fighting fake news must be adapted, that there must be critical thinking, as already mentioned by the Commissioner, and regulation has to be created. The Commissioner approached it in a very interesting way: there has to be regulation "if there's no rapid progress". If the actors that spread fake information do not react, regulation has to take place.

To finish, I would like to leave you with an idea that has been introduced into the Spanish Constitution. In the Spanish Constitution, the right to information is the right to "truthful" information. It isn't translated as "true". "Truthful" contains an element of reliability, it's more truthful than true. And I believe that this legal idea of protecting "truthful" information may be a way of approaching the phenomenon from the point of view of protecting information consumers' rights and the rights of information producers and the media.

Thank you very much for the invitation, it has been a great pleasure to be here with you.

SUSANA AMADOR

Muito obrigada. Este exercício não será fácil!

Queria, antes de mais, agradecer ao Anatoly Smirnov, ao Julian King e ao Ignacio Sánchez Amor pela riqueza das suas intervenções. Foi um painel, de facto, de imensa qualidade. Vou tentar fazer a síntese possível no tempo disponível. Quero também saudar o moderador, o João Fernando Ramos, e agradecer-lhe o estar aqui nesta primeira conferência de Lisboa.

Caros oradores, colegas e convidados, antes de mais um simples enquadramento inicial: as sociedades totalmente mergulhadas numa lógica de funcionamento em rede encontram-se dependentes do ciberespaço e isto foi transversal a todas as intervenções. Com a *internet of things*, com o desenvolvimento das redes de comunicações, com a globalização económica, com o conceito de cidades inteligentes, esta tendência tende a crescer, tal como os riscos daí resultantes. Às ameaças, muitos contrapõem a visão do ciberespaço como um espaço de liberdade e de oportunidade. Mas a História ensina-nos que, sem segurança, não há liberdade, o que, aliado à dimensão altamente disruptiva das novas ameaças, torna altamente pertinente e atual a problemática da cibersegurança e desta conferência.

Vivemos numa época dominada pelo virtual. Contudo, as ameaças que esta dimensão, aparentemente inócua, encerra são bem reais. De espaço reservado a uns quantos iniciados, o ciberespaço domina a vida de milhões de indivíduos, empresas, instituições governamentais. Tanto a nível interno como a nível internacional, são evidentes as capacidades de ativismos religiosos, criminosos ou terroristas para conduzir ações com impacto na segurança de estruturas vitais de informação, criando sérias ameaças à sobrevivência do Estado de direito democrático e ao espaço de liberdade, segurança e justiça.

A esse propósito, Sir Julian King, o comissário europeu para a União de Segurança, que ouvimos em vídeo, falou-nos do papel determinante da União Europeia na segurança, transparência e confiança do mundo cibernético. Sir Julian King destacou na sua mensagem a importância do tema desta conferência de Lisboa e sublinhou o facto de o nosso dia-a-dia estar rodeado de tecnologia, e de todas as tarefas da nossa rotina decorrerem no espaço da sociedade digital onde a Internet emerge de forma crescente. Considera que a Internet é uma miríade de oportunidades, mas que é também povoada por um lado negro e obscuro. Os ciberataques invadem o espaço individual e as infraestruturas das empresas e dos estados.

As motivações, tal como referiu Sir Julian King, são de natureza financeira, mas igualmente encerram motivos políticos e estratégicos, de que os últimos atos eleitorais dão conta. Os governos nacionais têm, sim, de estar na linha da frente desses combates. A cooperação europeia a esse nível é absolutamente central e indispensável. Sir Julian King deu-nos uma importante *overview* sobre as medidas e o pacote legislativo da União Europeia, que estão em curso e que visam fortalecer a resiliência da União Europeia neste domínio, reforçar a transparência, aumentar a confiança e segurança no espaço cibernético, considerando que as redes sociais, como o Facebook ou o Twitter, têm de ser mais colaborativas, mais transparentes, e devem prestar contas.

A fim de se reforçar ainda mais a cibersegurança da União, atribuiu-se um mandato sólido e permanente à Agência de Cibersegurança, à Agência da União Europeia para a Segurança das Redes e da Informação, e estabeleceu-se um quadro em matéria de certificação de cibersegurança.

Julian King disse-nos mesmo que é fundamental reforçar esta resiliência e a Agência da União Europeia para a Cibersegurança é também a palavra de ordem. Falou-nos da necessidade de reforçar a capacidade da União Europeia para a cibersegurança, e do interesse estratégico da União em assegurar que as ferramentas tecnológicas da cibersegurança sejam desenvolvidas para que a economia digital prospere, e, ao mesmo tempo, a nossa segurança seja protegida, bem como a sociedade e a democracia. Tal inclui, como ele referiu, a proteção do material informático e o *software* essenciais.

Referiu também o plano de ação para definir o modo como a Europa e os Estados Membros podem reagir rapidamente. Isso requer mais solidariedade, mais capacidade de ciberdefesa, cooperação internacional reforçada, e uma resposta eficaz do Direito Penal, com mais deteção e rastreabilidade na ação penal contra os cibercriminosos.

Mencionou, ainda, a necessidade de se investir nas competências e na investigação, e o combate eficaz ao terrorismo e às *fake news*. Disse-nos que a tolerância deve ser zero para conteúdos terroristas e outros, porque são ilegais, e têm de ser de imediato repudiados, e não são aceitáveis ou toleráveis. Não podemos, de modo nenhum, como disse, partilhar mensagens negativas.

Notou igualmente que é um trabalho nunca acabado, que é crucial para o futuro coletivo num mundo digital, onde a literacia digital tem de ser garantida à partida como forma de combate a campanhas empenhadas na construção de perceções coletivas

erradas. *Fake news* e manipulação em espaços digitais têm de ser obviamente evitados e controlados para a salvaguarda dos atos eleitorais. Um ambiente seguro e transparente é a meta da União Europeia.

Em seguida, Anatoly Smirnov fez na sua intervenção um conjunto de alertas.

Começou por referir que as guerras começam na cabeça das pessoas, e que alcançar a paz deve ser sempre, obviamente, um imperativo. O espaço da Internet é um espaço muito criativo, mas cada vez mais crítico e de confiança mútua entre os países. Fez referência ao ciberespaço cada vez mais complexo, e mais sofisticado, pelo que o cibercrime exige meios avançados por parte dos Estados. A prioridade deve ser, na opinião de Anatoly Smirnov, a adoção de um modelo universal para reforçar o ciberespaço. O conceito de ciberespaço deve ser tratado nos diversos domínios em todo o seu largo espectro.

Referiu-nos que a OSCE tem de ter um papel mais atuante neste domínio e que é fundamental que o trabalho internacional de combate às ameaças no campo da segurança internacional da informação possam, no fundo, inverter este aumento da desconfiança mútua. Falou-nos do escândalo que ocorreu em março de 2018, com a interferência nas campanhas eleitorais de muitos países do mundo, pela empresa Cambridge Analytica, que não fala sobre a "mão de Moscovo" mas sim sobre a "mão de Londres".

Para Anatoly Smirnov, é fundamental que a eficácia das atividades da OSCE possa aumentar, no sentido de garantir, no uso das TIC, uma maior resiliência e segurança e que nem sempre se tem conseguido por razões organizacionais. Entende que atualmente a organização funciona apenas numa plataforma para discussão de questões relacionadas com os problemas das TIC e que é fundamental que a OSCE possa, no fundo, ressuscitar, garantindo maior segurança no uso das TIC, e otimizar o seu trabalho nesta faixa.

Referiu-nos a importância do plano de ação do Conselho de Ministros dos Negócios Estrangeiros de Hamburgo, em 2016, e acredita que esse plano não perdeu relevância e que deve servir de fundamento para discussões sobre a revisão e simplificação dos processos de negociação na OSCE.

Por último, Anatoly Smirnov diz-nos que a quarta revolução industrial irá criar novas e mais profundas ameaças, e que a Rússia tem uma experiência bastante rica para o estabelecimento e a proposta de partilha neste domínio. Reanimar a OSCE e a Assembleia Parlamentar dando mais força e mais vida para que possamos trabalhar de forma una e conectada, criando grupos de especialistas, que nos habilitem a trabalhar mais e com melhor eficácia no ciberespaço.

Passo agora à intervenção de William Sweeney, ele que é o presidente e diretor-geral da Fundação para os Sistemas Eleitorais.

William Sweeney diz-nos que devemos cada vez mais estar empenhados na proteção dos órgãos eleitorais. Este é o trabalho desta Fundação que tem mais de 30 anos na proteção. Um trabalho que se confunde com a própria vida de William Sweeney, que desde sempre esteve ligado a estas questões ao longo da sua vida.

A confiança é um vetor fundamental para a segurança dos atos eleitorais e é um bem que tem de ser preservado. Falou-nos da necessidade de estarmos atentos, ao assalto aos valores democráticos no ciberespaço, que é cada vez mais crítico, e constitui uma ameaça à democracia que não podemos aceitar.

William Sweeney diz-nos que vivemos num mundo em mutação e aceleração digital, e que todas as tecnologias estão em ligação e estão juntas, e que isso também torna o sistema mais vulnerável. Há, assim, inúmeros desafios aos atores locais e políticos para que, no fundo, possam eliminar suspeitas mútuas e que os sistemas políticos possam assegurar a missão da defesa da eficácia dos mesmos e do Estado de direito, para que não ocorram manipulações, deturpações ou fraudes que ponham em causa esses mesmos sistemas políticos dos Estados. O Twitter, o Google e outras plataformas interferem de forma direta e constroem potenciais disrupções, às quais temos de estar atentos.

Chamou-nos a atenção para a necessidade da integridade da informação, para a privacidade do cidadão eleitor, que é vital, e, se não garantirmos esta integridade de informação e esta privacidade no eleitor, colocamos em causa o processo democrático, geramos caos e insegurança junto dos eleitores, e por isso é fundamental todo o conjunto de medidas que possam detetar as intrusões. As eleições presidenciais nos Estados Unidos foram uma importante lição, da qual temos, obviamente, de tirar as devidas ilações, protegendo o sistema, tornando-o mais resiliente, mas nunca deixando de pensar que é fundamental garantir este espaço de liberdade, segurança e privacidade dos cidadãos.

Ignacio Sánchez Amor, especialista em Direito Constitucional e presidente da nossa Comissão de Democracia na OSCE, fala-nos na sua intervenção, também muito interessante, que a área da cibersegurança não pode ter águas turvas. Ela tem de ter uma destrinça de conceitos e criar racionalidade no sistema.

As *fake news*, tal como ele referiu, e também tema recorrente no debate que fizemos, são algo já antigo, não são uma realidade nova. Mas a desinformação e as notícias falsas encontraram no ciberespaço um canal e um veículo com um vasto auditório.

Os *hackers* clássicos, do antigamente, apenas deixavam a sua simples assinatura, como nos disse Sánchez Amor. Hoje, os impactos são muito mais corrosivos, como a *Wikileaks*, os *Panama Papers* e os *e-mails* de Hillary Clinton bem demonstraram, são informação real e cuja proteção foi perigosamente quebrada.

Os objetivos das *fake news* são objetivos, infelizmente, de desinformação. Encerram em si motivações políticas e estratégicas perigosas que conduzem à manipulação. Tal como nos referiu Sánchez Amor, ontem os cidadãos não tinham acesso pleno à informação, e isso era um défice, um défice de democracia, não poderem ter esse acesso. Mas hoje têm acesso a informação que não é segura, não é fidedigna, e também não deixa de ser um défice de democracia, dos sistemas, que essa

acessibilidade e clareza de informação não exista nessa selva, que é uma selva, de vários ruídos. Uma selva digital na qual os cidadãos muitas vezes se perdem. E quando se perdem os cidadãos, perde-se também a democracia. O que fazer?, diz-nos Sánchez Amor. Temos de lutar contra as "fake news" e temos de fazer regulação, regulação, regulação, tal como nos desafia também a União Europeia.

No debate, as questões estiveram todas muito ligadas à necessidade de prevenir. A prevenção é sempre um investimento. A necessidade da democracia e da sua vulnerabilidade, e de as TIC poderem encontrar, no fundo, soluções para uma maior resiliência, a novidade não é a utilização desta ferramenta, a novidade é o que se faz com a manipulação da informação, com a pulverização da tecnologia. Por isso temos de encontrar o devido equilíbrio de que nos falava Ascenso Simões, não podemos criar uma fortaleza que pode ser perversa nem criar limites à comunicação e à informação.

A tecnologia que invadiu o nosso quotidiano precisa também de partir de uma consciência individual das ameaças por parte dos cidadãos, reforçando os processos eleitorais.

Em conclusão, caros oradores e convidados, as novas tecnologias criam inúmeras oportunidades, mas colocam também desafios que atravessam os fundamentos da própria democracia nas sociedades modernas. A velocidade crescente a que a informação circula e a sua disseminação nas redes sociais levantam questões muito sérias sobre a necessidade de se moderar a informação não fidedigna, em particular quando esta circula sob forma concertada e massificada ao serviço de campanhas empenhadas na construção de perceções coletivas erradas e com potencial de corrosão da coesão e do próprio bem-estar das sociedades.

A atuação do Estado terá de passar naturalmente pela promoção da literacia digital, de modo a proteger as pessoas contra a manipulação em espaços digitais, mas também por uma atuação intransigente na proteção de dados dos utilizadores, das plataformas, e pelo robustecimento da capacidade para limitar a atuação de canais que ajam de forma articulada com o objetivo de colocar em causa os pilares da nossa vida coletiva.

A OSCE pode e deve reforçar a sua intervenção como plataforma de diálogo, criando *confidence building measures*, porque temos de visar na OSCE, todos os dias, uma democracia mais resiliente, que deve sobretudo defender valores preferentes, como os da liberdade e da justiça. A OSCE quer fazer ouvir a sua voz e "se não for agora, quando será"?

Muito obrigada.

SUSANA AMADOR

Thank you. This won't be an easy exercise.

I would first like to thank Anatoly Smirnov, Julian King and Ignacio Sánchez Amor for the richness of their speeches. It was, in fact, a very high-quality panel. I'll try to make what summary I can in the time available. I would also like to express my greetings to the moderator, João Fernando Ramos, and thank him for being here at this first Lisbon conference.

Dear speakers, colleagues and attendees, I would first like to give a brief initial overview: societies completely immersed in a rationale of network operations are dependent on cyberspace, and this was present in all the speeches. With the internet of things and the development of communication networks, with the globalisation of the economy, with the concept of smart cities, this trend shows a tendency to grow, as do the risks resulting from them. Many counter the idea of threats with a view of cyberspace as a space of freedom and opportunity. But history has taught us that without security, there is no freedom, which,

along with the highly disruptive side to new threats, makes the current issue of cyberspace and this conference extremely relevant.

We are living in an age dominated by the virtual. Nonetheless, the threats that this apparently innocuous dimension involves are very real. From an area restricted to a few initiates, cyberspace now dominates the lives of millions of individuals, companies, government institutions. At domestic and international levels, the capacity of religious, criminal or terrorist activisms to carry out acts with an impact on the security of vital information structures is clear, which creates serious threats to the survival of democratic states based on the rule of law and the space of freedom, security and justice.

On this matter, Sir Julian King, European Commissioner for the Security Union, who we heard via video, has told us of the European Union's determining role in security, transparency and confidence in the cyber world. In his message, Sir Julian King emphasised the importance of the theme of this Lisbon conference and underlined the fact that our day-to-day lives are surrounded by technology, and that all the tasks in our routines happen in the space of the digital society, where the internet is increasingly present. He believes that the internet represents myriad opportunities but that it is also inhabited by a dark, shadowy side. Cyberattacks invade individual space and company and state infrastructures.

The motivations behind them, just as Sir Julian King mentioned, are financial, but there are also political and strategic motivations, of which these latest elections are a sign. National governments must, then, be at front line of such struggles. European cooperation is absolutely central and indispensable in this regard. Sir Julian King gave us an important overview of the European Union's measures and legislative package, which are ongoing and aim to strengthen the European Union's resilience in this field, strengthen transparency, enhance confidence and security in cyberspace, considering that social networks, such as Facebook or Twitter, must be more cooperative, more transparent and accountable.

In order to further reinforce the Union's cybersecurity, a sturdy, permanent mandate has been assigned to the Cybersecurity Agency, to the European Union Agency for Network and Information Security, and a framework on cybersecurity certification has been established.

Julian King also told us that reinforcing this resilience is fundamental and that the European Union Agency for Cybersecurity is the watchword too. He spoke to us about the need to reinforce the European Union's cybersecurity capacity and about the Union's strategic interest in providing technological cybersecurity tools that are developed so that the digital economy can prosper and, at the same time, our security, as well as society and democracy are protected. This includes, as he mentioned, the protection of IT equipment and essential software.

He also told us of the action plan to set the way in which Europe and the Member States can react quickly. This requires greater solidarity, greater capacity for cyber defence, reinforced international cooperation, and an effective response from criminal law, with better detection, traceability in penal action against cybercriminals.

He also spoke of the need to invest in skills and research and the effective combat against terrorism and fake news. He further told us that there should be zero tolerance for terrorist and other content, because it is illegal; it must be immediately rejected and is not acceptable or tolerable. We cannot in any way, as he said, share negative messages. He also mentioned that it is a job that is never finished, which is crucial for the collective future in a digital world, where digital literacy must be guaranteed from the beginning as a way to fight against campaigns committed to building incorrect collective perceptions. Fake news and manipulation in digital spaces must of course be prevented and controlled to safeguard elections. A secure, transparent environment is the European Union's target.

Afterwards, Anatoly Smirnov made several warnings in his speech.

He began by mentioning that wars begin in people's minds, and that achieving peace should always, naturally, be an imperative. The space of the internet is a highly creative one, but it is increasingly critical and involves mutual trust among countries. He mentioned the increasingly complex and more sophisticated nature of cyberspace, which means that cybercrime requires more advanced resources from states. The priority should be, in Anatoly Smirnov's opinion, to adopt a universal model for strengthening cyberspace. The concept of cyberspace should be dealt with in different fields covering all of its broad spectrum.

He also mentioned to us that the OSCE must have an active role in this area and that it is fundamental for international work to combat threats in the international information security field can, in fact, reverse this growth in mutual mistrust. He also spoke to us about the scandal in March 2018, with interference in election campaigns in several of the world's countries by the company Cambridge Analytica, which speaks not to the "hand of Moscow" but to the "hand of London".

For Anatoly Smirnov, it is fundamental for the OSCE's actions to become more effective, in order to guarantee greater resilience and security when using ICTs, and that this has not always been achieved due to organisational reasons. He understands that the organisation currently functions only on a discussion plat-form for issues related to ICT problems and that it is fundamental for the OSCE to, in fact, be able to revive, ensuring greater security in ICT use and optimise its work in this area.

He also mentioned the importance of the action plan of the Council of Ministers of Foreign Affairs in Hamburg in 2016, and believes that this plan has become no less relevant and should serve as the foundation for discussions on the review and simplification of negotiation processes in the OSCE.

Finally, Anatoly Smirnov told us that the Fourth Industrial Revolution will create new, deeper threats and that Russia has quite extensive experience to establish and propose sharing in this field. Reviving the OSCE and the Parliamentary Assembly, giving greater strength and more life so we can work in a united, connected way, setting up groups of specialists that allow us to work more and in a more effective way in cyberspace.

I now move on to the speech by William Sweeney, President and CEO of the International Foundation for Electoral Systems.

William Sweeney tells us that we have to be increasingly committed to protecting electoral bodies. This is the work carried out by the Foundation, which has more than 30 years' work on protection. This work is blurred with William Sweeney's own life, which has always been connected to these issues throughout his life.

Trust is a fundamental factor for the security of elections and it is an asset that must be preserved. He discussed the need for us to be alert to attacks on democratic values in cyberspace, which is increasingly critical and is a threat to democracy that we cannot allow.

William Sweeney said that we are living in a changing, digitally accelerated world and that all technologies are connected and are together, and that this also makes the system more vulnerable. There are therefore numerous challenges for local and political players so that they can actually eradicate mutual suspicions and political systems can ensure the mission of defending their effectiveness, and states based on the rule of law, so there are no manipulations, distortions or fraud that may call those state political systems into question. Twitter, Google and other platforms directly interfere with and build potential disruptions, and we must be alert to these.

He drew our attention to the need for integrity of information, the privacy of voters, which is vital, and if we cannot guarantee the integrity of information and the privacy of voters, we put the democratic process at risk, we produce chaos and insecurity among voters. And that is why all measures that can detect intrusions are fundamental, and the presidential elections in the United States were an important lesson, from which we must all learn, of course, protecting the system, making it more resilient, while never failing to believe that it is fundamental to provide this space of freedom, security and privacy to citizens.

Ignacio Sánchez Amor, specialist in constitutional law and Chair of the OSCE's Democracy Committee, told us in his also highly interesting speech that the cybersecurity field cannot be one of murky waters. It must have its concepts untangled and create rationality in the system.

Fake news, as he mentioned and which came up repeatedly in our debate, is an old phenomenon, not a new situation. But disinformation and fake news have found a channel in cyberspace and a vehicle with a huge audience.

The classic hackers of the past left behind their simple signature, as Sánchez Amor told us. Now, today, the impacts are much more corrosive, as WikiLeaks, the Panama Papers and Hillary Clinton's emails clearly demonstrate, this is real information, the protection of which was dangerously breached.

Fake news' goals are, unfortunately, the goals of disinformation. It involves political, strategic motivations that are dangerous, leading to manipulation. As Sánchez Amor told us, citizens did not have full access to information before, and that was a deficit, a deficit of democracy, the fact that they could not have access to it. But today they have access to information that is not safe, it is not reliable, and this remains a deficit of democracy, of systems; the accessibility and clarity of information does not exist in that jungle, and it is a jungle, filled with different noises. A digital jungle in which citizens often get lost. And when citizens become lost, democracy is also lost. "What can we do?" Sánchez Amor asks us. We have to fight against fake news and we have to make regulation, regulation, regulation, just as the European Union also challenges us to do.

In the debate, the questions were all particularly connected to the need for prevention. Prevention is always an investment. The need for democracy and its vulnerability, and for ICTs to be able to find, in fact, solutions for greater resilience. What

is new is not the use made of this tool, what is new is what is done with the manipulation of information, with the spread of technology, and that is why we have to find the right balance, which Ascenso Simões was telling us about, we cannot create a fort, which may be perverse, or impose limits on communication and information.

The technology that has invaded our everyday lives also needs to come from individual awareness by citizens, strengthening electoral processes.

In conclusion, dear speakers and attendees, new technologies create numerous opportunities but also pose challenges that span the foundations of democracy itself in modern societies. The growing speed at which information circulates and its spread on social networks raises very serious questions about the need to moderate unreliable information, in particular when this information is concertedly and broadly circulated in favour of campaigns committed to creating incorrect collective perceptions that have the potential to corrode the cohesion and well-being of societies.

States' actions will naturally need to involve promoting digital literacy in order to protect people against manipulation in digital spaces, but also acting unwaveringly in protecting the data of users, platforms, by strengthening the capacity to restrict the actions of channels operating in collaboration with the aim of calling into question the pillars of our collective life.

The OSCE can and should further its intervention as a platform for dialogue by creating confidence-building measures because, at the OSCE, we have to strive every day for a more resilient democracy, one that above all defends priority values, such as freedom and justice. The OSCE wishes to make its voice heard and "if not now, when?"

Thank you very much.

Da esquerda para a direita: Luís Antunes, Nilza de Sena, Rosa Ostrauskaite e Pedro Veiga
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04892/2018
From left to right: Luís Antunes, Nilza de Sena, Rosa Ostrauskaite and Pedro Veiga
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04892/2018

DESAFIOS TECNOLÓGICOS DO CIBERESPAÇO
TECHNOLOGICAL CHALLENGES OF CYBERSPACE

LUÍS ANTUNES

Muito obrigado e bom dia a todos.

Queria começar por agradecer o convite às senhoras deputadas Isabel Santos e Nilza de Sena. É um prazer estar aqui e é um prazer estar aqui a falar sobre este assunto. Diria, como tenho dito em algumas palestras que tenho feito em que tenho falado sobre a tensão existente entre o desenvolvimento tecnológico e um direito fundamental que é a privacidade, tal como aconteceu com o Cambridge Analytica – finalmente é público. Para nós, tecnológicos, finalmente é público, e percetível ao cidadão comum.

E queria começar mesmo por aí. Nós, tecnológicos, e durante os próximos dois minutos, quando falar de "nós", estou a falar de tecnológicos, e a fazer *mea culpa*. Nós, tecnológicos, fizemos desenvolver a tecnologia, como nunca foi feito no passado, e através dela a própria sociedade.

A Internet começou em 1964, e a melhor forma de explicar o enorme desenvolvimento tecnológico das últimas décadas é através dos meios digitais de armazenar dados. Lembro-me de, na faculdade, em 1989, armazenar dados em cartões perfurados, em fitas, disquetes de 5 e 1/4 , e a tecnologia evoluiu até que hoje nós guardamos dados, e guardamos um grande volume de dados, num sítio que fisicamente desconhecemos, *i.e.*, na *cloud*.

Ao fazermos desenvolver a tecnologia, demos por garantido um conjunto de direitos, liberdades e garantias existentes no mundo físico, e que demoraram séculos a serem conquistados e que, de repente, estão a ser postos em causa neste novo mundo que mistura o físico com o digital.

Existem muitas pessoas a desafiar aquilo que os nossos antepassados tão arduamente conquistaram, ou seja, proativamente, é o cidadão que prescinde de um conjunto de direitos fundamentais, tais como a privacidade, fazendo o *post* de vários factos da sua intimidade, sem que nunca lhe tenha sido dada a capacidade de controlar a sua exposição neste mundo digital.

O problema é que nós não resolvemos um conjunto de tecnologias que garantam a transposição dos direitos fundamentais, liberdades e garantias para o mundo digital. Nunca fomos desafiados, nós, tecnológicos, nós universitários, a desenvolver esse conjunto mecanismos no mundo digital.

Se a tecnologia nos trouxe até aqui, na minha opinião é a tecnologia que deve resolver este problema em que estamos hoje em dia. E, por isso, uma das primeiras perguntas que me tinham feito é esta – se as futuras tendências podem afetar ou alterar o comportamento dos seres humanos – e eu acho que sim.

Eu não gostava de deixar aos meus filhos uma sociedade em que eles vivessem vigiados 24 horas por dia, sete dias por semana. Acho que isso condicionava claramente a liberdade deles. Assim, é a nossa responsabilidade, é a responsabilidade da minha geração, deixar uma sociedade livre aos nossos filhos e aos nossos descendentes. E está na hora de o fazermos.

Quais são os desafios, atuais e futuros?

A questão é que, no desenvolvimento tecnológico, e na construção da Internet, a questão da segurança nunca foi um fator.

A Internet foi desenhada por militares e, portanto, a característica fundamental é a resiliência a falhas. E agora começamos a falar em princípios como segurança por desenho, como privacidade por desenho, e se o tivéssemos feito há quarenta, cinquenta anos, estaríamos claramente muito mais à frente do que aquilo que estamos hoje.

Portanto, enfrentamos dois desafios: tentarmos resolver tudo aquilo que nós herdamos, até hoje, e que tem imensos problemas de segurança; e o segundo desafio é evitar que isto volte a acontecer, ou seja, de que forma é que nós conseguimos evitar que isto volte a acontecer. Regulatória, sim ou não, consciência social, formação, mas temos de ter uma estratégia para o futuro.

Deixo aqui um conjunto de desafios que tenho começado a dar aos meus estudantes na universidade e o mais simples é o seguinte: há quatro anos, a Fundação para a Ciência e a Tecnologia convidou-me para fazer uma palestra e a palestra era sobre a Internet das coisas e o grande volume de dados que a Internet das coisas gera.

Decidi começar a contar, há quatro anos, o número de aparelhos que eu tinha em casa ligados à Internet. Tenho dois filhos, por isso, podem imaginar: consolas e *tablets*, e quando cheguei aos dez, decidi parar. Parar. Dez aparelhos ligados à Internet e ainda faltavam alguns. E comecei a achar que, por exemplo, eu tinha de ter a capacidade de controlar a exposição da minha família no mundo digital. Ou seja, todos os dados que estes aparelhos estão a gerar sobre mim e sobre a minha família, eu tenho de ser capaz de controlar essa exposição. E não só eu.

Neste momento, não conseguimos controlar essa exposição. Se o nosso frigorífico tiver uma ligação à Internet, pode estar a dizer que nós não temos ovos. Isto é o mínimo que podemos estar a fazer. É claro que se a nossa televisão for uma *smart* TV e estiver ligada à Internet, alguém pode estar a ver o que estamos a fazer na sala e ouvir o que estamos a falar na sala.

Estamos agora a desenvolver uma tese de doutoramento com um estudante, e que está com algum sucesso, que é desenhar uma camada de *software* que eu possa pôr no meu *router* de casa (o *router* é o sítio por onde passa todo o tráfego da minha casa) e eu consiga barrar tudo aquilo que são estes dados. Barrar e controlar. Depois podemos fazer uma coisa: podemos continuar a valorizar estes dados e podemos dizer às pessoas: "olhe, agora pode fazer um leilão e pode tentar vender os seus dados". Mas é uma decisão individual. É a pessoa que tem a capacidade de dizer "eu quero" ou "eu não quero" fazer isto.

O pior que nos pode acontecer e que mina a confiança nestes sistemas é isto estar a acontecer sem que as pessoas saibam que isto se está a passar.

Um outro desafio que me tinham lançado é a construção de parcerias e cooperação. Creio que é inevitável. E a situação em que estamos hoje em dia, e eu penso que de tarde vamos falar sobre isto quando falarmos sobre questões de cibersoberania, nós estamos numa luta muito desigual, nós, Europa, relativamente aos Estados Unidos e relativamente à China.

Na Europa somos 27 países, cada um a tentar garantir a sua cibersoberania, e, consequentemente, temos de ter 27 vezes a capacidade para o fazer, quando em outras latitudes nós temos países que são um continente e estão a lutar pela cibersoberania enquanto continente.

Assim, vamos ter de encontrar esse equilíbrio na Europa e na parte do "ciber" já não são só países; nós temos grandes grupos tecnológicos, com uma capacidade no ciberespaço muito superior à capacidade que a maioria dos países tem. Logo, começamos a ter novos atores neste ecossistema do digital que conseguem claramente influenciar a nossa liberdade, que conseguem claramente influenciar o nosso desenvolvimento enquanto sociedade.

Temos de enfrentar este facto, parar, refletir e pensar no modelo de sociedade que queremos deixar para os nossos filhos.

Nesta questão das parcerias, e agora falando um bocadinho para o espaço europeu, penso que é inevitável a colaboração e vamos ter de confiar. O problema da confiança é que só temos de confiar quando perdemos o controlo. Eu só preciso de

confiar num sistema de votação eletrónica quando deixei de o controlar. Porque enquanto eu o controlar, eu não preciso de confiar: eu controlo.

Por conseguinte, neste espaço europeu a 27 países, em que a cooperação vai ter de existir, a confiança é muito importante, mas temos de ter mecanismos residuais, por muito residuais que sejam, para cada um destes países sentir que controla alguma coisa. E tecnicamente é possível. Sentir que têm algo, um *software*, em cima da solução europeia, para sentir que conseguem garantir alguma cibersoberania. De outra forma, eu acho que vai ser muito difícil termos os 27 países alinhados. E, principalmente, quando temos países da NATO a escutarem outros líderes de países da NATO, é muito difícil construir a confiança quando sabemos que isto está a acontecer diariamente.

Por fim, o último desafio: será que as capacidades ofensivas no ciberespaço conseguem garantir a subsistência dos mais frágeis? A grande vantagem do ciberespaço é que não existem os mais frágeis.

Portugal, como país muito pequenino, pode ter um conjunto de pessoas que são brilhantes no ciberespaço, e temos o exemplo disso: um aluno da Faculdade de Ciências do Porto, a que pertenço, foi considerado o *hacker* do momento a nível global. Temos estas capacidades, estamos a formar estas capacidades, temos é de ter uma estratégia de reter estas pessoas. Não devíamos estar a formar estas pessoas para elas irem trabalhar para um país terceiro, para elas irem trabalhar para um desses atores tecnológicos, nós temos de ter uma estratégia nacional.

Quando vimos há bocado o comissário europeu a falar na formação, é disto que estamos a falar, capacitar o país. E, no ciberespaço, quando nós falamos em capacitar, é técnico, sim, temos de desenvolver tecnologias, mas é capacitar com recursos humanos, é muito importante nós termos recursos humanos altamente especializados que consigam fazer isto.

Vou terminar só com uma *disclosure*: quando aterrei em Lisboa, recebi a notificação da publicação de um artigo científico de um aluno de doutoramento português, um aluno de doutoramento do Porto, que conseguiu atacar um protocolo *multiparty computation* que põe em causa o *blockchain*. Havíamos comunicado previamente a um conjunto de parceiros nacionais de órgãos de soberania que tínhamos conseguido fazer isto – acho que é importante passar este conhecimento para estes órgãos – mas nós temos essa capacidade. Ou seja, quando falamos em desequilíbrio, esta é uma daquelas áreas em que o conhecimento é um grande valor. O conhecimento representa muito valor e nós devemos ter uma estratégia de retenção deste conhecimento.

LUÍS ANTUNES*

Thank you, good morning everyone.

I would like to begin by thanking the Honourable Members Isabel Santos and Nilza de Sena for the invitation. It is a pleasure to be here and a pleasure to be here to talk about this subject. I would say, as I have said at several talks I have given in which I've talked about the tension between technological development and the fundamental right of privacy, as arose with Cambridge Analytica, which is finally public. For us, technologists, it's finally public and can be seen by ordinary citizens.

And I would like to start with that. We, technologists, and for the next two minutes, when I say "we", I mean technologists, and I would like to issue a "mea culpa". We, technologists, pushed forward the development of technology in a way that had never been done in the past, and through technology, we pushed forward the development of society.

The internet began in 1964, and the best way to illustrate the enormous technological development of the last decades is with digital means of data storage. I remember being at university in 1989 and storing data on punched cards, on tapes, on 5 1/4-inch disks, and technology has evolved so today we save data, and we save a large amount of data, in a place that we have never physically seen: the cloud.

By making this technological development, we have taken for granted a set of rights, freedoms and guarantees that exist in the physical world and took centuries to be attained and, suddenly, are called into question in this new world that mixes the physical with the digital.

There are many people challenging what our ancestors fought so hard to achieve, in other words, it is citizens who proactively forego a range of fundamental rights, such as privacy, by posting several facts about their intimate lives, without ever being given the ability to control their exposure in this digital world.

The problem is that we have not resolved a range of technologies that guarantee the transposition of those rights, freedoms and guarantees into the digital world. We have never been challenged – we, technologists, we, academics – to develop that range of mechanisms in the digital world.

If it was technology that brought us here, then in my opinion it is technology that should solve this problem we find ourselves up against today. And so one of the first questions I was asked is this one, about future trends, whether they can affect or alter human beings' behaviour, and I believe they can.

I would not like to leave my children a society in which they live under surveillance 24 hours a day, seven days a week. I think that would clearly restrict their freedom. It is therefore our responsibility, and my generation's responsibility, to leave behind a free society for our children and our descendants. And now is the time for us to do it.

What are the current and future challenges? The question is that, during the development of technology, during the building of the internet, the issue of security was never a factor.

The internet was designed by the military and so its main feature is resilience to faults. And now we are starting to talk about principles like security by design, privacy by design, and if we had done so forty, fifty years ago, we would clearly be a long way ahead of where we are today.

So we are faced with two challenges: firstly, trying to resolve what we have inherited to the present day, which has many security problems; and secondly, the challenge is to avoid this happening again, in other words, how we can manage to avoid this happening again. Regulations, yes or no, social awareness, training, but we have to have a strategy for the future.

I would like to leave you a set of challenges that I have started to give my students at university, and the most simple one is the following: four years ago, the Foundation for Science and Technology invited me to give a talk, and the talk was about the internet of things and the huge amount of data that the internet of things generates.

I decided to start counting, four years ago, the number of devices I had at home that were connected to the internet. I have two children, so you can imagine, consoles, tablets, and when I got to ten, I decided to stop. Stop. Ten devices connected to the internet, and that wasn't all of them. I began to find that, for example, I needed to have the ability to control my family's exposure in the digital world. In other words, all the data that these devices produce about me and my family, I have to be able to control that exposure. And not just me.

At the moment, we are unable to control that exposure. If our fridge has an internet connection, it could be telling someone that we don't have eggs. This is the least we can do. And of course, if our television is a smart TV connected to the internet, someone may be watching what we're doing in the living room or listening to what we're saying in the living room.

We are now working on a PhD thesis with one student, who is having some success designing a layer of software that I can put on my router at home (the router is the point all internet traffic in my house passes through) and I can block all this data. Block and control it. Then we can do something: we can keep valuing this data and we can tell people: "listen, now you can hold an auction and you can try and sell your data." But it's an individual's decision. And the person has the power to say I want or I don't want to do this.

The worst thing that could happen to us, and what undermines confidence in these systems, is that this is happening without people knowing it's happening.

Another challenge I've been set is to build partnerships and cooperation. I think that's inevitable. And the situation we're in today, and I think we're going to talk about that this afternoon when we discuss cyber sovereignty issues, we're in a highly unequal battle – us, in Europe – compared with the United States and China.

There are 27 countries in Europe, each one trying to ensure its cyber sovereignty, so, let's see: we have to have 27 times the capacity to do so, when in other areas we have countries that are entire continents and are struggling for cyber sovereignty as a continent.

We are therefore going to have to find that balance in Europe, and the "cyber" part is no longer just formed of countries; we have large technology groups, with capacity in cyberspace that goes far beyond the capacity most countries have. And so we are beginning to see new players in this digital ecosystem that are clearly able to influence our freedom, that are clearly able to influence our development as a society.

We clearly need to face up to this situation, we need to stop, reflect and think about the model of society we want to leave behind for our children.

In this question of partnerships, and now I'm talking a bit about the European space, I think cooperation is inevitable, completely inevitable, and we are going to have to trust. The problem of trust is that we only have to trust when we lose control. I only need to trust in an electronic voting system when I stop controlling it. Because while I control it, I don't need to trust: I have control.

So, in this European space of 27 countries, where cooperation will need to take place, trust is very important, but we have to have residual mechanisms, however residual they may be, so that each of these countries feels it controls something. And technically it's possible. Feeling that they have something, some software, on top of the European solution, to feel they are able to guarantee some cyber sovereignty. Otherwise, I think it will be very difficult for us to get 27 countries lined up. And, mostly, when we have NATO countries listening in on other leaders of NATO countries, it's very difficult to build confidence when we know that this is happening on a daily basis.

Finally, the last challenge is: are offensive capacities in cyberspace able to guarantee the survival of the weakest? The great advantage of cyberspace is that there are no weakest.

Portugal, as a small country, may have a group of people who are brilliant in cyberspace, and we have an example of this: a student at the Faculty of Science in Porto, to which I belong, was considered the hacker of the moment in the world. We have these abilities, we are training these abilities, we must have a strategy for retaining these people. We shouldn't be training these people so they go and work for a third country, for them to go and work for one of those technology players, we need to have a national strategy.

When we saw the European Commissioner discussing training a while ago, that is what we're talking about, empowering the country. And in cyberspace, when we talk about empowering, it is technical, yes, we need to develop technologies, but we need to empower human resources, it is much more important for us to have highly specialised human resources that are able to do this.

I'm going to end today with a disclosure: when I landed in Lisbon, I received notification of the publication of a scientific article by a Portuguese PhD student, a PhD student in Porto, who managed to attack a multiparty computation protocol that puts blockchain at risk. We had previously notified a range of national partners of bodies that exercise sovereign power that we had managed to do this – I think it is important to pass this knowledge on to such bodies – but we have that capability. In other words, when we talk about imbalance, this is one of the areas where knowledge is highly valuable. Knowledge represents a great deal of value and we have to have a strategy for retaining that knowledge.

---

* Editor's note: the translation of this presentation has not been reviewed by the autor. It is published after editorial review.

PEDRO VEIGA

Começo por cumprimentar as senhoras deputadas e os senhores deputados, especialmente a nossa moderadora e relatora, o senhor presidente da Assembleia Parlamentar da OSCE, as senhoras embaixadoras e embaixadores aqui presentes, as autoridades civis, militares, nacionais e estrangeiras, minhas senhoras e meus senhores.

Em nome do Centro Nacional de Cibersegurança, queria agradecer o convite para estar aqui presente. Face às limitações de tempo, e porque eu tenho um vídeo para apresentar que demora cerca de quatro minutos, vou passar os meus *slides* muito rapidamente e espero conseguir poder passar a mensagem, que depois poderá ser reforçada na parte do debate.

Assistimos, nos últimos 30 anos, à chamada convergência tecnológica. Basicamente houve três indústrias (a informática, as telecomunicações e os media), que começaram a convergir para o digital. Mas isto teve uma aceleração espantosa nos últimos dez anos, é aquilo que se chama a "transformação digital".

Todos os nossos conteúdos passaram a estar sob a forma binária, de zeros e uns. Portugal não esteve alheio a esta problemática e na sequência da aprovação da estratégia europeia de cibersegurança, em 2013, passados dois anos, foi aprovada a estratégia nacional.

Esta estratégia está organizada segundo seis eixos e eu queria chamar a atenção para o eixo que está mais à direita, que é o eixo da cooperação. É uma área em que a cooperação é fundamental, porque os problemas são transfronteiriços, e a identificação de ataques, o tratamento de ataques, mas também vários desafios existentes e que já foram falados na sessão anterior, passam muito pela cooperação.

Há um outro aspeto da nossa estratégia para o qual queria chamar a atenção. A nossa estratégia orienta-se em três grandes áreas. Não são as únicas, mas são aquelas que eu queria aqui realçar – a cibersegurança, que trata de nos prepararmos para sermos resilientes e sobrevivermos no mundo digital; a área da ciberdefesa, que trata da proteção das nossas organizações ligadas à defesa, e que também é extremamente importante (o vídeo que vou mostrar dá ênfase a isso); e, depois, os crimes cometidos no ciberespaço também merecem uma grande atenção, e, portanto, a terceira área que eu queria salientar é o cibercrime. Claro que, como a caixa de baixo do lado direito chama a atenção, há o ciberterrorismo e hoje em dia o prefixo "ciber" aparece à frente de muitas outras coisas, espelhando exatamente o resultado da transformação digital.

Uma pergunta que me fazem frequentemente, mas que creio que nesta audiência já todos terão pensado, é o que é o ciberespaço? O termo ciberespaço foi criado na década de 1980 num romance, e é descrito como o mundo virtual dos computadores e blocos de informação. Naturalmente inclui informação, sistemas e redes de comunicação, mas o mais importante são as pessoas. E estas pessoas precisam de ser capacitadas para os desafios que existem neste novo mundo digital.

Na sessão anterior também falou sobre o Facebook, os cuidados que as pessoas devem ter no Facebook, e isso passa por uma capacitação das pessoas. As pessoas são o elemento crucial em que devemos intervir. E é essa uma das preocupações do Centro e das políticas nacionais e europeias nessa área. Aliás, o comissário Julian King também falou da importância das pessoas.

A nossa equipa tem uma dependência direta do primeiro-ministro, se bem que com competências delegadas na senhora ministra da Presidência e da Modernização Administrativa. Devido à grande transversalidade da problemática da cibersegurança, foi criado, em agosto passado, um Conselho Superior de Segurança do Ciberespaço, que faz a governação da estratégia e neste momento estamos a fazer a revisão da estratégia. Esperamos, ao longo deste mês de maio, ter aprovada a nossa versão da estratégia 2.0. que trata de problemas que até há pouco tempo não eram tão gritantes, como a proteção não só de infraestruturas mas também dos serviços essenciais.

O alerta para os serviços essenciais também resultou da diretiva de segurança das redes e dos sistemas de informação, que formalmente tem de ser transposta até à data de amanhã, como o comissário Julian King referiu e que está na Assembleia da República neste momento.

Quanto às dimensões da cibersegurança, e estou a preparar-me para passar para o vídeo, muitas vezes as pessoas pensam que é só uma componente técnica e tecnológica. Não é. Tem que ver com a política das organizações, ao nível mais alto, ao Conselho de Direção, em inglês, *Board of Directors*, tem de haver uma perceção da importância dos problemas de cibersegurança – que podem ter implicações legais e económicas enormes – empresas que podem desaparecer ou ter sérias perdas financeiras devido ao problema de a cibersegurança não ter sido devidamente tomado em conta. Depois, na última linha, podemos ver que o elemento humano, as pessoas, as componentes psicológicas, o cibercrime hoje em dia tem novas dimensões, aquilo que se costuma chamar a "engenharia social" para manipular as pessoas obriga a enormes cuidados.

Nós, no Centro de Cibersegurança, temos uma pequena intervenção ao nível da OSCE. Eu próprio, e algumas pessoas da minha equipa, temos participado em algumas reuniões da OSCE, nomeadamente na implementação das *confidence building measures*. Nós operamos a linha de passagem de informação sobre ciberincidentes para depois serem passados para a dimensão política e militar, caso seja adequado.

Contúdo, isto mostra a importância do eixo da cooperação. É muito importante que, se existirem incidentes, eles sejam notificados de uma maneira rigorosa, muito eficiente, para evitar mal-entendidos e uma escalada de problemas.

Para terminar, eu ia pedir a ajuda de uma pessoa, de um português que todos conhecem, até mesmo os nossos participantes estrangeiros, mas devo fazer um pequeno enquadramento. Há cerca de dois meses, a esta pessoa, que é engenheiro de formação base, foi atribuído o grau de *Doutor Honoris Causa* aqui em Portugal, na minha universidade, a Universidade de Lisboa.

Num discurso de uma hora e pouco, durante quatro minutos esta pessoa falou dos desafios do ciberespaço. E deu ênfase a algo que já foi falado e que eu queria reforçar, que são os ataques às nossas infraestruturas críticas, nomeadamente, ataques a redes de energia elétrica, a portos, a redes de abastecimento de água, ao sistema financeiro. É preciso muita atenção, do ponto de vista da cibersegurança, tornar resilientes essas empresas e organizações.

A atenção também deve incidir na Internet das coisas. O meu colega de mesa já referiu que a Internet das coisas está a penetrar no nosso dia-a-dia, desde pulseiras para monitorar a atividade física, e que, se não houver cuidado, pode causar intrusões graves à nossa privacidade. Vão entrar nos nossos lares, em muitos casos já entraram sob a forma de *smart TV*, vão aparecer como assistentes pessoais, etc., e é preciso imenso cuidado.

Apresentado o vídeo com uma pequena nota: como numa cerimónia esta pessoa é homenageada como engenheiro, dá-se uma ênfase grande ao papel dos engenheiros no ciberespaço. "Por outro lado, quando olhamos para a engenharia, para a ciência e para a tecnologia, encontramo-nos perante um dos outros mais importantes domínios, em que são maiores as expectativas e ..." Durante o teste funcionou, hoje de manhã. São palavras do Eng.º António Guterres que, como é sabido, é secretário-geral das Nações Unidas, mas também é engenheiro, e ele fala, com a autoridade que tem e com o conhecimento que tem dos problemas do ciberespaço, sobre os ataques e a falta de legislação internacional que trate dos desafios do ciberespaço (é esse de baixo).

"Por outro lado, quando olhamos para a engenharia, para a ciência e para a tecnologia, encontramo-nos perante um dos outros domínios mais importantes, em que são maiores as expectativas e as potencialidades para melhorar a vida da Humanidade e para projetar enormes crescimentos das economias, e, ao mesmo tempo, onde se apresentam alguns dos dilemas éticos mais dramáticos em relação ao futuro do nosso planeta. Estou a referir-me agora às tecnologias de informação e comunicação e, em particular, ao chamado ciberespaço. Hoje existem, de forma mais ou menos escondida, episódios de ciberguerra no mundo entre Estados. E, pior do que isso, não há nenhum esquema regulatório em relação a esse tipo de guerra. Não está claro como as convenções de Genebra, o direito geral humanitário, se aplicam à ciberguerra. E eu estou absolutamente convencido de que, ao contrário do passado, das batalhas da Primeira e da Segunda Guerra Mundiais, que começavam sempre com grandes barragens de artilharia, depois das Guerras do Golfo, em que tudo começava sempre com maciços bombardeamentos aéreos, ou com mísseis de cruzeiro, estou absolutamente convencido de que a próxima guerra entre dois Estados será antecedida por um maciço ciberataque, com o objetivo de destruir as capacidades militares, sobretudo de comando, controlo e comunicação do inimigo, e de paralisar as suas próprias infraestruturas básicas, como, por exemplo, as redes elétricas. E, no entanto, sabendo nós isto, encontramo-nos completamente despojados dos mecanismos regulatórios básicos para garantir que esse novo tipo de guerra obedeça àquele progressivo desenvolvimento de leis da guerra para garantir um carácter mais humano àquilo que é sempre uma tragédia de proporções extraordinariamente dramáticas. Mas não é apenas a ciberguerra; hoje, todos têm como preocupação essencial nas atividades económicas, nas atividades sociais, na vida política, na vida governativa, os problemas da cibersegurança, e aí vemos engenheiros procurando proteger-nos, a todos nós, com ações extremamente meritórias, e vemos engenheiros a serem instrumentos de utilização das potencialidades destas tecnologias, quer por organizações de natureza criminosa, quer mesmo por organizações de natureza terrorista, na chamada *deep web*, ou na chamada *dark web*. E esta é uma questão central que nos deve preocupar a todos, porque, uma vez mais, as formas de regulação tradicionais, quer feitas pelos Estados ou por convenções internacionais, dificilmente se podem aplicar aí, e em relação à chamada Internet das coisas, ou *internet of things*, que no fundo tem a ver com todos os conteúdos, ou todas as operações, que decorrem a nível da rede, nós verificamos que estamos hoje desprovidos de quaisquer mecanismos regulatórios ou sequer de protocolos que definam algumas regras básicas para garantir que a Internet seja um instrumento, fundamentalmente, ao serviço do bem."

Senhora deputada Nilza de Sena, terminei. Peço desculpa por ter ocupado mais de dez minutos no total.

PEDRO VEIGA

I would like to begin by greeting the Honourable Members, particularly our moderator and rapporteur, the President of the OSCE Parliamentary Assembly, the ambassadors present here, the civil, military, national and foreign authorities, ladies and gentlemen.

On behalf of the National Cybersecurity Centre, I would like to thank you for the invitation to be here. In view of the time restraints, and because I have a video to show you that lasts roughly four minutes, I'll show my slides very quickly and I hope I can transmit the message, which can be enhanced in the debate afterwards.

We have seen the so-called technological convergence over the last 30 years. There have essentially been three industries (IT, telecommunications and media) that have begun to converge towards the digital. But this has seen a staggering acceleration in the last ten years, what is called the "digital transformation".

Our content has all shifted to a binary format of zeroes and ones. Portugal has been no exception to this, and following approval of the European cybersecurity strategy in 2013, the domestic strategy was passed two years later.

This strategy is organised around six pillars, and I would like to draw attention to the pillar on the right, which deals with cooperation. This is a field in which cooperation is fundamental because the problems cross borders, and identifying attacks, dealing with attacks, but also challenges of different types that exist, and this was already discussed in the previous session, greatly involve cooperation.

There is another aspect of our strategy to which I would like to draw your attention. Our strategy is guided by three main areas. They are not the only ones, but they are the ones I'd like to highlight here. They are: cybersecurity, which involves preparing ourselves to be resilient and to survive in the digital world; then we have the area of cyber defence, which deals with the protection of our organisations connected to defence, which is also extremely important (and the video that I am going to play emphasises this); and, after that, crimes committed in cyberspace also deserve extensive attention and so the third area I'd like to highlight is cybercrime. Of course, as the box underneath the right-hand side highlights, then we have cyberterrorism, and today the prefix "cyber" appears before many other things, reflecting precisely the result of the digital transformation.

One question that I'm often asked, but that I think everyone in this audience will have already pondered, is: what is cyberspace? The term cyberspace was coined in the 1980s in a novel, and it is described as the virtual world of computers, blocks of information; of course it includes communication networks, systems and information, but people are the most important thing. And people need to be empowered for the challenges that exist in this new digital world.

Facebook has already been mentioned in the previous session, the care that people should take on Facebook, and this involves empowering people. People are the crucial element in which we should intervene. And this is one of the concerns of the Centre and national and European policy in this area. In fact, Commissioner Julian King also mentioned the importance of people.

Our team is directly dependent on the Prime Minister, although with competences delegated to the Minister of the Presidency and Administrative Modernisation. Due to the cross-cutting nature of the cyberspace issue, a High Council for the Security of Cyberspace was set up in August last year, which governs strategy, and at the moment we are revising the strategy, specifically, we hope that in May we will have approved our version of strategy 2.0, which deals with problems that until recently were not glaring, such as protection, not only of infrastructure but also of essential services.

And the warning for essential services also came out of the directive on security of network and information systems, which must formally be transposed by tomorrow, as Commissioner Julian King also pointed out, and which is at the Assembly of the Republic of the moment.

The dimensions of cybersecurity, and I'm getting ready to put the video on, often people think that it's just a technical and technological component. That is not the case. It has to do with organisations' policies, at the highest level, in the Board of Directors, there must be an understanding of the importance of cybersecurity problems, which may have huge legal and economic implications, companies that may disappear or suffer serious financial losses due to the problem of cybersecurity not being duly taken into account. And then, later, at the bottom line, we can see the human element, people, psychological components, cybercrime today has new dimensions, something which is usually called "social engineering" to manipulate people, which create the need for extreme care.

At the Cybersecurity Centre, we have a small intervention at OSCE level. I myself and some people on my team have taken part in some OSCE meetings, specifically the implementation of confidence-building measures, we operate

the line for passing on information about cyberincidents so it can be passed to the political or military spheres, as appropriate.

But this shows the importance of the cooperation pillar. It is very important, if there are incidents, that they are communicated thoroughly, very efficiently, to avoid misunderstandings and problems escalating.

And, to finish, I'm going to ask for someone's help, a Portuguese person, who you all know, all of you, even our participants from abroad, but I should provide some background: around two months ago, this person, whose background training is in engineering, was awarded a doctorate honoris causa in Portugal, at my university, the University of Lisbon.

During a speech that lasted just over an hour, there are four minutes during which this person spoke about the challenges of cyberspace. And he emphasises something that has already been spoken about and that I would like to highlight, which are attacks on our critical infrastructures, specifically, there have been attacks on electrical grids, water supply networks, the financial system, we need to pay careful attention, from a cybersecurity point of view, and make these companies and organisations resilient.

Attention also needs to be paid to the internet of things. My fellow panel member has already said that the internet of things is penetrating our day-to-day lives, from wristbands that monitor physical activity and that, if we do not take care, may be serious invasions of our privacy, but they are going to come into our homes, and they often have already come into them in the form of smart TVs, and they will emerge as personal assistants, etc., and great care is needed.

So, I'll leave the video with a short note: this person, as this was at a ceremony where he was being honoured as an engineer, places great emphasis on the role of engineers in cyberspace.

"On the other hand, when we look to engineering, to science and to technology, we find ourselves standing before one of the other great fields, where the expectations are greater and ..." It worked this morning, during the test. So, it's Mr António Guterres, who, as you know is the Secretary-General of the United Nations, but also an engineer, and he speaks, with the authority he enjoys and the knowledge he has of the problems of cyberspace, about attacks, the lack of international legislation that deals with the challenges of cyberspace... (it's the bottom one).

"On the other hand, when we look to engineering, to science and to technology, we find ourselves standing before one of the other great fields, where the expectations are greater and the potential to improve humankind's quality of life and produce enormous growth in economies and, at the same, where there are some of the most dramatic ethical dilemmas regarding the future of our planet. I am talking, of course, about information and communication technologies and, in particular, what is known as cyberspace. Today there are, in a more or less concealed way, episodes of cyberwarfare between states in the world. And, worse than that, there is no regulatory scheme regarding that type of war. It's not clear how the Geneva conventions, general humanitarian law, apply to cyberwarfare. And I am fully convinced that, unlike in the past, the battles of the First and Second World Wars, which always began with great barrages of artillery, after the Golf Wars, where everything always began with mass air bombings, or with cruise missiles, I am fully convinced that the next war between two states will be preceded by a mass attack, a cyberattack, a mass cyberattack, with the aim of destroying the military capabilities, above all command, control, communication, of the enemy and paralysing its basic infrastructures, such as electricity grids, for example. And although we know this, we are completely deprived of basic regulatory mechanisms to ensure that this new type of warfare adheres to the progressive development of the laws of warfare to ensure a more humane character for something that is always a tragedy of extraordinarily dramatic proportions. But it is not only cyberwarfare; today, everyone holds the problems of cybersecurity as key concerns in economic activities, social activities, in political life, in governmental life, and we find engineers there who are trying to protect us, all of us, with extremely praiseworthy actions, we find engineers being instruments for using the potential of these technologies by both criminal organisations and even by terrorist organisations on the deep web or dark web. And this is a central question that should concern us all because, once again, the traditional forms of regulation, whether drawn up by states or by international conventions, are hard to apply, and in relation to the internet of things, which really deals with all content, or all operations, that take place at network level, we find that we are lacking any regulatory mechanisms or even protocols that define some basic rules to ensure the internet is an instrument that fundamentally serves good."

Honourable Member Nilza de Sena, I have finished. I apologise for having taken more than ten minutes, overall.

RASA OSTRAUSKAITE

Excelências
Senhoras e senhores
Caros colegas

Permitam-me agradecer aos nossos anfitriões portugueses desta reunião da AP o convite para proferir uma intervenção nesta sessão sobre os desafios tecnológicos do ciberespaço.

Nesta intervenção, gostaria de sublinhar como, na resposta aos desafios tecnológicos do ciberespaço – sobretudo no desafio da atribuição –, os Estados participantes da OSCE adotaram o conjunto mais abrangente de medidas geradoras de confiança do mundo, com o objetivo de reduzirem os riscos de conflitos resultantes da utilização de cibercapacidades.

É evidente que as tecnologias de informação e comunicação criaram oportunidades de emancipação económica, envolvimento político e mobilidade social sem precedentes. No entanto, é igualmente verdade que produziram novos perigos e vulnerabilidades que podem ser explorados por utilizações mal-intencionadas das TIC.

Ao nível de alcance e efeitos, estes ataques podem ter um impacto verdadeiramente global e acarretam potenciais escaladas que vão além dos efeitos imediatos.

O maior desafio continua a ser a atribuição técnica, jurídica e política. Os ciberataques são difíceis de prever, custa seguir-lhes o rasto, são eminentemente negáveis e os autores podem ser estatais ou não, muitos ou poucos, podem agir de forma direta ou indireta e podem estar localizados em qualquer lugar.

Na pior das hipóteses, um ciberincidente de pequena dimensão, mas mal atribuído, pode desencadear uma escalada em espiral com grande impacto nas relações bilaterais ou multilaterais, podendo até criar um conflito que envolve meios cinéticos.

Não quer isto dizer que os Estados não estejam já a fazer uso de cibercapacidades:

- Em 2015, um ciberataque complexo contra as empresas de eletricidade na Ucrânia ocidental deixou mais de 200 000 pessoas sem energia durante até seis horas.
- No ano passado, o ataque de *ransomware NotPetya* provocou perdas financeiras na ordem de 900 milhões de dólares. Entre os lesados, estava o serviço nacional de saúde britânico, que se viu obrigado a recusar tratamento a doentes com cirurgias agendadas.
- Mais recentemente, os EUA e o Reino Unido descobriram grandes ataques contra *routers*, alguns no seio de infraestruturas críticas, que permitiam que o autor controlasse, modificasse e impedisse o tráfego da Internet.

Tais episódios realçam a necessidade de os Estados lidarem com as seguintes questões: como atribuir os ciberataques sem quaisquer dúvidas; como promover a confiança e o comportamento responsável dos Estados no ciberespaço; e como o direito internacional se aplica a ciberincidentes que envolvam dois ou mais Estados.

Esta questão está a tornar-se cada vez mais importante, dado que o âmbito dos ataques está a alargar-se rapidamente, com o desenvolvimento da inteligência artificial, a Internet das coisas e a computação em nuvem.

No entanto, responder a estas questões continua a ser um desafio. O mais recente Grupo de Peritos Governamentais da ONU[1] que trabalha nestas matérias não conseguiu chegar a um consenso. Na verdade, muitos peritos consideraram que as posições nacionais estão a ficar mais rígidas e que a desconfiança entre Estados sobre questões de ciber-segurança é muito grande.

Temos, pois, de redobrar os nossos esforços para prosseguir a implementação das medidas já existentes, de modo a reduzir os riscos de conflito que resultam da utilização das TIC. Um aspeto parece ser evidente: o uso das TIC pelos Estados vai intensificar-se e o risco de conflito também.

A OSCE tem, desde 2012, um papel vanguardista na redução de riscos de conflito, tendo o Conselho Permanente da OSCE criado, naquele ano, um grupo de trabalho informal encarregue de elaborar umas Medidas Geradoras de Confiança (MGC) para reduzir o risco de conflito que advém do uso das TIC.

O resultado é um conjunto de 16 MGC concebidas para reforçar a transparência entre Estados e melhorar a previsibilidade, através da redução do risco de perceções erróneas e erros de cálculo associados com o uso das TIC pelos Estados ou os seus procuradores.

As MGC são de natureza prática e, deste modo, reconciliam as diferenças ideológicas entre Membros participantes com pontos de vista diferentes no que toca às políticas cibernéticas internacionais. Constituem uma variedade de medidas de transparência e de cooperação que são agrupadas em três núcleos.

No primeiro, surgem as MGC que permitem que os Estados interpretem a posição de outro Estado e definam linhas vermelhas de comportamento inaceitável no uso das TIC. As MGC desta categoria incentivam os Estados a partilharem, de forma proativa, informações sobre estratégias nacionais em matéria de cibernética, doutrina militar relevante, bem como cibercapacidades nacionais.

Estas informações podem tornar o ciberespaço um pouco mais previsível, na medida em que fica mais fácil determinar a origem de um ciberataque com mais confiança. Mais concretamente, permitem que os Estados cheguem a conclusões mais fiáveis sobre o autor de um ataque, sobre o tipo de contra-medidas a tomar, e decidam se desejam ou não relacionar-se com outro Estado a nível diplomático.

O segundo núcleo de MGC define um mecanismo de comunicação de crises para realizar consultas sobre ciberincidentes capazes de criar conflitos, com o objetivo de acalmar eventuais tensões.

Neste sentido, os Membros participantes da OSCE escolheram pontos centrais com a autoridade de encetar a "ciberdiplomacia". Os esforços também se centram na criação de vias de comunicação seguras[2] e em procedimentos para levantar preocupações sobre um determinado ciberincidente importante.

A terceira categoria de MGC promove a preparação nacional, a devida diligência e a cooperação entre Membros participantes para enfrentarem os desafios cibernéticos e das TIC. Estas medidas de cooperação servem para criar confiança através do envolvimento prático sobre questões de interesse comum ou que preocupam os Membros participantes da OSCE. É notável que um ponto central destes esforços seja a proteção de infraestruturas críticas apoiadas nas TIC, que é um tema sensível para qualquer governo.

Em suma, as MGC formam um quadro que permite que os Estados evitem escaladas através de relações entre decisores antes que uma situação se descontrole. Permitem também que os Estados operacionalizem quadros normativos, jurídicos e de princípios aplicáveis *online* e *offline* para criar as condições para estes quadros funcionarem na prática.

Ao nível da implementação das MGC, os Membros participantes estão a progredir bem, embora não sejamos imunes ao ambiente geral das relações internacionais.

Em síntese: a implementação precisa de vontade política, de liderança e, sobretudo, de capacidades e consciência! As MGC têm de estar preparadas para enfrentar a próxima crise provocada pelas TIC, seja qual for a altura em que surge.

Da nossa parte, a OSCE e o seu Departamento de Ameaças Transnacionais continuarão a prestar apoio aos Membros participantes e aos seus decisores na operacionalização das MGC. Estamos disponíveis para trabalhar convosco para enfrentar estes novos desafios, promover a ciberestabilidade e construir um "bairro cibernético" seguro.

Muito obrigado pela atenção.

---

[1] Designação completa: Grupo de Peritos Governamentais das Nações Unidas para o Desenvolvimento no Domínio da Informação e das Telecomunicações no Contexto de Segurança Internacional.

[2] Ver FSC.DEC/5/17 sobre o USO DA REDE DE COMUNICAÇÕES DA OSCE NO APOIO DA IMPLEMENTAÇÃO DAS DECISÕES DO CONSELHO PERMANENTE N.º 1039, N.º 1106 E N.º 1202.

RASA OSTRAUSKAITE

Excellences
Ladies and gentlemen
Colleagues

Allow me to thank our Portuguese hosts of this PA meeting for inviting me to address this session on technological challenges of cyberspace.

In my intervention I would like to highlight how in response to technological challenges of cyberspace – chiefly the attribution challenge – OSCE participating States adopted the world's most comprehensive set of confidence building measures to reduce the risks of conflict stemming from the use of cyber capabilities.

Clearly, Information and Communication Technologies have created opportunities for unprecedented economic empowerment, political engagement and social mobility. However, it is equally true that it has brought to life new dangers and vulnerabilities that can be exploited through malicious uses of ICTs.

In terms of reach and effects, such attacks can have an impact on a truly global scale, and carry the potential for escalation that exceeds their immediate effects.

The biggest challenge remains technical, legal and political attribution. Cyber-attacks are hard to predict, challenging to trace, eminently deniable, with perpetrators that can be state actors or not, many or few, acting directly or indirectly, and stationed anywhere.

In the worst case scenario, a misattributed, limited cyber incident can trigger an escalation spiral that can significantly impact on bilateral or multilateral relations, or even lead to a conflict with kinetic means.

This is not to say that Sates are not already making use of cyber capabilities:

- In, 2015 a complex cyber attack against electric utilities in Western Ukraine deprived over 200,000 people of power for up to six hours.
- Last year the global NotPetya ransomware attack led to financial losses in the region of $900 million. Victims included the UK National Health Service which had to turn away patients scheduled for operations.
- Most recently the US and UK discovered large scale attacks on routers including of critical infrastructure allowing the perpetrator to monitor, modify and deny internet traffic.

Such incidents underscore the necessity for States to address questions over how to attribute cyber-attacks beyond reasonable doubt, how to promote confidence and responsible state behaviour in cyberspace, and how international law applies to cyber incidents involving two or more States.

This is becoming increasingly important as the attack surface is rapidly growing with the development of artificial intelligence, the internet of things and cloud computing.

Finding answers to these questions, however, remains challenging. The latest UN Group of Governmental Experts[1] working on these issues could not reach consensus. In fact, many experts felt that national positions are hardening, and levels of distrust between States related to questions of cyber security are sky high!

We therefore need to re-double our efforts in pursuing the implementation of already existing measures to reduce the risks of conflicts stemming from the use of ICTs. One thing appears to be evident: the use of ICTs by States will proliferate and so will the risk for conflict.

The OSCE has played a pioneering role in reducing the risks of such conflict since 2012, when the OSCE Permanent Council created an Informal Working Group tasked to develop Confidence Building Measures, or CBMs, to reduce the risks of conflict stemming from the use of ICTs.

The result is 16 CBMs designed to enhance interstate transparency and predictability by reducing the risk of misperception and miscalculation associated with the use of ICTs by States or proxies.

The CBMs are practical, thereby bridging ideological differences between non-like-minded participating States when it comes to international cyber policy. They constitute a mix of transparency and co-operative measures, loosely structured into three clusters.

First, CBMs which allow States to "read" another State's posturing in cyberspace and to draw red lines of unacceptable behaviour in the use of ICTs. CBMs which fall under this category encourage participating States to proactively share information on national cyber strategies, pertinent military doctrines but also national cyber capabilities.

Such information can make cyberspace that little bit more predictable in that it becomes easier to determine the origin of a cyber-attack with more certainty. Specifically, it allows States to make a better judgement call who may be behind the attack, what sort of counter measures to take, and whether to engage with another State on the diplomatic level.

The second cluster of CBMs establishes a crisis communication mechanism to hold consultations over cyber incidents that could escalate into conflict with the goal of defusing potential tensions.

To this end, OSCE participating States nominated focal points with the authority to engage in "cyber diplomacy". Efforts also focus on establishing secure communication channels[2] and procedures on how to raise concerns over a significant cyber incident.

The third category of CBMs promotes national preparedness, due diligence and co-operation between participating States to address cyber/ICT challenges. These co-operative measures serve to build trust through practical engagement on issues that are of shared interest or concern to OSCE participating States. What's remarkable is that a key focus of such efforts is the protection of ICT-enabled critical infrastructures, a very sensitive topic for any government.

All in all the CBMs offer a framework that allows States to prevent escalation through the engagement of decision makers before things get out of control. They also allow States to operationalise principles, norms and legal frameworks applicable offline and online and create the conditions for such frameworks to function in practice.

In terms of implementation of the CBMs, participating States are making good progress though we are of course not immune to the general atmosphere in international relations.

The bottom line is: implementation needs political will, leadership, vision and, most importantly, capacities and awareness! The CBMs need to be ready to tackle the next major ICT-induced crisis, whenever it may come.

For our part, the OSCE and its Transnational Threats Department will continue to assist participating States and their decision makers in operationalizing the CBMs. We stand ready to work with you on tackling these new challenges, promoting cyber stability and building a secure "cyber neighborhood".

Thank you for your attention.

---

[1] Full title: UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.
[2] See FSC.DEC/5/17 on the USE OF THE OSCE COMMUNICATIONS NETWORK TO SUPPORT IMPLEMENTATION OF PERMANENT COUNCIL DECISIONS No. 1039, No. 1106 AND No. 1202

NILZA DE SENA

Bom dia a todos!

Dando continuidade aos nossos trabalhos, quero, em primeiro lugar, saudar todos os oradores pelas suas intervenções e tentar o exercício não exaustivo de resumir as suas alocuções neste painel, sem lhes retirar qualidade.

Gostaria de começar por dizer que todos temos consciência de que vivemos na era da digitalização, em que a informação tecnológica se transformou numa ferramenta indispensável nos nossos dias. Usá-la já não é hoje uma questão de escolha, é uma necessidade absoluta, imperativa mesmo, para cada um de nós. Provavelmente, se cada um pensar nas alturas em que se esquece do telemóvel em casa, tem a sensação de que falta qualquer coisa. Este é um exemplo da transformação do modo como vivemos e como programamos as nossas vidas.

A rapidez das mudanças está a transformar radicalmente as nossas sociedades. São mudanças inquestionáveis que colocam sistemáticos desafios de adaptação, ao mesmo tempo que geram alguma dependência.

No passado ano 2000, quando as Nações Unidas aprovaram os desafios de desenvolvimento do milénio, tínhamos a era digital no início e, de acordo com os relatórios do Banco Mundial, existiam apenas um bilião de telemóveis e cerca de 400 milhões de utilizadores de Internet.

Hoje, um dia típico na Internet comporta cerca de 2,3 biliões de gigas de tráfego na *web*, 207 biliões de emails enviados, 36 milhões de compras na Amazon ou 4,2 biliões de buscas no Google! Isto dá-nos a ideia da transformação e quão rápida ela foi. No entanto, isto não é um fim em si mesmo. É apenas o desafio, ou seja, o começo daquilo que temos para o futuro. E isso foi muito patente nas intervenções que aqui ouvimos.

Os temas abordados pelos nossos oradores mostram que, se queremos alcançar mais impacto, e também mais segurança, é fundamental que os diferentes Estados da OSCE possam implementar medidas de literacia digital e políticas que ajudem na adaptação às novas realidades tecnológicas.

Estamos perante uma revolução que vai comportar a inteligência artificial de que falou Rasa Ostrauskaite, mas também a nanotecnologia, os veículos não tripulados, a especialização tecnológica, as impressões 3D, a Biologia sintética, entre outras alterações que hoje vão mudar completamente o paradigma vivido até agora e introduzir grande impacto no mercado de trabalho. Estas alterações irão colocar desafios no campo laboral e, como disse o Professor Luís Antunes e bem, exigir dos Estados mudanças na forma como se programa tudo.

A necessidade de uma segurança quase "por desenho", e aqui sou textual, a "privacidade por desenho", a necessidade de reinventarmos a forma como educamos os nossos filhos serão determinantes, mas também as necessidades de nos protegermos dentro das nossas casas. Esta realidade, até hoje ultrapassada de forma simples com trancas na porta, passará a implicar outros requisitos de maior sofisticação e exigência.

Luís Antunes referiu existirem países da NATO a espiar outros países da NATO, mas espiar o que faz o vizinho do lado também será acessível e implicará um mecanismo de proteção da privacidade de cada família.

O futuro trará muitas exigências de proteção individual e, por isso, Pedro Veiga trouxe-nos a componente humana, porque, aliás, tudo começa aí. Sem ela provavelmente nem sequer estaríamos a falar aqui de tecnologia, pois ela partiu de nós! Essa dimensão, como explicou, deve estar patente ao nível da cibersegurança, do cibercrime, da ciberdefesa e deve implicar, por princípio, um investimento absolutamente concreto sob pena de ficarmos vulneráveis.

Pessoas individuais, famílias, jovens, que são utilizadores frequentes e regulares de Internet são vulneráveis na medida em que nem sempre se compreende os perigos da exposição em rede. Chegar a um qualquer hotel do mundo, por exemplo, e pedir a senha do wifi, expõe-nos, tornando-nos frágeis! Mas o paradoxo é que já ninguém quer estar de fora da Internet e sem acesso a dados.

Entre as necessidades hoje tidas como importantes, está a ligação em rede, com o uso da Internet! Quando Maslow pensou na pirâmide das necessidades básicas, não imaginou eventualmente esta possibilidade, mas hoje ela é completamente premente na vida de cada um de nós e representa também uma urgente necessidade de regulamentação.

Aludindo ao vídeo que aqui foi exibido, com uma mensagem de António Guterres, ficou patente essa exigência a propósito da ciberguerra, mas também de outras dimensões mais restritas. Nesse domínio, Rasa Ostrauskaite referiu igualmente a imprevisibilidade de ataques cibernéticos e, forçosamente, o espírito de cooperação e a necessidade de trabalho conjunto entre os diferentes Estados. Mesmo assumindo que cada Estado tenha a sua soberania própria para poder resolver ou implementar uma estratégia, ganha escala o objetivo da cooperação numa área complexa e sensível.

Procurei focar as mensagens essenciais expressas anteriormente e quero repetir uma mensagem que aqui ouvimos: o principal é haver visão política e vontade política! Sem elas nenhum Estado consegue fazer aquilo que aqui está a ser preconizado. Sem elas, porventura estaremos sempre mais expostos, vulneráveis e indefesos à medida dos avanços da tecnologia.

Portanto, terminava com este desafio: levar esta mensagem de consciência para fora desta sala, para que a sociedade desinformada esteja mais consciente das vulnerabilidades da tecnologia, quando já sente as suas vantagens de forma evidente.

Muito obrigada e mais uma vez agradeço aos nossos oradores por participarem nestas primeiras conferências de Lisboa.

Obrigada a todos.

NILZA DE SENA

Good morning everyone!

Continuing our proceedings, I would first like to thank all the speakers for their words and I shall try to give a non-exhaustive summary of their input on this panel, without taking away any quality.

I should like to begin by saying that we are all aware that we live in the age of digitalisation, where technological information has been transformed into an indispensable tool for our days. Using it is now no longer a matter of choice, it is an absolute necessity, even imperative, for every one of us. If you all think about when you forget your mobile phone and leave it at home, it probably seems like something is missing. And this is an example of the transformation in the way we live and how we programme our lives.

The speed of the changes is radically transforming our societies. They are unquestionable changes that pose systematic adaptation challenges, and at the same time generate some dependence.

In the year 2000, when the United Nations approved the millennium development goals, we were at the start of the digital age and there were, according to World Bank reports, only one billion mobile phones and roughly 400 million internet users.

Now, a typical day on the internet involves roughly 2.3 billion gigabytes of web traffic, 207 billion emails sent, 36 million purchases on Amazon or 4.2 billion Google searches! This gives us an idea of the transformation and how fast it has been. But this is not an end in itself. This is only a challenge, i.e. the beginning of something we have for the future. And that has been very clear in the speeches we have heard here.

The topics discussed by our speakers show that if we want to create a bigger impact, and also achieve more security, it is fundamental for the different states in the OSCE to be able to implement digital literacy measures and policies that aid adaptation to new technological realities. We are facing a revolution that will involve the artificial intelligence of which Rasa Ostrauskaite spoke, but also nanotechnology, unmanned vehicles, technological specialisation, 3D printing, synthetic biology, among other changes which are today going to completely change the paradigm we have experienced in up to this point and have a significant impact for the labour market. They will pose challenges in the employment area and, as rightly mentioned by Professor Luís Antunes, they will demand changes from states in the way everything is programmed.

The need for there to be security that is almost "by design", and I'm quoting here, "privacy by design", the need to reinvent the way we raise our children will be decisive. But so will the need for us to protect ourselves in our homes. This is a situation that before today could be easily remedied with locks on the door, but will now involve other more sophisticated and demanding requirements.

Luís Antunes mentioned that there are NATO countries spying on other NATO countries, but spying on what our next-door neighbour is doing will also be possible and will involve a privacy protection mechanism for every family.

The future will bring many individual protection requirements and, for that reason, Pedro Veiga brought us the human component because, actually, everything starts with that. Without it, we would likely not even be here discussing technology, because this was our initiative! That dimension, as he explained, should be clear in terms of cybersecurity, cybercrime, cyber defence and should involve, as a matter of principle, absolutely concrete investment or else we may be left vulnerable.

Individuals, families, young people who are frequent and regular internet users are vulnerable because the dangers of exposure online are not always understood. Arriving at any hotel in the world, for example, and asking for the Wi-Fi password, exposes us, weakens us! But the paradox is that no one wants to be left out of the internet, with no data access.

A connection to the network with internet use is among the needs that are seen as being important today! In fact, when Maslow thought of the pyramid of basic needs, he had not yet imagined this possibility, which is today a completely pressing one in all our lives and also represents an urgent need for regulation.

Thinking about the video that was shown here, with a message from António Guterres, that need became clear with regard to cyberwarfare but also other, more limited areas. In that field, Rasa Ostrauskaite also mentioned the unpredictability of cyberattacks and of course the spirit of cooperation and the need for joint work among different states. Even assuming that every state has its own sovereignty to be able to resolve or implement a strategy, the goal of cooperation in a complex, sensitive area is growing.

I have tried to focus on the essential messages expressed previously, and I would like to repeat a message we have heard here: what is essential is for there to be political vision and political will! Without them, no state is able to do what is being set out here. Without them, perhaps we will always become more exposed, vulnerable and defenceless as technology advances.

And I would therefore end with this challenge: take this message of awareness outside this room, so that uninformed society can be more aware of the vulnerabilities of technology, in the same way it already clearly feels its advantages.

Thank you very much and once again I would like to thank our speakers for taking part in the first Lisbon conferences.

Thank you everyone.

Da esquerda para a direita: Fernando Jorge Pires, Jorge Miguel Medeiros, Kristian Vigenin e António Gameiro Marques
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04899/2018
From left to right: Fernando Jorge Pires, Jorge Miguel Medeiros, Kristian Vigenin and António Gameiro Marques
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04899/2018

SOBERANIA E SEGURANÇA DIGITAL
SOVEREIGNTY AND DIGITAL SECURITY

FERNANDO JORGE PIRES*

Na sociedade actual existe a percepção de que se vive numa "Aldeia Global" construída largamente sobre o ciberespaço, infraestrutura virtual que pulveriza distâncias e torna instantânea a troca de informação. O ciberespaço constitui-se, assim, como um novo domínio virtual de interacção económica, social e cultural. Esta situação apresenta novos desafios, tanto no domínio da segurança (de pessoas e bens), como da defesa (dos interesses das nações).

A maioria dos países têm estratégias globais que englobam a segurança e a defesa para uma efetiva proteção do ciberespaço, onde as diversas entidades do Estado com competências na matéria estão contempladas e envolvidas.

No caso de Portugal, está para ser aprovada uma nova Estratégia Nacional de Segurança do Ciberespaço, a qual contempla as questões ligadas à cibersegurança, à ciberdefesa, ao cibercrime e outras, e que atualiza uma primeira versão promulgada em 2015.

As forças armadas, não sendo a principal entidade responsável por garantir a "cibersegurança nacional", são também parte ativa no esforço cooperativo para se conseguir este desiderato.

As competências na atuação no ciberespaço têm o paralelismo do mundo físico. Assim sendo, a defesa dos interesses nacionais no ciberespaço prossegue linhas de ação que, incluindo mas não se limitando à proteção, incluem também ações de cariz ofensivo, essenciais para a plena prossecução do objetivo mais lato de garantir a capacidade nacional de utilizar o ciberespaço em qualquer circunstância ou contexto.

No que respeita à componente defensiva, existe uma questão de fundo que dificulta substancialmente as ações de prevenção e de reação a ciberameaças que tem que ver com a "imputação" (attribution).

A atual legislação limita a possibilidade de se conseguir imputar uma conduta no ciberespaço a um determinado sujeito. Esta situação decorre em grande parte da legislação que protege a privacidade, em particular os dados pessoais, e lacunas no

direito internacional que não está ainda adaptado às questões particulares que se colocam agora no ciberespaço, por exemplo no que respeita à territorialidade.

Podemos considerar que a legislação existente acentua substancialmente a assimetria entre os atores presentes no ciberespaço, permitindo que agentes maliciosos operem sob a cobertura das regras que garantem o direito à privacidade para ocultarem a sua atividade e identidade, condicionando fortemente a ação dos agentes responsáveis pela segurança do ciberespaço.

Além da questão jurídica, existem aspetos de cariz técnico que facilitam o anonimato, tornando mais complexa a atividade daqueles que protegem a nossa sociedade no ciberespaço.

A questão de quem deve agir no combate a atividades maliciosas perpetradas através do ciberespaço prende-se com a problemática da atribuição dessa atividade aos atores envolvidos. A dificuldade de determinar com exactidão quem são, onde se encontram e como atuar sobre estes atores (em alguns dos casos também eles protegidos pela nação que os alberga) leva a que muita dessa atividade seja difícil de combater e mesmo de dissuadir.

No ciberespaço considera-se que não existem fronteiras, baseando-se no facto de que a informação flui livremente, de forma praticamente imediata, entre as diversas nações e, à partida, sem quaisquer barreiras.

No entanto, também podemos afirmar que todos os recursos (pessoas, equipamentos, infraestruturas) se encontram de alguma forma sediados dentro de fronteiras físicas dessas mesmas nações, podendo assim ser-lhes atribuída uma quota-parte na responsabilidade de agir em caso de atividades criminosas.

Para que se possa alcançar um ciberespaço mais seguro e protegido, ao dispor de todas as nações e ao serviço da sociedade, com o correto equilíbrio entre o direito à privacidade, por um lado, e o direito ao usufruto em segurança, por outro, há que avançar de alguma forma na regulação da Internet, e do ciberespaço de forma mais genérica.

Este assunto é amplamente discutido em fóruns internacionais, sem que se consiga alcançar consensos sobre a forma mais eficaz de o fazer, sem que para tal se tenha de limitar excessivamente a abertura e a liberdade de utilização.

A existência de protocolos, memorandos de entendimento ou outros documentos formais entre países e organizações ajudam a este esforço conjunto ao potenciar a criação de regras e condutas voluntárias.

A segurança do ciberespaço tem de ser fundada em confiança que só se consegue com ampla e aberta colaboração entre todos os atores.

O ciberespaço, domínio largamente imaterial, construído pela Humanidade para seu uso e benefício exclusivo, apresenta desafios de natureza muito diversa daqueles que se nos apresentam no domínio material.

São necessárias novas aproximações, novos conceitos e novas soluções para garantirmos que dele podemos disfrutar em segurança e para que possa ser um espaço de aproximação entre povos e culturas, e para que nele a sociedade e os indivíduos se possam realizar.

---

* Nota do editor: o texto da intervenção não foi objeto de revisão pelo autor e é publicado apenas com a revisão editorial.

FERNANDO JORGE PIRES*

In today's society, there is an understanding that we live in a "global village", largely built in cyberspace, a virtual infrastructure that atomises distances and makes exchanging information instantaneous. Cyberspace is, then, a new virtual domain of economic, social and cultural interaction. This situation brings new challenges in the field of security (of people and goods), as well as defence (of nations' interests).

Most countries have global strategies that include security and defence for effective protection of cyberspace, where the different state bodies responsible for the matter are considered and involved.

In Portugal's case, a new national cyberspace security strategy is to be approved, which covers issues connected to cybersecurity, cyberdefence, cybercrime and others and updates a first version enacted in 2015.

The armed forces, although not the main body responsible for guaranteeing "national cybersecurity", are also an active part of the cooperative effort to achieve this goal.

The responsibilities for acting in cyberspace find parallels in the physical world. So the defence of national interests in cyberspace follows lines of action that, including but not limited to protection, also include offensive actions, essential to fully pursuing the broader objective of guaranteeing national ability to use cyberspace in any circumstance or context.

As for the defensive component, there is a background issue that makes prevention and reaction actions to cyberthreats more difficult and has to do with attribution.

Current legislation limits the possibility of attributing a conduct in cyberspace to a particular person. This is largely the result of legislation that protects privacy, particularly personal data, and gaps in international law, which has not yet been adapted to the specific issues that are now arising in cyberspace, for example, as regards territoriality.

We may believe that existing legislation substantially highlights the lack of symmetry between actors present in cyberspace, which allows malicious agents to operate under the cover of rules that guarantee the right to privacy to hide their actions and identity, significantly limiting the actions of agents responsible for cyberspace security.

As well as the legal issue, there are technical aspects that favour anonymity, making the actions of those who protect our society in cyberspace more complex.

The question of who should act in the fight against malicious activities perpetrated in cyberspace is linked to the problem of attribution of those actions to the actors involved. The difficulty in precisely determining who they are, where they are, and how to act on these actors (who are in some cases protected by their host nations) means that much of those actions are hard to fight or even to simply discourage.

It is believed that there are no borders in cyberspace, based on the fact that information flows freely, practically immediately, between the different nations and, in theory, without any barriers.

Nonetheless, we can also say that all the resources (people, equipment, infrastructures) are in some way based within the physical borders of those nations, and therefore some of the responsibility to act in cases of criminal activities can be attributed to them.

So that we can create a safer and more protected cyberspace, available to all nations and serving society, with the proper balance between right to privacy on one side and the right to enjoy security on the other, we must move forward in some way with the regulation of the internet and cyberspace more generally.

This matter is widely discussed in international forums, although consensus has not been reached on the most effective way of doing so without excessively limiting openness and freedom of use.

The existence of protocols, memoranda of understanding and other formal documents between countries and organisations contribute to this joint effort by helping create rules and voluntary conducts.

The security of cyberspace has to be founded on trust, which can only be achieved with wide and open cooperation among all actors.

Cyberspace, a largely immaterial area, built by humanity for its own use and exclusive benefit, poses challenges that are very different from those facing us in the physical world.

New approaches, new concepts and new solutions are needed to guarantee that we can enjoy it safely and so it can be a space for bringing together people and cultures and where societies and individuals can find fulfilment.

---

* Editor's note: this presentation has not been reviewed by the author. It is published after editorial review.

ANTÓNIO GAMEIRO MARQUES

Começo por agradecer o convite que me foi endereçado para estar presente nesta conferência, em particular no painel dedicado a um tema que me é particularmente caro, intitulado "Soberania e Segurança Digital".

Esta é uma oportunidade para partilhar com todos os presentes algumas reflexões sobre o tema do "Poder da informação nos conflitos no ciberespaço", incluindo a medida em que o atual estado de todo o sistema internacional no ciberespaço pode

condicionar a nossa soberania naquele domínio de ação, que é cada vez mais relevante face à inexorável digitalização da nossa sociedade. Saúdo igualmente os membros do painel.

O ciberespaço é, nos dias de hoje, um domínio fulcral para o desenvolvimento e a modernização das sociedades, sendo potenciador do respetivo crescimento económico. Porém, ele é, igualmente, um espaço estratégico de potencial confrontação, no qual se utiliza a informação e todos os artefactos que o constituem (infraestrutura e ativos de redes, computadores, redes sociais, motores de busca, etc.) como forma de condicionamento da ação do outro.

Na última Web Summit, Jared Cohen, CEO da Google Jigsaw, referiu, na sua intervenção a 8 de novembro, que "todas as guerras vão começar como ciberguerras", frisando que estamos prestes a entrar numa era mais complexa do que a do mundo bipolarizado da Guerra Fria, do mundo unipolar do pós-Guerra Fria e do mundo multipolar pós-11 de setembro.

No dia 13 de setembro de 2017, no seu discurso do Estado da União, o presidente da Comissão Europeia, Jean-Claude Junker, declarou que os ataques perpetrados através do ciberespaço podem ser mais perigosos para a estabilidade das democracias e das economias do que armas e carros de combate.

De facto, estamos numa *Knowledge Intensive Society* em que o conhecimento, providenciado pela informação que decorre da combinação dos dados com os respetivos meta-dados, tem um valor capital, sendo hoje em dia exfiltrada de grandes bases de dados, para depois ser vendida ilegalmente ou cifrada para posteriormente exigir aos seu proprietário o pagamento de avultadas somas para recuperar o respetivo acesso. A informação que permanentemente é recolhida sobre o nosso comportamento enquanto seres humanos, sem que nós nos demos conta disso, é imensa, estando, cada vez mais, na ordem do dia os assuntos relacionados com a privacidade e o respetivo equilíbrio com a segurança. Factos do passado muito recente, envolvendo a maior rede social do mundo e uma empresa de *business intelligence*, são disto um exemplo irrefutável.

A informação tornou-se, assim, o ouro negro do século XXI.

Com este pano de fundo, gostaria de vos dar uma perspetiva geoestratégica centrada na crescente relevância da informação e nos "artefactos que constituem o ciberespaço" que há pouco mencionei e que são, afinal, o veículo para a sua transmissão, o seu processamento e armazenamento.

Tal como os domínios físicos (mar, terra e ar), o ciberespaço, o único criado pelo ser humano, existe, entre outras coisas, para desenvolver os interesses económicos dos cidadãos e dos Estados no contexto da economia digital (mais segurança -> mais desenvolvimento).

Todos os domínios possuem pontos de confluência e de concentração que, na vertente física, se consubstanciam nos pontos de convergência associados às linhas de comunicação e fluxos de pessoas e bens (marítimo, terrestre e aéreo), mas que no ciberespaço, atenta as suas características mais significativas (ubiquidade, inexistência de fronteiras físicas, dispersão e descentralização), conduzem à identificação de vários pontos de concentração (de poder) que importa caracterizar e relacionar no contexto geoestratégico: o primeiro é a infraestrutura física que existe à escala global e cujos ativos são predominantemente provenientes de um só fabricante, a CISCO.

Ciente deste facto, a China, com a Huawei, está a ganhar terreno, havendo mesmo evidências fundamentadas que nalguns países estão a "oferecer" toda a infraestrutura de rede dos edifícios governamentais.

Refira-se que as poucas empresas europeias com estas competências (e.g. Ericsson, Nokia, Alcatel) quase que desapareceram, deixando a Europa sem qualquer relevância estratégica neste contexto. De igual modo, os cabos submarinos mais importantes têm todos pontos de amarração nos EUA.

O segundo ponto de concentração estratégica reside nos próprios dispositivos que utilizamos quase permanentemente para aceder à Internet: a maioria tem a sua conceção nos EUA e o seu fabrico na China e em Taiwan.

Para que qualquer destes dispositivos funcione corretamente, é necessário um sistema operativo. Este representa o terceiro ponto de concentração estratégica uma vez que o predominante, com 85%[1] de penetração à escala global, é o Windows da Microsoft. O seguinte, com 9%, é o MAC OS da Apple. Ambos de um mesmo país. No caso dos SO móveis, o Android da Google e o IOS da Apple contam, no conjunto, com mais de 99% (70% e 29%) do mercado. Assim, verifica-se mais uma vez, uma clara dominância de um só Estado.

O quarto ponto de concentração estratégica refere-se aos *browsers*, às redes sociais e aos motores de busca.

Não há muito a dizer: relativamente aos *browsers*, que são os programas que utilizamos para navegar na Internet, de acordo com a NetMarketShare, com referência a abril de 2018, o Chrome da Google conta com cerca de 61% do mercado de procura. Mas a Google não se fica por aqui, pois o seu motor de busca, com os seus algoritmos de procura, tem 67% deste mercado.

É de relevar que os motores de busca exercem um poder enorme sobre as ideias das pessoas porque determinam o que é importante e o que não é, através dos primeiros lugares da lista dos resultados da pesquisa. E a Google faz isto mais de mil milhões de vezes por dia.

Se na era da informação e do conhecimento isto não é poder, então o que é ter poder? Ciente deste potencial estratégico, a China envidou esforços para erradicar a Google do seu território, que teve de se instalar em Hong Kong, a partir de 2010. Hoje, o motor de busca chinês Baidu possui cerca de 81% de quota de mercado na China, mais de 400 milhões de internautas chineses e cerca de 20,5% à escala global.

Na Europa, com mais habitantes que os EUA, nada existe também neste contexto.

O quinto ponto de concentração estratégico refere-se aos sistemas de computação e armazenamento na nuvem (*cloud computing*). Também aqui a predominância é das empresas dos EUA. Ainda que algumas possuam centros de dados no continente europeu, são empresas norte-americanas e guardam a larga maioria da informação existente à escala global em formato digital.

Finalmente, o último ponto de concentração estratégico é constituído pelos fóruns de governação do ciberespaço. Devido à sua génese na comunidade académica, tendem a ser predominantemente espaços de partilha de conhecimento em vez de fóruns de controlo.

No entanto, a I&D e inovação nestes e noutros domínios encontra-se muito desenvolvida através de centros de R&D ligados às universidades norte-americanas e, por isso, os EUA continuam a exercer aqui também o seu poder de influência (*soft power*) e de predominância. Vejam, por exemplo, quem lidera a I&D na IA, nos veículos autónomos, na mobilidade elétrica, apesar do nível de sofisticação da indústria automóvel europeia.

É, por isso, e por ora, evidente que as empresas norte-americanas dominam os pontos de concentração estratégicos do ciberespaço, com a China a crescer de importância de forma evidente e sustentada. Todavia, julgo que não restam dúvidas de que há claramente uma supremacia de um só Estado sobre o ciberespaço, que importa acompanhar e sobretudo tem que nos levar a agir enquanto União Europeia, uma vez que a UE se encontra claramente numa posição de grande dependência em todos os aspetos que descrevi.

A realidade é clara: o ciberespaço é hoje um domínio eminentemente unipolar. Assim, as perguntas que importa procurar responder são as seguintes: O que pode a União Europeia fazer para mitigar este facto e assim reganhar no ciberespaço alguma da soberania? Em que é que nos podemos diferenciar? Numa maior regulação centrada no cidadão (*EU Cyber Security* ACT, Diretiva NIS, RGPD)? No investimento nas competências das pessoas para as tornar mais resilientes do ponto de vista digital? São temas que julgo de relevo para o nosso debate.

Para finalizar, voltaria a referir o CEO da Google Jigsaw Jared Cohen[2] (cito): "O que existe hoje é um sistema internacional que tem uma frente física e uma frente digital, e todos os desafios do mundo físico que conhecemos há décadas e séculos estão a derramar para o *online*. (...). Foi sempre a economia, a política e o poder militar a determinar quais são os Estados mais poderosos. Estes são atributos que permanecem inalterados. Só que, doravante, os Estados mais poderosos serão aqueles capazes de projetar influência não só naquelas áreas, mas também no domínio virtual".

Deixo-vos com uma pergunta: **O que devem a União Europeia e Portugal fazer para tirar partido da situação quase unipolar no ciberespaço que hoje se verifica?**

---

[1] https://netmarketshare.com/ (8MAI18).
[2] WEB SUMMIT, Lisboa 8.11.2017.

ANTÓNIO GAMEIRO MARQUES

I shall begin by expressing my thanks for the invitation I was given to be present at this conference, particularly on the panel dedicated to a theme that is particularly important to me: "Sovereignty and Digital Security".

This is an opportunity for me to share with everyone some reflections on the theme of the "Power of information in conflicts in cyberspace", including the way in which the current state of the entire international system in cyberspace may

limit our sovereignty in that field of action, which is increasingly relevant considering the relentless digitisation of our society. I would also like to greet the members of the panel.

Today, cyberspace is a crucial area for the development and modernisation of societies and it boosts their economic growth. But it is also a **strategic space for potential confrontation**, in which the information and all the items that form it (network infrastructure and assets, computers, social networks, search engines, etc.) are used as a way of conditioning others' actions.

At the last Web Summit, Jared Cohen, CEO of Google Jigsaw, mentioned in his presentation on 8 November that "all wars are going to begin as cyber wars", underlining that we are about to enter an era that is more complex than the bipolar world of the Cold War, the unipolar world post-Cold War and the multipolar world since September 11.

On 13 September 2017, in his speech on the State of the Union, the President of the European Commission, Jean-Claude Juncker, said that attacks perpetrated over cyberspace could be more dangerous to the stability of democracies and economies than weapons and tanks.

In fact, we are living in a knowledge-intensive society in which knowledge, provided by the information resulting from the combination of data and relevant metadata, has a capital value and is today extracted from large databases to then be sold illegally or encrypted to later demand the owners pay large sums to regain access. The information that is constantly being collected about our behaviour as human beings without our realising is enormous, and matters related to privacy and the balance with security are increasingly on the agenda. Very recent events involving the world's largest social network and a business intelligence company are an indisputable example of this.

Information has therefore become the black gold of the 21st century.

Against this background, I would like to give you a geostrategic perspective focused on the growing importance of information and the "objects that form cyberspace" that I just mentioned which are, ultimately, the vehicles for information to be transmitted, processed and stored.

As in the physical realms (sea, earth and air), cyberspace, the only space created by humankind, exists to, among other things, develop citizens' and states' economic interests in the context of the digital economy (more security -> more development).

All realms have points of convergence and concentration that, in the physical world, form the points of convergence connected to lines of communication and flows of people and goods (by sea, land or air). In cyberspace, however, due to its most significant characteristics (ubiquity, lack of physical borders, dispersion and decentralisation), these points lead to several points of concentration (of power), which it is important to describe and link to the geostrategic context: the first is the physical infrastructure that exists at global level, the assets of which predominantly come from a single manufacturer, CISCO.

Aware of this, China, is making inroads with Huawei and there is even justified evidence that, in some countries, they are "giving away" the entire network infrastructure for government buildings. The few European companies with these skills (e.g. Ericsson, Nokia, Alcatel) have practically disappeared, leaving Europe with no strategic relevance in this field. Similarly, the most important submarine cables all have landing points in the USA.

The second point of strategic concentration lies in the very devices we use almost constantly to access the internet: most are designed in the USA and made in China and Taiwan.

An operating system is required for any of these devices to work properly. This is the third point of strategic concentration, since the most dominant system, with almost 85%[1] penetration at global level, is Microsoft Windows. The second, with 9%, is Apple's MAC OS. Both are from the same country. In the case of mobile OSs, Google's Android and Apple's iOS together hold more than 99% of the market (70% and 29% respectively). There is once again clear dominance by one state.

The fourth point of strategic concentration concerns browsers, social networks and search engines.

There is not a great deal to say: in the world of browsers, which are the programs we use to surf the internet, Google Chrome held 61% of market demand in April 2018, according to NetMarketShare. But Google does not stop there, because its search engine, with its search algorithms, has 67% of that market.

It is important to highlight that search engines have enormous power over people's ideas because they establish what is important and what is not depending on what they place in the top positions in the list of search results. And Google does this billions of times a day.

If in the age of information and knowledge this is not power, than what is having power? Aware of this strategic potential, China made efforts to eradicate Google from its territory, and it had to move to Hong Kong in 2010. Today, the Chinese search engine Baidu has a roughly 81% market share in China, of the more than 400 million Chinese internet users, and around 20.5% worldwide.

In Europe, which has more residents than the USA, there is also nothing in this field.

The fifth point of strategic concentration relates to cloud computing and storage. This is another field where US companies dominate. Although some have data centres in the European continent, they are North American companies and they store the vast majority of information in existence at global level in digital format.

Finally, the last point of strategic concentration is the formed of cyberspace governance forums. Due to their beginnings in the academic community, they tend to be predominantly spaces for sharing knowledge rather than control forums.

However, R&D and innovation in these and other fields is very much advanced through R&D centres connected to North American universities, and that is why the USA continues to exercise its soft power and dominance in this area. Look at, for example, who is leading R&D in AI, autonomous vehicles, electric mobility, despite the European automotive industry's level of sophistication.

It is clear, for these and other reasons, that North American companies dominate the points of strategic concentration in cyberspace, with China's importance clearly and consistently growing. Nonetheless, I believe there is no doubt that one state evidently has supremacy over cyberspace, and it is important to monitor this and, above all, it must drive us to act as the European Union, since the EU is clearly in a position of great dependence on all the components I have described.

The situation is clear: cyberspace is today an eminently unipolar field. So the questions which are important to answer are as follows: What can the European Union do to mitigate this situation and regain some sovereignty in cyberspace? How can we make ourselves stand out? Through greater regulation focused on citizens (EU Cyber Security Act, the NIS Directive, GDPR)? Through investment in people's skills to make them more resilient from a digital perspective? These are themes that I believe are important for our debate.

To finish, I would like to once again return to the CEO of Google Jigsaw, Jared Cohen[2] (I quote): "There's now just one international system and it has a physical front and it has a digital front, which means that all the challenges that have plagued the streets, all of the physical world challenges that we've known for decades and centuries are now spilling over online. (...) It's always been the case that economics, politics and the military determine which states are powerful and which are not. These attributes remain the same except the powerful states are going to be the ones that can project influence in those areas, in both a physical and cyber domain."

I leave you with a question: **What should the European Union and Portugal do to draw on this almost unipolar situation found today in cyberspace?**

---

[1] https://netmarketshare.com/ (8 May 18).
[2] WEB SUMMIT, Lisbon 8.11.2017.

KRISTIAN VIGENIN

Em primeiro lugar, gostaria de felicitar a Isabel Santos e toda a delegação portuguesa por esta iniciativa. Considero-a muito oportuna, muito útil, e temos tido um excelente debate até ao momento, excelentes comunicações. Creio que já quase tudo foi dito. Como tal, farei algumas observações sobre o tema e espero poder contribuir para a qualidade dos debates de hoje.

Permitam-me que comece por identificar o elemento essencial do nosso debate neste painel, a soberania. Trata-se, naturalmente, de um termo em evolução. Existem diferentes explicações sobre o seu significado exato. Eu diria que é o

controlo de um governo democraticamente eleito sobre um Estado, um território, e o mundo digital está a pôr em questão este conceito: como podemos definir território no cibermundo?

Um dos maiores desafios é explicar e entender a natureza do problema, compreender por que motivo e de que forma nos tornámos tão vulneráveis na era atual. Eu diria que o conhecimento da esfera política, dos líderes políticos, é demasiado limitado. Para muitos, o ciberespaço é algo assustador, misterioso, invisível, que nos rodeia e, como é evidente, dificilmente podemos regulamentar o que não compreendemos.

Este é, pois, um elemento importante do nosso trabalho, do trabalho de quem, como nós, enfrenta esta questão. A tecnologia está a desenvolver-se rapidamente, criando enormes melhorias e uma grande eficiência, possibilitando novos serviços e colocando o ponto mais longínquo do mundo a um clique de distância. Tal torna muito tentador para os Estados e as empresas abraçar estas oportunidades, acelerando processos, mas também os leva a expor-se a novas vulnerabilidades, sem serem capazes de prever todos os desafios e de se protegerem e defenderem eficazmente destas vulnerabilidades.

O ciberespaço não pode existir sem um mundo físico. Contudo, sobretudo em alguns domínios, as infraestruturas físicas estão cada vez mais subordinadas à dimensão digital. A dimensão digital, a que eu chamaria a quarta dimensão do nosso mundo, está a tornar-se o sistema circulatório da nossa economia, segurança e vida quotidiana. Já existem pessoas que vivem vidas digitais mais estimulantes e ativas do que as suas vidas reais. Trata-se de um fenómeno que é necessário ter em conta nos nossos debates.

Se pudermos contaminar o sangue, os resultados serão devastadores e irão depender dos agentes contaminantes. Assim, para mantermos a independência e a soberania, para protegermos as nossas conquistas democráticas, bem como os frutos do progresso tecnológico, temos de evitar as ameaças, contrariá-las, protegermo-nos delas e, é claro, conseguir sarar as feridas após ataques dessa natureza.

Temos de desenvolver um sistema imunitário complexo que impeça a invasão de agentes ou objetos estranhos e que seja capaz de destruir rapidamente os que conseguem entrar no sistema. É extremamente importante discutir a ideia apresentada, creio, no primeiro painel, de que é essencial educar as pessoas, as empresas, os Estados, para evitarem os riscos. É a chamada "higiene digital". Parece fácil, mas é uma missão extremamente complexa, que exige um esforço substancial a diferentes níveis, a partir das idades precoces dos nossos filhos, que enfrentam estes desafios desde o início das suas vidas.

Do trabalho já em curso a diferentes níveis, gostaria de referir, pelo menos, os esforços da União Europeia neste domínio. Muitos dos oradores já o mencionaram, mas o facto de a UE já estar a promover a ideia de criar uma agência para a cibersegurança constitui um passo muito positivo, mas que, inevitavelmente, suscita algum ceticismo.

Concretamente, tal como referi, como irá esta agência para a cibersegurança trabalhar ou coordenar-se com as agências nacionais? Podemos definir "território"? E como o definimos? Qual seria, na prática, o âmbito de ação de uma agência para a cibersegurança? Não é a questão habitual de ter ou não fronteiras, de saber quais as fronteiras que tentamos proteger em diferentes áreas, consoante as suas características. No ciberespaço é difícil defini-las. E já constatámos que alguns Estados-Membros já estão bastante céticos nesta matéria e tentam manter um maior controlo dos seus sistemas a nível nacional.

O segundo elemento, que já foi debatido e me parece extremamente importante, é a necessária normalização comum. Atualmente, temos diferentes normas e sistemas de normalização na União Europeia e os diversos produtos, sistemas, equipamentos e programas têm de cumprir requisitos de certificação diferentes, o que, na minha opinião, nos torna mais vulneráveis.

Um sistema comum acrescentaria valor e facilitaria o nosso trabalho. Espera-se que a conjugação de esforços nos torne menos vulneráveis. Ao mesmo tempo, a confiança, sobretudo neste domínio, é relativamente baixa entre Estados, como constatei em várias discussões a este respeito, pelo que, provavelmente, será necessário algum tempo até haver um trabalho real e substantivo das diferentes agências neste âmbito. Creio, contudo, que o distinto colega de painel da Autoridade de Segurança portuguesa nos pode dizer algo mais a este respeito.

No início, referi os governos eleitos e gostaria de chamar a vossa atenção para um elemento que também esteve presente no nosso debate e do qual gostaria de dar alguns exemplos práticos. No ano transato, ficou provado que as tecnologias permitiram uma interferência direta no processo eleitoral. E o governo em questão é realmente um governo democraticamente eleito ou houve abusos através das novas tecnologias e das novas oportunidades? Existe uma utilização abusiva dos instrumentos democráticos de que dispomos? Tal utilização permite também influenciar diretamente a opinião pública.

Podemos chamar guerra híbrida, ou simplesmente propaganda sofisticada, à utilização de notícias falsas cuidadosamente criadas e direcionadas. A verdade é que a adulteração de eleições destrói os alicerces das nossas democracias, e o condicionamento da opinião pública num ou noutro sentido, sobretudo a partir do exterior ou em nome de interesses estrangeiros, também é um ataque direto à nossa soberania. Temos de encontrar uma forma eficaz de combater estes fenómenos.

Gostaria de vos dar alguns exemplos concretos relacionados sobretudo com formas de influenciar a opinião pública através das novas tecnologias. Esta situação pode representar uma ameaça interna para a estabilidade de um país. Pode provocar tensões étnicas. Vimos recentemente sítios *Web* de notícias falsas a promover, por exemplo, a notícia falsa de que UE irá obrigar as autoridades búlgaras, o governo búlgaro, a dar mais dinheiro à população cigana, comparando os subsídios mensais com as pensões, os salários mínimos, etc. Esta notícia cria, por um lado, hostilidade contra a UE e, por outro, tensões étnicas e hostilidade contra a população cigana. No entanto, ao mesmo tempo, muitas pessoas continuam a acreditar nestas notícias. E apresento este caso como um exemplo de uma ameaça direta. Não são apenas notícias falsas inócuas, são notícias que criam ameaças diretas para a sociedade.

Um outro exemplo, que consiste em propaganda direta anti-UE, é a utilização da ministra para a Presidência da UE, ou Presidência do Conselho da União Europeia, numa série de publicações, semana após semana, em que é constantemente visada, criando uma imagem de uma pessoa associal e fria, que afirmou que os pensionistas não precisam de aumentos nas reformas, porque vão morrer em breve e que é necessário direcionar mais dinheiro para os jovens e pessoas ativas ou, por exemplo, que não devem ser gastos mais recursos nos pensionistas, e que os respetivos familiares devem enviar-lhes mais remessas se trabalharem no estrangeiro.

Como é natural, isto parece cómico para alguns de nós, mas muitas pessoas acreditaram realmente nestas notícias. Condenaram-nas e elogiaram-nas, partilharam-nas maciçamente nas redes sociais, tornando-se, assim, na verdade, ajudantes dos iniciadores destas notícias falsas e destes conteúdos que constituem, a meu ver, propaganda muito sofisticada.

Como tal, esta é uma realidade que temos de levar muito a sério. Sabemos que a UE tem uma equipa para combater a propaganda, mas trata-se, devo dizer, de uma resposta muito frágil, baseada no Serviço Europeu para a Ação Externa, que não parece ser a melhor instância para uma equipa deste tipo.

No entanto, o mais importante é o que fazemos a nível nacional. Continuo a acreditar que a nível nacional, nós – políticos, deputados, governantes – tendemos a subestimar a influência desta propaganda.

Posso dar-vos só um exemplo: faço um esforço pessoal neste combate, tanto quanto me é possível, e uma das minhas amigas no Facebook, por exemplo, ficou extremamente surpreendida quando comecei a escrever comentários sob cada notícia falsa que ela partilhava naquela rede social. E percebeu, repentinamente, com grande surpresa, que pode haver notícias falsas em sítios *Web* de informação. Muitas pessoas acreditam que se uma notícia está na Internet, nos jornais, nos sítios *Web*, tem de ser verdadeira. A minha amiga disse-me depois o seguinte: "Passei a ter receio de partilhar notícias, porque procuro confirmar cada notícia." Penso que este é apenas um exemplo, mas trata-se de uma pessoa com formação superior, uma pessoa inteligente. A sua surpresa foi uma surpresa para mim, mas se aconteceu com esta pessoa, pensemos como estas notícias podem influenciar pessoas menos instruídas, porventura não tão inteligentes. E esta é uma ameaça direta à soberania de um Estado.

Mencionei a contaminação do sistema circulatório do nosso mundo atual: se contaminarmos redes, computadores, podemos repará-los, alterá-los, substituí-los; quando são contaminadas as mentes das pessoas, como resolvemos esse problema? Por conseguinte, a prevenção neste domínio é extremamente importante. Infelizmente, por vezes é demasiado tarde para o fazer, mas não é o caso. Temos apenas de estar muito atentos e perceber melhor como este processo pode ter consequências nefastas para as pessoas e, como referi noutra ocasião, quando as pessoas são influenciadas desta forma é muito difícil inverter a sua posição e as suas opiniões, levá-las a pensar e a verificar cuidadosamente o que leem, ouvem, partilham, etc.

Gostaria de repetir algumas ideias, alguns elementos já mencionados, porque a OSCE desempenha um papel importante neste processo. Referi a UE, mas trata-se de um sistema diferente, com uma união específica de países, que têm muito em comum. A OSCE tem 57 países membros e os esforços desenvolvidos na OSCE, especialmente quando produzem resultados suficientes, podem ter um impacto muito mais forte nestas questões.

A atividade mais recente foi a adoção das medidas de reforço da confiança para reduzir os riscos relacionados com as TIC. A decisão do Conselho Permanente foi adotada em 2016 e, posteriormente, houve uma reunião da Assembleia Parlamentar

da OSCE em 2017, em Andorra, na qual participaram perto de 200 parlamentares, sob o tema principal "Cibersegurança". Mais tarde, foi adotada a última resolução da AP da OSCE sobre cibersegurança, em Istambul, numa sessão em 2013.

Queria fazer esta referência, mas o mais importante é tratarmos o ciberataque como tratamos um ato de agressão convencional. É muito importante sublinhar este facto e tê-lo em mente também nos debates internos nos nossos países. Esta resolução insta-nos a intensificar esforços para convencer os parlamentos e os governos dos países membros de que as ameaças com origem no ciberespaço estão entre os maiores desafios de segurança do nosso tempo, algo que já foi referido várias vezes hoje.

A meu ver, esta conferência segue precisamente essa orientação. Assim, creio que nós, enquanto Assembleia Parlamentar, podemos contribuir muito para a segurança e a cooperação no espaço da OSCE e utilizar os nossos instrumentos interparlamentares para aumentar a sensibilização para estas questões.

Com a criação desta comissão *ad hoc*, a OSCE está a tentar acrescentar valor à luta contra a cibercriminalidade. Além disso, há um aspeto muito importante que também é um dos resultados desta conferência: a nossa vontade e disponibilidade para cooperar com outros intervenientes fundamentais para se garantir a segurança e o desenvolvimento neste domínio.

Reconhecemos o significado do contributo para um quadro de segurança internacional coerente e abrangente. E, sendo eu o relator na primeira comissão, um dos elementos mais importantes da elaboração da resolução de Berlim será a cibersegurança.

Há vários elementos focados aqui e agora, no seguimento do debate de hoje, e penso que, minutos antes de distribuirmos a primeira versão da resolução, devemos acrescentar a necessidade de legislação internacional vinculativa em matéria de cibersegurança. É algo que falta ao nosso sistema, sendo necessário um trabalho ativo; esta legislação internacional pode ter diferentes elementos, naturalmente, mas é importante uma regulação mais forte a esse nível.

Podemos dizer que tal será inevitável, mas quanto mais cedo chegar, melhor será para todos nós, e pode vir a ser muito útil que a Assembleia Parlamentar, através das suas resoluções, inste a comunidade internacional a fazê-lo, a fim de incentivar uma maior participação e um trabalho mais ativo.

Obrigado a todos pela vossa atenção e participarei com interesse no debate após o nosso painel.

KRISTIAN VIGENIN

First of all, I would like to congratulate Isabel Santos and the whole Portuguese delegation for this initiative. I think it is very timely, very useful, and we had an excellent discussion so far, excellent reports. I'm afraid that almost everything was said already. So I'll make some remarks on the topic and I hope it will add some quality to the debates today.

Let me start by identifying the substance of our discussion in this panel, sovereignty. Of course, that's a term in development. There are different explanations about what it exactly is. I would say it's a democratically elected government's control over a state, territory, and the digital world is putting this under question, because how can you define territory in the cyber world?

One of the biggest challenges is to explain and to understand the nature of the problem, why and how we've become so vulnerable in the current era. The knowledge of political level, political leadership, I would say, is too limited. For many, cyberspace is something scary, mysterious, invisible that surrounds us, and, of course, you can hardly regulate it if you don't understand it.

So this is an important element of our work, of those of us who are dealing with this issue. Technology is developing fast, creating enormous improvements and efficiency, offering new services, making the farthest point in the world a click away, very tempting for states and businesses to embrace these opportunities, further accelerating the process, but also opening new vulnerabilities, without being able to foresee all challenges, and without being able to protect and defend effectively from these vulnerabilities.

Cyberspace cannot exist without a physical world. But more and more, especially in some areas, physical infrastructure becomes subsidiary to the digital dimension. Digital dimension, what I would call the fourth dimension of our world, becomes the blood vessel system of our economy, security, everyday life; we have already people who live digital lives that are much more exciting and active than the real lives. This is a phenomenon that we have to take into account in our discussions.

If you can contaminate the blood, the results will be devastating, depending on the agents. So, to keep our independence and sovereignty, to protect our democratic achievements as well as the fruits of the technological progress, we need to avoid threats, to counter threats, to protect from threats and of course to be able to heal after attacks of such nature.

We need to develop a complex immune system that is preventing foreign agents or subjects to invade, that is able to quickly destroy those who succeed to enter the system. And what is extremely important to discuss is that during the first panel, I think, it is very important to educate people, businesses, states, to avoid risks. What we call hygiene, digital hygiene. It sounds easy, but it is an extremely complex undertaking, which needs a lot of effort at different levels, starting from an early age of our kids, who face these challenges from the beginning of their lives.

What we are already doing at different levels, I would at least mention the efforts of the European Union, in this area. Many of the speakers mentioned it already, but the fact that the EU is already promoting the idea of creating a cyber security agency is a very positive step, which of course comes not without some skepticism.

As I mentioned, how is this cyber security agency going to work with or coordinate with the national agencies? How can you or can you define "territory"? Such a cyber security agency, what would this agency cover, actually? It's not the usual term of having borders and which borders are you going to try to protect in different areas by different kinds. In cyberspace it is difficult to define. And we've seen already that some member states are already quite skeptical on that issue and try to keep more control of their own systems, nationally.

The second element, which was already under discussion and which I think is extremely important, the common standardization, which is needed. Now we have different standards and standardization systems within the European Union, and different product, systems, hardware and software have to go through, different certification requirements, which I believe make us more vulnerable.

Such a common system would add value and make our efforts easier. Joining efforts is supposed to make us less vulnerable. At the same time, the confidence, especially in this area, is relatively low between states, we can say it, because I know it from different discussions, so it will probably take time before there is a real and substantive work of the different agencies on that, but I suppose our distinguished panelist from the Portuguese security agency can tell us more about that.

I have mentioned at the beginning the elected governments and would like to draw your attention to an element that was also part of our discussion but I would like to give also some practical examples.

Last year it was proved that the new technologies allowed for direct interference in the electoral process. And such government – is it really democratically elected or this is a misuse through the new technologies and the new opportunities. Is there a misuse of the democratic tools that we have? That allows also direct influence on the public opinion.

Call it hybrid warfare, or simply sophisticated propaganda, which is using fake news carefully created and targeted. I mean, stealing elections destroys the fundamentals of our democracies, and influencing the public opinion in one or another direction, especially if it comes from the outside or is in the interest of foreign interests, that also is direct attack on our sovereignty. And we need to find an effective way to counter that.

I, especially on the issue of influencing public opinion through the new technologies, I would like to give you some very concrete examples. This can pose an internal threat to the stability of the country. This can provoke ethnic tensions. For example, recently we've seen such fake news websites promoting for example the fake news that EU will force Bulgarian authorities, Bulgarian government, to give more money to Roma population, comparing the monthly allowances, to the pensions, minimum salaries and so on.

On the one hand, that creates sentiments against the EU and on the other hand that creates ethnic tensions and sentiments against the Roma population. But at the same time, somehow, a lot of people still believe in such news. And I give this as an example of a direct threat. It's not just innocent fake news, it's something that's directly creating threats for the society.

Or another example, which is directly anti-EU propaganda, using the Minister for the EU Presidency, or Presidency of the Council of the European Union, in a number of publications following week after week, she was constantly targeted, creating an image of anti-social, cold person, who said that pensioners don't need to receive more money because they will anyway pass away soon and more money must be spent for young people or active people, or, for example, no money for pensioners should be spent, their relatives should send them more money, if working abroad.

You can imagine, that may sound funny for some of us, but a lot of people just believe in that. They condemned or praised, shared massively in the social media, thus becoming actually aides to the initiators of this fake news and of this, I would say, very sophisticated propaganda.

So this is something that we need to take very seriously. We know that EU has a team on countering propaganda, but that is, I must say, a very weak response and it's based on the European external action service, which I don't think is the best place for such a team.

However, it is more important what we do at national level. Because I still think that at a national level we tend to – when I say we, I mean politicians, members of Parliament, government – we underestimate the influence of this propaganda.

I can give you just an example: I make my personal effort in that direction, as much as I can, and one of my Facebook friends, for example, she was extremely surprised when I started to make comments under every fake news she was sharing on Facebook. And then suddenly she realized, and she was so surprised to realize that there may be false news on the news websites. Many people believe that if it is on the internet, in the news, websites, it must be true. And then she said: "I'm now afraid to share any news, because I try to double check every news". I think this is just one example, but I talk about a person who has high education, is an intelligent person, I was personally surprised that she was surprised, but if she is surprised, imagine how many people who are less educated, maybe not that intelligent, imagine how they are influenced by this. And this is a direct threat to the sovereignty of a state.

I was speaking about a contamination of the blood vessel system of our world today, but if you can contaminate networks, computers – you can heal, you can change, you can buy new; when people's minds are contaminated, how could you overcome that? So prevention here is extremely important. I'm afraid sometimes we are late with that but it is never too late. We just have to be very focused and to understand better how damaging this process can be on people and as I've said, once people get influenced this way it is very difficult to change them and their minds back, to make them think and check carefully what they're reading, listening, sharing and so on.

I need to say a few words again, some elements have been mentioned already, but OSCE has its important role to play in this process. I mentioned EU, but it's a different system, with a specific union of countries, which share a lot in common, but OSCE has 57 member states and the efforts in OSCE, especially if they're successful enough, can have a much stronger impact on these issues.

So the most recent activity was the adoption of the confidence building measures to reduce risk related to ICTs. The Permanent Council decision was adopted in 2016, then the OSCE Parliamentary Assembly meeting in 2017 in Andorra, where close to 200 members, parliamentarians, were in attendance, with its main topic "Cyber security", then, the last OSCEPA resolution on cyber security was adopted in Istanbul, in a session in 2013.

I'm just mentioning that, but what is important is that we classify the cyber attack as the same as a conventional act of aggression, this is very important to underline and to keep it in mind also in our internal national discussions. We have been urged through this resolution to intensify our efforts in convincing parliaments and governments in their countries that threats originating from cyberspace are one of the most serious security challenges of present time, which has been mentioned many times today and I think that today's conference is exactly in this direction.

Then we, as Parliamentary Assembly, I think we can contribute a lot to security and cooperation in the area of OSCE and use our parliamentary tools to raise awareness on these issues.

Through the establishment of this ad-hoc committee the OSCE is striving to add value in the fight against cyber crime.

And what I think is very important and is one of the outcomes of this conference, is our readiness and willingness to cooperate with other actors, who are crucial to ensuring security and development in this area.

We recognize the significance of the contribution towards a coherent and comprehensive international security framework. And since I am the rapporteur in the First committee, in the preparation of the Berlin resolution one important element of it will be the cyber security.

There are several elements which are mentioned there and now, following today's discussion, I think that just minutes before we distribute the first draft of the resolution, I think we should also add the need for binding international law on cyber security. This is something lacking in our system, more active work is needed, this international law could have different elements, of course, but a stronger regulation at that level becomes important.

We can say this is inevitable, but the sooner it comes, the better for all of us and maybe if the Parliamentary Assembly, through its resolutions, can urge the international community to do so, to encourage the stronger involvement and more active work, that might be also very useful.

Thank you for your attention and I'll be interested to follow the discussion after our panel.

JOSÉ MIGUEL MEDEIROS

Antes de mais, quero agradecer o honroso convite que me foi formulado para ser o moderador/relator deste painel. Gostaria de proferir algumas palavras no contexto desta oportuna conferência subordinada a um dos temas mais complexos e inquietantes da sociedade dos nossos dias.

Vou, então, tentar fazer um apanhado das principais questões abordadas nas excelentes intervenções e comentar algumas das questões mais relevantes que foram abordadas neste magnífico painel.

Trata-se de uma tarefa difícil porque as intervenções foram bastante amplas nas abordagens e tocaram muitos aspetos, alguns dos quais já haviam sido levantados nos painéis antecedentes. Portanto, mais do que reportar o que cada um dos conferencistas aqui disse, tentarei fazer uma síntese daquilo que me parece poder extrair-se desta sessão.

Quero, igualmente, sinalizar a qualidade das intervenções proferidas, seja pela sua amplitude, seja pelos aspetos muito relevantes e desafiantes que nos colocaram. Os elementos do diagnóstico aqui realizado são elucidativos do cerco a que estão sujeitos alguns dos valores civilizacionais que consideramos como referência.

Um cerco que em muito se acentuou por força de uma silenciosa, mas profundíssima revolução digital operada nos mais variados domínios contextos e até em recentes desenvolvimentos geopolíticos associados a alterações geoeconómicas.

De facto, todos nós sabemos quais foram as origens das fronteiras físicas que determinaram as diferentes soberanias e, por seu turno, se materializam nos Estados e nas nações que constituem o concerto da comunidade internacional.

Essas fronteiras, tal como as que conhecemos hoje, foram sempre estabelecidas na sequência de disputas pelo controlo de recursos, traduzidas em disputas territoriais entre comunidades populacionais que, em regra, se traduziram em confrontos militares entre povos, ao longo de séculos.

Foi esta conjuntura que levou os povos a compreenderem que o caminho da paz e da concórdia provavelmente seria um caminho mais útil e mais interessante do que o caminho da guerra permanente. Com o tempo, as comunidades evoluíram, criaram civilizações cada vez mais evoluídas e a comunidade internacional foi começando a criar regras mais favoráveis à cooperação e dissuasoras do conflito, privilegiando a sua resolução pacífica e negociada.

Existe hoje, todavia, um novo espaço de potencial conflito, de confronto entre as regras e a ausência delas, entre a lei e o crime, entre a guerra e a paz, entre a ordem e o caos, que designamos por ciberespaço, ou espaço cibernético e cujos perigos e vantagens temos estado aqui hoje a discutir e analisar. Podemos desde logo concluir que são muitos e novos os desafios que se colocam neste espaço, no domínio da segurança e da defesa das nações e dos indivíduos. E é esse o cerco que importa quebrar.

Por conseguinte, como ficou claro aqui, é urgente regulamentar e criar normas de utilização que permitam, de facto, que quem utiliza o ciberespaço se sinta seguro e possa ter a garantia de que essa segurança existe, pelo menos nos limites daquilo que está ao nosso alcance e ao alcance dos Estados e das instituições internacionais.

Em boa verdade, a segurança absoluta provavelmente nunca existirá, mas, pelo menos, uma segurança próxima daquilo que já temos hoje, nos diferentes espaços tangíveis com que lidamos e nos quais nos movemos. É o esforço mínimo que os cidadãos esperam dos seus governos e administrações e que é sua obrigação garantir.

E aqui surge um outro problema, o problema dos limites que se colocam ao controlo deste espaço por parte dos Estados, tanto entre si como na sua relação com os seus cidadãos, com particular ênfase no respeito pela sua privacidade.

Ouvimos nesta conferência ilustres constitucionalistas e proeminentes jurisconsultos referir que a regulamentação e o crivo não podem ser concebidos à custa da limitação das liberdades individuais que se encontram constitucionalmente garantidas nas sociedades modernas. Nem podemos omitir que estes espaços constituem hoje, como todos nós reconhecemos, um vasto campo de produção altamente benéfico para a sociedade, gerando cooperação e articulação internacional e permitindo progressos nunca vistos e a um ritmo também nunca visto nas sociedades. Logo, é vital regulamentar com prudência e razoabilidade.

Temos consciência de que, se há algo que podemos extrair das várias preleções ocorridas durante o encontro, como, por exemplo, na intervenção do senhor comodoro Fernando Jorge Pires, é que a existência de questões técnico-jurídicas muito complexas, por um lado, e a presença constante de assuntos estratégicos relevantes, por outro, acabam por gerar, de forma muitas vezes espontânea, confrontos de interesses, especialmente no espaço europeu, na medida em que somos uma Europa

a 27, mas que é somente a 27 nesta geometria da União Europeia, porque, na verdade, passam a 57 Estados quando o âmbito é a OSCE e para mais de 200 quando nos deslocamos para a ONU.

Deste modo, conforme se disse no primeiro painel da manhã, é necessário edificar, *step by step,* um conjunto de medidas de confiança e de regulação que permitam à sociedade aproveitar este magnífico produto da inteligência humana, que é a Internet e o ciberespaço, um espaço criado pela inteligência humana, e que, em princípio, tem todas as condições e os ingredientes para ser um espaço bom para a humanidade, apesar da existência de alguns problemas muito intricados e complexos, como bem referiu, na sessão anterior, o senhor professor Dr. Luís Antunes.

Na verdade, eu concordo com ele. Concordo que a tecnologia acabará, efetivamente, por ajudar a resolver o problema, mas, como eu próprio e ele comentávamos há pouco, acreditamos que não iremos morrer até lá e que não seremos vítimas, de uma forma fatal, deste processo!

O senhor almirante Gameiro Marques centrou bastante a sua intervenção, e muito bem, em questões vitais do papel que este espaço assume não apenas no potenciamento do crescimento económico, mas revelando-se como um espaço estratégico para todo um conjunto de atividades dos dias de hoje e que são decisivas para a sobrevivência da própria espécie. No entanto, é, ao mesmo tempo, um espaço de confronto evidente, sujeito a múltiplas tentativas de o condicionar, como todos os espaços que as sociedades conquistaram e organizaram desde que a Humanidade é Humanidade.

De facto, no passado, muitas guerras, noutros espaços, começaram igualmente nas frentes e nas fronteiras menos conhecidas e menos compreendidas. Portanto, é necessário trabalhar para que este não seja, também, um espaço favorável para a eclosão de novas guerras, conservando, assim, a esperança de que o progresso tecnológico seja, também, um progresso civilizacional.

É justamente neste contexto que gostaria de fazer uma transição para a intervenção de Kristian Vigenin, que foi muito interessante, sobretudo quando ele questiona se é possível ajudar as crianças, os jovens e os adultos a melhorarem a sua capacidade de autodefesa, de serem eles próprios protetores dos seus dados, de serem utilizadores seguros. Afinal, estamos perante algo cuja compreensão é difícil, ou seja, que ainda é preciso compreender bem – como é que funciona este espaço, como é que ele se organiza.

Na ponta final, ouvimos aqui falar de outras facetas do ciberespaço, de um "elefante na sala" que está presente sempre que se debate o ciberespaço, e que é o que habitualmente se designa por *dark net* e *deep net*, que são aqueles espaços cuja utilização só é parcialmente conhecida e que estarão *out of control*.

Como referiu o senhor almirante Gameiro Marques, provavelmente ainda não temos muita consciência do que é que se passa aí, mas debaixo deste tapete estarão certamente coisas muito mais complexas do que julgamos ou podemos imaginar.

A receita que aqui ouvimos de todos é uma receita que, de facto, esteve na base da construção do atual concerto das nações, que começou de uma forma periclitante e que hoje tem organizações consolidadas, como a União Europeia, a própria OSCE, a Organização das Nações Unidas, e que tem uma palavra-chave comum: *cooperação, cooperação, e mais cooperação.* Resulta de um enorme esforço de compreensão mútua, de respeito pelos interesses das partes, e, portanto, tudo isto faz parte de um caminho que, à semelhança de outros caminhos feitos no passado, vamos ter de fazer de ora em diante.

O ciberespaço, como sabemos, está a confrontar as soberanias tradicionalmente definidas, consensualizadas e regulamentadas, e que estão presentes nos instrumentos legais de todos os Estados e em todos os tratados depositados nas diferentes instituições e organizações internacionais, nos mais diversos domínios da cooperação e da segurança comum.

No fundo, estamos perante um novo espaço, um espaço que nos faz lembrar um pouco aquela imagem (pelo menos, nós, os portugueses, temos muito essa imagem) dos velhos e épicos filmes *Western*, muito assente na conquista de um espaço que está completamente em aberto e onde a lei do mais forte se impõe.

Neste momento, temos consciência de que esse, na realidade, é um aspeto que caracteriza o espaço cibernético, e que, portanto, vendo o que nós vimos e o que ouvimos aqui hoje, sobre a diferença de "capacidade de fogo" dos vários países, a começar pelos países onde nasceu a Internet, independentemente de ter surgido primeiro na Europa, como o senhor professor aqui precisou, mas nomeadamente naqueles países que capturaram a tecnologia e que têm hoje a maior capacidade instalada. Constata-se que essa capacidade, como o senhor almirante muito bem referiu, está muito concentrada, e, por isso, estando muito concentrada, isso provoca um desequilíbrio brutal entre os atores em presença, Estados e indivíduos, que é preciso ultrapassar e cujo desequilíbrio é imperioso reduzir rapidamente.

Tudo isto também pode traduzir-se numa outra palavra que o Kristian aqui várias vezes referiu e que é a palavra "confiança". É preciso confiança entre as partes e essa confiança conquista-se, degrau a degrau, com gestos que gerem respeito mútuo.

Para terminar, gostaria de deixar aqui uma nota final e algumas referências a intervenções no período de debate: a primeira diz respeito ao senhor Carlos Carvalho cuja intervenção foi muito interessante. Retive algo que me lembrou outros sectores que não têm que ver diretamente com o ciberespaço, embora o utilizem muito.

Lembrei-me da posição de Portugal no sector automóvel hoje em dia. Nós estamos num patamar concreto da cadeia de valor, que é a indústria de moldes. E temos um valor acrescentado brutal, de tal maneira que hoje não se fala em indústria automóvel no mundo sem falar de Portugal e dos moldes portugueses.

Presumi que estava a dizer qualquer coisa parecida relativamente ao que podemos fazer com os imensos especialistas, como, por exemplo, aquele caso do jovem indivíduo que o professor Luís Antunes aqui referiu hoje de manhã, que foi considerado o *hacker* do ano, ou, como diríamos em Portugal, o "craque" do ano, uma espécie de "Cristiano Ronaldo do sector".

A questão que muitas vezes se coloca é a de saber como aproveitar esse enorme potencial, criando a oportunidade de ele poder direcionar o seu trabalho para os aspetos e aproveitamentos da Internet, a favor de novas conquistas civilizacionais.

Parece-me, também, que este é um caminho desejável e no rumo certo. Não só porque nos permite utilizar essa dimensão para fazermos melhor o que sabemos fazer e podemos fazer, como, especificamente no caso de países como Portugal e outros países de média e de pequena dimensão.

Naturalmente, gostemos ou não, percebe-se que existe uma hierarquia também no ciberespaço, mesmo que ela seja informal e não seja reconhecida nos tratados. Essa hierarquia torna-se evidente quando, por exemplo, uma iniciativa de regulação (ou de desregulação, bem entendido!) do ciberespaço parte de uma grande potência, como os Estados Unidos. Por exemplo, ou, a título meramente exemplificativo, quando essa iniciativa partir de Portugal ou de outro pequeno ou médio país, o impacto e a aceitação são, obviamente, diferentes.

Em suma, tudo isto tem de ser ponderado nesse "jogo de forças", sendo certo que o que está aqui em causa, e eu não gostaria de terminar sem dizer isto, também é que o modelo de funcionamento e utilização do ciberespaço está longe de ser democrático, e o Kristian colocou, e bem, bastante ênfase nesta questão, à semelhança, aliás, de outros intervenientes ao longo do dia.

De facto, é necessário transpor e adaptar ao ciberespaço o modelo de funcionamento de Estados de direito, livres, responsáveis, cooperantes na comunidade internacional, que visam a paz, a concórdia e o progresso.

E isso é que é preciso defender, porque se conseguirmos defender isso e fazer isso, certamente estamos a fazer o bem para cada um de nós, para cada um dos países individualmente considerado, e para o conjunto da comunidade das nações.

É por isso que julgo que esta conferência veio no momento certo e vai constituir um importante contributo para uma reflexão aberta e útil sobre um tema que tanto nos preocupa e que necessita do nosso acompanhamento e da nossa intervenção. Se há coisa que, para mim, ficou clara, é que este não é apenas, nem principalmente, um debate entre técnicos e especialistas, mas sim um debate em que todos temos o dever de participar ativamente.

Para concluir, quero agradecer a todos a paciência com que me ouviram e a atenção que me dispensaram, pedindo desculpa por, eventualmente, a minha síntese não ter sido a melhor ou aquela que esperariam.

A todos, muito obrigado.

JOSÉ MIGUEL MEDEIROS

Well, I'm going to try, although it may be difficult, because the speeches were quite wide-reaching and touched on a lot of points, some of which had also already been raised in the morning.

So, rather than being here to report on what each person said, although I'm going to cite some of the things that were said here, I'll try to make a summary of what we can take away from this session.

All of us know about the origins of borders, physical borders that later established the different sovereignties that are embodied in the states and nations that form the concert of the international community. And those borders, as we know them today, have always been established following struggles, military confrontations over the centuries and, as we know them today, they are also confrontations of those peoples, and of recognition because, in the meantime, over

time, civilisation has been evolving and the international community has been beginning to create rules and peoples have understood that the path of peace and harmony would likely be a more useful and interesting road to follow than the road of constant war.

There is today, however, a new space for potential conflict, for confrontation between the law and crime, between war and peace, between order and chaos, which is called cyberspace, and that is what we have been discussing here today and where we find there are consequences and many new challenges for the field of nations' security and defence.

And it is therefore urgent, as has become clear here, it is urgent to regulate and create rules of usage that in fact make it possible for those who use it to feel safe and have guarantees that such security is in place, as far as possible, for us to be safe. Even in other physical, more tangible spaces, we come across that difficulty.

Absolutely security will likely never exist. But at least security and safety approaching what we have today, in the different tangible spaces we deal with and in which we move.

But, on the other hand, we have also heard from prominent constitutionalists this morning, and prominent specialists, who said that this cannot be done at the cost of unacceptably restricting individual freedoms and the possibility of these spaces also being, as we all acknowledge, spaces that are highly beneficial for society, which have produced cooperation and international links to enable unprecedented progress at an unprecedented pace in societies. It is, therefore, necessary to balance this.

We are aware that, if there is something we can take away from the different speeches, there are issues, as in the first speech we had today from Commodore Fernando Jorge Pires, there are many complex legal questions, there are many highly complex technical questions, there are strategic questions that naturally produce conflicts of interests because, of course, it was stated here this morning, we are a Europe of 27, but that is the 27 of the European Union, which may extend to 57 of we go to the OSCE, and may extend to 200 or more when if look at the UN.

So it is therefore necessary to go, to use an English expression, step by step, to gradually build, as was mentioned in the first panel this morning, confidence-building measures and regulation to enable society to make use of the magnificent product of human intelligence that is the internet and cyberspace, which is a space created by human intelligence, we have to acknowledge that.

And so, in principle, it has all the conditions and all the ingredients to become a good space for humanity.

But it is, of course, going through some complex problems, as Professor Luís Antunes said to us in the previous session; he believed, and I agree with him, that technology will actually end up helping to solve the problem but, as he and I were saying a while ago, over lunch, during the meal, let's hope not to die in the meantime, right? And not become fatal victims of this process.

Admiral Gameiro Marques very rightly focused his speech on vital matters of the role of this space, the enhancement of economic growth, the space is strategic for the entire range of activities that we have today and that are decisive for the survival of the very species; but, at the same time, it is an area of clear confrontation, there are many attempts to restrict it, as in all the spaces that we, let's say, have already conquered and organised ever since humanity became humanity.

It is necessary for the many wars that will likely take place, although we hope not, will begin here just as in the past many wars in other spaces also started on the least known and least understood fronts.

And now I shall shift to Kristian's speech, which was very interesting when he says that, well, but how can we help children and young people and adults, obviously, to improve their self-defence abilities so they themselves be the protectors of their data, they can be safe users, if we are facing something that is hard to understand. In other words, we still need to properly understand how this space works, how it is organised.

In the final point, we heard something, which is probably the elephant in this room, which is the dark net and the deep net, which are those areas that we are still trying to process, still only at the tip of the iceberg, as the Admiral says, we likely are not very aware of what happens there, but under this rug there are probably many much more complex things and so we need to understand.

Well, the prescription we have all heard here is one that, in fact, was at the heart of building the current concert of nations, which had a shaky start but now has mature organisations, such as the European Union, like the OSCE itself, like the United Nations and, of course, it has a common keyword: cooperation, cooperation, cooperation. Mutual understanding, respect for the interests of the parties and, therefore, all of this is a road that must be built.

This space, as we know, is calling into question, in a totally – how can I put it? …I wouldn't say in an absolute way, but in a brutal way – sovereignties as they are traditionally defined, agreed upon and regulated and that are present in the legal instruments of all states and all treaties that are lodged in the different spaces where organisations meet and where international organisations have their headquarters.

But what is true is that this space is still a space that reminds me a little of our idea (at least the idea that we, Portuguese people, have) of cowboy films, of Westerns, of conquering a space that is completely open and that the law of the strongest wins.

We are aware, at the moment, that this is in fact something that characterises cyberspace and that, therefore, seeing what we have seen here, hearing what we have heard here about the different 'firepowers' of different countries, starting with the countries where it emerged, regardless of whether it arose here in Europe, as the Professor stated, but those who capture the technology and today have the installed capacity; we have seen that such a capacity, and the Admiral very rightly drew our attention to this, that capacity is highly concentrated.

And, as it is highly concentrated, there is a massive inequality among the actors present that must be overcome. That inequality must be reduced, and that can also be translated into another word that Kristian mentioned several times, which is the word 'confidence'. We need confidence among parties and that confidence is won over, step by step, through mutual acts in which everyone respects one another. Those who are here also have the right to exist and use it in similar ways.

I wouldn't like to end without mentioning two notes that have actually been made here. One, made by Mr Carlos Carvalho, who said something very interesting here. That reminded me of other sectors that are not directly related to cyberspace, despite using it heavily. I remembered Portugal's position in the automotive sector today. We are at a specific tier in the value chain, which is the mouldmaking industry. And we have massive added value, so that today we cannot talk about the automotive industry in the world without mentioning Portugal and Portuguese moulds.

I assumed that he was saying something similar regarding what we can do with many specialists, such as the one Professor Luís Antunes mentioned here this morning, the young man who won and was considered hacker of the year, or a star, the Cristiano Ronaldo of these things.

That is to say that it does, in fact, seem to me that this is the right path, because this path not only enables us to use our size to do better what we already can or are able to do, but also makes it possible to make other powers, let's call them, or drive them to respect us and also understand the advantage of having us in that position. This is for medium-sized and small countries.

Naturally, whether we like it or not, we understand that there is a hierarchy, even if it is an informal, unacknowledged one. Often, for treaties, there is a hierarchy and it is different when the United States decide to regulate or decide not to regulate, or if it is Portugal that is deciding to regulate or not to regulate, then, the impact is different and, therefore, all this needs to be considered in this game.

It is true that what is also at stake, and I wouldn't like to finish without saying that a model that operates democratically – and Kristian highlighted these matters in his speech, well, everyone did, actually, throughout the day – which means the defence of an operating model for states based on the rule of law and are free, responsible, cooperate in the international community, that aim for peace, harmony and progress.

And that is what must be defended, because if we are able to defend that, and do that, we are surely doing good for each one of us, for each one of the countries considered individually, and for the community of nations as a whole.

And I shall bring things to a close. I don't think I have anything else to say but to thank everyone for their patience and for listening. I apologise if my summary may not have been what you were expecting or may not have been the best.

Thank you very much.

Da esquerda para a direita: Luísa Meireles, Graça Mira Gomes, Luís Campos Ferreira, Makis Voridis e Pedro Verdelho
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04917/2018
From left to right: Luísa Meireles, Graça Mira Gomes, Luís Campos Ferreira, Makis Voridis and Pedro Verdelho
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04917/2018

A AMEAÇA DO CIBERTERRORISMO NO ESPAÇO OSCE
THE THREAT OF CYBER-TERRORISM IN THE OSCE AREA

PEDRO VERDELHO

Boa tarde a todos. Dirijo um especial agradecimento à senhora deputada Isabel Santos por ter desafiado o Ministério Público a estar presente nesta sessão, que se me afigura extremamente interessante e, sobretudo, extremamente importante.

O acaso fez com que esta apresentação fosse antecedida de uma comunicação muito interessante, da qual anotei pontos muito válidos, dos quais gostaria apenas de sublinhar que o senhor deputado palestrante terminou a referir os velhos filmes de *cowboys*, passados no velho faroeste.

Na verdade, o senhor deputado referia-se a fronteiras ou à falta delas. A ideia pareceu-me muito interessante porque no mundo moderno já não há fronteiras. Hoje em dia não há verdadeiras fronteiras. Esta não é uma mera afirmação vaga que fazemos em reprodução de ideias generalizadas só porque sim, em conversa fácil. De modo nenhum: na verdade, os criminosos circulam pelo mundo inteiro. Os seus crimes têm consequências no mundo inteiro. Pelo contrário, quem tem de aplicar a lei não está autorizado a persegui-los livremente pelo mundo inteiro. Recuperando agora a parábola dos *cowboys*, a mesma transporta-nos para a memória daqueles velhos filmes sobre o oeste americano, em que um xerife solitário persegue um bandido a cavalo e, subitamente, chega à fronteira do seu Estado (o Texas, ou o Arizona) e tem de parar porque chega ao limite do seu Estado. Para lá da fronteira, já não tem legitimidade para continuar a perseguição. E o bandido foge.

No contexto das investigações criminais na Internet, nos dias que correm, lamentavelmente, esse paradigma reproduz-se. Aqueles de nós que temos de aplicar a lei, temos de conviver com ele e com as limitações que nos impõe, resultantes da circunstância de vivermos num Estado soberano que tem de respeitar a soberania de outros Estados soberanos.

Porém, estas limitações não se aplicam aos criminosos nem às organizações criminosas que circulam pela Internet e desenvolvem as suas atividades ilegais na rede. Também não se aplicam aos que usam a *dark web* para explorar negócios ilícitos. Como igualmente não se aplicam a empresas privadas, que prosseguem os seus interesses privados, naturalmente legítimos e com certeza com contornos e fins socialmente relevantes, na generalidade dos casos. Também para estas não existem fronteiras, já que hoje em dia lhes é permitido atuar a nível global, em todo o planeta, ignorando por completo as fronteiras e ignorando as soberanias dos Estados.

Destas considerações gostava de retirar uma primeira observação, introdutória, recuperando o que foi dito no painel anterior. Gostava de deixar uma ideia fundamental: a investigação criminal e a possibilidade de a realizar com eficácia mudou de paradigma. Neste aspeto particular, o modelo antigo, baseado na capacidade de o Estado impor a sua lei, extinguiu-se. Vivemos agora num ambiente novo e muito adverso. E é este mundo novo que temos de enfrentar. É sobre este contexto novo que temos de refletir, para podermos resolver os inúmeros novos problemas que nos apresenta.

Esta questão não é nova. O nosso mundo, como o temos hoje em dia, é já o resultado da evolução de séculos. No século XVI ou XVII, Hugo Grócio, na Holanda, inventou a teoria do *mar aberto* por contraponto ao *mar fechado*, que Portugal e Espanha tinham imposto, na sequência do Tratado de Tordesilhas. Hoje em dia vivemos, provavelmente, num *ciberespaço aberto*, ainda à espera de regulação, que ainda não conseguimos consensualizar.

Ao nível da Organização das Nações Unidas, de quem se esperava que dirigisse o diálogo das nações a este propósito, não se tem conseguido avançar. Portanto, a ONU não tem conseguido congregar esforços na resolução dos problemas existentes no *ciberespaço aberto*. E não tem conseguido, antes de mais, porque há interesses muito divergentes, frequentemente contraditórios, entre os vários atores principais do mundo.

A questão suscitada pelo nosso colega de reflexão, presente neste seminário, professor Smirnov, da Rússia, respeitante à soberania dos Estados, revela uma das dificuldades essenciais: apesar de não existirem fronteiras, apesar de a Internet ser omnipresente, há Estados que insistem em manter a sua soberania, tal como ela foi concebida desde o histórico tratado de Vestefália. Esta posição de recondução aos princípios clássicos não é novidade – é invocada a respeito da chamada soberania sobre o ciberespaço, mas não o é de forma isolada, porque é igualmente invocada noutros cenários. A Rússia tem optado por esta linha de discurso, de forma clara e firme, há muito tempo. Além da Rússia, também a China tem seguido esta linha política, insistindo na defesa intransigente da soberania e do seu respeito, nas investigações criminais.

Pelo contrário, em Portugal, como no resto da União Europeia e noutros países do hemisfério ocidental, tem-se assumido que o conceito de soberania evoluiu. Os Estados têm vindo a prescindir de parte daquilo que em tempos incluíam na sua esfera de soberania. Os vários movimentos integradores de Estados em organismos ou entidades internacionais espoletaram a evolução nesse sentido.

Por outro lado, a globalização também deu um forte impulso para o mesmo lado. No presente, assume-se, numa boa parte do mundo, que o conceito de soberania nacional e a capacidade de a exercer são algo completamente diferente daquilo que alguns Estados ainda julgam ter. Assume-se que o conceito se degradou, por exemplo, pela ascensão de sociedades comerciais que, com intuito lucrativo, atuam no mundo inteiro, com mais poder real (e económico, claro) que muitos dos Estados nacionais – e entre eles, muitos dos Estados da Europa. O poder destas sociedades de direito privado – e sobretudo dos chamados *gigantes da Internet* –, obriga-nos a revisitar a noção real de soberania, reequacionando-a.

Um dos campos principais em que o conceito de soberania tem de ser reequacionado é o da investigação criminal. Senão pondere-se um pequeno exemplo: se as legítimas entidades de investigação criminal apreenderem, com observação de todas as regras de direito processual, um telemóvel ou um *tablet* e nele (ou por ele) acederem ao conteúdo do correio eletrónico do suspeito, porventura alojado por um dos tais *gigantes da Internet* (Gmail, Yahoo! ou outro), quiçá num país estrangeiro, estão a violar a soberania do Estado onde tal correio está alojado – Estado esse que, com toda a probabilidade, nem sabe, nem quer saber desse correio eletrónico? A lei portuguesa (Artigo 15.º, n.º 5, da Lei do Cibercrime) autoriza as autoridades portuguesas, em certas circunstâncias, a proceder como se descreveu. Mas não se sabe o que pensam as autoridades dos eventuais Estados onde tal correio esteja alojado.

Estas dúvidas reforçam uma ideia essencial a este respeito que é o papel crucial que assume a cooperação internacional. É evidente que, atualmente, a cooperação entre Estados é essencial no combate aos crimes desenvolvidos nas redes de comunicação e, por isso, também às atividades relacionas com o terrorismo. É também claro que esta cooperação pode superar a insuficiência da ação de Estados isolados. Sozinhos, apenas por si mesmos, os Estados não conseguem enfrentar

os fenómenos criminais que cruzam o ciberespaço – não só aqueles que afetam o próprio ciberespaço, como também aqueles que o usam para fins ilícitos (como o terrorismo).

Que não haja ilusões: qualquer crime cometido no ciberespaço ou por via do ciberespaço é, pela sua mesma natureza, hoje em dia, um crime internacional. Repare-se, por exemplo, no caso muito simples e menos relevante daquela pessoa que utiliza uma conta de correio Gmail, ou Yahoo!, ou Hotmail para ameaçar uma outra pessoa. Mesmo que a pessoa em causa estiver em Portugal e o seu alvo for português, estando ambos em território nacional, sendo, portanto, os factos eventualmente configuráveis num tipo de crime, segundo a lei portuguesa, este crime é *internacional* porque na sua prática se utilizam recursos técnicos que estão localizados fora do país. E, portanto, a recolha de prova do crime tem de realizar-se no estrangeiro, requerendo-se, pois, cooperação internacional.

Este exemplo simples fornece-nos um bom modelo da criminalidade atual: hoje em dia, quase todo e qualquer crime que ocorra, por mais simples que ele seja, pode vir a supor a obtenção de elementos de prova que estão fora das fronteiras de cada país, exigindo, assim, o recurso a mecanismos de cooperação internacional.

E se assim é quanto a crimes mais simples, muito mais o é quanto a crimes complexos e sérios, como os que se relacionam com o terrorismo.

Deste modo, a cooperação internacional é o tópico que me parece mais importante sublinhar nesta sessão, tanto mais que tenho tempo muitíssimo limitado. E neste contexto de crimes nas redes de comunicações, quando se fala de cooperação internacional é incontornável referir a Convenção de Budapeste, ou Convenção sobre Cibercrime do Conselho da Europa.

Trata-se de um tratado internacional muito divulgado, nascido no Conselho da Europa, tendo, portanto, génese europeia. Nasceu na Europa, mas, claramente, hoje em dia, saltou fora das fronteiras da Europa e já não é apenas uma convenção europeia. Com efeito, este tratado chegou já a cerca de um terço dos países das Nações Unidas – nesta data, 61 Estados do mundo inteiro já ratificaram a convenção e há mais dez, ou 12 talvez, no seu caminho para a ratificação. Portanto, mais do que 70 Estados, o que significa mais do que um terço (já a caminho de dois quintos) dos Estados-Membros das Nações Unidas aderiram à Convenção. Além disso, há membros da Convenção de Budapeste em qualquer dos continentes do mundo: países tão distantes como Tonga, países culturalmente tão distantes da Europa como as Filipinas, ou como a Ilha Maurício, ou como o Senegal, ou como o Gana, para não referir já todos os países do hemisfério norte, cobrindo toda a Europa (com exceção de um deles – é público: a Rússia) e cobrindo uma boa parte dos países do continente americano (Norte, Centro e Sul da América) e também alguns países da Ásia.

Apesar de focar o cibercrime, e não especificamente o terrorismo, a Convenção de Budapeste tem tido grande utilidade prática no combate ao terrorismo.

Não vou explorar aqui a temática específica do terrorismo, que não é a minha área de especialidade. Pelo contrário, com muito interesse, no decurso desta conferência, aprenderei mais sobre o tema. Enquanto conceito, aqueles que se dedicam à investigação criminal nas redes de comunicações têm alguma dificuldade de apreender e interiorizar o conceito de terrorismo. Já nos é mais fácil identificar atos de terrorismo.

A Convenção de Budapeste não refere expressamente terrorismo, nem atos de terrorismo. Dela não consta nenhum conceito de terrorismo. Porém, é claramente assumido pelo Comité Cibercrime do Conselho da Europa (Comité T-CY), o qual está encarregado de acompanhar a implementação da Convenção, que o texto da mesma é muito útil no combate ao terrorismo, por três razões: (i) antes de mais, porque a Convenção define como crimes atos que, em si mesmo, podem ser atos de terrorismo; (ii) depois, porque alguns dos crimes previstos pela Convenção servem para *facilitar* (no sentido anglófono) ou para auxiliar a prática de atos de terrorismo; (iii) por último, porque a Convenção de Budapeste inclui normas processuais, isto é, normas de investigação criminal e normas de cooperação internacional em matéria penal que são muito úteis na investigação de casos concretos de terrorismo.

Quanto à primeira razão (a de alguns dos crimes da Convenção de Budapeste poderem ser, eles mesmos, atos de terrorismo), adiantava como exemplos a sabotagem informática, ou o acesso ilegítimo a sistemas informáticos, ou ainda a falsidade informática. Todos estes crimes podem ser praticados num contexto de terrorismo.

No que respeita à segunda razão (alguns dos crimes da Convenção de Budapeste poderem também ser auxiliares de atos de terrorismo), podem avançar-se como exemplo os mesmos crimes. Todos eles podem ser praticados de forma instrumental a ações terroristas mais vastas. E se assim acontecer, o quadro jurídico de enquadramento de tais crimes é, a nível internacional, a Convenção de Budapeste.

Porém, a vertente mais importante da relevância da Convenção de Budapeste a este respeito é a terceira razão acima apontada: a da investigação criminal. É que, quanto a medidas de investigação criminal, várias das normas processuais da Convenção de Budapeste podem ser utilizadas no combate ao terrorismo. A Convenção prevê normas concretas de investigação criminal que não se aplicam diretamente.

Estamos a falar de um tratado internacional e, portanto, supõe-se que cada Estado que o ratificou introduza na sua legislação interna essas mesmas normas. Portugal já o fez, tal como o fizeram 46 de entre os 47 Estados Membros do Conselho da Europa, da mesma forma que muitos outros países do mundo.

Estas normas processuais, tais como, por exemplo, as buscas informáticas, a apreensão de dados informáticos, as preservações de dados informáticos, entre várias outras, podem ser utilizadas na investigação de crimes de terrorismo. Esta utilização pode ser meramente a nível doméstico, em investigações em cada um dos países, mas também permite a cooperação internacional entre Estados.

Neste contexto, gostava de sublinhar em particular uma ferramenta de investigação criminal e de cooperação, com grande potencial na área do terrorismo: a chamada Rede 24/7 de pontos de contacto que está prevista no artigo 35.º da Convenção. Trata-se de uma rede operacional de pontos de contacto com ligação a todos os Estados Parte da Convenção, disponível 24 horas por dia, 7 dias por semana, a qual está vocacionada para o auxílio técnico de uns países a outros, em investigações criminais concretas. Funciona por via do contacto direto e imediato entre os vários pontos de contacto, dos vários países que, por esta via podem trocar informações respeitantes a um caso concreto e pedir mesmo a realização de algumas diligências processuais.

Muito obrigado pela vossa atenção.

PEDRO VERDELHO

Good afternoon. In particular, I would like to thank Mrs Isabel Santos, honourable Member of the Parliament, for challenging the Prosecutor General's Office to attend this session, which I find to be extremely interesting and, above all, extremely important.

Chance led to this presentation being preceded by a very interesting communication, from which I noted very valid points – of the various ones, I would now only like to point out that the honourable speaker ended up referring to the old western cowboys' movies.

In fact, the honourable Member of the Parliament referred to frontiers or lack thereof. The idea seemed very interesting because in the modern world there are no borders. Nowadays there are no real borders. This is not a mere vague statement, which we make reproducing in generalized ideas, without a reason, in easy talking. Not at all: indeed, criminals circulate all over the world. Their crimes have consequences all over the world. On the contrary, those who have to apply the law are not allowed to pursue them freely throughout the world. Reclaiming the parable of the cowboys now, it transports us into the memory of those old American West movies, where a lone sheriff chases a thug on horseback and suddenly arrives at the border of his State (Texas or Arizona) and must stop, because it reaches the limit of the State. Beyond the border, it has no longer the power to pursue the criminal. And the outlaw runs away.

In the context of criminal investigations on the internet, this paradigm is regrettably in the present day. Those of us who have to apply the law have to live with it and the limitations it imposes on us, resulting from the fact that we live in a sovereign State, which has to respect the sovereignty of other sovereign States.

However, these limitations do not apply to criminals or criminal organizations, which circulate on the internet and carry out illegal activities on the network. Nor do they apply to those who use the dark web to explore illicit business. Nor do they apply to private companies, which pursue their private interests, which are naturally legitimate and certainly with socially relevant ends, in most cases. Also, for them there are no borders, since in these times they are allowed to act on a global level, across the planet, completely ignoring the borders and ignoring the sovereignties of the States.

From these considerations, I would like to make a first introductory remark, retrieving what was said in the previous panel. I would like to leave a fundamental idea: criminal investigation and the possibility of doing it effectively changed the paradigm. In this particular aspect the old model, based on the capacity of the State to impose its law, was extinguished. We now live in

a new and very adverse environment. And it's this new world we have to face. It is on this new context that we have to reflect, in order to be able to solve the numerous new problems presented to us.

This question is not new. Our world, as we have it today, is already the result of the evolution of centuries. In the sixteenth or seventeenth century, Hugo Grotius in the Netherlands, invented the theory of the open sea by counterpoint to the closed sea, which Portugal and Spain had imposed, following the Treaty of Tordesilhas. Nowadays, we live, perhaps, on an open cyberspace reality, still awaiting regulation, which we have not yet been able to reach consensus on.

At the level of the United Nations, who was expected to lead the world dialogue in this regard, no progress has been made. Therefore, the UN has not been able to join forces in solving the problems that exist in open cyberspace. And it has failed, first of all, because there are very divergent, often contradictory, interests among the various leading actors in the world.

The question raised by our fellow Member for discussion at the seminar, Professor Smirnov, from Russia, concerning State sovereignty, reveals one of the essential difficulties: although there are no borders, although the internet is omnipresent, there are States that insist on maintaining its sovereignty, as it has been conceived since the historic treaty of Westphalia. This position of renewal of the classical principles is not new – it is invoked as regards so-called sovereignty over cyberspace, but it is not in isolation, because it is also invoked in other scenarios. Russia has chosen this line of speech, clearly and firmly, for a long time. Besides Russia, China has also followed this political line, insisting on the intransigent defence of sovereignty and its respect in criminal investigations.

On the contrary, in Portugal, as in the rest of the European Union and in other countries of the western hemisphere, it has been assumed that the concept of sovereignty has evolved. States have been dispensing with part of what they once included in their sphere of sovereignty. The various integrating movements of States in international organizations or entities have spurred developments in this direction.

On the other hand, globalization has also given a strong impetus to the same side. At the present time it is assumed in a large part of the world that the concept of national sovereignty and the capacity to exercise it are something completely different from what some States still think they have. It is assumed that the concept has degraded, for example, by the rise of commercial companies operating worldwide with aim of profit, with more real (and economic, of course) power than many of the nation States – and among them many States of Europe. The power of these private companies – and above all the so-called internet giants – obliges us to revisit the real notion of sovereignty.

One of the main fields in which the concept of sovereignty has to be re-equated is that of criminal investigation. If not, consider a small example: if legitimate law enforcement agents seize, with observance of all rules of procedural law, a mobile phone or a tablet and access the content of the suspect's email, perhaps stored in one of these internet giants (Gmail, Yahoo!, or other), perhaps in a foreign country, are those agents violating the sovereignty of the State where such mail is stored – a State that in all likelihood neither knows nor wants to know of this email? The Portuguese law (Article 15 (5) of the Law on Cybercrime) authorizes the Portuguese authorities, in certain circumstances, to proceed as described. But it is not known what the authorities of other states may think at this respect.

These doubts reinforce an essential idea in this respect, which is the crucial role of international cooperation. It is clear, today, that cooperation between States is essential in combating crimes developed in the communication networks and, therefore, also in activities related to terrorism. It is also clear that this cooperation can overcome the insufficiency of the action of isolated states: on their own, States cannot cope with the criminal phenomena that develop across cyberspace – not only those that affect cyberspace itself, but also those that are used for illicit purposes (such as terrorism).

Let there be no illusions: any crime committed in cyberspace or via cyberspace is, by its very nature, an international crime. Notice, for example, the very simple and less relevant case of the person using a Gmail, Yahoo Mail, or Hotmail account to threaten another person. Even if the person concerned is in Portugal and his target is a Portuguese, both being in the national territory, and therefore, the facts may be configurable as a type of crime, according to the Portuguese law, this crime is international because in practice resources that are located outside the country have been used. And therefore, the collection of evidence of the crime has to be carried out abroad, thus requiring international cooperation.

This simple example provides us with a good model of current crime: nowadays, almost every crime that may occurs, regardless how simple it may be, may lead to the obtaining of evidence that is outside the borders of the country, thus requiring the use of international cooperation mechanisms.

And if this is the case with simpler crimes, it is much more so than complex and serious crimes, such as those related to terrorism.

International cooperation is thus the most important topic I would like to emphasize in this session, especially since I have a very limited time. And in this context of crimes in the communication networks, when talking about international cooperation it is essential to mention the Budapest Convention, or the Convention on Cybercrime of the Council of Europe.

It is a widely publicized international treaty, born in the Council of Europe, and therefore has a European origin. It was born in Europe, but clearly now jumped off the borders of Europe and is no longer just a European convention. In fact, this treaty has already reached about one third of the United Nations Member States – at this date, 61 States around the world have ratified the convention and there are 10 or 12 more, perhaps, on their way to ratification. Therefore, more than 70 States, which means more than a third of the United Nations countries have acceded to the Convention. In addition, there are members of the Budapest Convention on any of the continents of the world: countries as far away as Tonga, countries culturally as far away from Europe as the Philippines, or as Mauritius, or as Senegal, or as Ghana, all the countries of the Northern Hemisphere, covering all of Europe (except for one of them – it is public: it is Russia) and covering a large part of the American continent (North, Central and South America) and also some countries of Asia.

Despite focusing on cybercrime, and not specifically terrorism, the Budapest Convention has had great practical use in combating terrorism.

I will not address here the specific issue of terrorism, which is not my area of expertise. On the contrary, with much interest, during this conference, I will learn more about the subject. As a concept, those engaged in criminal investigation in the communication networks have some difficulty in apprehending and internalizing the concept of terrorism. It is easier for us to identify acts of terrorism.

The Budapest Convention does not expressly refer to terrorism or acts of terrorism. There is no concept of terrorism. However, it is clearly assumed by the Cybercrime Committee of the Council of Europe (T-CY Committee), which is charged with monitoring the implementation of the Convention, that its text is very useful in combating terrorism, for three reasons: (i) first and foremost, because the Convention defines as criminal offenses acts which in themselves may be acts of terrorism; (ii) later, because some of the crimes provided for in the Convention serve to facilitate or to assist in the commission of acts of terrorism; (iii) finally, because the Budapest Convention includes procedural rules, i.e. criminal investigation standards and international cooperation standards in criminal matters, which are very useful in the investigation of specific cases of terrorism.

As for the first reason (some of the crimes of the Budapest Convention may themselves be acts of terrorism), I would mention as examples computer sabotage, or illegal access to computer systems, or computer forgery. All of these crimes can be committed in a context of terrorism.

As regards the second reason (some of the crimes of the Budapest Convention may also be auxiliary to acts of terrorism), the same crimes can be advanced as an example. They can all be practiced instrumentally to larger terrorist actions. And if so, the legal framework for framing such crimes is, at the international level, the Budapest Convention.

However, the most important aspect of the relevance of the Budapest Convention in this regard is the third of the reasons given above: that of criminal investigation. In terms of criminal investigation measures, several of the procedural rules of the Budapest Convention can be used in the fight against terrorism. The Convention provides for specific criminal investigation rules, which do not apply directly.

We are talking about an international treaty and, therefore, it supposes that each ratifying State introduces in its domestic legislation those same rules. Portugal has already done so, as did 46 of the 47 Member States of the Council of Europe, in the same way as many other countries in the world.

These procedural rules, such as computer searches, the seizure of computer data, the preservation of computer data, among many others, can be used to investigate terrorist crimes. This use may be purely at the domestic level, in investigations in each of the countries, but also allows international cooperation between States.

In this context, I would particularly like to emphasize a tool for criminal investigation and cooperation, with great potential in the area of terrorism: the so-called 24/7 network of contact points, provided for in Article 35 of the Convention. It is an operational network of contact points with links to all States Parties to the Convention, available 24 hours a day, 7 days a week, which is designed to provide technical assistance from one country to another in specific criminal investigations. It

works by means of direct and immediate contact between the various contact points of the various countries which, through this route, can exchange information regarding a specific case and even request that certain procedural steps be taken.

Thank you for your attention.

GRAÇA MIRA GOMES

O ciberespaço é cada vez mais central para o desenvolvimento de políticas de segurança nacionais e para a diplomacia, tendo em vista promover a estabilidade e reforçar a confiança entre os Estados e outros atores de projeção global.

A cooperação internacional sobre matérias de cibersegurança, tanto a nível bilateral como multilateral, assume-se como fundamental. À OSCE, pela sua especialização em questões de segurança em sentido lato, e enquanto fórum de diálogo intergovernamental, caberá assumir responsabilidades acrescidas na área da cibersegurança e assim promover uma maior aproximação das perceções entre os Estados participantes. A começar pela própria perceção do que constitui uma ameaça à cibersegurança, bem assim quanto à definição de prioridades na abordagem a adotar.

A OSCE seguiu, desde os anos 70, uma abordagem global (*comprehensive approach*) da segurança, nela incluindo várias dimensões de igual relevância. Foi das primeiras instituições a fazê-lo. A esse conceito abrangente está associado o da cooperação entre os Estados participantes e do qual todos beneficiam, reforçando, desse modo, o próprio conceito de segurança global e da sua indivisibilidade. Assim, Direitos Humanos e Liberdades Fundamentais, Governação Económica e Ambiental foram – e são – consideradas áreas tão importantes para a paz e a estabilidade como a cooperação político-militar.

É neste conceito global de segurança que nos revemos e é neste quadro geral que se trabalha no dia a dia, no âmbito de uma organização regional de 57 Estados Participantes, de Vancôver a Vladivostoque, que do otimismo inicial se adaptou à necessidade de dar resposta à existência de conflitos na sua área.

A OSCE veio evoluindo, gerindo os diferentes elementos do conceito global de segurança, enfrentando os desafios que se colocaram e correspondendo ao que os Estados participantes dela têm pretendido.

Vejam-se, por exemplo, os trabalhos sobre radicalização, sobre extremismo violento, bem como sobre terrorismo, enquanto prioridade de todos os Estados participantes, e sobre o desenvolvimento social e económico. De salientar que a OSCE tem efetuado uma contribuição abrangente aos esforços internacionais contra o terrorismo liderados pelas Nações Unidas.

Contudo, se a OSCE tem evoluído ao longo dos anos, ela mantém muitas das características funcionais do seu início, em particular o caráter intergovernamental, com o papel crucial da Presidência em exercício na condução dos trabalhos da Organização e na busca do consenso para a adoção das decisões.

Em dezembro de 2017, os Ministros dos Negócios Estrangeiros dos 57 Estados adotaram mais uma decisão em matéria de cibersegurança, reafirmando a necessidade de intensificar os esforços da OSCE para reforçar a confiança e reduzir os riscos de conflito decorrentes da utilização das tecnologias de informação e das comunicações, e recordando anteriores decisões ministeriais, mais substantivas, em que foram elencadas medidas geradoras de confiança. Entre essas medidas, figuram a partilha de informações sobre estruturas nacionais e a designação de pontos de contacto.

Não estive pessoalmente envolvida na preparação deste último texto, mas estou em crer, por recentes experiências em funções de negociação, que o texto correspondeu, no final, ao entendimento possível, talvez com alguma frustração para a Presidência em exercício, que, como seria natural, almejava mais conteúdos. Com efeito, a Presidência austríaca tinha vindo a investir nesta área, tal como estará por certo a fazer a atual Presidência italiana – mas, não obstante a promoção de uma abordagem cooperativa e coordenada a todos os níveis, incluindo a coordenação com as entidades nacionais, nos trabalhos da OSCE, o resultado ficou por certo aquém das suas expetativas e da relevância que o tema merece.

Também nesta área teremos de aguardar para que evoluções políticas permitam um reforço da cooperação, baseada em conceitos e prioridades efetivamente partilhados entre os Estados participantes. No âmbito da OSCE, como noutros fóruns internacionais, não está atualmente consolidada a confiança entre os Estados participantes de forma a permitir avançar na elaboração de recomendações ou, por vezes, até para efetuar os debates.

Contudo, estou em crer que, entre realismo e pragmatismo, pela relevância que o tema "Cibersegurança" assume na atualidade, os trabalhos no âmbito da OSCE poderão vir a progredir.

Onde poderemos assistir a tais progressos?

Nos planos parlamentar, governamental e – cabe particularmente sublinhar – no relacionamento com a sociedade civil.

A sociedade civil poderá assumir um papel preponderante, incluindo no combate ao ciberterrorismo, não apenas no cumprimento do que é um dever de todos os cidadãos (de comunicar crimes às entidades competentes) mas, neste caso, mais com uma responsabilidade passiva, ou seja, com a adoção de práticas seguras de higiene informática e com a devida manutenção dos sistemas de informação à sua guarda.

As potencialidades da OSCE devem, pois, ser exploradas também para abordar entidades não-governamentais, como sejam as universidades, grupos económicos e de reflexão político-securitária, com objetivos informativos, de prevenção e de formação. A Presidência em exercício da OSCE decerto tem margem para continuar a promover iniciativas, incluindo mesmo sobre experiências de parcerias público-privadas.

Conclusão

O reconhecimento político ao mais alto nível de que a cibersegurança é hoje estrategicamente tão importante como a tradicional defesa militar é igualmente o reconhecimento da vulnerabilidade do ciberespaço.

Nesse sentido, o secretário-geral das Nações Unidas vem alertando para os perigos da ciberguerra entre países. António Guterres considerou necessário unir forças e estabelecer redes globais com o intuito de proteger civis. Ofereceu o sistema das Nações Unidas para facilitar o processo de construção de uma proteção abrangente, com vista a eventuais futuros ataques com potencialidades de destruir capacidades militares e civis.

Estas palavras constituem um alerta muito importante e muito forte que não posso deixar de aqui também repercutir.

Obrigada.

GRAÇA MIRA GOMES

Cyberspace is increasingly central to the development of national security policies and diplomacy, with a view to promoting stability and enhancing trust among states and other global actors.

International cooperation on cybersecurity issues is fundamental at both bilateral and multilateral level. The OSCE's specialisation in security with a comprehensive approach and as a forum of intergovernmental dialogue, means it has to take further responsibilities in the area of cyberspace and therefore encourage greater proximity in perceptions among Participating States. Starting with the very perception of what a threat to cybersecurity is, as well as the definition of priorities in the approach to be taken.

The OSCE has followed a comprehensive approach to security since the 70s, including several dimensions of equal importance. It was one of the first institutions to do so. This broad concept is joined by one of cooperation between Participating States, from which everyone benefits, thereby enhancing the very concept of global security and its indivisibility. Human rights and fundamental freedoms, economic and environmental governance have been and continue to be considered as important to peace and stability as political-military cooperation.

We identify ourselves with this global concept of security and it is within this general framework that our day-to-day work is carried out, within the scope of a regional organisation of 57 Participating States, from Vancouver to Vladivostok, which has been adjusted from the initial optimism to the need to find answers to conflicts still existing in its area.

The OSCE has been evolving, managing the different elements of the global concept of security, facing the challenges that have emerged and responding to what the Participating States needed.

Let us look, for example, at the work done on radicalisation, on violent extremism and terrorism, which constitute a priority of all Participating States, and also on social and economic development. It should be noted that the OSCE has made a broad contribution to international efforts against terrorism led by the United Nations.

However, while OSCE has evolved over the years, it keeps many of its initial functional characteristics, particularly its intergovernmental nature, with a crucial role played by the Chair-in-Office in running the Organisation's proceedings and in the search for consensus to adopt decisions.

In December 2017, the Foreign Affairs Ministers of the 57 States adopted another decision on cybersecurity, reasserting the need to intensify the OSCE's efforts to enhance trust and reduce the risk of conflict arising from the use of information and communication technologies and recalling previous, more substantive, ministerial decisions which listed trust-building measures. These measures include the sharing of information on national structures and the appointment of contact points.

I was not personally involved in preparing this text but I believe, based on recent experiences and on previous negotiations' meetings, that in the end the text corresponded to the possible understanding achieved, perhaps with some frustration for the Chair-in-Office which, naturally, was aiming for more. In fact, the Austrian Chairmanship had been investing in this theme, and the current Italian Chairmanship will no doubt be doing the same, but despite the focus on a cooperative and coordinated approach at every level, including coordination with national bodies, in the OSCE's work, the result was certainly below the expectations and below the prominence that the theme deserves.

Also in this area, we will have to wait for political developments which will allow enhanced cooperation based on concepts and priorities that are effectively shared by Participating States. Within the scope of the OSCE, as in other international *fora*, trust among Participating States is not currently entrenched so as to allow recommendations to be drawn up or, sometimes, even to hold debates. But I do believe that, between realism and pragmatism, and due to the importance of the theme "Cybersecurity" at present, work within the OSCE may achieve progress.

Where will we be able to see such progress?

At parliamentary and governmental levels and – allow me to underline it – in the relationship with civil society.

Civil society can play a determining role, including in the fight against cyberterrorism. Not only in fulfilling the duty of any citizen (communicating crimes to the competent judicial bodies) but, in this case, assuming a more passive responsibility, i.e. by adopting safe practices in IT and with the proper maintenance of the information systems in their care.

The OSCE's potential should therefore also be explored and enlarged to approach non-governmental bodies, such as universities, economic groups and political/security think thanks which aim to inform people and provide prevention actions and training. The OSCE's Chair-in-Office certainly has leeway to continue to promote initiatives, even including those that reflect experiences with public-private partnerships.

Conclusion

Political recognition, at the highest level, that cybersecurity is nowadays strategically as important as traditional military defence also means recognition of the vulnerability of cyberspace.

The UN Secretary-General has been warning of the dangers of cyberwars between countries. António Guterres has also considered necessary to join forces and to establish global networks in order to protect civilians. He has offered the United Nations system to facilitate the process of building wide-reaching protection with a view to possible attacks in the future which may have potential to destroy military and civil capacities.

These words constitute a very important and very strong warning that I cannot fail to repeat here.

Thank you.

MAKIS VORIDIS

Muito obrigado! Permitam-me que comece por agradecer a todos o convite, a calorosa hospitalidade, mas também a vossa força e persistência, já que estão aqui desde manhã e esta é uma das últimas intervenções.

Penso que fizeram um bom trabalho, e devo felicitar-vos pela vossa coragem depois de todas estas intervenções. Por outro lado, tenho de agradecer pessoalmente à Isabel Santos por tornar um sonho realidade.

Estive há dez anos neste Parlamento numa visita turística. E quando entrei neste magnífico edifício e, em especial, nesta sala, disse para comigo: "gostava de, um dia, estar aqui como orador". E o sonho tornou-se realidade, graças à Isabel, por isso muito obrigado.

Agora, minhas senhoras e meus senhores, criámos, e eu presido, lidero, a Comissão que criámos, como referido anteriormente, em junho de 2017, na Assembleia Parlamentar da OSCE, e esta foi na verdade a resposta da nossa Assembleia a uma preocupação crescente dos nossos cidadãos, dos nossos eleitorados, no combate a um fenómeno que estava a adquirir e continua a ter enormes dimensões, constituindo uma séria ameaça à segurança dos nossos cidadãos.

Era um período em que os ataques maciços estavam a aumentar, em que havia execuções em massa, no Bataclan, em Estados de toda a Europa, em muitos países, em muitas das nossas capitais, nas nossas cidades, pelo que os nossos cidadãos, os nossos povos, exigiam uma resposta.

Somos uma Assembleia Parlamentar, não um órgão executivo, considerámos que a resposta teria de demonstrar a nossa preocupação, criando-se uma comissão *ad hoc*, e começámos a trabalhar nesse sentido.

A partir desse dia, temos uma grande preocupação. O que podemos fazer para apoiar o combate ao terrorismo? Que medidas práticas pode tomar a Assembleia Parlamentar, o que podemos acrescentar, qual é a nossa mais-valia neste esforço universal? E começámos a trabalhar nestas questões.

Falarei um pouco mais sobre este tema, mas queria apenas que tivessem em mente a nossa preocupação e a forma como abordamos a situação. Assim, a verdade é que todos sabemos agora que o mundo digital está realmente presente.

Em 2018, relatórios mundiais sobre o mundo digital [indicam] que quatro mil milhões de pessoas em todo o mundo utilizam a Internet e que, além disso, mais de três mil milhões de pessoas utilizam as redes sociais, o que é muito importante. O valor total do comércio eletrónico em 2017 atingiu quase 1,5 biliões de dólares.

Assim, naturalmente, neste mundo, a nossa comunidade está a transformar-se rapidamente numa sociedade plenamente digital, com repercussões significativas na segurança. Neste contexto, é fácil perceber por que motivo estão a aumentar os riscos relacionados com o ciberterrorismo.

No ano passado, por exemplo, o ataque Wanna Cry afetou mais de 10 000 organizações, incluindo grandes hospitais e empresas em 150 países de todo o mundo. Além disso, todos testemunhámos como o Daesh e outras organizações criminosas usaram a Internet para disseminar as ideologias radicais e espalhar o medo nas nossas sociedades. O escândalo da Cambridge Analytica foi referido nesta sala, não vou aprofundar esse tema, mas é um outro exemplo.

Deste modo, quando falamos de ciberterrorismo, referimo-nos geralmente à pirataria e à perturbação diretas de redes críticas em linha e à utilização da Internet e das plataformas das redes sociais para forçar a violência e a radicalização, bem como para recrutar diretamente terroristas.

Pode parecer que estou a apresentar apenas mais algumas definições. No entanto, as definições são importantes no nosso trabalho. E falarei sobre esse assunto. É que, na minha opinião, e temos de ser sinceros entre nós, esta é uma das principais questões no plano político. E esta questão, como muito bem referiu o senhor procurador, foi intencionalmente excluída de muitos documentos da comunidade internacional. E porquê? Porque a sua inclusão tem grandes implicações políticas.

No nosso esforço para agrupar o máximo possível de países, tentamos evitar este debate. Tentamos evitá-lo porque, se assim não fosse, os países não estarão todos unidos, já que não conseguem chegar a acordo sobre este tipo de definições.

Contudo, como explicarei mais à frente, estes pontos são essenciais, sobretudo quando falamos não de questões em que todos chegamos facilmente a acordo, em que a unanimidade é muito fácil, por exemplo, a pirataria, em que é fácil chegar a um consenso, mas quando passamos a questões mais delicadas, questões relacionadas, por exemplo, com a radicalização, o extremismo violento e o recrutamento. Aqui, como sabem, temos de encontrar o equilíbrio entre o problema e a proteção da liberdade de expressão.

E, uma vez que, nestes crimes, a Internet é apenas uma plataforma onde as pessoas conversam entre si, estamos no cerne da questão da liberdade de expressão. Por conseguinte, temos de tomar decisões. Talvez ainda não estejamos preparados, talvez não tenhamos a convicção de que já construímos um consenso. No entanto, a dada altura, teremos de tomar decisões. E alguns países já o fizeram.

A Bélgica tomou decisões, porque tem de enfrentar esta preocupação crescente. Por exemplo, para dizer a verdade, foi um choque para todos nós perceber que milhares dos nossos cidadãos saíam da Europa para a Síria, para aderir ao EI, combater naquela região, cometer as atrocidades que o EI comete – torturar pessoas, matar pessoas, humilhar pessoas –, e agora

estão a regressar. Os combatentes estrangeiros, estas pessoas estão a regressar. Mas deixaram os nossos países, os nossos cidadãos, para viver lá. É natural, portanto, que tenhamos ficado chocados.

O papel da Internet no recrutamento, na disseminação dos discursos de ódio, na disseminação da propaganda é uma questão central. Por esse motivo, teremos de a enfrentar de uma forma ou de outra.

Falarei agora dos domínios mais problemáticos, em que são necessárias medidas urgentes. Para combater o ciberterrorismo de uma forma mais abrangente, é da máxima importância aumentar a [variedade] de partes interessadas e incluir os interlocutores relevantes do setor da cibernética e das TIC.

Este aspeto foi referido, creio, pela senhora secretária-geral, e muito bem, e é necessário perceber que um instrumento poderoso neste contexto é a criação de uma parceria público-privada forte, sendo uma coordenação estruturada com as empresas das TIC fundamental para se entender melhor e abordar adequadamente os desafios tecnológicos que enfrentamos.

Dois casos significativos neste contexto são o fórum mundial da Internet para lutar contra o terrorismo (*Global Internet Forum to Counter Terrorism*, GIFCT), que inclui grandes empresas, nomeadamente Google e Facebook, e a plataforma de tecnologia contra o terrorismo (*Tech Against Terrorism*).

Enquanto o GIFCT trabalha em soluções tecnológicas para ajudar a impedir a utilização da Internet para fins terroristas, a segunda plataforma visa reforçar as capacidades de empresas de TIC de menor dimensão neste âmbito. E penso que este é um aspeto crucial. Os terroristas teriam claramente como alvo preferencial as pequenas e não as grandes empresas.

Em segundo lugar, como tenho vindo a referir, é importante não pormos em causa as nossas liberdades fundamentais na proteção da segurança dos cidadãos. E esta é uma afirmação natural, todos estamos de acordo neste ponto.

Contudo, mais uma vez, se pensarmos no terreno e tivermos de tomar decisões, teremos de fazer escolhas sérias, enquanto legisladores, teremos necessariamente de fazer escolhas sérias e difíceis.

Não poderemos dormir tranquilamente quando tivermos de tomar decisões deste tipo. Estamos a falar de propaganda terrorista em linha. Cumprir os dois objetivos exige novas formas de pensar sobre que conteúdo deve ser proibido. Que conteúdo deve ser proibido? Em alguns casos, será uma escolha muito fácil. Noutros, será difícil decidir.

Senhor procurador, o que fazemos se alguém elogiar os crimes do EI? Mas, por outro lado, se não fizer nenhum apelo? Essa pessoa está ou não a cometer um crime? Afinal, elogia os crimes. Talvez esteja a cometer um crime, talvez não. Em determinadas legislações sim, noutras não. E se essa pessoa fizer um apelo à adesão? O apelo não teve sucesso. Foi apenas uma tentativa, mas não temos um ato consumado. E se tivermos pessoas com um discurso radicalizado? Mais uma vez, devem ser punidas pelos crimes que cometem? E afirmar que tem de haver alguma reação? Como enquadramos essa afirmação? Trata-se de liberdade de expressão? Ou estamos perante um caso de propaganda?

Por conseguinte, temos decisões difíceis a tomar. Mas temos de tomar estas decisões e assumir uma posição clara no combate ao terrorismo. Além disso, todos entendem que é necessário reforçar os canais de partilha de informação aos níveis local, nacional, regional e internacional.

O objetivo é assegurar um intercâmbio regular e fiável de dados operacionais com vista a melhorar os mecanismos de prevenção e resposta na luta antiterrorista.

Minhas senhoras e meus senhores, creio que temos pela frente tempos muito, muito exigentes. No tratamento desta questão, devemos ser corajosos e arrojados, e temos de estar empenhados no combate ao terrorismo. Esperamos, na AP OSCE, poder acrescentar valor aos esforços já desenvolvidos pela comunidade internacional. Muito obrigado.

Muito obrigado, Isabel, por este sonho tornado realidade.

MAKIS VORIDIS

Thank you very much, and let me start by thanking you all, for the invitation, for the warm hospitality, but also for your strength and stamina, since you're here since the morning and this is one of the last speeches.

I think you've handled it quite well, so you have to be congratulated for your courage after all these speeches. And another thing is, I have to personally thank Isabel Santos for making a dream come true.

I was ten years ago here visiting this Parliament as a tourist. And when I entered this wonderful building and especially this room I said: "well, I'd like sometime in my life to come here and give a speech". And here it became true, thanks to Isabel, so thank you so much.

Now, ladies and gentlemen, we have created, I am presiding, I am leading the committee we have created, it was mentioned earlier, at 2017, June, at the Parliamentary Assembly of OSCE, and this was actually the response that our Assembly has made towards a growing concern of our citizens, our electorates, against a phenomenon that was taking and has actually huge dimensions and poses a serious threat to the security of our citizens.

It was the time where the massive attacks was evolving, we had massive killings, in Bataclan, we had the States all over Europe, many countries, many of our capitals, in our cities, so our citizens, our people demanded a response.

We're a parliamentary assembly, we're not an executive body, we thought the response would be to show our concern by creating and ad-hoc committee and we started working on that issue. From that day, we have one major concern. What can we do in order to contribute to the fight against terrorism? What is the practical thing that the Parliamentary Assembly can do, what could we add, what is the added value in this universal effort? So, we started working on that.

I'll tell you a bit more about that, but I just wanted you to have in front of you our concern and the way we approach things. So, the truth is that yes we all know now that, you know, the digital world is actually present.

In 2018 global digital reports indicate that four billion people around the world use the internet, in addition, more than three billion people use social media, very important, the total value of e-commerce in 2017 reached almost 1,5 trillion US dollars.

So this world, our community is quickly transforming into a fully digital society with important security implications. Now, against this backdrop is self-evident why the risks related to cyberterrorism are growing.

Last year, for instance, the Wanna Cry attack impacted more than 10 000 organizations, including major hospitals and companies in 150 countries around the world. In addition, we have all witnessed how Daesh and other criminal organizations have used the web to disseminate the radical ideologies and spread fear in our societies. The Cambridge Analytica scandal has been referred in this room, so I'm not going into that, but this is also another example.

So, when we are talking about cyberterrorism, we usually refer to the direct hacking and disruption of critical online networks and the use of internet and of social media platforms to force their violent and radicalization as well as to directly recruit terrorists.

This might appear just as some additional definitions. But definitions in our line of work do matter. And I will come to that issue. Because in my view, politically, and we have to be frank among us, this is one of the key issues. And this issue, as the prosecutor very correctly addressed, very purposely is not addressed in many texts of the international community. And why it's not that? It is that because this has high political implications.

We try to regroup as many nations together, we try to avoid this debate. We try to avoid it, otherwise they're not going to be all together, because they cannot agree on this kind of definitions.

But as I will explain later, those are key points, especially when we're talking not, let's say, on issues where we could very easily agree, and theirs is a very easy unanimity on this, like hacking, of course, this is something easy to agree on, but when we move to more delicate issues, issues that are related, for example, with radicalization, with violent extremism, with recruitment, then, we have, you know, to see the balance with the question and the protection of the freedom of speech.

Since, for these crimes, the internet is just a platform where people talk, we are the core of the issue of the freedom of speech. So, then we have to make decisions. Maybe we're not ready yet, maybe we don't feel we have built the consensus yet. But at a certain point we will have to make decisions. And some countries have.

Belgium has made decisions, because they face this growing concern. For example, to tell you the truth, we were all shocked when we found out that thousands of our citizens were leaving Europe to go to Syria and join Isis, fight there, do these atrocities they did, torture people, kill people, humiliate people, and now they're coming back. Foreign fighters, these guys, they are coming back. But they have left our countries, our citizens, to go there. So, of course we were shocked.

And the question there of the role of the internet into recruitment, into disseminating hate speeches, into disseminating propaganda, this kind of questions are the core. So, we will have to address these issues one way or the other.

Now, challenge areas, where action is urgently required. To address cyberterrorism more comprehensively, it is paramount to grow the [variety] of stakeholders involved and include the relevant counterparts from the cyber and the ICT sector.

This has been mentioned, I think, by the Secretary-General, quite correctly, and one has to understand that a powerful tool in this context is the creation of a strong public-private partnership, a structured coordination with ICT companies paramount to better understand and to properly address the technological challenges we're facing.

Two cases in point are the Global Internet Forum to Counter Terrorism (the GIFCT), which includes major companies, Google and Facebook, and the Tank Against Terrorism platform.

While the GIFCTs are working on technological solutions, to help thwart terrorist use of the internet, the second platform aims at building capacity for smaller ICT companies, on this issue. And I think that's a crucial one. Terrorists would much more prefer smaller companies than big ones.

Second: as I've been saying, it is important that we do not compromise our fundamental freedoms while safeguarding the security of the citizens. And this is an easy proposition, you know, we could all agree on that.

But again, if we put it on the field, on the field, and we have to make decisions, there you will have to make some serious, as law makers, you're going to have, we're going to have to make some very serious and difficult choices.

We won't sleep easily at night when we have to decide on these issues. We're looking at online terrorist propaganda. Meeting both objectives requires new thinking. On what is the content to ban? What is the content to ban? In some cases it will be very, very easy. In some other cases, you can't easily decide.

Prosecutor here, what if someone praises Isis's crimes? But on the other hand, makes no appeal. Does he commit a crime or not? He does praise the crimes. Maybe he does, maybe he does not. In some legislation he would do, in some others, not. What if he has made a call to join? The call was not effective. He just had an attempt there. But we don't have a complete act. What if we have people using radicalized speech? Again they should be punished for the crimes they do. And saying that there must be some reaction. Where do you put that? Is it freedom of speech there? Or do you see a case of propaganda?

So, we have difficult decisions to make. But we must make these decisions and we must take positions and we must take a clear position in fighting terrorism. And also, everyone understands that, there's a need to strengthen information sharing channels at local, national, regional and international levels. This is to ensure regular and reliable exchange of operational data aimed at enhancing counterterrorism preventive and response mechanisms.

Ladies and gentlemen, I think that ahead of us we are having very, very challenging times. In dealing with this issue, we must be brave, we must be courageous and we must be dedicated in combating terrorism. And we hope, in the OSCE PA that we will be able to add some value to the effort already being made by the international community. Thank you very much.

Thank you, Isabel, for a dream come true.

LUÍS CAMPOS FERREIRA

Muito obrigado, Luísa. Penso que as intervenções, que desde já agradeço, dos senhores oradores foram muito interessantes, e muito completas, por isso, cabe-me não estragar aquilo que foi feito.

De uma forma muito sucinta, queria fazer apenas dois ou três sublinhados, que serão pontos comuns àquilo que foram as intervenções dos senhores oradores.

O primeiro é que estamos perante um mundo novo. Um mundo novo que gera comportamentos novos e onde não há fronteiras. Um mundo novo que tem, como todos os mundos novos, virtualidades e complexidades, vantagens e problemas. Um mundo novo que tem o lado bom de permitir pluralidade de ideias, intercâmbio de culturas. Um mundo novo que permite uma comunicação mais fácil, que tem um lado que permite organizar crimes com outra facilidade para quem os organiza, e com outra dificuldade para quem tem de os evitar.

E os crimes são variados. Foram citados aqui alguns tipos de crimes, desde corromper dados, e desativar estruturas físicas e promover ataques terroristas, através deste espaço. Portanto, é esse mundo novo que nos leva a novos comportamentos, que obriga a um maior entendimento entre os Estados. Ou seja, o conjunto de convenções e cooperações que existem ainda não permitem dar uma resposta suficientemente forte e musculada àquilo que são as adversidades que este mundo novo nos coloca.

Por outro lado, os Estados também têm dificuldades em ultrapassar algumas questões a questão da soberania, por exemplo, como ouvimos nesta última reflexão e que foi promovida no debate. Isso vai ter de constituir um desafio que leve os Estados a entenderem-se melhor, a entenderem-se de uma forma mais eficaz, mas a entenderem-se também com um cuidado, que foi aqui salientado, que é garantir que este mundo novo, que este novo palco, continue a ser um espaço de liberdade, mas também um espaço que possa dar segurança às pessoas, nas mais diversas áreas.

E é esta conciliação, muitas vezes, entre o direito à liberdade individual, o direito à privacidade e o direito à segurança que pode dificultar uma regulamentação jurídica, mesmo que não seja transnacional, que seja só nacional. E é o que me parece mais importante salientar das intervenções destes senhores oradores.

Muito obrigado à senhora embaixadora e secretária-geral, muito obrigado ao senhor presidente da Comissão Ad-Hoc para o Combate ao Terrorismo, muito obrigado ao senhor procurador, e que seja muito feliz e muito eficaz na difícil missão que lhe cabe. Muito obrigado à nossa jornalista, Luísa Meireles, por ter vindo ao Parlamento moderar este importante debate.

LUÍS CAMPOS FERREIRA

Thank you, Luísa. I think that the speeches, which I am grateful for, by the speakers have been very interesting and very complete, so it is up to me not to spoil what has been done.

And so I would like to very briefly highlight two or three things. And these things will be points common to the speeches that the speakers have made.

The first is that we are dealing with a new world. A new world that produces new behaviour where there are no borders. A new world that has, like all new worlds, virtualities and complexities, advantages and problems. A new world that has the good side of allowing for a plurality of ideas, exchange of cultures. A new world that enables easier communication, but this is also a world that has a side allowing crimes to be organised more easily by those who organise them, and harder for those who have to avoid them.

And the crimes are varied. Some types of crimes have been mentioned here, from corrupting data, deactivating physical structures, promoting terrorist attacks, using this space. And that is why it is that new world that drives us towards new behaviour, which forces greater understanding among states. In other words, a range of conventions and cooperation that exist do not yet enable a response that is strong and powerful enough for the adversities that this new world puts in our path.

On the other hand, states also have difficulties in overcoming some issues. The issue of sovereignty, for example, as we heard in this last observation, which was developed in the debate. This will have to form a challenge that drives states to get along with each other better, to get along with each other more effectively, but also to get along with each other carefully, which was emphasised here, which means guaranteeing that this new world, that this new stage, remains a space of freedom, but also a space that can provide people with security in many different fields.

And it is that conciliation, often between the right to individual freedom, the right to privacy and the right to security that may hinder legal regulation, even if it is not transnational, even if it is only domestic. And that's what seems most important to me to highlight from the speeches by these speakers.

Thank you very much, Ambassador and Secretary-General, thank you, Chair of the Ad Hoc Committee on Countering Terrorism, many thanks to the Public Prosecutor, and may he be very happy and effective in his difficult mission. Many thanks to our journalist, Luísa Meireles, for coming to the Parliament to moderate this important debate.

Da esquerda para a direita: Marcos Perestrello, Miguel Santos e João Soares
Foto de André Pereira, 2018 ©Arquivo Fotográfico da Assembleia da República, GAR 04919/2018
From left to right: Marcos Perestrello, Miguel Santos and João Soares
Photo by André Pereira, 2018 ©Parliamentary Photographic Archive, GAR 04919/2018

ENCERRAMENTO
CLOSING SESSION

MARCOS PERESTRELLO

Minhas senhoras e meus senhores,

É hoje uma realidade indiscutível que o mundo está mais interconectado e interdependente, ou seja, globalizado, e que as nossas sociedades estão cada vez mais digitalizadas.

À infraestrutura física, tecnológica e informacional que acelerou a digitalização e a inter-conectividade das sociedades, a uma escala verdadeiramente mundial, designamos hoje ciberespaço. É através desse ciberespaço, sem geografias, ou fronteiras definidas, que a globalização das economias e das sociedades se aprofunda a passo cada vez mais acelerado. Exemplo disso são alguns dos seguintes indicadores:

- De acordo com relatórios internacionais, a largura de banda utilizada no ciberespaço aumentou 45 vezes desde 2005 e é expectável que se multiplique por um fator de dez nos próximos cinco anos;
- Existem neste momento mais de 4 biliões de seres conectados à Internet e a expectativa é serem 7 biliões em 2020, ou seja, mais de 80% da população mundial;
- Cerca de 400 milhões de seres humanos utilizam as facilidades de comércio eletrónico internacional;
- Os dispositivos ligados e controlados remotamente pela Internet, ou seja, a *internet of things*, aumentarão para cerca de 100 biliões até 2020, criando um sistema de sistemas que vão desde as fábricas às empresas, passando pelas nossas casas, cujo tronco nervoso central será o ciberespaço;
- Verifica-se um incremento vertiginoso de novas formas de organizar o processo produtivo e serviços, como sejam os modelos Uber, AirBnB, Amazon, Ali-Baba, E-Bay, entre outros.

Faço esta introdução para constatar o óbvio – o ciberespaço passou a ser central ao desenvolvimento da economia global e à própria sociedade humana, tornando-se, assim, num espaço comum da humanidade, como o mar, o ar e o espaço exterior.

Todos os espaços comuns da humanidade são sujeitos a tensões que resultam de interesses ilegítimos e particulares de atores estatais e não estatais. No entanto, o interesse do próprio espaço para a comunidade global supera, a prazo, qualquer tentativa unilateral de domínio, controlo, ou utilização disruptiva.

Nesse sentido, como se fez para o mar, um dos passos mais relevantes para a sua defesa, enquanto bem comum, será uma regulação que vincule os diversos agentes que nele atuam, com regras claras que imponham uma ética de partilha e corresponsabilização.

Proponho mesmo que concluamos que a maior defesa da resiliência digital de Estados democráticos, com a dimensão e massa crítica de Portugal, passará certamente pela regulação internacional do ciberespaço.

O país deverá, em todos os *fora* em que participa, incluindo as alianças onde se insere, lutar pela regulação internacional desse espaço. Apenas desta forma, países pequenos e médios, da nossa dimensão, poderão usufruir das vantagens e oportunidades do ciberespaço e da economia e sociedade digitalizadas, em igualdade de circunstâncias com Estados e organizações mais poderosos.

Num contexto puramente nacional, o Estado e a Sociedade devem promover as suas capacidades de forma a garantirem o livre acesso ao ciberespaço e à economia global, a preservação da informação de interesse nacional, a infraestrutura de comunicações e dados e o funcionamento dos sistemas conectados, ou dependentes do ciberespaço. O livre e seguro acesso ao ciberespaço é, hoje, sinónimo de desenvolvimento económico e social.

Neste quadro parece-me relevante para Portugal uma concentração de capacidades e uma forte organização da sociedade nacional numa rede comum de defesa e segurança no ciberespaço. Essa rede terá de implicar necessariamente as forças armadas, as forças de segurança, os serviços de informações, a Administração do Estado, o sector empresarial, as universidades e centros de investigação nacionais.

A resiliência do Estado no mundo digital dependerá de reações rápidas e decisivas, do desenho, teste e da formalização de planos de contingência, da flexibilidade e adaptabilidade permanente às ameaças e da monitorização permanente do ambiente no ciberespaço.

Essa monitorização e reação requererão uma forte partilha de informação nacional e internacional com a abrangência e a capilaridade suficientes para defender um perímetro complexo e hiperconectado. No entanto, importa garantir a essência das nossas sociedades democráticas, a liberdade individual. Fenómenos como o terrorismo e o crime organizado, que utilizam o ciberespaço e a digitalização da sociedade, têm criado tensões que levam a colocar em discussão direitos e garantias associados à liberdade individual, e que me parecem desfocadas e perigosas.

A banalização das escutas ou a permissividade com que se aceitam comportamentos cerceadores da liberdade individual em nome da segurança e da defesa podem significar um caminho mais curto e eficaz no curto prazo, certamente tentador, mas necessariamente prejudicial ao nosso modelo de sociedade e à liberdade tão arduamente conquistada.

Uma sociedade só será capaz de evoluir se enfrentar os novos desafios sem comprometer os seus princípios, pois nada prova que não existam caminhos alternativos que compatibilizem as necessidades e os ideais.

Um dos caminhos passará certamente por fomentar uma cultura de segurança na utilização do ciberespaço, através da implementação de boas práticas no Estado e nas empresas, assim como introduzir essas mesmas preocupações no sistema formativo do país, na preparação das futuras gerações.

Em resumo, considero a resiliência digital do Estado democrático um assunto da maior relevância com implicações na forma como a sociedade portuguesa aproveitará a digitalização e a globalização da economia, não perdendo oportunidades nem, por outro lado, vulnerabilizando-se.

MARCOS PERESTRELLO

Ladies and gentlemen,

It is undeniably true that the world today is more interconnected and interdependent, in other words, globalised, and that our societies are increasingly digitised.

The name we now give the physical, technological and informational infrastructure that has accelerated the digitisation and interconnectivity of societies at a truly global scale is cyberspace. It is through this cyberspace, free from geography or defined borders, that the globalisation of economies and societies becomes greater at a faster and faster pace. The following indicators are examples of this:

- According to international reports, the amount of bandwidth used in cyberspace has grown 45 times larger since 2005 and it is projected to increase by an additional ten times over the next five years;
- There are currently 4 billion people connected to the internet and there are expected to be 7 billion in 2020, in other words, 80% of the world population;
- Roughly 400 million human beings use international e-commerce facilities;
- The number of devices that are connected to and remotely controlled via the internet, the internet of things, will rise to 100 billion by 2020, creating a system of systems that range from factories to companies and passing through our homes, the central nervous system of which will be cyberspace;
- There has been a staggering increase in new ways of organising the production process and services, such as the models used by Uber, AirBnB, Amazon, Ali-Baba, eBay, etc.

I make this introduction to state the obvious, which is that cyberspace has become central to the development of the global economy and human society itself, therefore becoming part of the commons of humanity, like the sea, air or outer space.

All the commons of humanity are subject to the tensions that arise from illegitimate, private interests of state or non-state actors. Nonetheless, the interest of the space itself for the global community will, over time, overcome any unilateral attempt for dominance, control or disruptive use.

So, as was done for the sea, one of the most important steps for defending it as part of the commons is to regulate it, as a way of holding the different actors that operate within it responsible, with clear rules that impose the ethics of sharing and co-responsibility.

I can therefore conclude that the best defence for the digital resilience of democratic States with the size and critical mass of Portugal will certainly involve the international regulation of cyberspace.

The country should, then, in all the areas in which it participates, including the alliances of which it is part, struggle for international regulation. That is the only way that small and medium-sized countries, the size of ours, can enjoy the advantages and opportunities of cyberspace and the digital economy and society on an equal footing with more powerful states and organisations.

In a purely domestic setting, the state and society should enhance their capacities in order to guarantee free access to cyberspace and the global economy, the preservation of intelligence of national interest, communications and data infrastructure and the operation of systems connected to or dependent on cyberspace. Free, safe access to cyberspace is, today, synonymous with economic and social development.

In this framework, it seems to me that it is important for Portugal to concentrate capacities and implement extensive organisation of national society into a common network of defence and security in cyberspace. That network will have to involve the armed forces, the security forces, intelligence services, the administration and the state, the business sector and national universities and research centres.

The resilience of a state in the digital world will rely on rapid, decisive reactions, and the design, testing and formalisation of contingency plans, constant flexibility and adaptability to threats and the permanent monitoring of the atmosphere in cyberspace.

Monitoring and reaction will require extensive sharing of national and international intelligence with enough scope and breadth to defend a complex, hyperconnected area. Nonetheless, it is important to guarantee the essence of our democratic

societies: individual freedom. Phenomena such as terrorism and organised crime that use cyberspace and the digitisation of society have created tensions that call on us to discuss rights and guarantees connected to individual freedom and appear to me to be unfocused and dangerous.

The trivialisation of wire tapping, the laxness with which behaviours that restrict individual freedom are accepted in the name of security and defence may mean a shorter and more effective path in the short term, which is certainly tempting, but it will be harmful to our model of society and our so hard-won freedom.

A society will only be able to evolve if it can face new challenges without compromising its principles, since nothing proves that there are no alternative routes that match needs and ideals.

One of the paths will certainly involve encouraging a culture of security in cyberspace use by implementing best practices within the state and companies, as well as introducing those same concerns to the country's training system when preparing future generations.

In short, I believe that the digital resilience of a democratic state to be a highly important matter with implications for the way Portuguese society will make use of the digitisation and globalisation of the economy, without missing opportunities or, on the other hand, becoming vulnerable.

JOÃO SOARES

Agradeço ao presidente em exercício, meu amigo e meu colega na Assembleia Parlamentar da OSCE e no Parlamento português, Miguel Santos, ter-me dado uso da palavra.

Queria, em primeiro lugar, dirigir-me ao presidente da Assembleia Parlamentar da OSCE, e meu amigo, George Tsereteli, para lhe sublinhar o prazer que tenho em estar aqui hoje a vosso convite. Quando a nossa comum amiga, e vice-presidente, Isabel Santos, me transmitiu, ela e Nilza de Sena, o convite para aqui estar, eu fiquei imediatamente extremamente contente pela possibilidade de reencontrar velhos amigos de tantos combates que travámos em nome dos valores que são os valores da OSCE.

Sei que a conferência correu bem, não pude cá estar durante a manhã, mas tenho o maior prazer em estar aqui hoje convosco e em felicitar-vos, como, aliás, fez o secretário de Estado, Marcos Perestrello, com uma intervenção boa em que fez uma panorâmica sobre este conjunto de questões, de uma forma completamente clara e penso que absolutamente sincera.

Eu costumava dizer, quando tive responsabilidades na Assembleia Parlamentar da OSCE, que nós temos o melhor secretariado que eu já vi a funcionar no mundo. E, portanto, saúdo também o secretariado da Assembleia Parlamentar na pessoa do meu amigo e velho colega de trabalho, Roberto Montella, na pessoa do Gustavo Palhares, que ali está em cima, na pessoa do embaixador Andreas Notella, com quem estive já na sexta-feira, e que é também um veterano da Assembleia Parlamentar, na pessoa do Andreas Baker, que não vejo aqui, mas que provavelmente estará aqui, ou estará noutro lado qualquer a trabalhar para a Assembleia Parlamentar da OSCE, e lembrando os exemplos de dois veteranos, o Spencer Oliver e a Tina Schön, que tiveram um papel determinante neste modelo de funcionamento que eu continuo a considerar um modelo absolutamente exemplar e talvez mesmo único no mundo.

Uma equipa muito pequena, de gente muito eficaz, com um orçamento muitíssimo reduzido, e que faz um trabalho admirável. E que está na ponta daquilo que é o trabalho que a própria Organização de Segurança e Cooperação Europeia tem feito, desde que existe.

Como saberão, a Assembleia Parlamentar começou uns anos depois da Ata Final de Helsínquia, em agosto de 1975, portanto, uns anos depois da criação formal da Organização de Segurança e Cooperação Europeia, que se transformou de uma conferência, uma conferência permanente, numa organização.

Contudo, é, como disse muito bem um grande embaixador português que representou Portugal na OSCE, o embaixador Seixas da Costa, uma "sedimentação relutante" de uma conferência em organização. E eu acho que isso dá a medida e dá as potencialidades que são as mais-valias que a OSCE trouxe ao cenário internacional.

Há pouco, o meu amigo pessoal, não político, Luís Campos Ferreira, sublinhou isso: neste mundo controverso e de mudança e conflitos permanentes que estamos a viver, o papel da OSCE continua a ser, e pode ser, e tem sido muitas vezes (outras vezes tem estado aquém), um papel absolutamente decisivo na construção da paz e da cooperação internacional. E, dentro da OSCE, a Assembleia Parlamentar tem tido sempre, digamos, que um papel pioneiro.

E, mais uma vez, ao tratar as questões da cibersegurança, são questões de primeira grandeza neste mundo conturbado em que vivemos.

Eu acho que é nessa linha que a Assembleia Parlamentar tem de continuar. Longe de mim recomendar o que quer que seja. A experiência que tive aqui foi uma experiência muito rica e muito gratificante. Sinto-me muito honrado por ter tido a possibilidade, sempre muito modestamente, de desempenhar aqui funções, em contextos que foram contextos complicados, de conflitos às vezes bem complexos.

Estou a lembrar-me, por exemplo, da crise da Ucrânia, onde estivemos em Donetsk na véspera das eleições legislativas na Ucrânia, que elegeram o presidente Porochenko.

Estou a lembrar-me de muitos outros países, da Bielorrússia, do Cazaquistão, onde a Nilza de Sena e eu estivemos no final de umas eleições, que foram eleições controversas, e onde tivemos de dar a conferência de imprensa no dia seguinte, para a avaliação do processo eleitoral. Não foi fácil, mas foi qualquer coisa que nos deu uma imensa satisfação.

E, sobretudo, estou a lembrar-me de uma ida a Odessa. Muita gente não queria que nós o fizéssemos numa certa altura, quando as coisas estavam mais complicadas na Ucrânia, ou começavam a estar mais complicadas na Ucrânia. Nós lá fomos, sempre numa lógica de fidelidade aos valores da Ata Final de Helsínquia, de 1975. Foi aquilo que há pouco o Luís Campos Ferreira sublinhou, e que o nosso secretário de Estado também deixou perfeitamente claro: que é a construção de um mundo de diálogo num quadro de diversidade.

É preciso conhecer a nossa História para tirar partido daquilo que nós trouxemos ao mundo, de Vancouver a Vladivostok, como se diz na gíria da OSCE; em termos de construção da paz e do diálogo, isso é que é absolutamente essencial.

E acho que, em momentos decisivos, nós demos uma contribuição, modesta terá sido, mas demos uma contribuição para que não se retomasse a velha lógica da Guerra Fria, que de um lado e de outro espreita sempre. Porque é muito cómodo pensar nos velhos esquemas da Guerra Fria – de um lado estão os bons e do outro lado estão os maus. Sendo que nós estamos sempre do lado dos bons, seja qual for o lado em que estejamos e os outros, aqueles que não pensam como nós, estão, evidentemente, do lado dos maus.

E eu acho que essa é a mais-valia mais importante. E ela está bem simbolizada no facto de, no quadro da OSCE, e, muito em particular, no quadro da Assembleia Parlamentar, a Federação Russa ainda ter felizmente, na minha modesta opinião, um papel de *primus inter pares*, de par com os Estados Unidos, no que diz respeito à condução daquilo que são as opções geoestratégicas internacionais que têm lugar no quadro da OSCE.

Eu acho que aquilo que tem vindo a ser feito aqui é particularmente interessante e tem potencialidades de continuar a ser extremamente interessante e de estar à altura daquilo que são os desafios complexos que o mundo contemporâneo tem de enfrentar.

É verdade que a organização governamental do lado em Viena cresceu muito. Era também exemplar quando deu os seus primeiros passos nos inícios dos anos 80, e tornou-se relativamente pesada e burocrática. Também vimos isso em vários momentos.

Recordo-me da crise entre a Geórgia e a Federação Russa, da guerra entre a Geórgia e a Federação Russa, a propósito do incidente que teve lugar na Ossétia do Sul, ainda antes do reconhecimento da Ossétia do Sul como um Estado independente, e lembro-me do que aconteceu a alguns relatórios que se perderam na infinidade dos corredores de Viena, e do peso burocrático dessa cidade.

Viena começou com um escritório relativamente pequeno e com pouca gente, e hoje tem, seguramente, umas centenas de pessoas ao serviço de uma burocracia que, às vezes, pesa mais do que devia pesar.

A Assembleia Parlamentar também tem essa leveza e essa ligeireza. E tem sido, ao longo da sua história, capaz de convidar para estarem aqui os melhores.

Sublinho a presença da senhora embaixadora Graça Mira Gomes como um dos símbolos dessa vontade de renovar e dos grandes quadros que a OSCE, a nível parlamentar, também deu ao mundo em que vivemos, nessa lógica de fazer frente, com alguma audácia e com imaginação, aos desafios que temos pela nossa frente.

Continuo a acreditar profundamente nos valores da OSCE, acho que é preciso continuar a trabalhar naquilo que se designava tradicionalmente como "os três cestos", sem privilegiar nenhum em particular.

Há muito trabalho para fazer. Houve muita coisa que evoluiu de forma positiva, outras coisas evoluíram de uma forma menos positiva, mas eu penso, sinceramente, que a Europa e o mundo continuam a precisar de uma organização com uma visão tão vasta, tão ampla, e, ao mesmo tempo, tão dinâmica e tão flexível como aquela que a OSCE teve nos seus melhores tempos e, seguramente, está a continuar a ter.

Mais uma vez, parabéns à vice-presidente Isabel Santos, de quem eu sou um fã desde há muito, parabéns à presidente da Segunda Comissão, minha amiga pessoal, não política, Nilza de Sena, e parabéns ao presidente George Tsereteli.

Sinto-me muito feliz por te ver aqui, querido George Tsereteli. Estiveste aqui várias vezes em Lisboa, de uma das vezes a meu convite, e isso deu-me uma grande satisfação, como presidente da Assembleia Parlamentar.

E uma saudação amiga ao Roberto Montella, ao Gustavo Palhares, ao Andreas Notella, e a todos os que aqui estão.

Muito obrigado.

JOÃO SOARES

I would like to thank the serving Head, my friend and colleague at the OSCE Parliamentary Assembly and the Portuguese Parliament, Miguel Santos, for giving me the floor.

I would first like to address the President of the OSCE Parliamentary Assembly and my friend, George Tsereteli, to underline my pleasure in being here today, following your invitation.

When our common friend, and Vice-President, Isabel Santos, gave me, she and Nilza de Sena, the invitation to be here, I was immediately extremely happy for the opportunity to be reunited with old friends from so many struggles we have defended in the name of OSCE values.

I know the conference went smoothly, I was unable to be here this morning, but I am very happy to be here with you today and congratulate you, as did the Secretary of State, Marcos Perestrello, actually, with a good speech in which he gave an overview of all these questions in a very clear and I think absolutely sincere way.

When I had commitments at the OSCE Parliamentary Assembly, I used to say that we have the best secretariat in that I've ever seen operating in the world.

And so, I would also like to express my greetings to the Parliamentary Assembly's secretariat, to my friend and old work colleague, Roberto Montella, to Gustavo Palhares, who is up there, to Ambassador Andreas Notella, who I was with on Friday, and who is also a Parliamentary Assembly veteran, to Andreas Baker, who I don't see here but is likely here, or somewhere else working for the OSCE Parliamentary Assembly, and remember the examples of two veterans, Spencer Oliver and Tina Schön, who played a determining role in this operating model, which I still believe is an absolutely exemplary and perhaps unique model in the world.

A very small team of highly effective people with a very limited budget who do admirable work. And it is at the forefront of the work that Organisation for Security and Co-operation in Europe has done, also, for as long as it has existed.

As you will know, the Parliamentary Assembly began a few years after the Helsinki Final Acts in August 1975, so, a few years after the Organisation for Security and Co-operation in Europe was formally set up, which was transformed from a conference, a permanent conference, into an organisation.

But it is, as the great Portuguese ambassador who represented Portugal at the OSCE, Ambassador Seixas da Costa, said, a 'reluctant sedimentation' of a conference into an organisation. And I think that this provides the measure and the potential that are the assets that the OSCE has brought to the international landscape.

A little while ago, my personal, not political, friend, Luís Campos Ferreira, underlined this: in this controversial, changing world of constant conflicts in which we live, the OSCE's role continues to be, and can be, and frequently has been (but sometimes it has not got that far) an absolutely decisive role in peace-building and international cooperation.

And, within the OSCE, the Parliamentary Assembly has always had, let's say, a pioneering role.

And, once again, when dealing with issues of cybersecurity, they are major issues in this turbulent world in which we live. I think that the Parliamentary Assembly must continue along this path. Far be it from me to recommend anything. The

experience that I had here was a very rich and gratifying one. I feel honoured to have had the chance, always very modestly, to play a role here in contexts that were complicated, of sometimes very complex conflicts.

I remember, for example, the Ukraine crisis, when we were in Donetsk on the eve of legislative elections in Ukraine, which elected President Porochenko, I remember many other countries, from Belarus to Kazakhstan, where Nilza de Sena and I were at the end of some elections, which were controversial elections, and where we had to give a press conference the following day to assess the electoral process. It wasn't easy. But it was something that gave us enormous satisfaction.

And, above all, I remember a trip to Odessa, many people who didn't want us to do it at a certain time, when things were more complicated in Ukraine, or were starting to get more complicated in Ukraine, there we went, always following an approach of faithfulness to the 1975 Helsinki Final Acts. That was what Luís Campos Ferreira emphasised, and what our Secretary of State also made perfectly clear: that it is the building of a world of dialogue within a framework of diversity.

We need to know our history to draw on what we have brought to the world, from Vancouver to Vladivostok, to use OSCE parlance, in terms of building peace and dialogue that is what is absolutely essential.

And I think that, at decisive times, we have made a contribution, it would have been a modest one, but we have made a contribution to avoid returning to the old approach of the Cold War, which is always lurking around. Because it is very convenient to think about the old schemes of the Cold War where we have the good on one side and the bad on the other. With us always on the good side, whichever side we're on, and those who don't think like us are, of course, on the bad side.

And I think that is the most important asset. And it is properly symbolised in the fact that, within the OSCE framework and, in particular, in the Parliamentary Assembly framework, the Russian Federation still has, luckily, in my modest opinion, a role as primus inter pares, alongside the United States, in terms of leading the international geostrategic options that take place in the OSCE framework.

I think that what has been being done here is particularly interesting and has the potential to carry on being extremely interesting and able to meet the complex challenges that the contemporary world has to face.

It is true that the neighbouring governmental organisation in Vienna has grown a lot, it was also an example when it took its first steps at the start of the 1980s, and it has become relatively cumbersome and bureaucratic, we have also seen that at several times.

And I remember the crisis between Georgia and the Russian Federation, the war between Georgia and the Russian Federation, about the incident which took place in South Ossetia, even before South Ossetia was recognised as an independent state, and I remember what happened to some reports that were lost in the infinite corridors of Vienna, the bureaucratic burden of Vienna.

Vienna began as a relatively small office with few people, and today it surely has several hundred people working for a bureaucracy that, at times, is more cumbersome than it should be.

The Parliamentary Assembly also has that levity and lightness. And it has, throughout its history, been able to invite the best to be here.

And I underline the presence of Ambassador Graça Mira Gomes as one of the symbols of that desire for renewal and of the great frameworks that the OSCE, at parliamentary level, has also given the world in which we live, in that rationale of facing up to, with some audacity and imagination, the challenges we have before us.

I still deeply believe in the OSCE's values, I think we need to keep working on what was traditionally called "the three baskets", without favouring any one in particular.

There is a lot of work to be done. A lot of things have evolved, have evolved positively, other things have evolved less positively, but I sincerely think that Europe and the world still need an organisation with such a vast, such a broad and, at the same time, such a dynamic and flexible vision as the OSCE has had at its best moments and surely still has.

Once again, thanks to Vice-President Isabel Santos, of whom I have been a fan for a long time, congratulations to the Chair of the Second Committee, my personal, not political, friend, Nilza de Sena, and congratulations to President George Tsereteli.

I feel very happy to have you here, dear George Tsereteli. You have been in Lisbon several times, once on my invitation, and that made me very pleased, as President of the Parliamentary Assembly.

And I would also like to express my friendly greetings to Roberto Montella, Gustavo Palhares,

Andreas Notella and everybody here.

Thank you very much.

MIGUEL SANTOS

Senhor vice-presidente
Senhor presidente da Assembleia Parlamentar da OSCE
Senhor secretário de Estado
Senhora presidente da delegação portuguesa
Senhoras deputadas e senhores deputados
Senhoras e senhores conferencistas
Senhoras e senhores convidados

Gostaria de começar por agradecer a todos a vossa presença, que em muito contribuiu para o sucesso deste nosso evento que marca o início de um ciclo de Conferências a realizar no nosso Parlamento, a cada dois anos.

Assim, podem considerar-se todos, desde já, convidados para a segunda edição das Conferências de Lisboa da Assembleia Parlamentar da OSCE, a realizar em 2020.

O tema escolhido para o arranque das Conferências de Lisboa da Assembleia Parlamentar da OSCE – A Resiliência Digital de um Estado Democrático –, surge como prioridade nos tempos atuais e no futuro próximo.

Temos hoje novas preocupações que têm por origem o ciberespaço, mas cujos efeitos poderão ser sentidos no nosso dia-a-dia, nas nossas tarefas mais comuns e simples das rotinas diárias.

O desenvolvimento das novas tecnologias, o acesso às mesmas por parte de todos, e a possibilidade de aceder a informação complexa de forma simples, trazem muitas vantagens à nossa sociedade, ajudando à qualidade de vida de todos os cidadãos e facilitando todos os aspetos da sociedade, desde a vida pessoal à economia do país, no mercado de trabalho e até a saúde dos nossos cidadãos.

Efetivamente, todos os sectores da sociedade sofrem as influências positivas, mas também as negativas, do rápido crescimento e desenvolvimento das novas tecnologias.

Temos, por isso, de estar atentos e vigilantes para os desafios que iremos enfrentar e, sobretudo, devemos estar preparados para responder de forma rápida e assertiva aos inevitáveis perigos.

Não se trata de uma questão de – se –, mas de – quando – iremos enfrentá-los.

O nosso evento apontou muitos caminhos e muitas reflexões, como a capacitação de uma nova área de especialização e a formação de todos os cidadãos no seu relacionamento com a Internet.

A forma como interagimos e a cooperação ao nível dos Estados está já a mudar e a partilha de informação entre todos é também uma dimensão que deverá ser trabalhada e desenvolvida.

Nos últimos dias do mês de abril, Portugal juntou-se ao Centro Multinacional e Interdisciplinar de Conhecimento na Área da Ciberdefesa da NATO, na Estónia, onde irá colaborar com especialistas, militares, professores e estudiosos na área da ciberdefesa.

Sabemos que o caminho a percorrer é multidisciplinar.

Na nossa Conferência, tivemos a possibilidade de ouvir e aprender com especialistas da academia, militares, políticos e sociedade civil.

A nossa preparação terá de ser, sem dúvida, multidisciplinar e incluir todos os sectores da sociedade, da mesma forma que a OSCE tem uma abordagem integrada sobre as questões da segurança, tendo sempre em consideração as três dimensões político-militar, humana e económico-ambiental.

A responsabilidade deverá ser partilhada e as nossas estratégias alinhadas.

A preparação é a palavra de ordem sempre que se fala em cibersegurança, em todas as suas vertentes.

Preparemo-nos, então, e preparemos os nossos cidadãos de todas as faixas etárias.

Só tendo consciência de que todos temos responsabilidade e um papel a desempenhar, seremos capazes de nos tornarmos mais fortes e mais resilientes perante os desafios que nos coloca o ciberespaço.

Muito obrigado.

MIGUEL SANTOS

I would like to begin by thanking everyone for their presence here, which has greatly helped make a success of our event, which marks the beginning of a series of conferences to be held at our Parliament every two years.

You are all, then, invited to the second set of Lisbon Conferences of the OSCE Parliamentary Assembly which will be held in 2020.

The theme chosen to start the Lisbon Conferences of the OSCE Parliamentary Assembly – Digital Resilience of a Democratic State – is a priority at present and will continue to be one in the near future.

We have new concerns that have their origins in cyberspace, but the effects of which can be felt in our day-to-day lives, in the most common and simple tasks of our daily routines.

The development of new technologies, their availability to everyone and the opportunity to have simple access to complex information bring many advantages to our society, helping improve quality of life for all citizens and streamlining all aspects of society, from personal life to the country's economy, labour market and even citizens' health.

In fact, all sectors of society undergo the positive, but also negative, influences of the rapid growth and development of new technologies.

We therefore have to be alert to and vigilant about the challenges that we will face and, above all, we have to be prepared to quickly and assertively respond to the inevitable dangers.

It is not a question of *if* but *when* we will face them.

Our event has suggested many paths and reflections, such as the creation of a new area of specialisation and training for all citizens in their relationship with the internet.

The way we interact and state-level cooperation are already changing, and the sharing of information among everyone is also an area that will need to be worked on and developed.

In the final days of April, Portugal joined the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, where it worked with specialists, military personnel, educators and academics in the field of cyber defence.

We know that the path to be followed is a multidisciplinary one.

At our conference, we have had the chance to hear and learn from academic, military, political and civil society specialists.

Our preparation will undoubtedly have to be multidisciplinary and include all sectors of society, just as the OSCE has an integrated approach to issues of security, always bearing in mind the three dimensions: political and military, human, and economic and environmental.

Responsibility should be shared and our strategies aligned.

Preparation is the watchword whenever talking about cyberspace in all its aspects.

Let us prepare ourselves, then, and let us prepare our citizens of all ages.

Only with an awareness that we all have responsibility and a part to play will we be able to become stronger and more resilient in the face of the challenges that cyberspace poses to us.

Thank you very much.

PROGRAMA

9h30 ABERTURA

Jorge Lacão (Vice-Presidente da Assembleia da República, em representação do Presidente da Assembleia da República)

George Tsereteli (Presidente da Assembleia Parlamentar da OSCE)

Isabel Santos (Presidente da Delegação Portuguesa à AP OSCE)

9h50 CIBERSEGURANÇA & DEMOCRACIA: CONFIDENCE BUILDING MEASURES

Julian King (Comissário Europeu para a União da Segurança (mensagem por vídeo))

Anatoly Smirnov (Professor, Diretor-Geral da Associação Nacional para Segurança Internacional da Informação de Moscovo)

William Sweeney (Presidente e Diretor-Geral International Foundation for Electoral Systems)

Ignácio Sanchez Amor (Presidente da Comissão de Democracia, Direitos Humanos e Questões Humanitárias da AP OSCE)

RELATORA Susana Amador (Deputada)

MODERADOR João Fernando Ramos (Jornalista)

DEBATE

11h30 DESAFIOS TECNOLÓGICOS DO CIBERESPAÇO

Luís Antunes (Diretor do Centro de Competências em Cibersegurança e Privacidade, Universidade do Porto)

Pedro Veiga (Coordenador do Centro Nacional de Cibersegurança (CNCS))

Rasa Ostrauskaite (Coordenadora das Atividades de Combate às Ameaças Transnacionais da OSCE)

RELATORA Nilza de Sena (Deputada)

MODERADOR Lourenço Medeiros (Jornalista)

DEBATE

14h00 SOBERANIA E SEGURANÇA DIGITAL

Fernando Jorge Pires (Comodoro, Direção de Comunicações e Sistemas de Informação, Estado- Maior-General das Forças Armadas (EMGFA))

António Gameiro Marques (Contra-Almirante, Diretor-Geral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança)

Kristian Vigenin (Relator da Comissão de Assuntos Políticos e Segurança da AP OSCE)

RELATOR José Miguel Medeiros (Deputado)

MODERADOR José Alberto Carvalho (Jornalista)

DEBATE

15h30 A AMEAÇA DO CIBERTERRORISMO NO ESPAÇO OSCE

Pedro Verdelho (Procurador da República, Coordenador do Gabinete de Cibercrime da Procuradoria-Geral da República)

Graça Mira Gomes (Embaixadora, Secretária-Geral do Sistema de Informações da República Portuguesa (SIRP))

Makis Voridis (Presidente da Comissão *Ad Hoc* para Combate ao Terrorismo da AP OSCE)

RELATOR Luís Campos Ferreira (Deputado)

MODERADOR Luísa Meireles (Jornalista)

DEBATE

17h00 ENCERRAMENTO

Marcos Perestrello (Secretário de Estado da Defesa Nacional)

João Soares (Antigo Presidente da Assembleia Parlamentar da OSCE)

Miguel Santos (Vice-Presidente da Delegação Portuguesa à AP OSCE)

PROGRAMME

9:30 OPENING SESSION

Jorge Lacão (Vice-President of the Assembly of the Republic, representing the President of the Assembly of the Republic)

George Tsereteli (President of the OSCE Parliamentary Assembly)

Isabel Santos (President of the Portuguese Delegation to the OSCE PA)

9:50 CYBERSECURITY & DEMOCRACY: CONFIDENCE BUILDING MEASURES

Sir Julian King (European Commissioner for the Security Union (video message))

Anatoly Smirnov (Professor, Director-General of the National Association for International Information Security of Moscow)

William Sweeney (President and CEO International Foundation for Electoral Systems)

Ignácio Sanchez Amor (Chairman of the OSCE PA Committee for Democracy, Human Rights and Humanitarian Issues)

RAPPORTEUR **Susana Amador** (MP)

MODERATOR **João Fernando Ramos** (Journalist)

DEBATE

11:30 TECHNOLOGICAL CHALLENGES OF CYBERSPACE

Luís Antunes (Director of the Center of Competence in Cyber Security and Privacy, University of Porto)

Pedro Veiga (Co-ordinator of National Cybersecurity Centre Portugal)

Rasa Ostrauskaite (Co-ordinator of Activities to Address Transnational Threats of the OSCE)

RAPPORTEUR: **Nilza de Sena** (MP)

MODERATOR: **Lourenço Medeiros** (Journalist)

DEBATE

14:00 SOVEREIGNTY AND DIGITAL SECURITY

Fernando Jorge Pires (Commodore Directorate of Communications and Information Systems, EMGFA)

António Gameiro Marques (Rear Admiral, National Security Office, GNS – Director-General)

Kristian Vigenin (Rapporteur for the General Committee on Political Affairs and Security of the OSCE PA)

RAPPORTEUR: **José Miguel Medeiros** (MP)

MODERATOR: **José Alberto Carvalho** (Journalist)

DEBATE

15:30 THE THREAT OF CYBER-TERRORISM IN THE OSCE AREA

Pedro Verdelho (Prosecutor, Head of the Cybercrime Office of the Portuguese Attorney General's Office)

Graça Mira Gomes (Ambassador, Secretary-General of the Portuguese Intelligence System)

Makis Voridis (Chair of the OSCE PA Ad Hoc Committee on Countering Terrorism)

RAPPORTEUR: **Luís Campos Ferreira** (MP)

MODERATOR: **Luísa Meireles** (Journalist)

DEBATE

17:00 CLOSING SESSION

Marcos Perestrello (Secretary of State for National Defense)

João Soares (Former President of the OSCE Parliamentary Assembly)

Miguel Santos (Vice-President of the Portuguese Delegation to the OSCE PA)

NOTAS BIOGRÁFICAS DOS AUTORES
AUTHORS' BIOGRAPHICAL NOTES

Anatoly Smirnov

Diretor-geral da Associação Nacional para a Segurança da Informação Internacional em Moscovo e professor do Instituto Estatal de Relações Internacionais de Moscovo.

Foi diplomata e, após se ter retirado do serviço diplomático, tornou-se membro do Conselho Consultivo da Comissão para a Segurança da Duma russa e presidente da ONG "Instituto Nacional de Investigação em Segurança Mundial".

Director-General of the National Association for International Information Security of Moscow and Professor of the Moscow State Institute of International Relations.

He was a diplomat and after retired he became member of the Advisory Council of the Committee for Security of the State Duma of Russia and President of the NGO "National Institute of Research of Global Security".

António Gameiro Marques

Contra-almirante, diretor-geral do Gabinete Nacional de Segurança e Autoridade Nacional de Segurança e preside ao Conselho Superior de Segurança do Ciberespaço. É licenciado em Ciências Militares Navais e mestre em *Electrical and Computer Engineering*.

Desempenhou diversas funções na Marinha e na Organização do Tratado do Atlântico Norte (OTAN), nomeadamente nas áreas das tecnologias de informação e comunicação e da cibersegurança.

Rear Admiral, Director-General of the National Security Office and National Security Authority and he also chairs the Cyberspace High Security Council. He holds a degree in Marine Military Science and a Master's degree in Electrical and Computer Engineering.

He has held various positions in the Portuguese Navy and in the North Atlantic Treaty Organization (NATO), in particular in the areas of information and communication technologies and cybersecurity.

Fernando Jorge Pires

Comodoro, diretor de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas. É licenciado em Ciências Militares Navais, *Master of Science in Electrical Engineering* e *Electrical Engineer.*

Desempenhou ao longo da carreira funções na Marinha e do Ministério da Defesa Nacional, nas áreas das Tecnologias de Informação, Simulação e Modelação. Foi, ainda, professor e coordenador de Departamento da Escola Naval e professor convidado no Instituto Superior de Estatística e Gestão da Informação da Universidade Nova de Lisboa.

Commodore, Directorate of Communications and Information Systems of the Armed Forces General Staff. He holds a degree in Marine Military Science, Master of Science in Electrical Engineering and Electrical Engineer.

Throughout his career he has held positions in the Portuguese Navy and the Ministry of National Defense in the areas of Information Technology, Simulation and Modeling. He was also professor and coordinator of the Naval School Department and professor at the Higher Institute of Statistics and Information Management at the Universidade Nova, Lisbon.

George Tsereteli

Presidente da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa e deputado no Parlamento da Geórgia, integrando a Comissão de Relações Exteriores e a Comissão de Saúde e Assuntos Sociais.

Anteriormente foi vice-presidente do Parlamento georgiano, vice-primeiro ministro e ministro do Trabalho, Saúde e Proteção Social da Geórgia e presidente do Fórum Parlamentar Europeu sobre População e Desenvolvimento.

President of the Parliamentary Assembly of the Organization for Security and Cooperation in Europe and Member of the Georgian Parliament and he is member of the Committee on Foreign Affairs and the Committee on Health and Social Affairs.

In the Georgian Parliament, he served as Deputy Chairman and he was Georgia's Deputy Prime Minister and Minister of Labor, Health, and Social Protection. He was also President of the European Parliamentary Forum on Population and Development.

Graça Mira Gomes

Embaixadora, secretária-geral do Sistema de Informações da República Portuguesa (SIRP).

Desempenhou as funções de embaixadora de Portugal junto da Organização para a Segurança e Cooperação na Europa (OSCE) e foi representante portuguesa no Comité Político e de Segurança da União Europeia (COPS).

Ambassador, Secretary-General of the Portuguese Intelligence System.

She served as Portugal's ambassador to the Organization for Security and Cooperation in Europe (OSCE) and was the Portuguese representative to the EU Political and Security Committee (COPS).

Ignácio Sanchez Amor

Deputado do Parlamento espanhol e presidente da Comissão para a Democracia, Direitos Humanos e Questões Humanitárias da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa (AP OSCE).

Exerceu anteriormente diversos cargos públicos, entre os quais o de vice-presidente da Junta da Extremadura.

Spanish Member of Parliament and President of the General Committee on Democracy, Human Rights and Humanitarian Questions of the Parliamentary Assembly of the Organization for Security and Cooperation in Europe (OSCE PA).

Previously he held several public positions, including Vice President of the Regional Government of Extremadura (Junta de Extremadura).

Julian King

Comissário Europeu para a União da Segurança, responsável, entre outras áreas, pelo combate ao crime cibernético através de maior segurança cibernética e inteligência digital.

É diplomata e desempenhou anteriormente funções de embaixador em França e a Irlanda e de diretor-geral Económico e Consular e diretor-geral para a Irlanda do Norte do Ministério dos Negócios Estrangeiros britânico.

European Commissioner for the Security Union, responsible among other areas for fighting cybercrime through enhanced cybersecurity and digital intelligence.

He is a diplomat and has previously served as Ambassador in France and Ireland and as Director-General Economic and Consular and Director-General of the Northern Ireland Office of the Foreign and Commonwealth Office of the United Kingdom

Kristian Vigenin

Relator da Comissão de Assuntos Políticos e Segurança da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa (AP OSCE) e deputado búlgaro.

Anteriormente foi o representante especial da AP OSCE no Cáucaso do Sul e vice-presidente da Delegação Búlgara à AP OSCE. Foi ainda ministro dos Negócios Estrangeiros da Bulgária.

Rapporteur for the General Committee on Political Affairs and Security of the OSCE PA and Member of the Bulgarian Parliament

He served as the OSCE PA Special Representative on the South Caucasus and as Deputy Head of the Bulgarian Delegation to the OSCE PA. Previously he was Minister of Foreign Affairs of Bulgaria.

Luís Antunes

Diretor do Centro de Competências em Cibersegurança e Privacidade da Universidade do Porto e professor e presidente do Departamento de Ciência de Computadores da Faculdade de Ciências da mesma Universidade.

Colabora regularmente com o Gabinete Nacional de Segurança (GNS), com a Comissão Nacional de Proteção de Dados e a Procuradoria-Geral da República na área do cibercrime e é perito na European Union Agency for Network and Information Security) (ENISA) nas áreas de *eID, eGov* e *eHealth*.

Director of the Competence Centre for Cybersecurity and Privacy, University of Oporto and Professor and Chair of the Computer Science Department at Faculty of Sciences of the same University.

Collaborates regularly with the Portuguese National Security Agency, Data Protection Authority and the General Attorney in the area of cybercrime and is an expert in the European Union Agency for Network and Information Security (ENISA) in the areas of eID, eGov and eHealth.

Makis Voridis

Presidente da Comissão *Ad Hoc* para Combate ao Terrorismo da Assembleia Parlamentar da Organização para a Segurança e Cooperação na Europa (AP OSCE) e deputado grego.

Anteriormente, foi ministro da Reconstrução, Transportes e Redes e Ministro da Saúde da Grécia. Na AP OSCE foi presidente da Comissão de Assuntos Políticos e de Segurança e representante especial para a Imigração.

Chair of the Ad Hoc Committee on Countering Terrorism of the Organization for Security and Cooperation in Europe Parliamentary Assembly (OSCE PA) and Member of the Greek Parliament.

Previously he was Minister of Reconstruction, Transportation and Network and Minister of Health. In the (OSCE PA) he served as President of the Committee for Political and Security Affairs and Special Representative for Immigration.

Marcos Perestrello

Secretário de Estado da Defesa Nacional.

Foi deputado, vice-presidente da Câmara Municipal de Lisboa e secretário de Estado da Defesa Nacional e dos Assuntos do Mar.

Secretary of State for National Defense.

Previously he was Member of the Portuguese Parliament, Secretary of State for National Defense and Maritime Affairs and Deputy Mayor of Lisbon.

Pedro Veiga

Coordenador do Centro Nacional de Cibersegurança e Professor da Faculdade de Ciências da Universidade de Lisboa.

Foi fundador e presidente do capítulo português da Internet Society e presidente do Conselho Executivo da Fundação para a Computação Científica Nacional. Foi, ainda, membro do *Government Advisory Committee* do *Internet Corporation for Assigned Names and Numbers* (ICANN) e membro do *Management Board* da *European Union Agency for Network and Information Security* (ENISA).

Coordinator of National Cybersecurity Centre of Portugal and Professor of the Faculty of Sciences of the University of Lisbon.

He was founder and President of the Portuguese chapter of the Internet Society and President of the Executive Council of the Foundation for National Scientific Computation. He was also a Member of the Government Advisory Committee of the Internet Corporation for Assigned Names and Numbers (ICANN) e Member of the Management Board of the European Union Agency for Network and Information Security (ENISA).

Pedro Verdelho

Procurador da República, Coordenador do Gabinete de Cibercrime da Procuradoria-Geral da República.

Tem representado Portugal na União Europeia e nas Nações Unidas, em assuntos relacionados com a cibercriminalidade e, ainda, no Comité da Convenção do Cibercrime do Conselho da Europa (Convenção de Budapeste).

Prosecutor, Head of the Cybercrime Office of the Portuguese Attorney General's Office.

He has represented Portugal in the European Union and in the United Nations in matters related to cybercrime and also in the Committee of the Convention on Cybercrime of the Council of Europe (Budapest Convention).

Rasa Ostrauskaite

Coordenadora das Atividades de Combate às Ameaças Transnacionais da Organização para a Segurança e Cooperação na Europa (OSCE), mestre em Relações Internacionais e Estudos Europeus e mestre em Ciência Política.

Anteriormente foi diretora-adjunta do Serviço de Apoio a Políticas no Centro de Prevenção de Conflitos da OSCE e desempenhou funções em diversas instituições da União Europeia.

Coordinator of Activities to Address Transnational Threats at the Organization for Security and Co-operation in Europe (OSCE) and Master in International Relations and European Studies and Master of Philosophy in Political Science.

She served as Deputy Director for Policy Support Service at the OSCE's Conflict Prevention Centre. Previously she worked in various capacities at the European Union.

William Sweeney

Presidente e diretor-geral da Fundação Internacional de Sistemas Eleitorais (IFES).

É membro do Comité Consultivo da Comissão Mundial para as Eleições, a Democracia e a Segurança do IDEA (Instituto Internacional para a Democracia e Assistência Eleitoral). É também membro do Conselho de Administração da Fundação do Conselho de Comércio Externo dos EUA.

Anteriormente, fundou e dirigiu o Instituto de Gestão de Campanhas da Universidade Americana em Washington e participou em diversas Missões de Observação Eleitoral nos vários continentes.

President and CEO of International Foundation for Electoral Systems (IFES).

He is a member of the Advisory Committee for International IDEA's Global Commission on Elections, Democracy and Security. He also serves on the board of directors of the National Foreign Trade Council Foundation.

He was a founder and Director of the Campaign Management Institute at American University in Washington and has participated in several Electoral Observation Missions, throughout the world.

FICHA TÉCNICA

TÍTULO / TITLE
Resiliência Digital de um Estado Democrático / Digital Resilience of a Democratic State
Conferência: Assembleia da República, 8 de maio de 2018 (PDF)
Conference: Assembly of the Republic, 8 May 2018 (PDF)

INICIATIVA / INITIATIVE
Assembleia da República – Delegação portuguesa à Assembleia Parlamentar da OSCE
Assembly of the Republic – Portuguese delegation to the OSCE Parliamentary Assembly

TRADUÇÃO / TRANSLATION
Língua Franca – Línguas e Tradução, Lda.
Thomas Williams

EDIÇÃO / PUBLISHER
Assembleia da República. Divisão de Edições
Assembly of the Republic. Publications Division

COORDENAÇÃO EDITORIAL E REVISÃO / EDITORIAL COORDINATION AND PROOFREADING
Conceição Garvão

TRANSCRIÇÕES / TRANSCRIPTION
Marta Dias

FOTOGRAFIA / PHOTOGRAPH
André Pereira

PAGINAÇÃO / DESIGN
Undo

ISBN 978-972-556-699-2

Lisboa, junho 2020