CONSELHO DA UNIÃO EUROPEIA

Bruxelas, 22 de julho de 2013 (24.07)
(OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
para:	Delegações
n.º doc. ant.:	11357/13
Assunto:	Conclusões do Conselho sobre a comunicação conjunta da Comissão e da Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança intitulada "Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido"

Junto se enviam, à atenção das delegações, as conclusões do Conselho sobre a comunicação conjunta da Comissão e da Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança intitulada "Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido", adotadas pelo Conselho (Assuntos Gerais) de 25 de junho de 2013.

ANEXO

Conclusões do Conselho sobre a comunicação conjunta da Comissão e da Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança, intitulada "Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido"

O Conselho da União Europeia,

1. RECONHECENDO que o ciberespaço, que tem, por inerência, um caráter transnacional, consiste em redes e infraestruturas informáticas interdependentes, nomeadamente a Internet e as redes de telecomunicações, constitui um dos canais presentes e futuros mais importantes para satisfazer as necessidades, interesses e direitos dos cidadãos e Estados-Membros da UE e representa um ativo indispensável para o crescimento económico da UE,

2. SALIENTANDO o papel e os direitos dos particulares, do setor privado e da sociedade civil no campo da cibernética, e a importante ação da UE para apoiar e manter um ciberespaço aberto, seguro e resiliente, baseado nos valores fundamentais da UE, como a democracia, os direitos humanos e o Estado de direito, a bem das nossas economias, administrações e sociedades e em prol do bom funcionamento do mercado interno,

3. RECONHECENDO a necessidade de melhorar a confidencialidade, disponibilidade e integridade das redes e infraestruturas, bem como das informações nelas contidas,

4. RECONHECENDO que são necessárias salvaguardas e medidas para prevenir as ameaças associadas ou prejudiciais às redes e infraestruturas informáticas interdependentes, bem como para proteger o ciberespaço, tanto no âmbito civil como militar,

5. REAFIRMANDO a posição da UE segundo a qual as normas, princípios e valores defendidos pela UE em todos os outros campos, nomeadamente a Carta dos Direitos Fundamentais da UE, devem também aplicar-se no ciberespaço,

6. RECONHECENDO que o direito internacional, nomeadamente as convenções internacionais como a Convenção do Conselho da Europa sobre o Cibercrime (Convenção de Budapeste) e as convenções pertinentes sobre direito internacional humanitário e direitos humanos, tais como o Pacto Internacional sobre os Direitos Civis e Políticos e o Pacto Internacional sobre os Direitos Económicos, Sociais e Culturais, proporciona um quadro jurídico aplicável ao ciberespaço. Por conseguinte, deverão ser envidados esforços para assegurar que esses instrumentos sejam também respeitados no ciberespaço, pelo a UE não preconiza a criação de novos instrumentos jurídicos internacionais para as questões cibernéticas,

7. AFIRMANDO que a cibersegurança deve ser abordada de uma forma integrada, multidisciplinar e horizontal, e que as medidas adotadas deverão abarcar uma vasta gama de questões que afetam o ciberespaço,

8. RECORDANDO as numerosas iniciativas lançadas pela UE e a nível internacional no domínio da cibersegurança, nomeadamente as que figuram no anexo do presente documento,

9. RECORDANDO as disposições do artigo 222.º do Tratado sobre o Funcionamento da União Europeia e tendo em conta os debates em curso sobre a sua aplicação,

10. CONSCIENTE de que os esforços para aumentar a cibersegurança e a luta contra o cibercrime têm de ser desenvolvidos não só no interior da União Europeia mas também nos países terceiros, incluindo os países a partir dos quais as organizações cibercriminosas operam,

PELAS PRESENTES CONCLUSÕES

11. CONGRATULA-SE com a comunicação conjunta da Comissão e da Alta Representante da UE sobre a Estratégia da UE para a Cibersegurança,

12. CONSIDERA essencial e urgente aprofundar e implementar uma abordagem abrangente da política ciberespacial da UE que:

- proteja e promova o exercício dos direitos humanos e assente nos valores fundamentais da UE que são a democracia, os direitos humanos e o Estado de direito,

- fomente a prosperidade europeia e os benefícios sociais e económicos do ciberespaço, incluindo a Internet,

- promova uma cibersegurança eficaz e melhorada em toda a UE e no resto do mundo,

- estimule os esforços para colmatar a clivagem digital e promova a cooperação internacional em matéria de cibersegurança,

- reflita o papel e os direitos dos particulares, do setor privado e da sociedade civil no campo da cibernética, reforçando nomeadamente a cooperação entre o setor público e o setor privado e o intercâmbio de informações,

E

13. CONVIDA os Estados-Membros, a Comissão e a Alta Representante a colaborarem, na observância das respetivas esferas de competência e do princípio da subsidiariedade, com vista à consecução dos objetivos estratégicos estabelecidos nas presentes conclusões.

Valores

14. SALIENTA que, ao desenvolver a política e as práticas relativas ao ciberespaço e a correspondente legislação, é imperioso respeitar sempre os direitos humanos individuais, nomeadamente a liberdade de expressão e a privacidade, e toma nota das negociações em curso para adotar um quadro jurídico da UE relativo à proteção dos dados pessoais suscetível de funcionar eficazmente no ciberespaço,

15. RECONHECE que os valores e interesses promovidos e protegidos na União deverão ser também promovidos nas suas políticas externas relacionadas com as questões cibernéticas,

16. EXORTA a UE e os seus Estados-Membros a:
    - defenderem uma posição una e forte relativamente à aplicabilidade universal dos direitos humanos e das liberdades fundamentais, nomeadamente as liberdades de opinião, expressão, informação reunião e associação no ciberespaço,

    - estabelecerem a forma de fazer cumprir no ciberespaço as obrigações existentes,

17. CONVIDA a UE e os seus Estados-Membros a promoverem a literacia digital e a ajudarem os utilizadores a adquirir uma maior consciência da sua responsabilidade individual quando introduzem dados pessoais na Internet,

18. SALIENTA o importante papel da UE na manutenção do modelo multilateral de governação da Internet,

19. CONVIDA os Estados-Membros a tomarem todas as medidas razoáveis para assegurar que todos os cidadãos da UE possam ter acesso à Internet e desfrutar dos seus benefícios,

Prosperidade

20. CONVIDA a Comissão a velar especialmente pela promoção do Mercado Único Digital e a avançar nas questões conexas no âmbito da União e nas instâncias internacionais (nomeadamente a Organização Mundial do Comércio e as negociações do Acordo sobre as Tecnologias da Informação), bem como a garantir o acesso ao mercado nestes setores ao negociar acordos de comércio livre com países terceiros,

21. SALIENTA a importância de a legislação neste setor ser tecnologicamente neutra e exorta a propiciar tanto quanto possível a neutralidade da rede, de modo a não entravar a concorrência por práticas discriminatórias contra o comércio em linha transfronteiras e os novos modelos empresariais,

22. CONGRATULA-SE por ter sido reconhecida a necessidade de investir na investigação e desenvolvimento no domínio do ciberespaço, setor importante que poderá trazer consigo a criação de empregos de alta qualidade e o crescimento económico,

23. REALÇA:

- que é essencial que a UE disponha de um forte setor de tecnologias da informação e da comunicação (TIC) e de segurança das TIC de modo a permitir reforçar a cibersegurança, e CONVIDA os Estados-Membros e a Comissão a estudarem e comunicarem as medidas que poderão ser tomadas em apoio do desenvolvimento deste setor,

- que a legislação em apoio da cibersegurança deverá fomentar a inovação e o crescimento e centrar-se na proteção das infraestruturas e das funções vitais que os Estados-Membros considerem de importância crítica,

- que a economia digital é um importante motor do crescimento, da inovação e do emprego, e que a cibersegurança é essencial para proteger a economia digital;

- a importância a nível nacional da Proteção das Infraestruturas Críticas da Informação.

Consecução da resiliência cibernética

24. CONGRATULA-SE com os objetivos da proposta de diretiva da Comissão que estabelece medidas para reforçar:

    - a segurança das redes e da informação em toda a UE,

    - o grau de preparação e as capacidades em matéria de cibersegurança à escala nacional,

    - a cooperação entre os Estados-Membros e na UE e o estímulo a uma cultura de gestão dos riscos nos setores público e privado,

25. EXORTA todas as instituições, órgãos e organismos da UE a, em cooperação com os Estados-Membros, tomarem as medidas necessárias para garantir a sua própria cibersegurança, reforçando para o efeito a sua segurança de acordo com as normas de segurança apropriadas, em cooperação com a ENISA, a fim de satisfazer as melhores práticas, em conformidade com o Regulamento XXX/2013[1],

26. RECORDA que foi instituída uma Equipa de Resposta a Emergências Informáticas (CERT) para as instituições, órgãos e organismos da UE na sequência de uma fase-piloto de um ano e de uma avaliação satisfatória do seu papel e eficácia,

27. SALIENTA a importância primordial da ENISA no apoio aos esforços dos Estados-Membros e da União para alcançar um elevado nível de segurança das redes e da informação, em especial contribuindo para o reforço das capacidades dos Estados-Membros e para o desenvolvimento de sólidas capacidades nacionais de resiliência cibernética, para os ciberexercícios europeus e para os esforços da União em matéria de I&D e de normalização, e CONVIDA a ENISA a cooperar com outras instituições, órgãos e organismos da União nas questões relacionadas com a segurança das redes e da informação, em conformidade com o Regulamento (UE) n.º 526/2013,

---

[1] JO L 165 de 18.6.2013.

28. DESTACA a necessidade de aumentar a resiliência das infraestruturas críticas à escala da UE e de reforçar a estreita cooperação e coordenação entre os intervenientes relevantes, inclusive entre intervenientes civis e militares e entre o setor público e o setor privado, na resposta aos incidentes e desafios em matéria de cibersegurança, mediante iniciativas como a elaboração de normas comuns, a sensibilização, a formação e educação e a avaliação e testagem (ou desenvolvimento) permanentes de mecanismos de alerta rápido e de resposta. Para enfrentar com eficácia os desafios cibernéticos, inclusive no que respeita à gestão dos incidentes, é também necessário assegurar uma cooperação e uma coordenação mais estreitas na resposta a ciberincidentes por parte dos intervenientes do setor da defesa, dos serviços de aplicação da lei, do setor privado e das autoridades encarregadas da cibersegurança,

29. CONVIDA os Estados-Membros a:

- tomarem medidas para assegurar a obtenção no seu país de um nível de cibersegurança eficiente, mediante o desenvolvimento e a implementação de políticas e capacidades organizativas e operacionais adequadas, de modo a proteger os sistemas de informação no ciberespaço, em particular os sistemas considerados críticos,

- estabelecerem um diálogo com as empresas e o mundo académico para estimular a confiança, elemento essencial da cibersegurança nacional, por exemplo através do estabelecimento de parcerias público-privadas,

- apoiarem atividades de sensibilização para a natureza das ameaças e para os aspetos fundamentais das boas práticas digitais, a todos os níveis,

- ajudarem os proprietários e os fornecedores de sistemas TIC a protegerem os seus próprios sistemas e os serviços essenciais por si prestados,

- favorecerem uma cooperação pan-europeia em matéria de cibersegurança, em particular reforçando os exercícios pan-europeus neste domínio,

- assegurarem uma cooperação e coordenação efetivas entre os Estados-Membros a nível da UE, com vista a estabelecer uma avaliação comum das ameaças,

- reforçarem e ampliarem a cooperação entre os utilizadores dos Estados-Membros e os da UE, tirando partido das estruturas existentes.

- terem em conta as questões de cibersegurança à luz dos trabalhos em curso sobre a cláusula de solidariedade.

Cibercrime

30. SAÚDA as conclusões do Conselho JAI de 6-7 de junho de 2013, que fixam as prioridades da UE para a luta contra a criminalidade grave e organizada entre 2014 e 2017 e dão particular destaque à luta contra o cibercrime,

31. SALIENTA que, segundo a avaliação da ameaça da criminalidade grave e organizada (SOCTA) efetuada pela Europol em 2013, o cibercrime constitui uma forma de criminalidade que representa uma crescente ameaça para a UE, sob a forma de violações de dados em grande escala, de fraudes em linha e de exploração sexual de crianças, estando o cibercrime com fins lucrativos a tornar-se um fator catalisador para outras atividades criminosas,

32. LOUVA a criação do Centro Europeu da Cibercriminalidade (EC3) no seio da Europol e CONVIDA os Estados-Membros a recorrerem a este centro para reforçar a cooperação entre organismos nacionais no âmbito do seu mandato,

33. CONVIDA a Europol e a Eurojust a continuarem a reforçar a sua cooperação com todas as partes interessadas, nomeadamente os organismos da UE, a Interpol, toda a rede de equipas de resposta a emergências informáticas (CERT) e o setor privado, na luta contra o cibercrime, nomeadamente pondo a tónica nas sinergias e complementaridades em conformidade com os respetivos mandatos e competências,

34. ANTECIPA a rápida ratificação, por todos os Estados-Membros, da Convenção de Budapeste sobre o Cibercrime,

35. SOLICITA à Comissão, à Europol, à CEPOL e à ENISA, que apoiem a formação e a melhoria das competências nos Estados-Membros em que os governos e as autoridades de aplicação da lei precisem de criar capacidades cibernéticas para combater o cibercrime,

36. CONVIDA a Comissão a:

- apoiar os Estados-Membros que assim o solicitem a detetar as lacunas e reforçar as suas capacidades para investigar e combater o cibercrime,

- utilizar o Fundo para a Segurança Interna, dentro dos limites do seu orçamento (tendo simultaneamente em conta as suas outras prioridades), para ajudar as autoridades competentes na luta contra o cibercrime,

- utilizar o Fundo de Estabilidade para desenvolver a luta contra o cibercrime, bem como as iniciativas destinadas a reforçar as capacidades, nomeadamente a cooperação policial e judicial nos países terceiros a partir dos quais as organizações cibercriminosas operam,

- facilitar a coordenação dos programas de reforço das capacidades a fim de evitar as duplicações e de criar sinergias,

- prestar informações sobre os progressos da Aliança Mundial contra os abusos sexuais de crianças na Internet,

- continuar a facilitar a monitorização do enquadramento político da UE em matéria de luta contra o cibercrime, em particular à luz dos resultados e das informações estratégicas fornecidas pela Europol (EC3),

- continuar a favorecer a cooperação intercomunitária, em particular apoiando a Europol (EC3).

Política Comum de Segurança e Defesa (PCSD)

37. No âmbito da PCSD, DESTACA:

- a urgente necessidade de implementar e fazer avançar os aspetos da Estratégia relacionados com a ciberdefesa no âmbito da PCSD, a fim de desenvolver um quadro de ciberdefesa, se for caso disso, e de definir medidas concretas a este respeito, inclusive na perspetiva do debate do Conselho Europeu sobre segurança e defesa, previsto para dezembro de 2013. Deverá ser designado no seio do SEAE um ponto de contacto único para orientar estes esforços,

- a necessidade de reforçar as capacidades de ciberdefesa dos Estados-Membros, nomeadamente através da elaboração de normas comuns, bem com a sensibilização, através da formação e educação em matéria de cibersegurança, tirando partido da Academia Europeia de Segurança e Defesa e continuando a melhorar as oportunidades de formação e de exercício ao dispor dos Estados-Membros,

- a possibilidade de utilizar os mecanismos existentes de mutualização e partilha e de tirar partido das sinergias com políticas mais gerais da UE para criar da forma mais eficaz possível as necessárias capacidades de ciberdefesa dos Estados-Membros,

- a necessidade da investigação e do desenvolvimento. É prioritário incentivar os Estados-Membros a desenvolverem tecnologias seguras e resilientes em matéria de ciberdefesa, com uma forte participação do setor privado e das universidades, e reforçar os aspetos ligados à cibersegurança nos projetos de investigação da Agência Europeia de Defesa (AED), com base numa abordagem colaborativa, o que constituiria um bom exemplo da coordenação que pode ser estabelecida entre a AED e a Comissão, ao abrigo do Quadro Europeu de Cooperação, para uma capacidade de dupla utilização,

- a conveniência de reexaminar e testar os mecanismos de alerta rápido e de resposta à luz das novas ameaças cibernéticas, através do diálogo entre o SEAE, a ENISA, o EC3, a AED, a Comissão e os Estados-Membros, tendo em vista procurar sinergias e ligações com a comunidade da defesa,

- a necessidade de prosseguir e reforçar a cooperação UE-OTAN no domínio da ciberdefesa, determinando as prioridades para a continuação dessa cooperação no quadro existente, inclusive no que se refere à participação recíproca em exercícios e formações em matéria de ciberdefesa,

- a incorporação dos aspetos ligados à ciberdefesa na política mais vasta em matéria de ciberespaço.

Indústria/Tecnologia

38. RECONHECENDO a necessidade de a Europa continuar a desenvolver os seus recursos industriais e tecnológicos para alcançar um nível adequado de diversidade e de confiança no âmbito das suas redes e sistemas TIC, o Conselho CONGRATULA-SE vivamente com o apelo lançado na Estratégia da UE para a Cibersegurança no sentido de apoiar uma política industrial forte, a fim de promover a fiabilidade do setor europeu das TIC e da cibersegurança e de dinamizar o mercado interno graças à I&D,

39. CONVIDA os Estados-Membros, a Comissão e a ENISA a aumentarem os esforços de investigação e desenvolvimento no domínio das TIC e da cibersegurança, bem como a disponibilidade de profissionais bem preparados em matéria de cibersegurança, o que é essencial para impulsionar a competitividade das tecnologias europeias da informação e da comunicação (TIC) e dos setores dos serviços e da segurança e para reforçar a sua capacidade para desenvolver soluções fiáveis e seguras, pelo que o Conselho incentiva a Comissão a alavancar o Programa-Quadro de Investigação e Inovação "Horizonte 2020",

40. SALIENTA que o desenvolvimento de parcerias público-privadas será um instrumento pertinente para reforçar as capacidades de cibersegurança; por conseguinte, APELA à Comissão para que fomente, no âmbito do "Horizonte 2020", as sinergias entre os operadores de infraestruturas críticas e a investigação no domínio das TIC e da segurança sobre questões ligadas à cibersegurança e ao cibercrime, e com as políticas da União em matéria de segurança interna e externa,

41. SOLICITA aos Estados-Membros e à Comissão que tomem medidas específicas para apoiar a cibersegurança nas pequenas e médias empresas, particularmente vulneráveis aos ciberataques, e encoraja os Estados-Membros a desenvolverem tecnologias seguras e resilientes em matéria de cibersegurança, com a colaboração do setor privado e das universidades,

42. CONVIDA a Comissão a tomar em consideração as normas existentes no domínio da cibersegurança e SALIENTA que a cooperação e o intercâmbio de informações sobre normas – por exemplo, sobre gestão de riscos – deverão continuar a desenvolver-se, em cooperação com os Estados-Membros, a indústria e outras partes interessadas.

Cooperação internacional em matéria de ciberespaço

43. REITERA o empenho da UE em apoiar o desenvolvimento de medidas geradoras de confiança em matéria de cibersegurança, aumentar a transparência e reduzir o risco de más interpretações face à atitude dos Estados, promovendo para tal o estabelecimento de normas internacionais neste domínio,

44. SOLICITA à Comissão e à Alta Representante que, em conformidade com os procedimentos pertinentes dos Tratados:

- a) promovam a Convenção de Budapeste enquanto modelo para a redação da legislação nacional em matéria de cibercrime e enquanto base para a cooperação internacional neste domínio, b) promovam o respeito pelos direitos fundamentais no ciberespaço, e c) utilizar plenamente todos os instrumentos de cooperação internacional disponíveis para desenvolver a luta contra o cibercrime, bem como a cooperação policial e judicial nesse domínio com os países terceiros a partir dos quais as organizações cibercriminosas operam,

- recorram aos conhecimentos especializados dos Estados-Membros em matéria de política cibernética e às experiências por eles adquiridas na sua atuação/cooperação a nível bilateral, a fim de elaborarem mensagens comuns da UE sobre o ciberespaço e de colaborarem estreitamente com os Estados-Membros sobre os aspetos operacionais,

- em cooperação com os Estados-Membros, as organizações privadas pertinentes e a sociedade civil, tirem plenamente partido dos instrumentos de ajuda relevantes da UE para o reforço das capacidades no domínio das TIC, inclusive no que se refere à cibersegurança,

45. SOLICITA aos Estados-Membros, à Comissão e à Alta Representante que envidem esforços para instaurar uma política internacional da UE coerente em matéria de ciberespaço, em conformidade com os procedimentos pertinentes dos Tratados:

- reforçando as relações com os principais parceiros e organizações internacionais de modo a assegurar que todos os Estados-Membros possam beneficiar plenamente dessa cooperação,

- integrando as questões cibernéticas na PESC,

- melhorando a coordenação das questões cibernéticas de dimensão mundial e integrando a cibersegurança, incluindo as medidas geradoras de confiança e de transparência, no quadro geral das relações com os países terceiros e as organizações internacionais, nomeadamente através de uma coordenação reforçada entre os Estados-Membros, a Comissão e o SEAE no âmbito dos diálogos e de outras atividades em matéria de cibersegurança,

- melhorando a coordenação entre as instâncias preparatórias do Conselho relevantes (incluindo o Grupo dos Amigos da Presidência sobre questões cibernéticas),

- apoiando o reforço das capacidades nos países terceiros, mediante ações de formação e de assistência à instauração das políticas nacionais relevantes, tendo em vista permitir a realização de todo o potencial económico e social das TIC, apoiando o desenvolvimento de sistemas resilientes nesses países e limitando os riscos cibernéticos para as instituições da UE e os Estados-Membros, recorrendo simultaneamente às redes e instâncias encarregadas da coordenação política e do intercâmbio de informações.

Funções e responsabilidades respetivas

46. EXORTA as outras partes interessadas – setor privado, comunidades técnicas e académicas, sociedade civil e particulares – a assumirem as suas respetivas funções e responsabilidades para favorecer um ciberespaço aberto, livre e seguro,

47. SOLICITA à Comissão e à Alta Representante que as atividades empreendidas à escala europeia sejam concebidas para serem compatíveis com as estruturas nacionais, o direito constitucional e as iniciativas dos Estados-Membros em matéria de cibersegurança, a fim de garantir uma abordagem integrada e de evitar duplicações,

E

48. SOLICITA à Comissão e à Alta Representante que elaborem um relatório de situação sobre a Estratégia para a Cibersegurança que deverá ser apresentado na Conferência de Alto Nível a realizar em fevereiro de 2014, e PROPÕE que sejam realizadas periodicamente reuniões das instâncias preparatórias competentes do Conselho (em especial do Grupo dos Amigos da Presidência sobre questões cibernéticas), para ajudar à definição das prioridades cibernéticas e objetivos estratégicos da UE no âmbito de um quadro político geral, e para acompanhar e apoiar a implementação da Estratégia,

49. Para efeitos de aplicação das presentes conclusões do Conselho, apenas serão utilizados os fundos e os programas financeiros existentes, sem prejuízo das negociações sobre o futuro quadro financeiro; por conseguinte, o Conselho CONVIDA a Comissão a apresentar as modalidades de financiamento da Estratégia, tendo em conta as futuras negociações com o Parlamento Europeu.

ANEXO AO ANEXO

Referências

1. Parlamento Europeu, Conselho e Comissão

   – Carta dos Direitos Fundamentais da União Europeia[2]

2. Parlamento Europeu e Conselho

   – Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação[3]

   – Diretiva 2002/21/CE do Parlamento Europeu e do Conselho, de 7 de março de 2002, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas (diretiva-quadro), com a redação que lhe foi dada pela Diretiva 2009/140/CE[4]

3. Parlamento Europeu

   – Resolução do Parlamento Europeu, de 11 de dezembro de 2012, sobre uma Estratégia para a Liberdade Digital na Política Externa da UE

   – Relatório do Parlamento Europeu de 2012 sobre Cibersegurança e Ciberdefesa

4. Conselho

   – Programa de Estocolmo – uma Europa aberta e segura que sirva e proteja os cidadãos[5]

   – Uma Europa Segura num Mundo Melhor – Estratégia Europeia em matéria de Segurança, 12 de dezembro de 2003[6]

---

2 JO C 364 de 18.12.2010
3 JO L 77 de 13.3.2004
4 JO L 108 de 24.4.2002 e JO L 337 de 18.12.2009
5 Doc. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229
6 Doc. 15849/03 PESC 783

– Estratégia de Segurança Interna da União Europeia: "Rumo a um modelo europeu de segurança"[7]

– Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008 , relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção[8]

– Conclusões do Conselho sobre a comunicação da Comissão intitulada "Estratégia de Segurança Interna da União Europeia em Ação"[9]

– Conclusões do Conselho sobre a comunicação da Comissão relativa à proteção das infraestruturas críticas da informação ("Realizações e próximas etapas: para uma cibersegurança mundial")[10]

– Conclusões do Conselho que fixam as prioridades da UE em matéria de luta contra a criminalidade grave e organizada para o período de 2014 a 2017[11]

- Conclusões do Conselho sobre a criação de um Centro Europeu da Cibercriminalidade[12]

---

7 Doc. 5842/2/10 JAI 90

8 JO L 345 de 23.12.2008

9 Doc. 6699/11 JAI 124

10 Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. Esta comunicação dá seguimento à comunicação da Comissão relativa à proteção das infraestruturas críticas da informação "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência" (doc. 8375/09).

11 Doc. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434

12 Doc. 10603/12 ENFOPOL 154 TELECOM 116

– Proposta de diretiva do Parlamento Europeu e do Conselho relativa a ataques contra os sistemas de informação, que substitui a Decisão-Quadro 2005/222/JAI do Conselho. Aprovação do texto de compromisso final com vista a um acordo em primeira leitura com o Parlamento Europeu[13]

– Conclusões do Conselho sobre a Estratégia Europeia para uma Internet Melhor para as Crianças[14]

– Conclusões do Conselho sobre a luta contra a exploração sexual de crianças e a pornografia infantil na Internet – Reforçar a eficácia da ação policial nos Estados-Membros e nos países terceiros[15]

– Conclusões do Conselho sobre a aliança mundial contra os abusos sexuais de crianças em linha[16]

– Conclusões do Conselho relativas a uma estratégia de trabalho concertada e a medidas concretas contra o cibercrime[17] e conclusões do Conselho sobre um plano de ação destinado a pôr em prática a estratégia concertada de combate ao cibercrime[18]

– Orientação geral parcial do Conselho sobre a proposta da Comissão relativa a um regulamento que estabelece o "Horizonte 2020 – Programa-Quadro de Investigação e Inovação (2014-2020)"[19]

– Ação Comum do Conselho relativa à criação da Agência Europeia de Defesa[20]

---

13 Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673
14 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81
15 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53
16 Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46
17 Doc. 15569/08 ENFOPOL 224 CRIMORG 190
18 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32
19 Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511
20 Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121

– Proposta conjunta de decisão do Conselho relativa às regras de execução pela União da cláusula de solidariedade[21]

– Conclusões do Conselho sobre a literacia mediática no ambiente digital[22]

– Direitos Humanos e Democracia: Quadro Estratégico da UE e Plano de Ação da UE[23]

– Relatório sobre a Execução da Estratégia Europeia de Segurança[24]

5. Comissão

– Agenda Digital para a Europa[25], que é uma das sete iniciativas emblemáticas da "Europa 2020 – Estratégia para um crescimento inteligente, sustentável e inclusivo"[26], e "Agenda Digital para a Europa – Promover o crescimento da Europa com base nas tecnologias digitais"[27], que reorienta a Agenda Digital

– Comunicação sobre "Proteção da privacidade num mundo interligado – um quadro europeu de proteção de dados para o século XXI[28]

– Comunicação sobre "Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade"[29]

---

21 Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165

22 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380

23 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603

24 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139

25 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATAPROTECT 141

26 Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74

27 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216

28 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6

29 Doc. 8543/12 ENFOPOL 94 TELECOM 72

– Comunicação da Comissão sobre "Explorar plenamente o potencial da computação em nuvem na Europa"[30]

– Comunicação da Comissão relativa à proteção das infraestruturas críticas da informação – "Realizações e próximas etapas: para uma cibersegurança mundial"[31]

– Comunicação da Comissão relativa à proteção das infraestruturas críticas da informação – "Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência"[32]

6. Nações Unidas

– Resolução A/RES 57/239 da Assembleia Geral das Nações Unidas, sobre a criação de uma cultura mundial da cibersegurança

– Resolução A/HRC/20/L.13 do Conselho dos Direitos do Homem, de 29 de junho de 2012, sobre a promoção, a proteção e o exercício dos direitos humanos na Internet

– Resolução A/RES 67/27 da Assembleia Geral das Nações Unidas, sobre os progressos da informática e das telecomunicações no contexto da segurança internacional

– Criação de um grupo intergovernamental aberto de peritos em matéria de cibercrime, junto do GDC (Gabinete para a Droga e a Criminalidade), em conformidade com a Resolução 65/230 da Assembleia Geral das Nações Unidas

7. Conselho da Europa

– Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981

– Convenção do Conselho da Europa sobre o Cibercrime, de 23 de novembro de 2001

---

30 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585
31 Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.
32 Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46

8. Organização para a Segurança e a Cooperação na Europa (OSCE)

– Decisão n.º 1039 do Conselho Permanente, de 26 de abril de 2012: elaboração de medidas geradoras de confiança para reduzir os riscos de conflito decorrentes da utilização das tecnologias da informação e da comunicação

– Decisão Ministerial n.º 4/12, de 7 de dezembro de 2012: esforços desenvolvidos pela OSCE para fazer face às ameaças transnacionais

– Grupo informal aberto da OSCE encarregado de elaborar um projeto de medidas geradoras de confiança destinadas a reforçar a cooperação interestatal, a transparência, a previsibilidade e a estabilidade, bem como a reduzir os riscos de má interpretação, de escalada e de conflito suscetíveis de resultar da utilização das TIC (Decisão n.º 1039 do Conselho Permanente da OSCE, de 26 de abril de 2012)

9. Conferências, iniciativas e outros eventos

– Conferência Internacional sobre o Ciberespaço, realizada em Londres a 1 e 2 de novembro de 2011, seguida de uma Conferência Internacional sobre o mesmo tema, realizada a 4 e 5 de outubro de 2012, em Budapeste

– Exercício conjunto UE-EUA de simulação de ciberincidente ("Cyber Atlantic 2011") e exercícios pan-europeus de simulação de ciberincidente com a participação de todos os Estados-Membros ("Cyber Europe 2010" e "Cyber Europe 2012")

– Grupo *ad hoc* da Segurança Nuclear, que debateu e aprofundou a questão da segurança informática/cibersegurança no seu relatório final[33]

[33] Doc. 10616/12 AHGS 20 ATO 84

10. Outros

– Avaliação de 2013, pela Europol, da ameaça da criminalidade organizada grave (SOCTA)[34]

– Política de Segurança para a Garantia da Informação[35] e Orientações sobre a Defesa da Rede[36].

---

[34] Doc. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211

[35] Doc. 8408/12 CSCI 11 CSC 20

[36] Doc. 10578/12 CSCI 20 CSC 34