CIES e-Working Paper N.º 204/2016

Eurobarómetro como instrumento de política da Comissão Europeia.

Análise do Eurobarómetro Especial 371

Daniela Santos

CIES e-Working Papers (ISSN 1647-0893)

Av. das Forças Armadas, Edifício ISCTE, 1649-026 LISBOA, PORTUGAL, cies@iscte.pt

Daniela Santos é licenciada em Sociologia, com mestrado e doutoranda em Políticas Públicas, no ISCTE-Instituto Universitário de Lisboa. Tem um Minor em Segurança Internacional, pela Vrije Universiteit Amsterdam.
Participou no Strategic Decision Making Course & Exercise on Cyber Crisis Management, promovido pela Agência Europeia de Defesa, em 2014 e no II Curso de Cibersegurança e Gestão de Crises no Ciberespaço, do Instituto da Defesa Nacional (IDN). É membro do Grupo de Estudos sobre Contributos para uma Estratégia Nacional de Informação (GECENI), do IDN e tem trabalhado na área da formação e sensibilização para a segurança da informação.

Resumo

No presente trabalho são analisados alguns dados do Eurobarómetro Especial 371 (2011), dedicado ao tema da segurança interna da União Europeia, e identificadas algumas das suas limitações metodológicas, nomeadamente ao nível da construção do questionário e da análise e apresentação dos dados, além de uma crítica a este estudo como instrumento de política para a Comissão Europeia.

Este trabalho foca-se na análise dos dados respeitantes à perceção dos inquiridos sobre questões relacionadas com o cibercrime e constitui um contributo para a corrente que critica o Eurobarómetro como fonte de conhecimento e de análise estatística, em favor de uma visão do mesmo como um instrumento de política da Comissão Europeia – a entidade mais interessada, que financia e orienta a forma como são conduzidos estes estudos.

Palavras-chave: Eurobarómetro; metodologia; cibercrime; Comissão Europeia

Abstract

In the present work are analyzed some data of the Special Eurobarometer 371 (2011) dedicated to the issue of the European Union's Internal Security, and identified some of its methodological limitations, particularly in terms of construction of the questionnaire and the analysis and presentation of data, and a critique of this study as an European Commission's policy tool.

This work focuses on the analysis of data concerning the perception of respondents on issues related to cybercrime and is a contribution to the theoretical chain that criticizes the Eurobarometer as a source of knowledge and statistical analysis in favor of a view of it as an European Commission's policy tool, since it is the most interested party, who supports and guides the way these studies are conducted.

Key words: Eurobarometer; methodology; cybercrime; European Commission

I. Introdução

Os relatórios do Eurobarómetro, realizado desde 1973, baseiam-se na opinião pública dos cidadãos europeus sobre temáticas específicas que a Comissão Europeia (embora também outras instituições europeias) possa considerar pertinentes para o desenho, desenvolvimento e avaliação das políticas públicas europeias. As questões dos Eurobarómetros Especiais são integradas nas sondagens *standard* do Eurobarómetro.

O Eurobarómetro Especial 371 (EB Especial 371), em particular, é um inquérito de opinião sobre as perceções dos cidadãos europeus acerca de questões relacionadas com a segurança interna da União Europeia (UE). Este Eurobarómetro foi realizado em 2011, na sequência da aprovação da "Estratégia de Segurança Interna da UE em Ação: cinco etapas para uma Europa mais segura" (COM (2010) 673 final).

A cibersegurança[1] tem sido desde 1989 uma questão presente na agenda política da UE[2]. Face a isso, nesta Estratégia, a Comissão Europeia atualiza os principais desafios à segurança interna da UE, introduzindo o cibercrime como um dos cinco principais desafios e reconhece que a "Europa constitui um alvo fundamental para a cibercriminalidade devido à infra-estrutura avançada no domínio da Internet, ao elevado número de utilizadores, bem como à importância da Internet para o funcionamento das suas economias e sistemas de pagamento".

Neste contexto, a Estratégia apresenta um conjunto de ações a tomar nos quatro anos seguintes (2010-2014) para combater e prevenir, entre outros desafios, a cibercriminalidade, i.e., "um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais" (JOIN(2013) 1 final).

A análise aqui apresentada foca-se precisamente dos dados respeitantes à perceção dos inquiridos sobre as questões relacionadas com o cibercrime, excluindo outras matérias.

O objetivo do EB Especial 371 foi "providenciar uma visão estratégica através da comparação e contraste das perceções públicas com a abordagem tomada na Estratégia de Segurança Interna. Este Eurobarómetro foi desenhado para acompanhar o primeiro relatório anual da implementação da Estratégia de Segurança Interna da UE e para estabelecer *benchmarks* para futura reavaliação" (European Commission, 2011). Portanto, este relatório pode assim ser considerado um instrumento de política da Comissão Europeia para complementar a avaliação da implementação da Estratégia de Segurança Interna da União Europeia, publicada em 2010.

[1] Por cibersegurança entende-se as ações tomadas "para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas" (JOIN(2013) 1 final).

[2] Consultar Anexo, Figura 1, página 24.

II. Enquadramento

Cibersegurança

A evolução tecnológica permitiu a criação e o desenvolvimento de um sistema global de informação, onde a informação (muita dela, confidencial) já não se encontra armazenada num espaço específico e restrito, passando a estar num local – ciberespaço – que, devido à sua amplitude, torna mais difícil o controlo de quem tem acesso à informação, podendo torná-la até mais acessível a indivíduos com determinadas competências informáticas (*hackers*). Portanto, este sistema pode deixar os Estados e os cidadãos mais vulneráveis a ciberataques, normalmente realizados com o intuito de proporcionar o enriquecimento ilícito do atacante, a disrupção e desestabilização de Estados e/ou indivíduos.

Santos, Bessa e Pimentel salientam cinco fatores potenciadores desta realidade: "a redução do custo dos bens tecnológicos"; "a redução dos custos do acesso à Internet"; a "expansão rápida da banda larga"; "o aumento do conhecimento e acesso por parte de possíveis ofensores a técnicas e métodos de ocultação de provas digitais, nomeadamente: técnicas de encriptação, a compreensão digital, a esteganografia…", i.e., a arte de esconder informação; "o acréscimo de literacia computacional por parte da comunidade global de internautas" (Santos, Bessa, Pimentel, 2008).

Face a esta realidade, tal como já foi referido, a cibersegurança tem sido uma preocupação presente na agenda política da UE desde os anos 90, através da R(89)9 do Conselho da Europa, sobre o cibercrime, que visa a introdução de um conjunto de novas penalizações nos acervos penais nacionais, como a falsidade informática, o dano relativo a dados ou a programas informáticos, a sabotagem informática, o acesso ilegítimo, a interação ilegítima ou a reprodução ilegítima de programas protegidos.

Destacamos também a Convenção sobre Cibercrime, do Conselho da Europa, realizada a 23 de Novembro de 2001 em Budapeste, que assumiu algumas conceções e soluções já expressas na Resolução (89) 9 do Conselho da Europa. Esta Convenção foi o primeiro e mais importante trabalho realizado ao nível internacional relacionado com a cibersegurança, constituindo um reconhecimento da criminalidade informática como um problema transfronteiriço, que requer partilha de esforços e soluções coletivas e a Convenção traduziu-se nessa partilha de conhecimento e esforços e promoção do consenso, com o intuito de alcançar melhores políticas de combate à cibercriminalidade entre os Estados-Membros (EM) da UE.

A criação da Agência Europeia para a Segurança das Redes e da Informação (ENISA), em 2004, veio "contribuir para a segurança das redes e da informação de alto nível entre a comunidade (europeia) e o desenvolvimento de uma cultura de segurança das redes e da informação" (Regulamento nº 460/2004, do Parlamento Europeu e do Conselho).

A criação do Centro Europeu de Cibercrime (EC3), em 2013, no seio da Polícia Europeia (EUROPOL), veio apoiar os EM da UE na definição de estratégias e na

investigação de cibercrimes e aplicação da respetiva legislação, bem como na divulgação de informação relacionada com este tipo de crimes, contribuindo para a consciencialização sobre esta matéria.

A medida da UE mais recente e mais significativa nesta matéria foi a aprovação da "Estratégia da União Europeia para a cibersegurança: Um espaço aberto, seguro e protegido", em 2013, "que define cinco prioridades para a ação política nesta área: a garantia da resiliência do ciberespaço; a redução drástica da cibercriminalidade; o desenvolvimento das políticas e das capacidades no domínio da ciberdefesa, no quadro da PCSD; o desenvolvimento de recursos industriais e tecnológicos para a cibersegurança; o estabelecimento de uma política internacional coerente em matéria de ciberespaço para a UE, que promova os valores fundamentais da mesma (JOIN(2013) 1 final)" (Santos, 2014: 14).

Estatística e opinião pública

A estatística "constitui um objecto de estudo, uma ciência, tal como a Matemática, e compreende (…) um conjunto de princípios e métodos de recolha, classificação, síntese e apresentação de dados numéricos" (Reis, 2000: 15).

Numa "época em que a quantidade de informação aumenta tão rapidamente, os centros de decisão têm necessidade de se manterem actualizados e controlarem as grandes massas de dados com que são inundados quase diariamente (…) é necessário que a informação lhes seja apresentada de forma a possibilitar a sua interpretação e a identificação das relações mais importantes" (Reis, 2000: 15). Portanto, esta ciência é importante para as políticas públicas, na medida em que, através da recolha e do tratamento de uma grande quantidade de dados, simplificando-os em indicadores, quadros, gráficos e números, quando os dados são qualitativos, "permite descrever e compreender relações entre variáveis", facilitando a tomada de decisão.

Apesar da estatística tratar dados numéricos, as fontes de análise estatística não têm que se tratar, obrigatoriamente, de dados quantitativos. Os inquéritos de opinião, como o EB Especial 371, aqui analisado, também são fontes de análise estatística. Para isso, as questões e, principalmente, as respostas dos inquiridos são codificadas em categorias e apresentadas em números, facilitando e tornando mais célere a sua análise estatística e análises extensivas, como é este o caso, uma vez que se trata de um inquérito colocado a uma amostra de 26.840 cidadãos, com 15 anos ou mais, de todos os então 27 EM da UE.

Estes inquéritos de opinião são particularmente importantes para os decisores políticos porque lhes permitem perceber qual é a perceção dos públicos-alvo de determinadas medidas de política pública sobre as mesmas, assim como sobre o desempenho desses decisores, além de permitir legitimar as suas decisões, principalmente em áreas de atuação que possam ser consideradas controversas ou polémicas, como poderia ser a segurança interna da UE, principalmente numa altura em que se analisava e discutia as alterações em matéria de segurança e defesa, resultantes da aprovação do Tratado de Lisboa.

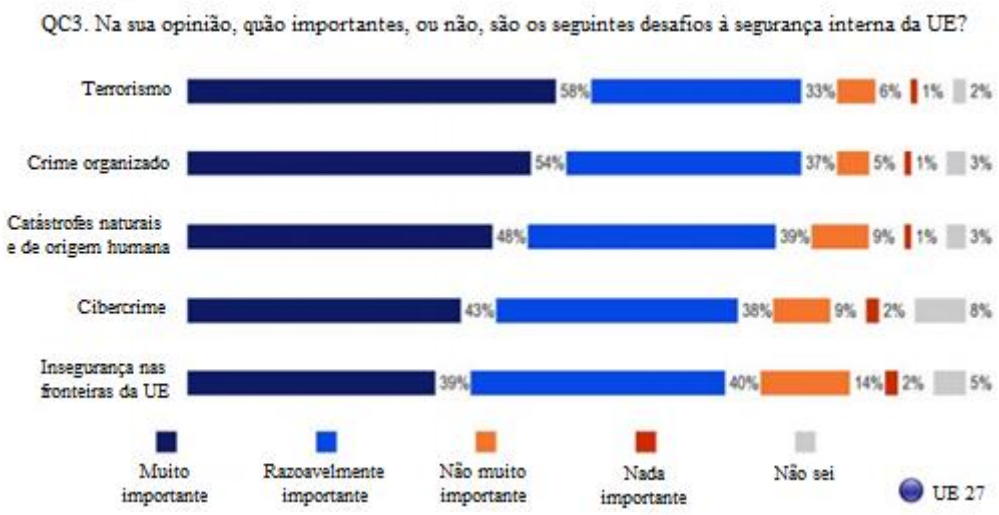
Contudo, são vários os autores (Karmasin e Pitters, 2008; Pausch, 2008; Haller, 2009; Nissen, 2012) que identificaram alguns limites metodológicos neste tipo de estudos, nomeadamente no Eurobarómetro, que se verificam também no EB Especial 371 e são identificados neste trabalho.

III. Dados do relatório

Dos dados apresentados no relatório do EB Especial 371, destaca-se a perceção dos inquiridos sobre: o grau de importância dos cinco principais desafios à segurança interna da UE; o grau de importância desses desafios para os concidadãos dos inquiridos; a evolução desses desafios nos três anos seguintes; a atuação da UE e dos governos europeus para enfrentar tais desafios. Estes são os dados que nos propomos analisar, por serem aqueles que mais informam acerca das perceções dos inquiridos sobre o cibercrime. Note-se que, apesar destes dados se referirem ao cibercrime, nem o questionário, nem o relatório apresentam uma definição de cibercrime que enquadre os dados recolhidos.

Quanto ao grau de importância atribuído aos cinco principais desafios à segurança interna da UE, tal como definidos na Estratégia de Segurança Interna da UE em Ação (2010) – criminalidade grave e organizada; terrorismo; cibercriminalidade; gestão das fronteiras externas; capacidade de resistência às catástrofes naturais e de origem humana –, o cibercrime ocupava o 4º lugar, com 43% dos inquiridos a considerarem-no um desafio "muito importante" e 38% "razoavelmente importante".

Figura 1: Importância dos cinco desafios à segurança interna da UE (%)



Fonte: Adaptado de European Commission, 2011, p. 25.

Um total de 81% dos inquiridos a considerarem a cibercriminalidade como um desafio, de alguma forma importante, à segurança interna da UE, é um indicador da consciência dos cidadãos europeus face aos perigos associados à dependência que a UE tem das redes e dos sistemas de comunicação e informação.

Este resultado não difere muito da visão estratégica da Comissão Europeia, nesta matéria, que coloca a cibercriminalidade, não em 4º, mas em 3º lugar, dos cinco maiores desafios colocados à segurança interna da UE, antes das catástrofes naturais e de origem humana.

A perceção dos inquiridos de que as catástrofes naturais e de origem humana seriam um desafio à segurança interna da UE, mais importante do que o cibercrime, contrariamente à priorização proposta pela Comissão Europeia, pode ter mais do que uma interpretação.

O inquérito foi realizado em 2011, ano que bateu o "recorde de perdas económicas com catástrofes naturais", de acordo com as estimativas da seguradora Swiss Re, como foi divulgado pelo Jornal de Negócios e pelo Público, entre outros meios de comunicação social, a 15 de dezembro de 2011. E, tal como divulgou o Centro Regional de Informação das Nações Unidas, já 2010 teria sido "um dos anos em que se registaram mais mortes provocadas por catástrofes naturais". Só na Europa, 20% do total de mortes teriam sido "consequência da vaga de calor que atingiu a Rússia" (UNRIC, 2011). Estes acontecimentos poderiam, por si só, justificar as respostas dadas, pelo terror e medo que provocam.

Contudo, nesses anos não aconteceram apenas catástrofes naturais, houve também vários ciberataques, embora as catástrofes, por provocarem morte e terror a quem passa por elas, bem como a quem assiste à distância, tendam a ser mais divulgadas e/ou a ficar mais na memória do que os ciberataques que, apesar de também provocarem enormes perdas aos seus alvos (e.g. financeiras e reputacionais) – normalmente grandes empresas, instituições financeiras ou Estados[3] –, geralmente poupam as vidas humanas.

Prova disso são alguns exemplos de ciberataques que, só em 2010 e 2011 (anos que deveriam estar mais presentes na memória dos inquiridos) provocaram graves danos na reputação e perdas financeiras avultadas aos seus alvos, mas que não foram tão divulgados como as catástrofes naturais (e.g. em 2010, a Paypal e uma Central Nuclear iraniana e em 2011 o governo da Índia, o governo do Canadá, a Citigroup, a Sony e a Epsilon foram alvos de ciberataques que se demonstraram onerosos, quer financeiramente, quer em termos reputacionais).

Ao analisarmos a importância atribuída a cada um dos cinco principais desafios à segurança interna da UE, por país [4], verifica-se que, apesar do nível de consciencialização dos cidadãos não ser exatamente igual em todos os EM da UE, os níveis de importância atribuída ao cibercrime, foram bastante elevados. Os inquiridos romenos foram aqueles que atribuíram menor importância ao cibercrime mas, mesmo assim, 73% consideraram-no como um desafio importante à segurança interna da UE.

[3] Muitos cidadãos, incluindo os europeus, são vítimas destes ciberataques, como os utilizadores de contas Google ou Paypal, mas como os fornecedores desses serviços necessitam garantir a confiança dos clientes nos seus serviços, para se manter no mercado, nem sempre divulgam a ocorrência deste tipo de incidentes, assumindo os custos e remediando essas situações, muitas vezes sem os clientes perceberem.

[4] Consultar Anexo, Figura 2, página 25.

Quando a questão se coloca como desafio à segurança dos cidadãos individuais, a importância atribuída ao cibercrime, como desafio à segurança interna da UE, diminui, passando de quarto para décimo lugar, entre um conjunto maior de possíveis desafios[5]. Os inquiridos que responderam a esta questão, consideraram as crises financeiras como o principal desafio à segurança dos cidadãos dos seus próprios países, no momento da aplicação do inquérito.

O inquérito foi aplicado em 2011, durante uma crise financeira, que tinha tido início em 2008 e que atingiu repercussões mundiais, tendo levado muitos europeus ao desemprego e ao risco de pobreza[6]. Este contexto, em conjunção com a, já referida, maior mediatização dos incidentes que provocam mortes e medo, assim como o facto das grandes organizações e governos serem alvos preferenciais de cibercrime[7] e não o divulgarem quando são vítimas desse tipo de crimes, mesmo que isso possa afetar os seus clientes, propicia a atribuição de menor importância ao cibercrime e maior importância às crises financeiras, que se refletem diretamente no dia-a-dia dos inquiridos, através da diminuição do seu poder de compra, por exemplo.

Estes dados são relevantes para os decisores políticos europeus, neste caso a Comissão Europeia, que encomendou o inquérito, na medida em que evidenciam que o facto do cibercrime não se refletir no dia-a-dia dos inquiridos (pelo menos de forma evidente) leva à desvalorização deste fenómeno, como um desafio à segurança dos cidadãos, para a maioria dos inquiridos. Isto poderá demonstrar a necessidade de investir mais na formação e consciencialização dos cidadãos europeus, para os riscos associados ao uso da Internet, assim como para a relação entre o uso desprotegido, da parte dos cidadãos, e a segurança das redes e dos sistemas informáticos dos seus Estados e da própria UE.

Note-se que, a cibersegurança da UE (mais premente para os inquiridos do que a cibersegurança dos cidadãos) depende da utilização que os cidadãos europeus fazem da Internet. Cidadãos com pouca informação e consciencialização sobre o cibercrime, que estão mais desprotegidos e que tenham determinado tipo de contacto com as instituições europeias (e.g. fornecedores, clientes, funcionários), podem ser "portas de entrada" para as redes e os sistemas informáticos estratégicos da UE. Por essa razão existe, desde 2004, a Agência Europeia para a Segurança das Redes e da Informação - ENISA -, que deve "promover uma abordagem global para as questões da segurança das redes e da informação na comunidade (europeia)", bem como, "o desenvolvimento de uma cultura de segurança das redes e da informação" (Regulamento nº 460/2004, do Parlamento Europeu e do Conselho).

No entanto, se analisarmos os resultados por país, verifica-se que os inquiridos que atribuíram maior importância ao cibercrime como desafio à segurança interna da UE, tenderam a atribuir-lhe também maior importância como desafio à segurança dos

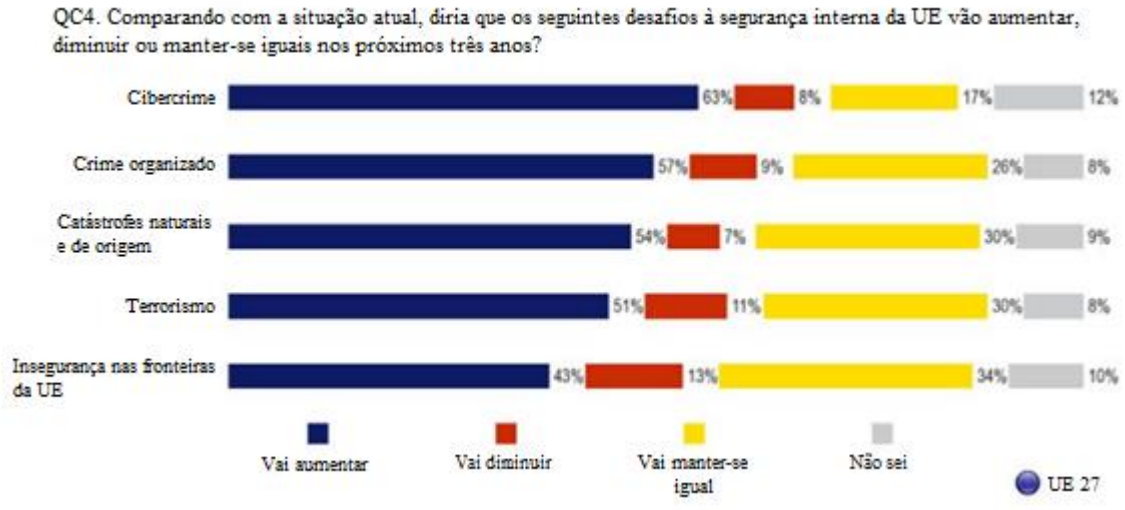
[5] Consultar Anexo, Figura 3, página 26.
[6] Consultar Anexo, Figuras 4 e 5, páginas 26 e 27.
[7] Os alvos preferenciais do cibercrime são grandes organizações e Estados, em detrimento de cidadãos individuais porque as motivações para este tipo de crime são geralmente financeiras ou políticas.

cidadãos do seu país (Alemanha, Holanda, Áustria e República Checa)[8]. Destes, destacam-se as respostas dos inquiridos da Alemanha, da Holanda e da República Checa, que atribuíram maior importância ao cibercrime como desafio à segurança dos cidadãos dos seus países do que à segurança interna da UE. Tais respostas poderão estar relacionadas com o facto destes três países terem publicado estratégias nacionais de cibersegurança em 2011[9], podendo os inquiridos ter assistido a debates públicos sobre esta matéria, no ano em que o inquérito foi aplicado e possivelmente estarem mais conscientes da existência da cibercriminalidade.

É interessante reparar que estes países não foram os únicos a publicar estratégias nacionais de cibersegurança em 2011, França e o Reino Unido também publicaram. Contudo, no mesmo ano, a redação do Semanário Charlie Hebdo, em Paris, sofreu um ataque terrorista e o Reino Unido viu a ameaça de ataques terroristas do NIRT (North Ireland Related Terrorism) aumentar (Home Office, 2011: 5). E, como já foi referido, o terror é mais mediatizado e tende a ficar mais na memória dos indivíduos, podendo ter contribuído para a priorização escolhida pelos inquiridos para cada um destes desafios à sua segurança.

Retomando a questão anterior, apesar dos inquiridos considerarem que o cibercrime estaria em 4º lugar, dos cinco maiores desafios à segurança interna da UE, consideraram que era aquele que mais iria crescer nos anos seguintes. Dos 26.840 inquiridos, 63% acreditava que o cibercrime iria crescer nos três anos seguintes, principalmente os inquiridos com níveis de escolaridade mais elevados e com a profissão "gestor" (72%)[10].

Figura 2: Evolução dos desafios à segurança interna da UE, nos próximos três anos (%)



Fonte: Adaptado de European Commission, 2011, p. 38.

[8] Consultar Anexo, Figura 6, página 27.
[9] A Áustria só publicou a sua Estratégia Nacional de Cibersegurança em 2012.
[10] Consultar Anexo, Figura 7, página 28.

Estes resultados demonstram a perceção que os inquiridos tinham do aumento da cibercriminalidade, ao qual temos vindo a assistir continuamente. Segundo um relatório das ameaças à cibersegurança, da McAfee, o número de incidentes de segurança (incluindo o cibercrime) duplicou entre 2009 e 2010 e continuou a crescer (McAfee, 2011).

O facto de os "gestores" estarem mais conscientes desta realidade poderá estar relacionado com o facto de serem aqueles que devem ter um conhecimento mais abrangente da realidade das suas organizações, uma vez que devem ser informados da ocorrência de todos os incidentes, incluindo os de segurança informática, principalmente aqueles que impliquem algum investimento para a sua resolução. A ocorrência desses incidentes tende a não ser transmitida aos restantes funcionários, para não se tornarem do conhecimento púbico, pois as organizações dependem da sua reputação e da confiança nelas depositada pelos clientes, para se manterem no mercado.

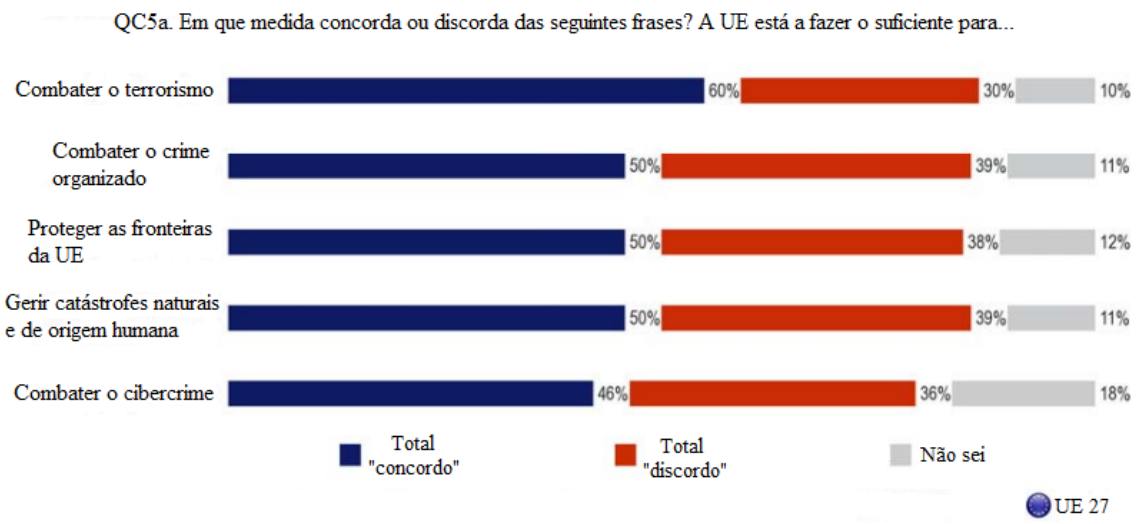
O mesmo se aplica aos Estados, que dependem da confiança neles depositada, para manterem a sua posição no cenário internacional, bem como a reputação das instituições públicas e do governo vigente.

Neste enquadramento, é possível perceber que muitos incidentes de segurança das redes e dos sistemas de informação poderão não ser divulgados pelas organizações, nem pelos Estados, distorcendo a realidade percebida pelos cidadãos, relativamente ao cibercrime. Face a isto, desde 2012, o Parlamento Europeu e o Conselho têm vindo a desenhar uma diretiva para a segurança das redes e dos sistemas de informação, que veio a ser aprovada em 2015 e obriga a informação do público, sobre a ocorrência de incidentes de segurança das redes e dos sistemas de informação, de forma a garantir a transparência e a correta informação dos cidadãos[11].

Quando questionados sobre a atuação da UE para combater o cibercrime, apenas 46% dos inquiridos consideraram que estaria a fazer o suficiente, sendo, dos cinco, o desafio perante o qual a UE teria um pior desempenho, como se pode verificar na figura seguinte.

[11] Nesse âmbito, em Portugal, a ANACOM (Autoridade Nacional de Comunicações) criou, em 2014, um centro de reporte de falhas das redes e serviços de telecomunicações e passou a obrigar os operadores de serviços de comunicações a notificar, em tempo real, "todas as violações de segurança ou perdas de integridade que causem perturbações graves no funcionamento das redes (…) ou nos serviços prestados aos utilizadores", além de terem que "informar o público, divulgando informação sobre os incidentes registados nos respetivos *sites* na Internet" (ANACOM, 2014).

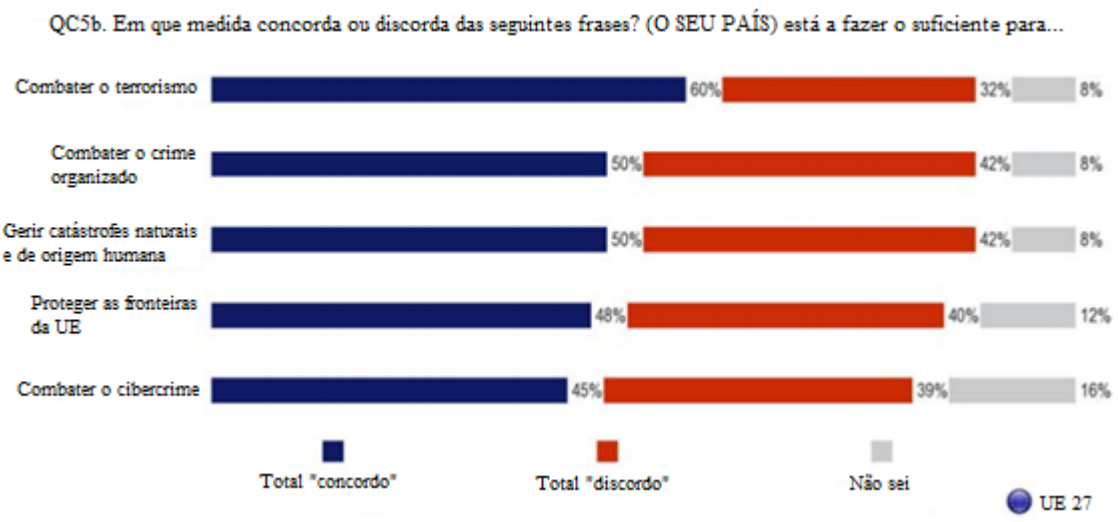
Figura 3: Atuação da UE para enfrentar os desafios à sua segurança interna (%)



Fonte: Adaptado de European Commision, 2011, p. 52.

A mesma questão foi colocada, mas em relação à ação dos Estados para combater o cibercrime, e os resultados foram semelhantes, como se pode verificar adiante.

Figura 4: Atuação dos Estados-Membros para enfrentar os desafios à segurança interna da UE (%)



Fonte: Adaptado de European Commission, 2011, p. 65.

Com base nestes valores, poder-se-ia inferir que a perceção de muitos dos inquiridos sobre as ações tomadas pela UE, pelo menos nesta matéria, teriam base nas ações nacionais, ou seja, aquelas que lhes são mais facilmente visíveis. Isto poderia indiciar a distância entre os cidadãos e as instituições e políticas europeias, para a qual as diferentes línguas e a diversidade cultural, cada vez maior, podem contribuir e que pode ser verificada através dos baixos níveis de sentimento de pertença à UE ou de confiança

nas instituições europeias, nomeadamente na Comissão e no Parlamento Europeu (ver Eurobarómetro Interativo, no *website* da Comissão Europeia).

Todavia, essa distância das instituições e políticas europeias pode também ser fruto das próprias ações nacionais, uma vez que os governos tendem a ficar com os créditos de medidas resultantes de orientações ou mesmo imposições da UE. Exemplo disso é o documento que cria o Centro Nacional de Cibersegurança, em Portugal (Decreto-Lei nº 69/2014, de 9 de maio), que não faz qualquer referência às orientações da UE, para a criação desta entidade, além de não ter sido muito divulgado.

Porém, através de uma análise destas respostas por país, constata-se que os mais descontentes com a atuação da UE, não foram os mesmos que consideraram que os seus países não estariam a fazer o suficiente para combater o cibercrime[12].

Os inquiridos dos países que são membros da UE há mais tempo (Holanda, França, Reino Unido, Luxemburgo e Alemanha) tenderam a estar mais descontentes com a atuação da União no combate ao cibercrime, o que poderá estar relacionado com o facto de poderem ter um relacionamento mais próximo e estar mais familiarizados com a história e o funcionamento da UE, conseguindo comparar melhor a atuação dos seus países com a de outros e da própria União, além de contribuírem mais para o orçamento da comunidade e possivelmente dependerem mais da infraestrutura de Internet para o normal funcionamento dos seus serviços e, por isso, estarem mais conscientes da necessidade de todos os países, pelo menos os da UE, terem políticas, legislação, bem como as capacidades necessárias para garantir a proteção contra o cibercrime.

Os inquiridos dos países que são membros mais recentes da UE (Letónia, Bulgária, Roménia, Lituânia) e a Grécia foram mais críticos com a atuação dos seus governos, possivelmente por se sentirem mais distantes (pelo menos fisicamente, da capital da UE, Bruxelas) e menos familiarizados com o seu funcionamento, tendo dependido apenas dos seus governos para garantir a sua segurança até poucos anos antes da aplicação do inquérito.

É relevante evidenciar que estes países fazem parte das fronteiras da UE, nomeadamente com a Rússia que, alegadamente, perpetrou um ciberataque massivo à Estónia (país vizinho e membro da UE), em 2007 e outro à Geórgia (também país vizinho), em 2008 (Clarke and Knake, 2012).

As respostas dos inquiridos eslovenos destacam-se por serem dos mais descontentes, tanto com a atuação da UE, como do próprio governo, para combater o cibercrime – 49% considerava que a UE não estaria a fazer o suficiente e 61% considerava que o seu país não estaria a fazer o suficiente para combater o cibercrime. Estas respostas podem justificar-se com o facto do governo esloveno ter começado a investir nesta área apenas

[12] Consultar Anexo, Figuras 8 e 9, páginas 28 e 29.

em 2011 e com projetos dedicados somente a dois públicos restritos, podendo não ter chegado informação aos restantes cidadãos eslovenos[13].

Houve também uma quantidade considerável de respostas "não sei" a estas questões, especialmente dos inquiridos da Irlanda, da Polónia, da Bulgária e de Malta (acima de 25% das respostas). Com estes resultados pode-se inferir que os inquiridos destes países estariam pouco familiarizados com a terminologia e/ou pouco informados e sensibilizados para os riscos associados ao uso da Internet, o que poderia ser reflexo da ausência de estratégias e políticas nacionais de cibersegurança nestes países, até ao momento da aplicação do inquérito[14].

As respostas dos inquiridos da Estónia destacam-se por ser as mais positivas em relação às ações da UE e do próprio país, para combater o cibercrime.

A posição extremamente positiva dos inquiridos estonianos poderá estar relacionada com o facto da UE e da OTAN, terem juntado esforços e recuperado rapidamente as redes e os sistemas de informação da Estónia, quando foi alvo de um ciberataque massivo, que afetou serviços da Administração Pública, serviços bancários, entre outros e na sequência desse ataque, a OTAN ter instalado um Centro de Excelência em Ciberdefesa na Estónia, que funciona, desde então, como um polo internacional de investigação em matéria de cibersegurança e ciberdefesa, tornando a Estónia num *hub* de conhecimento sobre esta matéria (Clark e Knake, 2012).

Possivelmente, é por ser um *hub* de conhecimento nesta matéria que os inquiridos da Estónia, que podem estar mais familiarizados com a terminologia relacionada com o ciberespaço, foram dos que deram menos respostas "não sei" às questões relacionadas com o cibercrime.

Os resultados apresentados informam os decisores políticos competentes da necessidade de informar e consciencializar mais os cidadãos dos países do leste da Europa (e.g. Letónia, Bulgária, Roménia, Lituânia) e ajudar os seus governos a divulgar melhor as suas iniciativas nesta área. Verifica-se também que os países que mais contribuem para o orçamento da UE (e.g. França, Reino Unido, Alemanha e Holanda), tendem a ser mais exigentes com a sua atuação no combate ao cibercrime, à semelhança do que acontece com os outros quatro desafios colocados à segurança interna da União.

Constata-se também a necessidade de ajudar especialmente alguns países (particularmente a Bulgária e Malta), nos quais grandes percentagens das respostas sobre a atuação dos seus governos ou da UE para combater o cibercrime foram "não

[13] Em 2011, o governo esloveno implementou duas medidas de consciencialização e desenvolvimento de uma cultura nacional de cibersegurança, embora apenas direcionadas para crianças e jovens, e empresas (Republic of Slovenia, 2016).

[14] A Polónia publicou uma Política Nacional de Proteção do Ciberespaço em 2013, Malta publicou uma Estratégia Digital Nacional em 2014 e um Livro Verde para a Cibersegurança Nacional em 2015, no mesmo ano em que a Irlanda publicou uma Estratégia Nacional de Cibersegurança. A Bulgária ainda não tem uma estratégia ou política publicada nesta área.

sei", o que sugere falta de conhecimento e esclarecimento sobre este assunto, tornando-os dos pontos mais vulneráveis da UE nesta matéria.

IV. Utilidade do EB Especial 371 para a avaliação da Estratégia de Segurança Interna da UE

Na introdução do relatório do EB Especial 371 constam os dois objetivos principais que se pretende alcançar com o mesmo: "providenciar uma visão estratégica através da comparação e contraste das perceções públicas com a abordagem tomada na Estratégia de Segurança Interna" da UE em Ação; "estabelecer *benchmarks* para futura reavaliação", uma vez que o relatório iria acompanhar o primeiro relatório anual da implementação da Estratégia (European Commission, 2011).

Considera-se que o primeiro objetivo foi alcançado, uma vez que as questões do inquérito foram desenhadas de forma a permitir comparar a perceção dos inquiridos com a abordagem tomada na Estratégia de Segurança Interna da UE em Ação.

As respostas à questão "Na sua opinião, quão importantes ou não são os seguintes desafios à segurança interna da UE?", permitem reiterar a importância atribuída a estes desafios, na Estratégia, já que, em média, 85% dos inquiridos considerou o conjunto destes desafios de alguma forma importante.

A Estratégia de Segurança Interna da UE aposta, por um lado, na sensibilização e consciencialização dos cidadãos europeus, como se pode verificar em algumas das medidas propostas: a criação de "um centro de cibercriminalidade (…) que apoiará o desenvolvimento da formação e a sensibilização nos domínios policial e judiciário"; o encorajamento aos EM para "desenvolver, até 2013, as suas capacidades nacionais em matéria de sensibilização e formação" e "assegurar a fácil comunicação pelos cidadãos a orientações sobre ameaças informáticas e as precauções a tomar" (COM(2010) 673 final).

Os resultados do inquérito confirmam essa necessidade de investir na formação e sensibilização dos cidadãos para as questões relacionadas com o cibercrime. Como vimos, o facto dos inquiridos considerarem que o cibercrime é um desafio mais importante para a segurança da UE do que a dos seus concidadãos, pode indiciar a necessidade de informar e consciencializar os cidadãos para a relação entre o uso individual desprotegido da Internet e o funcionamento das redes e dos sistemas informáticos da UE.

Confirmam também a necessidade de informar os cidadãos em geral, uma vez que os inquiridos com a profissão "gestor" tenderam a estar mais informados sobre a evolução do cibercrime, em comparação com os restantes inquiridos.

É de notar também que, como já foi referido, a maior percentagem de respostas "não sei" foi às questões relacionadas com o cibercrime, o que também nos permite inferir o

desconhecimento existente sobre esta questão, tão específica e possivelmente menos familiar para os inquiridos mais idosos, por exemplo.

Os resultados também transpareceram uma possível distância, já referida, entre os cidadãos e as instituições e as políticas europeias. Todavia, a própria Estratégia também já previa medidas para tentar solucionar esse problema, como a criação de "um centro de cibercriminalidade, através do qual os Estados-Membros e as instituições da UE poderão desenvolver capacidades operacionais e (…) a cooperação com parceiros internacionais" ou as orientações para os Estados-Membros, juntamente com a ENISA, "realizarem (…) exercícios nacionais e europeus" (COM(2010) 673 final).

Por outro lado, a Estratégia também aposta na capacitação da UE e dos Estados-Membros para garantir a cibersegurança da comunidade. Exemplos de medidas propostas neste âmbito são: o estabelecimento, até 2013, de "um centro de cibercriminalidade, através do qual os Estados-Membros e as instituições da UE poderão desenvolver capacidades operacionais e analíticas para as investigações"; o desenvolvimento de "um sistema europeu de alerta e partilha de informação (EISA – *European Information Sharing and Alert System*)"; o desenvolvimento de "medidas e instrumentos inovadores para melhorar a segurança (…) das infra-estruturas críticas, e a resistência das redes e das infra-estruturas de informação"; a orientação para os Estados-Membros disporem, "até 2012, de uma equipa de emergência de respostas no domínio informático" e construírem "até 2012 uma rede formada pelas suas equipas de emergências nacionais/governamentais de respostas no domínio informático"; orientações para os Estados-Membros elaborarem, juntamente com a ENISA, "planos de contingência nacionais e realizarem (…) exercícios nacionais e europeus em matéria de respostas a incidentes e recuperação em caso de catástrofe" (COM(2010) 673 final).

Os resultados do Eurobarómetro também confirmam a perceção dos inquiridos sobre a necessidade de capacitar melhor os Estados e a própria UE para combater o cibercrime, nomeadamente através do facto de 63% considerar que o cibercrime iria aumentar nos três anos seguintes à aplicação do inquérito sendo, dos cinco desafios, aquele que os inquiridos consideraram que mais iria aumentar nos anos seguintes e de apenas 46% considerar que a UE estaria a fazer o suficiente para o combater, enquanto também apenas 45% considerava que os seus países estariam a fazer o suficiente nessa matéria.

Estes resultados permitiram não só confirmar a necessidade de implementar medidas anteriormente propostas, mas também legitimar a aplicação de outras que, embora não constassem na Estratégia de Segurança Interna da UE em Ação, constavam noutros documentos emanados pela UE (e.g. COM(2001) 298; COM(2006) 251 final; COM(2009) 149 final; COM(2010) 245 final), tal como a criação de uma Estratégia da União Europeia para a Cibersegurança. Assim, considera-se que os resultados do EB Especial 371 não promoveram o desenvolvimento de novas medidas de política na área da cibersegurança, mas legitimaram aquelas já planeadas no seio da UE.

Permitiram legitimar a implementação de medidas possivelmente mais dispendiosas, como a criação do centro europeu de cibercriminalidade ou do sistema europeu de alerta

e partilha de informações (EISA), pois os inquiridos, de uma forma geral, consideravam que a UE não estaria a fazer o suficiente para combater o cibercrime. Tais resultados permitiram também a colocação de imposições aos EM, como a criação de equipas de resposta a emergências informáticas, até 2012, a criação de redes nacionais formadas por essas equipas, também até 2012 ou terem que assegurar a fácil comunicação aos cidadãos de atos de cibercriminalidade, uma vez que os inquiridos também consideravam que os seus países não estariam a fazer o suficiente nesta área e verificou-se algum desconhecimento e falta de sensibilização para a cibercriminalidade.

Relativamente ao segundo objetivo apresentado, verifica-se que o relatório deste Eurobarómetro Especial permite o estabelecimento de *benchmarks* da perceção dos inquiridos (podendo ser daí inferida a perceção dos cidadãos europeus) sobre questões relacionas com o cibercrime, como a atuação da UE e dos seus governos para o combater, no momento da aplicação do inquérito (cerca de um ano após a aprovação da referida Estratégia de Segurança Interna da UE), que poderiam ser comparados com futuros inquéritos, desde que fossem realizados nas mesmas condições e com as mesmas questões. Contudo, até ao momento, podendo ter havido alguma réplica do inquérito, para comparar os resultados e auxiliar na avaliação da implementação da Estratégia, não terá sido um Eurobarómetro Especial sobre a temática, nem terá sido publicado, o que sugere que o EB Especial 371 poderá ter sido encomendado com um principal intuito de legitimar as medidas propostas na Estratégia de Segurança Interna da UE, assim como outras medidas propostas nesta área de atuação.

Constatou-se que o primeiro relatório da implementação da referida Estratégia, ao qual terá sido anexado o relatório do EB Especial 371, não faz qualquer referência aos dados deste Eurobarómetro, transmitindo a ideia de que se trata de um documento auxiliar, com um propósito diferente do de avaliar a implementação da Estratégia. Além disso, muita da informação que pode ser inferida dos resultados do relatório do EB Especial 371, como a que é apresentada neste trabalho, não foi considerada para o desenho de medidas futuras, nomeadamente para o desenho de medidas específicas para os EM cujos inquiridos aparentem conhecer pior o fenómeno.

Christou (2016: 6) justificaria esta atuação da Comissão Europeia com o papel essencial da UE na criação de uma cultura de resiliência e cibersegurança, não apenas na Europa, mas também globalmente, o que implica mais investimento e implementação de mais medidas nesta área, que devem ser legitimadas pelos cidadãos europeus.

V. Metodologia

Como foi referido anteriormente, os estudos de opinião, por vezes, apresentam algumas limitações metodológicas, que têm vindo a ser analisadas por vários autores (Haller, 2009; Nissen, 2012; Höpner e Jurczyk, 2015) e que podem comprometer a sua utilidade como base para decisões políticas e investigação.

Contudo, algumas dessas "falhas metodológicas" podem ser fabricadas de acordo com o objetivo do estudo e, como foi possível constatar, os resultados do EB Especial 371 parecem contribuir mais para a legitimação da aplicação de mais medidas e investimento na cibersegurança do que para uma avaliação da implementação da Estratégia de Segurança Interna da UE em Ação, no que concerne ao cibercrime. Até porque a Comissão Europeia dispõe de instrumentos de avaliação muito melhores do que o Eurobarómetro (Comissão Europeia, 1993, 1999).

O EB Especial 371 apresenta algumas dessas limitações na tradução, na formulação das questões colocadas no inquérito, na análise dos dados recolhidos e ainda no facto da entidade contratante ser a Comissão Europeia.

O questionário do EB Especial 371, foi aplicado nas línguas dos países onde foram recolhidos os dados, tendo sido traduzido para todas essas línguas, através do método de "back-translation", ou seja, "um tradutor prepara a tradução do questionário e um segundo tradutor, que não conhece o questionário original, traduz novamente as questões para a língua original. A linguagem das duas versões é comparada e o texto na língua alvo é então adaptado e otimizado" (Wendt-Hilderbrandt *et al.*, 1983; Nissen, 2012).

No entanto, apesar de esta ser uma técnica refinada para apurar a competência dos tradutores, não permite ter o controlo necessário sobre a equivalência do significado das palavras ou das expressões, o que se pode refletir nas respostas e influenciar os resultados (e.g. as respostas críticas dos eslovenos, tanto face à ação da UE, como dos seus países, poderão estar relacionadas com a tradução) (Scheuch, 1993).

É relevante notar que apenas estão publicados os questionários em inglês, francês e alemão, o que impede os investigadores interessados de fazerem uma comparação de todas as traduções, para confirmar a sua qualidade e possíveis interferências nos resultados.

Quanto às questões colocadas, Höpner e Jurczyk (2015), com base em diversos manuais de metodologia (Ellard and Rogers, 1993; Bryman, 2004; Iarossi, 2006; Babbie, 2007) propõem a utilização de "10 mandamentos" considerados como boas práticas no estudo de opinião e que, segundo estes autores, os peritos na área de estudos de opinião, incluindo os responsáveis pelo Eurobarómetro, devem conhecer.

Segundo estas regras, as questões: 1) devem ser simples e percetíveis; 2) não devem ser hipotéticas; 3) devem exigir apenas conhecimento que os inquiridos têm realmente; 4) devem evitar estímulos duplos, i.e., evitar ter mais do que um assunto por questão; 5) devem evitar terminologia pouco clara; 6) devem evitar referências temporais pouco exatas; 7) com vários itens, devem ter opções de resposta positivas e negativas; 8) devem evitar insinuações e questões que possam influenciar as respostas; 9) devem ter opções de resposta equilibradas, logicamente completas e que não se sobreponham; 10) devem evitar efeitos contextuais, ou seja, as questões não devem ser ordenadas de forma estratégica influenciando as respostas seguintes.

Analisando as questões do inquérito, com base nestas regras, verifica-se que a questão em que se pede aos inquiridos para imaginar a evolução do cibercrime, nos três anos seguintes, não cumpre a segunda regra pois, apesar de se tratar da opinião dos inquiridos, é uma situação hipotética. Quanto à terceira regra, verifica-se que o questionário não inclui questões que testem o conhecimento dos inquiridos sobre o cibercrime, podendo até nem saberem do que se trata, uma vez que se poderia tratar de um fenómeno pouco conhecido para alguns, principalmente os cidadãos com menos literacia informática.

A quinta regra também parece não ter sido cumprida, já que o questionário não inclui a definição de cibercrime, por exemplo. Quanto à oitava regra, é discutível mas, por um lado, considera-se que a inclusão da expressão "quão importantes ou não importantes são os seguintes desafios" poderá ser algo "enviesadora", podendo ter sido substituída por "qual a importância dos seguintes desafios", imprimindo maior neutralidade à questão colocada. Por outro lado, a utilização da expressão "está a fazer o suficiente" também poderá enviesar as respostas, podendo ter-se questionado qual a opinião dos inquiridos sobre a atuação no combate ao cibercrime, com opções como: "muito adequada/muito boa"; "adequada/boa"; "nem adequada, nem desadequada/nem boa, nem má"; "pouco adequada/má"; "muito pouco adequada/muito má"; "Não sei", por exemplo.

Relativamente à nona regra, constata-se que as questões QC3, QC5a e QC5b[15] carecem de uma opção de resposta neutra, entre "razoavelmente importante" e "não muito importante" e entre "tendo a concordar" e "tendo a discordar".

Considera-se ainda que a décima regra também não foi cumprida neste Eurobarómetro, uma vez que a questão sobre a evolução do cibercrime nos três anos seguintes poderá condicionar as respostas às questões seguintes, sobre a suficiência da ação da UE e dos seus países, para o combater, dado que, se os inquiridos considerarem que determinado fenómeno irá crescer nos próximos anos, provavelmente considerarão que será necessário atuar mais nessa área, o que legitima a ação da UE (como vimos, já planeada) nesse campo.

A análise dos dados apresentada no relatório é principalmente descritiva, sem ter em atenção fatores que vão além dos socio-demográficos e que podem influenciar as respostas, assim como a própria comparabilidade dos dados.

Um desses fatores é o contexto em que o inquérito é aplicado. O inquérito foi aplicado em todos os países da UE no mesmo período temporal: entre 4 e 19 de junho de 2011. Porém, as realidades sociais e políticas podiam ser diferentes nos diversos países, sendo necessário contextualizar as respostas de acordo com essas realidades (e.g. em 2011 vários foram os países que estavam a desenvolver medidas na área da cibersegurança, nomeadamente a publicação das suas Estratégias Nacionais de Cibersegurança).

[15] Consultar Figuras 1, 3 e 4, das páginas 5 e 10.

Outro fator é o contexto cultural em que são aplicados os inquéritos. Os diferentes *standards* culturais e níveis de desenvolvimento existentes na UE podem influenciar as respostas e não são considerados na estandardização dos procedimentos de condução dos inquéritos, nem na análise dos resultados (Nissen, 2012: 722). Neste âmbito, Scheuch (1993) e Karmasin e Pitters (2008) demonstram que, contrariamente aos países do Norte e Centro da Europa, os residentes na Roménia, por exemplo, sentem alguma dificuldade em dar a sua opinião. Esta será outra possibilidade de explicação para a grande percentagem de respostas "não sei" em determinados países.

Ainda outro fator influenciador das respostas é o facto de o questionário ser aplicado presencialmente, por um entrevistador que representa, na realidade, a Comissão Europeia, que é a entidade que encomenda estes estudos. Neste âmbito, Haller (2009) defende a existência de uma correlação positiva entre a participação em inquéritos conduzidos pela UE e a tendência para responder de maneira positiva em relação à União.

A influência da Comissão Europeia nos resultados do Eurobarómetro, incluindo o Especial 371, não se verifica apenas desta forma. A Comissão financia o Eurobarómetro, nomeadamente através de contratos com a empresa de estudos de mercado que os realiza – TNS Opinion & Social -, determina as questões que são colocadas, tem o monopólio da interpretação dos dados e ainda publica os resultados (Tomaselli, 2003). Como assume Reif (1991), o que é e o que não é perguntado é reflexo das suas expectativas políticas de "bons resultados".

A Comissão, pelo menos numa primeira fase, tem acesso exclusivo aos dados e faz uso do seu monopólio da interpretação dos resultados do inquérito através da definição de quais são os resultados considerados relevantes e afastando a atenção daqueles que são considerados menos relevantes, garantindo que são apresentados de uma forma muito simplificada, por exemplo (Nissen, 2012: 724). É de salientar ainda que é publicada muito pouca informação metodológica. O EB Especial 371 não inclui, por exemplo, informação sobre as "não resposta" ou as condições de recolha dos dados.

Como forma de legitimar a credibilidade dos resultados, a "Comissão enfatiza que os relatórios refletem apenas a visão dos autores do Eurobarómetro e não da Comissão, mas não é dada mais informação sobre quem são esses autores (Pausch, 2008: 547), o que também se verifica no EB Especial 371, sugerindo alguma falta de transparência na apresentação dos resultados.

Além destas, o EB Especial 371 poderá apresentar outras limitações metodológicas, embora não sejam analisadas neste documento, principalmente pela dificuldade em encontrar informação pública (e.g. rigor na seleção da amostra e na aplicação dos questionários).

VI. Conclusões

Neste trabalho é feita uma análise dos resultados e das questões relacionadas com o cibercrime, colocadas no EB Especial 371, relativo à segurança interna da União Europeia.

Este Eurobarómetro foi encomendado pela Comissão Europeia à TNS Opinion & Social, uma empresa privada de estudos de mercado, com o propósito de "providenciar uma visão estratégica através da comparação e contraste das perceções públicas com a abordagem tomada na Estratégia de Segurança Interna da UE", assim como "estabelecer *benchmarks* para futura reavaliação" (European Commission, 2011: 4).

O relatório dos resultados iria "acompanhar o primeiro relatório anual da implementação da Estratégia de Segurança Interna da UE" em Ação, podendo assim, ser considerado um instrumento de política da Comissão Europeia.

Com base na análise dos dados, considera-se que o primeiro objetivo foi alcançado, uma vez que as questões do inquérito foram desenhadas de forma a permitir comparar a perceção dos inquiridos com a abordagem tomada na Estratégia. Confirmou-se que várias das medidas propostas e em fase de implementação viriam suprimir necessidades confirmadas com os resultados do relatório do Eurobarómetro.

No que respeita ao segundo objetivo, constata-se que o relatório permite estabelecer *benchmarks* da perceção dos inquiridos sobre questões relacionadas com o cibercrime, como a atuação da UE e dos seus EM para o combater, no momento da aplicação do inquérito, que poderiam ter sido comparados posteriormente, mediante a aplicação de um novo inquérito, nas mesmas condições e com as mesmas questões. Não obstante, até ao momento não terá sido publicado outro Eurobarómetro com as mesmas questões, que permitisse comparar os resultados e auxiliar na avaliação da implementação da referida Estratégia, o que poderá indiciar que o EB Especial 371 terá sido encomendado com o principal objetivo de legitimar a implementação de medidas planeadas na área da cibercriminalidade, incluindo as da Estratégia de Segurança Interna da UE.

É importante salientar o valor dos Eurobarómetros como base de estudo. Os Eurobarómetros são grandes fontes de informação que permitem análises extensivas e longitudinais sobre as mais variadas temáticas e comparações entre um grande conjunto de países. Não será por acaso que, desde que surgiram, em 1973, têm sido fontes de vários trabalhos de investigação (Höpner e Jurczyk, 2015). No entanto, tendem a apresentar algumas limitações metodológicas (Scheuch, 1993; Nissen, 2012; Karmasin e Pitters, 2008; Haller, 2009).

O EB Especial 371, à semelhança de outros, também apresenta limitações metodológicas, sendo a mais flagrante a falta da definição do conceito de cibercrime no questionário, sobre o qual os inquiridos têm que responder a diversas questões (não sendo assim possível confirmar o conhecimento dos inquiridos sobre o assunto). Apresenta também limitações ao nível da formulação das questões e das hipóteses de

resposta, assim como na análise dos resultados, que convergem em alguma falta de rigor e de transparência na apresentação dos resultados, contribuindo para a corrente que critica o Eurobarómetro como fonte de conhecimento e de análise estatística, em favor de uma visão do mesmo como um instrumento de política da Comissão Europeia – a entidade mais interessada, que financia e orienta a forma como são conduzidos estes estudos.

VII. Referências bibliográficas

ANACOM, 2014. *ANACOM cria centro de reporte de falhas das redes e serviços de telecomunicações*. Consultado em 19 de maio de 2016. Disponível em: http://www.anacom.pt/render.jsp?contentId=1248312#.V1c2o7grJdi

Babbie, E., 2007. *The Practice of Social Research*. Belmont: Thomson Wadsworth.

Bryman, A., 2004. Social Research Methods. Oxford: Oxford University Press.

Christou, G., 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Hampshire: Palgrave Macmillan UK.

Clarke, R. and Robert Knake, 2012. *Cyber War: The next threat to national security and what to do about it*. New York: HarperCollins.

Comissão Europeia, 1993. *Manual de Gestão do Ciclo do Projeto: Abordagem Integrada e Quadro Lógico*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias.

Comissão Europeia, 1999. *Evaluating socio economic development*. Luxemburgo: Serviço das Publicações Oficiais das Comunidades Europeias.

Comissão Europeia - COM(2001) 298 final (Segurança das redes e da informação: Proposta de abordagem de uma política europeia).

Comissão Europeia - COM(2006) 251 final (Estratégia para uma sociedade da informação segura – "Diálogo, parcerias e maior poder de intervenção")

Comissão Europeia - COM(2009) 149 final (Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência)

Comissão Europeia - COM(2010) 245 final (Uma Agenda Digital para a Europa)

Comissão Europeia - COM(2010) 673 final (Estratégia de Segurança Interna da UE em Ação: cinco etapas para uma Europa mais segura)

Comissão Europeia - COM(2011) 163 final (Protecção das infra-estruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial»)

Comissão Europeia – JOIN(2013) 1 final (Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido)

Decreto-Lei nº 69/2014, de 9 de maio (estabelece os termos de funcionamento do Centro Nacional de Cibersegurança)

Ellard, J. and Timothy Rogers, 1993. Teaching Questionnaire Construction Effectively: The Ten Commandments of Question Writing. *Contemporary Social Psychology*, 17(1), 17–20.

European Commission, 2008. *35 Years of Eurobarometer: European integration as seen by the public opinion in the Member States of the European Union: 1973-2008*.

European Comission, 2011. *Special Eurobarometer 371: Internal Security*. Brussels.

Faria, R., 2011. 2011 bate recorde de perdas económicas com catástrofes naturais. In: *Jornal de Negócios* (15 de dezembro de 2011). Consultado em 30 de maio de 2016. Disponível em: http://www.jornaldenegocios.pt/economia/detalhe/2011_bate_recorde_de_perdas_econoacutemicas_com_cataacutestrofes_naturais.html

Geraldes, H., 2011. Prejuízos causados por catástrofes batem recorde em 2011. In: *Público* (15 de dezembro de 2011). Consultado em 30 de maio de 2016. Disponível em: https://www.publico.pt/ciencia/noticia/custo-das-catastrofes-em-2011-atingiu-os-269-mil-milhoes-de-euros-e-bateu-recorde-1525186

Haller, M., 2009. *Die Europäische Integration als Elitenprozess: Das Ende eines Traums?* Wiesbaden: VS Verlag.

Home Office, 2011. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, London.

Höpner, M. and Bojan Jurczyk, 2015. *How the Eurobarometer Blurs the Line between Research and Propaganda*. MPIfG Discussion Paper 15/6.

Iarossi, G., 2006. *The Power of Survey Design: A User's Guide for Managing Surveys, Interpreting Results, and Influencing Respondents*. Washington, DC: The World Bank.

Karmasin, M. und Pitters, H., 2008. Methodenprobleme international vergleichender Umfragen amBeispiel des "Euro- barometer". In: Melischek, G., Seethaler, J.,Wilke, J. (eds.) *MedienundKommunikationsforschung im Vergleich*. VS, Wiesbaden, pp. 435–450.

Legge, J., 1998. *Sondagens e Democracia*. Lisboa: Instituto Piaget.

Leyden, J., 2011. EU Parliament Suspends Webmail After Cyber-Attack. In: *The Register* (31 de Março de 2011). Consultado em 12 de junho de 2016. Disponível em: http://www.theregister.co.uk/2011/03/31/eu_parliament_hack/

McAfee, 2011. *Threats Report: Fourth Quarter 2011*. McAfee Labs.

Moura, V., 2013. *A Identidade Cultural Europeia*. Lisboa: Fundação Francisco Manuel dos Santos.

Nissen, S., 2012. The Eurobarometer and the Process of European Integration: Methodological Foundations and Weaknesses of the Largest European Survey. *Quality & Quantity*, 48(2), 713–727.

Pausch, M., 2008. Die Eurobarometermacher auf der Zauberinsel: Konstruktion einer euro- päischen öffentlichen Meinung durch Umfrageforschung. In: *SWS-Rundschau*,48(3), pp. 356–361.

Payne, S. L., 1951. *The Art of Asking Questions*. Oxford: Princeton University Press.

Regulamento nº 460/2004, do Parlamento Europeu e do Conselho (criação da ENISA)

Regulamento nº 526/2013, do Parlamento Europeu e do Conselho (relativo à ENISA e que revoga o Regulamento nº 460/2004)

Reif, K., 1991. Organisatorische Randbedingungen und Probleme empirischer Sozialforschung aus europäischer Perspektive. Das Eurobarometer der EG-Kommission. In: Sahner, H. (ed.) *Sozialforschung im vereinten Deutschland und in Europa*. Oldenbourg, München, pp. 43–53.

Reis, E., 2000. *Estatística Descritiva*. Lisboa: Edições Sílabo.

Republic of Slovenia, 2016. *Cyber Security Strategy: Establishing a system to ensure a high level of cyber security*.

Santos, D., 2014. *A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança* (Dissertação de Mestrado). Lisboa: ISCTE – Instituto Universitário de Lisboa.

Santos, P., Ricardo Bessa e Carlos Pimentel, 2008. *Cyberwar: O Fenómeno, as Tecnologias e os Actores*. Lisboa: FCA.

Scheuch, E., 1993. The cross-cultural use of sample surveys: problems of comparability. *Hist. Soc. Res.*, 18(2), 104–138.

Signorelli, S., 2012. *The EU and Public Opinions: A Love–Hate Relationship? Notre Europe Studies and Reports 93*. Paris: Jacques Delors Institute.

Tomaselli V., 2003. *I Sondaggi dell'Eurobarometro: Valutazioni e Prospettive di Analisi*. Manuscript.

UNRIC, 2011. *Nações Unidas: 2010, um dos anos em que se registaram mais mortes provocadas por catástrofes naturais*. Consultado em 26 de maio de 2016. Disponível em: http://www.unric.org/pt/actualidade/30361-nacoes-unidas-2010-um-dos-anos-em-que-se-registaram-mais-mortes-provocadas-por-catastrofes-naturais

Vicente, P., Elizabeth Reis e Fátima Ferrão, 1996. *Sondagens: A amostragem como factor decisivo de qualidade*. Lisboa: Edições Sílabo.

Wendt-Hildebrandt, S., Hildebrandt und Krebs, 1983. *Zur interkulturellen Validität von Messinstrumenten*. ZUMA-Nachrichten 13, 45–57.

Websites consultados:

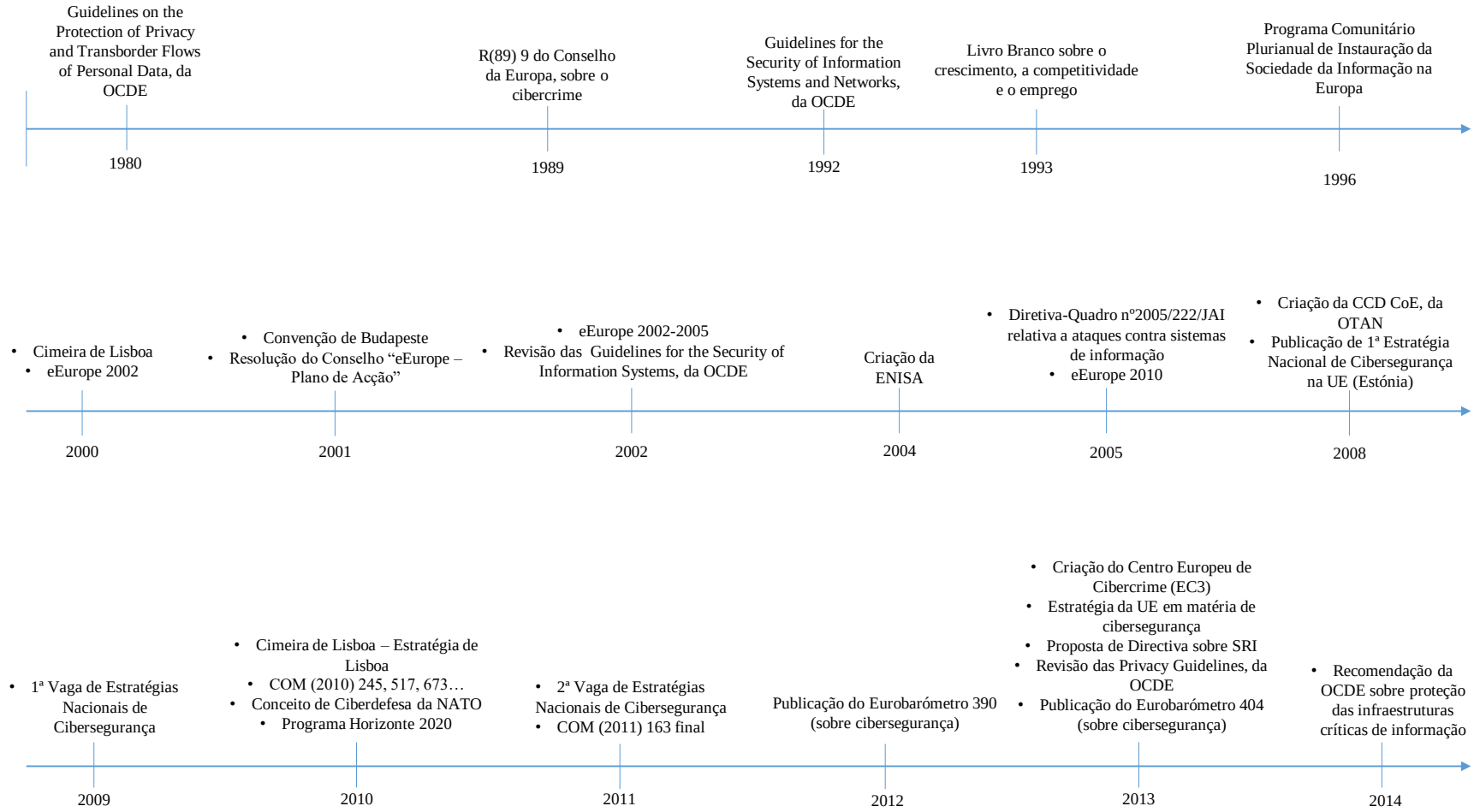
Comissão Europeia - http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/Chart/index.cfm

Ciberataques - http://list25.com/25-biggest-cyber-attacks-in-history/4/

PORDATA - http://www.pordata.pt

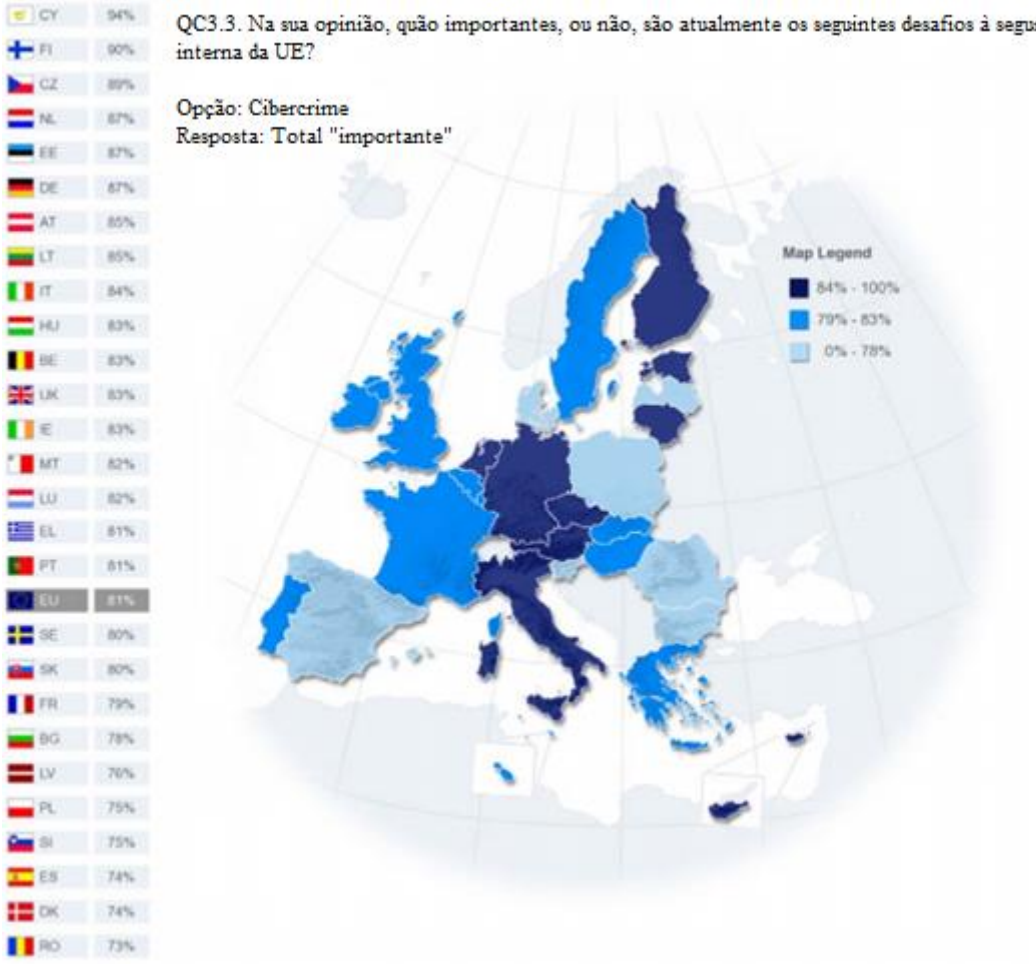
VIII. Anexo

Figura 1: Ação política em matéria de cibersegurança na União Europeia



Fonte: Santos, 2014, p. 82.

Figura 2: Importância do cibercrime como desafio à segurança interna da UE, por país (%)



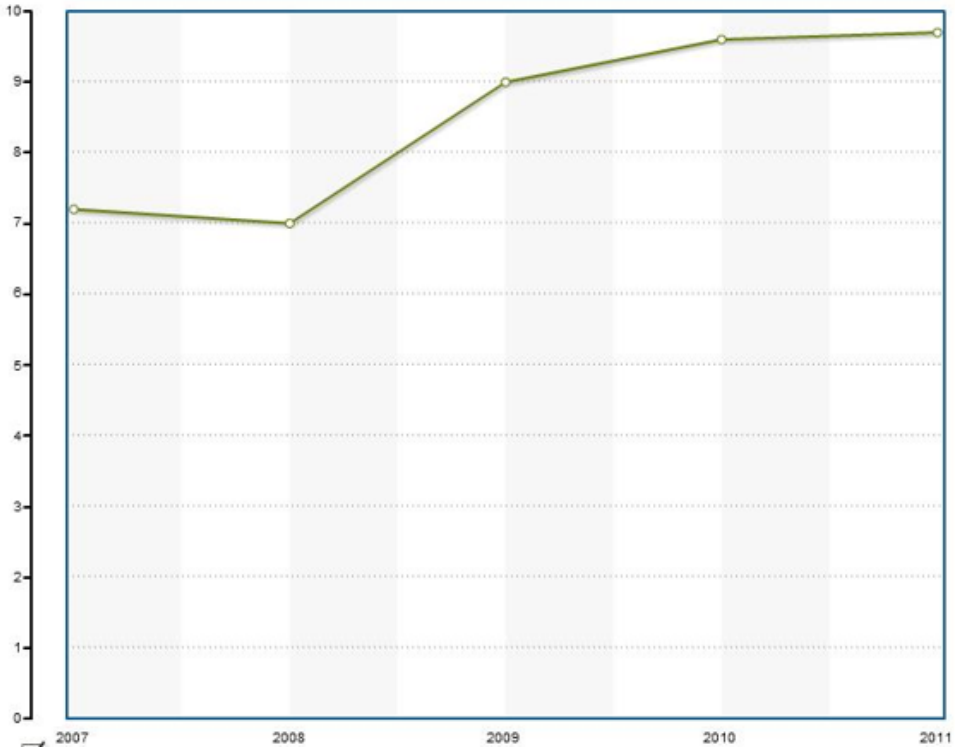
Fonte: Adaptado de European Commission, 2011, p. 32.

Figura 3: Importância do cibercrime como desafio à segurança interna da UE e como desafio à segurança dos cidadãos dos Estados-Membros

QC3. (…) desafios à segurança interna da UE? (5 desafios)		QC1. (…) desafios à segurança dos (NACIONALIDADE) cidadãos atualmente?	
Terrorismo/Crime organizado	1º	Terrorismo	2º
		Crime organizado	4º
Catástrofes naturais ou de origem humana	3º	Cibercrime	10º
Cibercrime	4º	Segurança das fronteiras	12º
Segurança das fronteiras	5º	Catástrofes naturais e de origem humana (crises financeiras 1º; catástrofes naturais 8º; catástrofes nucleares 11º)	

Fonte: Adaptado de European Commission, 2011, p. 26.

Figura 4: Taxa de desemprego, dos 15 aos 64 anos, na UE (%)



Fonte: PORDATA (Eurostat; Institutos Nacionais de Estatística – Inquérito ao Emprego).

Figura 5: População em risco de pobreza, na UE (%)

Anos	Total
	UE27 - União Europeia (27 Países)
2008	23,8
2009	23,3
2010	23,6
2011	24,2

Fonte: PORDATA (Eurostat; Entidades Nacionais – Painel Europeu dos Agregados Familiares; Estatísticas Europeias sobre Rendimentos e Condições e Vida).

Figura 6: Importância atribuída aos desafios à segurança dos cidadãos dos Estados-Membros da UE, por país (%)

QC1. Quais são os desafios para a segurança dos (NACIONALIDADE) cidadãos, que considera mais importantes neste momento?

	Crises económicas e financeiras	Terrorismo	Pobreza	Crime Organizado	Corrupção	Imigração ilegal	Crimes menores	Catástrofes Naturais	Questões ambientais	Cibercrime	Catástrofes nucleares	Insegurança das fronteiras da UE	Extremismo religioso	Guerras	Outro	Não sei
UE27	33%	25%	24%	22%	18%	13%	13%	11%	11%	10%	8%	6%	6%	4%	9%	8%
BE	32%	20%	27%	15%	8%	23%	31%	11%	16%	10%	9%	7%	11%	3%	12%	2%
BG	48%	4%	60%	23%	24%	1%	26%	10%	4%	0%	2%	1%	2%	1%	19%	2%
CZ	38%	14%	16%	39%	38%	10%	8%	22%	12%	16%	8%	6%	4%	5%	3%	4%
DK	30%	55%	5%	19%	2%	9%	6%	5%	19%	4%	4%	5%	11%	5%	21%	4%
DE	28%	34%	19%	32%	14%	8%	9%	12%	20%	27%	19%	7%	10%	5%	6%	4%
EE	22%	9%	17%	9%	11%	3%	12%	5%	6%	9%	3%	12%	1%	4%	19%	14%
IE	61%	10%	30%	45%	25%	8%	17%	5%	9%	6%	4%	2%	1%	2%	5%	3%
EL	56%	7%	50%	13%	39%	28%	15%	6%	7%	2%	4%	10%	1%	3%	4%	0%
ES	57%	38%	35%	11%	37%	16%	7%	10%	7%	4%	5%	3%	4%	4%	2%	2%
FR	15%	16%	20%	7%	7%	10%	31%	7%	8%	4%	7%	3%	7%	3%	26%	19%
IT	44%	26%	18%	31%	19%	24%	7%	13%	13%	8%	10%	8%	5%	9%	2%	2%
CY	54%	6%	15%	28%	21%	55%	15%	5%	7%	7%	1%	8%	1%	1%	26%	
LV	27%	2%	41%	13%	28%	2%	23%	3%	4%	2%	1%	2%	0%	2%	5%	16%
LT	41%	5%	41%	25%	42%	4%	17%	9%	6%	7%	6%	2%	0%	2%	8%	6%
LU	16%	4%	10%	13%	5%	11%	37%	6%	9%	4%	7%	6%	1%	1%	21%	11%
HU	52%	5%	51%	20%	27%	4%	9%	20%	16%	3%	4%	3%	1%	1%	8%	2%
MT	27%	6%	15%	20%	27%	38%	12%	5%	12%	9%	1%	5%	3%	5%	9%	10%
NL	22%	26%	14%	23%	7%	7%	31%	8%	20%	22%	6%	6%	15%	3%	26%	4%
AT	40%	11%	20%	39%	9%	23%	15%	20%	21%	16%	14%	19%	6%	3%	3%	4%
PL	22%	9%	21%	13%	11%	1%	7%	16%	4%	3%	2%	1%	1%	4%	6%	27%
PT	41%	9%	42%	24%	30%	6%	11%	7%	6%	3%	4%	7%	2%	4%	2%	7%
RO	41%	14%	55%	14%	56%	2%	4%	19%	9%	4%	6%	3%	1%	5%	2%	4%
SI	46%	3%	30%	31%	47%	2%	6%	17%	15%	4%	3%	1%	2%	1%	9%	3%
SK	40%	11%	36%	24%	31%	3%	20%	46%	14%	5%	9%	3%	1%	3%	2%	1%
FI	27%	16%	11%	22%	2%	12%	10%	11%	14%	8%	15%	9%	2%	4%	27%	8%
SE	17%	30%	4%	23%	3%	3%	5%	7%	21%	6%	9%	1%	6%	3%	27%	9%
UK	24%	47%	14%	25%	6%	23%	9%	3%	7%	11%	2%	8%	10%	3%	6%	9%

Fonte: Adaptado de European Commission, 2011, p. 12.

Figura 7: Evolução dos desafios à segurança interna da UE, por idade, escolaridade e ocupação (%)

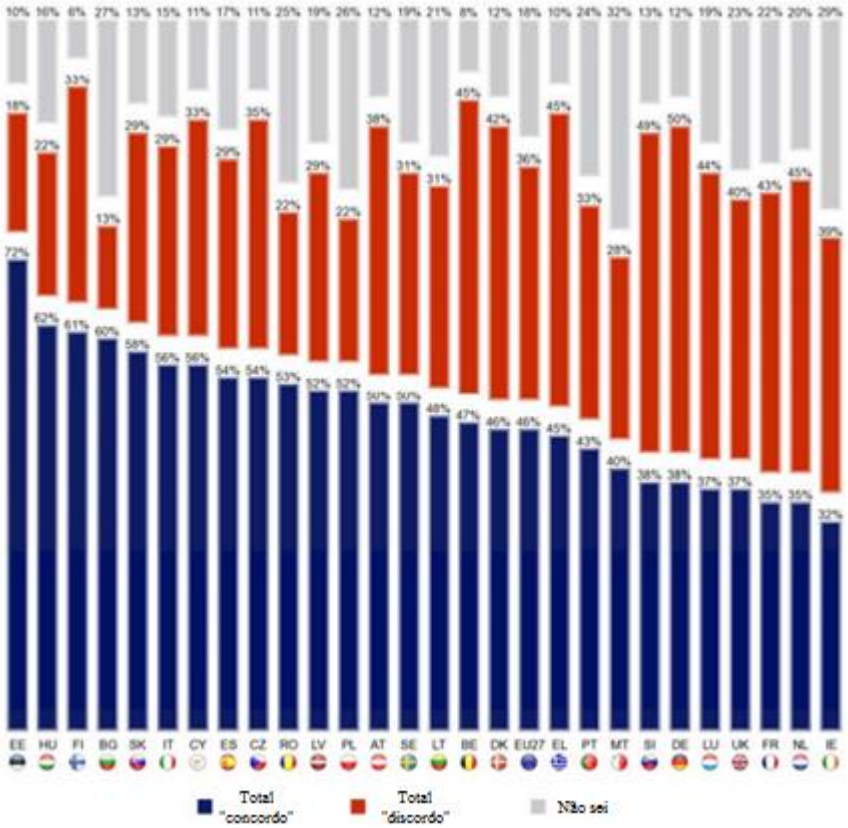
QC4. Comparando com a situação atual, diria que os seguintes desafios à segurança interna da UE vão aumentar, diminuir ou manter-se iguais nos próximos três anos? (Percentagem de "vai aumentar")

	Cibercrime	Crime organizado	Catástrofes naturais e de origem humana	Terrorismo	Insegurança nas fronteiras da UE
UE 27	63%	57%	54%	51%	43%
Idade					
15-24	63%	49%	55%	48%	38%
25-39	65%	55%	54%	50%	42%
40-54	67%	60%	54%	51%	44%
55 +	60%	60%	53%	54%	45%
Escolaridade (completa)					
15-	56%	61%	56%	54%	47%
16-19	65%	59%	56%	54%	44%
20+	70%	54%	50%	46%	39%
ainda a estudar	62%	47%	52%	46%	36%
Atividade profissional					
Trab. independentes	63%	56%	54%	50%	43%
Gestores	72%	56%	49%	49%	42%
Colarinhos brancos	67%	57%	55%	49%	41%
Operários	66%	59%	55%	53%	44%
Domésticos	59%	56%	57%	54%	44%
Desempregados	61%	56%	56%	49%	46%
Reformados	59%	61%	52%	55%	44%
Estudantes	62%	47%	52%	46%	36%

Fonte: Adaptado de European Commission, 2011, p. 51.

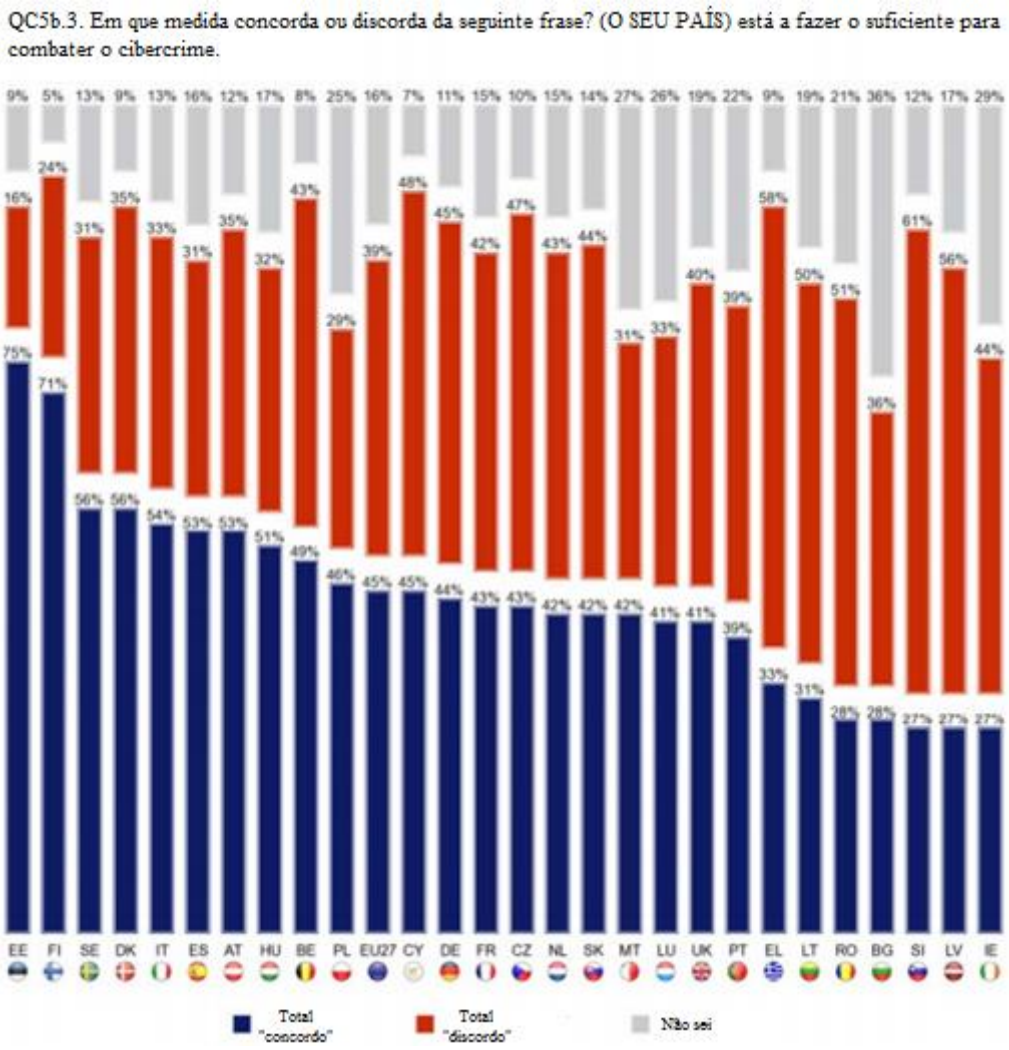
Figura 8: Atuação da UE no combate ao cibercrime, por país (%)

QC5a.3. Em que medida concorda ou discorda da seguinte frase? A UE está a fazer o suficiente para combater o cibercrime.



Fonte: Adaptado de European Commission, 2011, p. 61.

Figura 9: Atuação dos Estados-Membros da UE para combater o cibercrime, por país (%)



Fonte: Adaptado de European Commission, 2011, p. 74.