



Bruxelas, 10 de dezembro de 2019
(OR. en)

14972/19

| | |
|------------------------|-----------------|
| HYBRID 56 | EDUC 478 |
| DISINFO 18 | AUDIO 118 |
| AG 68 | DIGIT 179 |
| PE 257 | INF 332 |
| DATAPROTECT 300 | COSI 252 |
| JAI 1307 | CSDP/PSDC 575 |
| CYBER 328 | COPS 360 |
| JAIEX 177 | POLMIL 129 |
| FREMP 176 | IPCR 23 |
| RELEX 1147 | PROCIV 100 |
| CULT 141 | CSC 294 |

RESULTADOS DOS TRABALHOS

de: Secretariado-Geral do Conselho

para: Delegações

Assunto: Esforços complementares para aumentar a resiliência e combater as ameaças híbridas

- Conclusões do Conselho (10 de dezembro de 2019)

Junto se envia, à atenção das delegações, as conclusões do Conselho sobre os esforços complementares para aumentar a resiliência e combater as ameaças híbridas, adotadas na 3739.^a reunião do Conselho em 10 de dezembro de 2019.

Conclusões do Conselho sobre os esforços complementares para aumentar a resiliência e combater as ameaças híbridas

1. O Conselho recorda as conclusões pertinentes do Conselho Europeu¹ e do Conselho² e expressa o seu empenho constante em aumentar a resiliência da União e dos seus Estados-Membros face a ameaças híbridas multifacetadas e em constante evolução, bem como em reforçar a cooperação a fim de detetar, prevenir e combater essas ameaças.
2. O Conselho reconhece os progressos realizados na execução do Quadro comum em matéria de luta contra as ameaças híbridas (2016) e da Comunicação Conjunta sobre "Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas" (2018), bem como do Plano de Ação contra a Desinformação (2018), em consonância com as conclusões do Conselho pertinentes.
3. A principal responsabilidade na luta contra as ameaças híbridas cabe aos Estados-Membros. Os esforços desenvolvidos a nível da UE são de natureza complementar e sem prejuízo da responsabilidade exclusiva dos Estados-Membros em matéria de segurança nacional. Para fazer face às ameaças híbridas, é necessária uma abordagem global da segurança que abranja todas as administrações públicas e toda a sociedade, trabalhando em todos os domínios de ação relevantes de maneira mais estratégica, coordenada e coerente. É importante que seja seguida e aplicada também a nível da UE uma abordagem que abranja todas as administrações públicas.
4. Nas presentes conclusões, o Conselho define as prioridades relativas à proteção das nossas sociedades, dos nossos cidadãos e das nossas liberdades e à segurança da nossa União contra as ameaças híbridas no contexto da aplicação da Nova Agenda Estratégica para 2019-2024, através da promoção de uma abordagem global da segurança provida de melhor coordenação, melhores recursos e capacidades tecnológicas, com base no importante trabalho já realizado em diferentes domínios de ação, inclusive no quadro da cooperação da UE em matéria de segurança e defesa.

¹ Em particular as conclusões do Conselho Europeu de junho e março de 2019, de dezembro, outubro, junho e março de 2018 e de junho e março de 2015.

² Em particular os documentos ST 10048/19, ST 6573/1/19 REV 1, ST 10255/19, ST 12836/19, ST 7928/16.

5. Os esforços para proteger as nossas instituições democráticas das ameaças híbridas têm sempre que respeitar os direitos fundamentais, incluindo a proteção dos dados pessoais, a liberdade de expressão e de informação e a liberdade e a liberdade de associação, tal como consagrados na Carta dos Direitos Fundamentais.

6. A UE e os seus Estados-Membros deverão continuar a desenvolver, treinar e exercitar capacidades para detetar as atividades híbridas, analisar as suas origens e dar-lhes resposta, e deverão apoiar o reforço da resiliência a longo prazo dos Estados-Membros e das instituições, órgãos e organismos da UE face às ameaças híbridas, tirando plenamente partido dos instrumentos existentes adequados para esse efeito. O Conselho salienta a necessidade de atualizar o protocolo operacional da UE para a luta contra as ameaças híbridas, com base nos ensinamentos identificados e retirados de exercícios anteriores.

7. O Conselho sublinha que continua a ser necessário cooperar com organizações internacionais como a ONU, a OSCE e o Conselho da Europa, e com instâncias como o G7 a fim de defender a ordem mundial assente em regras, também no contexto da luta contra as ameaças híbridas, nomeadamente através da instauração de um clima de confiança e de outras medidas pertinentes.

8. O Conselho salienta o compromisso da UE de prosseguir uma cooperação estreita e sinérgica com todos os países parceiros relevantes, em particular na vizinhança da UE, e de os apoiar a fim de aumentar a resiliência e lutar contra as ameaças híbridas.

9. O Conselho apela a que sejam envidados esforços contínuos e sustentados para fazer avançar a implementação de todas as ações relacionadas com a luta contra as ameaças híbridas no âmbito do conjunto comum de propostas para a implementação das declarações conjuntas sobre a cooperação UE-OTAN, nomeadamente nos domínios do conhecimento da situação, da comunicação estratégica, da prevenção e resposta a crises e do reforço da resiliência. Neste contexto, reitera a necessidade de intensificar o diálogo político sobre a luta contra as ameaças híbridas, bem como de realizar periodicamente exercícios paralelos e coordenados (PACE) com a participação de todos os Estados-Membros da UE e os aliados da OTAN, e apela à conclusão atempada do novo plano relativo aos PACE. O Conselho salienta a necessidade de ter em conta os ensinamentos identificados e a importância de um intercâmbio de informações sem entraves que se desenrole de forma inclusiva e não discriminatória.

Além disso, o Conselho destaca os preciosos contributos do Centro Europeu de Excelência para Combate às Ameaças Híbridas em Helsínquia e incentiva a sua cooperação com os centros de excelência relevantes da OTAN. Saúda igualmente os intercâmbios periódicos e estruturados a nível do pessoal, nomeadamente a cooperação entre a célula de fusão da UE contra as ameaças híbridas do Centro de Situação e de Informações da UE (INTCEN) e a Célula de Análise de Ameaças Híbridas da OTAN.

10. O Conselho reconhece os esforços desenvolvidos pelos Estados-Membros, em cooperação com a Comissão e o Serviço Europeu para a Ação Externa (SEAE), para realizar o estudo sobre riscos híbridos previsto na ação 1 do Quadro comum em matéria de luta contra as ameaças híbridas (2016) e apela à continuação dos trabalhos e a uma eventual revisão do estudo sobre riscos híbridos a fim de responder melhor às vulnerabilidades.

Trabalhar de forma coerente para aumentar a resiliência e combater as ameaças híbridas

11. Ao desenvolver e utilizar tecnologias novas e emergentes, incluindo a inteligência artificial e as técnicas de recolha de dados, haverá que ter devidamente em conta as novas oportunidades para aumentar a resiliência, bem como as potenciais vulnerabilidades e os efeitos em cascata no contexto da luta contra as ameaças híbridas, a fim de reduzir os riscos globais, inclusive no processo de planeamento estratégico do programa-quadro de investigação e inovação.

12. O Conselho observa que as ciberatividades maliciosas podem fazer parte das ameaças híbridas e, neste contexto, sublinha a importância do conjunto de instrumentos de ciberdiplomacia da UE.

13. A relação entre as ameaças híbridas e a segurança económica é um elemento relevante que deverá ser tido em conta e que continua a ser essencialmente da responsabilidade dos Estados-Membros.

14. Os novos instrumentos, tais como o mecanismo previsto no regulamento relativo à análise dos investimentos diretos estrangeiros, deverão ser utilizados de forma eficaz para aumentar a resiliência e lutar contra as ameaças híbridas mediante a disponibilização de meios para identificar e combater os investimentos diretos estrangeiros suscetíveis de afetar a segurança ou a ordem pública.

15. O Conselho convida a Comissão a incluir a resiliência às ameaças híbridas no processo de avaliação de impacto para as futuras propostas legislativas sobre esta matéria, inclusive nos futuros programas-quadro de investigação e inovação.

16. O Conselho sublinha a importância de realizar periodicamente exercícios e debates com base em cenários hipotéticos no domínio da luta contra as ameaças híbridas, a nível ministerial e a outros níveis, bem como de incluir elementos híbridos noutras atividades de treino e de exercício relevantes da UE realizadas a todos os níveis, com o apoio dos seus Estados-Membros e dos organismos competentes, em particular o Centro Europeu de Excelência para Combate às Ameaças Híbridas, se for caso disso.

17. A fim de assegurar a coerência das próximas etapas da cooperação da UE em matéria de reforço da resiliência e de luta contra as ameaças híbridas, o Conselho convida a Comissão e o alto representante a elaborarem um levantamento exaustivo que tenha em conta as medidas tomadas até à data e os documentos pertinentes adotados, tendo em vista eventuais novas iniciativas.

Correlação entre segurança interna e externa

18. As autoridades de aplicação da lei, a proteção civil e as outras autoridades competentes deverão continuar a desenvolver a sua preparação para prevenir e combater as ameaças híbridas. A cooperação entre as autoridades nacionais competentes, e com as instituições, órgãos e organismos da UE, com base nos respetivos mandatos, em tudo o que diz respeito à correlação entre segurança interna e segurança externa deve ser constantemente melhorada e integrada em todas as atividades, reforçando ao mesmo tempo as sinergias e evitando a duplicação de esforços, nomeadamente através de métodos de trabalho horizontais, do intercâmbio voluntário de informações e da formação e exercícios que abranjam vários setores. Para o efeito, deverá ser continuar a ser avaliado o apoio e os contributos dos mecanismos e organismos da UE competentes, no quadro dos respetivos mandatos e no respeito das restrições orçamentais em vigor.

19. As instituições e órgãos da UE, em colaboração com os Estados-Membros, deverão continuar a desenvolver os mecanismos e instrumentos relevantes da UE de apoio à resposta dos Estados-Membros a ameaças transeitoriais e transfronteiras, nomeadamente o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR), o Mecanismo de Proteção Civil da União (MPCU) e o seu Centro de Coordenação de Resposta de Emergência (CCRE).

20. O Conselho reconhece a possibilidade de os Estados-Membros invocarem a cláusula de solidariedade (artigo 222.º do TFUE) para fazerem face a uma grave crise resultante de uma atividade híbrida.

Conhecimento da situação e análise das informações

21. A cooperação da UE em matéria de reforço da resiliência e de luta contra as ameaças híbridas deve pautar-se por uma avaliação da ameaça atualizada regularmente e um conhecimento aprofundado da situação. Estes devem ser desenvolvidos pelo INTCEN da UE e pela sua célula de fusão da UE contra as ameaças híbridas, a fim de melhorar a aptidão da UE e dos seus Estados-Membros para detetar, prevenir, combater e responder a atividades híbridas, respeitando ao mesmo tempo a competência dos Estados-Membros. O Conselho considera que o trabalho da célula de fusão da UE contra as ameaças híbridas deve continuar a ser reforçado, tendo em conta um nível adequado de recursos, incluindo conhecimentos especializados.

22. O Conselho recorda as suas conclusões sobre a luta contra as ameaças híbridas, de 19 de abril de 2016, nas quais apelava à mobilização de instrumentos da UE para prevenir e combater as ameaças híbridas à União e aos seus Estados-Membros, bem como aos seus parceiros. O Conselho sublinha a necessidade de continuar a desenvolver as funções de conhecimento da situação dos Estados-Membros e da UE, tendo em conta as origens das ameaças, e de melhor utilizar a análise de informações do INTCEN da UE e da sua célula de fusão contra as ameaças híbridas, em especial nos processos de elaboração de políticas da UE e de gestão de crises em matéria de luta contra as ameaças híbridas.

23. O Conselho reconhece o contributo relevante que as missões e operações da PCSD poderão dar, quando e se adequado, para identificar e analisar os indicadores de eventuais ações híbridas de terceiros, nomeadamente a desinformação destinada a desacreditar e dificultar a atuação da UE e dos seus Estados-Membros, e reconhece a utilidade de continuar a explorar a possibilidade de desenvolver esse contributo.

Proteção das infraestruturas críticas

24. A proteção das infraestruturas críticas nacionais e europeias, bem como das funções e dos serviços críticos para o bom funcionamento do Estado, da economia e da sociedade, constitui uma prioridade essencial, inclusive no contexto do reforço da resiliência às ameaças híbridas, e exige uma abordagem que abranja todas as administrações públicas e toda a sociedade. Este trabalho deve ter em conta as fortes interdependências entre as diferentes funções e serviços críticos, incluindo os serviços financeiros, o papel determinante do setor privado, a evolução do ambiente de segurança e os riscos emergentes, tanto no domínio físico como no do ciberespaço.

25. Além disso, para além dos requisitos jurídicos, regulamentares e de supervisão nacionais e da UE que regem a resiliência operacional e a continuidade das atividades, deverão ser promovidos acordos com proprietários e operadores de infraestruturas e serviços do setor privado a fim de garantir a continuidade dos serviços críticos e o acesso aos mesmos, inclusive em casos que não sejam de força maior, assegurando um nível de preparação aceitável para responder a todas as ameaças pertinentes, bem como a flexibilidade necessária para reagir a acontecimentos pouco prováveis mas com impacto elevado, para atenuar os seus efeitos e para recuperar dos mesmos.

26. O Conselho salienta que, se bem que a responsabilidade pela proteção das infraestruturas críticas seja essencialmente uma questão da competência nacional, o elevado grau de interdependência transfronteiras e transeitorial exige esforços coordenados ou, se for caso disso, harmonizados a nível da UE, nomeadamente tendo em vista o funcionamento ininterrupto do mercado interno.

27. Na sequência da avaliação de julho de 2019 sobre a execução da Diretiva (2008/114/CE) relativa à identificação e designação das infraestruturas críticas europeias (ICE), o Conselho convida a Comissão a consultar os Estados-Membros sobre uma eventual proposta de revisão da diretiva no início do novo ciclo legislativo, inclusive possíveis medidas adicionais para reforçar a proteção e a resiliência das infraestruturas críticas na UE, tendo em conta as estreitas interdependências entre as funções e os serviços críticos.

28. O Conselho convida a Comissão a continuar a colaborar com os Estados-Membros e, se for caso disso, a elaborar acordos de cooperação não vinculativos entre os Estados-Membros que partilham infraestruturas críticas interligadas.

29. O Conselho reconhece a importância da Diretiva Segurança das Redes e da Informação (Diretiva SRI) para o desenvolvimento de uma cultura de gestão de riscos e de segurança por parte dos operadores em setores críticos, bem como das capacidades e estratégias nacionais que asseguram um elevado nível de segurança das redes e dos sistemas de informação no seu território, inclusive no contexto das ameaças híbridas. O Conselho convida os Estados-Membros, a Comissão e a Agência da União Europeia para a Cibersegurança (ENISA) a continuarem a desenvolver a sua cooperação com base na recomendação da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (plano de ação) a todos os níveis pertinentes.

Combater a desinformação e garantir eleições livres e justas

30. O Conselho congratula-se com o relatório sobre a aplicação do Plano de Ação contra a Desinformação e reconhece que a sua implementação continuada continua a estar no cerne dos esforços da UE. O Conselho sublinha a necessidade de o plano de ação ser regularmente revisto e, se necessário, atualizado para garantir uma abordagem de longo prazo eficaz.

31. O Conselho sublinha que o trabalho da Divisão de Comunicação Estratégica do SEAE e, em particular, dos três grupos de trabalho (Leste, Balcãs Ocidentais e Sul), tem de ser apoiado com recursos suficientes que permitam o planeamento, a aplicação e a avaliação a longo prazo. Entre as suas funções, os três grupos de trabalho deverão poder continuamente detetar, analisar e combater as atividades de desinformação de intervenientes estatais estrangeiros e de intervenientes não estatais externos. Os grupos de trabalho devem igualmente continuar a contribuir para uma comunicação positiva eficaz e baseada em factos e para a promoção dos princípios, valores e políticas da União nos países da vizinhança oriental e meridional da UE e nos Balcãs Ocidentais, e bem assim para o reforço do ambiente mediático geral e da sociedade civil nas respetivas regiões. O Conselho convida o SEAE a avaliar as necessidades e as possibilidades de reforçar o seu trabalho de comunicação estratégica noutras zonas geográficas, como a África Subsariana, mantendo simultaneamente as capacidades necessárias para levar a cabo as atuais funções de comunicação estratégica.

32. O Conselho reconhece que é necessária uma abordagem global a todos os níveis para enfrentar os desafios da desinformação, nomeadamente as interferências destinadas a comprometer a realização de eleições europeias livres e justas, fazendo o melhor uso possível de todos os instrumentos disponíveis em linha e fora de linha. Tal deve incluir a monitorização e análise da desinformação e da manipulação, a execução das regras europeias em matéria de proteção de dados, a aplicação das salvaguardas eleitorais, os esforços para reforçar o pluralismo dos meios de comunicação social, o jornalismo profissional e a literacia mediática, bem como a sensibilização dos cidadãos. O Conselho recomenda que se continue a consolidar uma rede transeuropeia independente e ativa de verificadores de factos e de investigadores contra a desinformação. O Conselho reconhece a importância e o papel desempenhado pela sociedade civil, o meio académico e o setor privado na luta contra a desinformação e no reforço da resiliência.

33. O Conselho reconhece as potencialidades do sistema de alerta rápido no que respeita à luta contra a desinformação, em particular as interferências em eleições. Exorta a Comissão e o SEAE, juntamente com os Estados-Membros, a continuarem a desenvolver o sistema de alerta rápido tendo em vista uma plataforma global para que os Estados-Membros e as instituições da UE reforcem a cooperação, a coordenação e o intercâmbio de informações como os conhecimentos provenientes da investigação e de análises, as melhores práticas e os produtos de comunicação, a fim de apoiar o combate às campanhas de desinformação no âmbito de uma série de esforços a nível europeu e nacional.

34. O Conselho reconhece a utilidade das medidas e recomendações apresentadas pela Comissão em 12 de setembro de 2018 no seu pacote de medidas destinadas a assegurar eleições europeias seguras. O Conselho incentiva a Comissão e os Estados-Membros a analisarem as possibilidades de prosseguir as atividades das redes europeias de cooperação em matéria eleitoral para apoiar o intercâmbio de informações e de melhores práticas. O Conselho congratula-se com os esforços envidados pela Comissão no sentido de envolver todas as partes interessadas relevantes e de apoiar um vasto leque de medidas, tais como o exercício sobre a cibersegurança das eleições europeias (EU ELEX19), tendo em conta as competências nacionais neste domínio.

35. O Conselho reconhece a necessidade de continuar a trabalhar com as plataformas de redes sociais para alcançar níveis mais elevados de responsabilidade, transparência e prestação de contas no combate à desinformação. Além disso, deverá ser concedido acesso sem entraves aos dados anonimizados dos fornecedores de plataformas de redes sociais para a investigação académica, a fim de facilitar a adoção de políticas assentes em dados concretos. O Conselho convida a Comissão a apresentar iniciativas sobre a via a seguir para combater a desinformação nas plataformas em linha. Estas iniciativas devem basear-se numa avaliação da aplicação do Código de Conduta sobre Desinformação, que deverá ter em conta o trabalho analítico e os relatórios realizados pelo meio académico e as organizações da sociedade civil, o relatório de acompanhamento sobre o código elaborado pelo Grupo de Reguladores Europeus dos Serviços de Comunicação Social Audiovisual, bem como os ensinamentos retirados das eleições para o Parlamento Europeu de maio de 2019. Neste contexto, o Conselho convida a Comissão a ponderar formas, incluindo eventuais mecanismos de execução para as plataformas em linha, de continuar a reforçar a aplicação do código de conduta, nomeadamente através da inclusão de uma avaliação independente do cumprimento dos compromissos pelos signatários.

Segurança das instituições, órgãos e organismos da UE

36. A proteção do pessoal, instituições, órgãos e organismos da UE contra as ameaças híbridas e outras atividades maliciosas constitui um interesse partilhado pela UE e pelos seus Estados-Membros. O Conselho exorta as instituições, órgãos e organismos da UE, apoiados pelos Estados-Membros, a garantirem a capacidade da União para proteger a sua integridade e reforçar a segurança das redes de informação e comunicação e dos processos de tomada de decisão da UE contra atividades maliciosas de todos os tipos, com base numa avaliação global da ameaça. Para tal, as instituições, órgãos e organismos da UE, apoiados pelos Estados-Membros, deverão desenvolver e aplicar uma série de medidas abrangentes destinadas a garantir a sua segurança, em conformidade com o mandato do Conselho Europeu de junho de 2019. O Conselho sublinha a importância de assegurar a interoperabilidade das infraestruturas informáticas da UE para o intercâmbio de informações classificadas entre as instituições, órgãos e organismos da UE e os Estados-Membros.
