

# SEGURANÇA REAL E VIRTUAL: OS NOVOS DESAFIOS DAS TEORIAS DE SEGURANÇA.

André E R S Aprigio<sup>1</sup>

Isabel Estrada Carvalhais<sup>2</sup>

**RESUMO:** O artigo objetiva, de forma sumária, discorrer sobre os desafios contemporâneos das teorias de segurança, sob a visão europeia, apresentando diversos teóricos com uma visão desde o surgimento da Política Europeia de Segurança e Defesa (PESD), passando pelo advento da Política Comum de Segurança e Defesa (PCSD). O artigo lança um olhar mais contemporâneo em um mundo, cada vez mais, ligado, interligado, interdependente e complexo, e que enfrenta “novas ameaças” constantes à segurança, também no mundo virtual, sobretudo em razão do surgimento do ISIS.

**Palavras-chave:** Europa, Estratégia, Segurança, Virtual, ISIS.

**ABSTRACT:** This article aims to briefly discuss the contemporary challenges to the security theories, in a European perspective, presenting several theorists with a vision from the emergence of the European Security and Defense Policy (ESDP), through the advent of the Common Security and Defense Policy (CSDP). This article provides a more contemporary look in an increasingly interconnected world, interdependent and complex, and that faces constant “new threats” to security, notably in the virtual world, especially due to the emergence of ISIS.

**Keywords:** Europe, Strategy, Security, Virtual, ISIS.

## 1. No mundo real

Durante o período pós 2ª Guerra Mundial, manter e reforçar os laços transatlânticos entre a Europa e os Estados Unidos passou a ser uma preocupação na agenda da política externa do Reino Unido. Este viu-se como uma ponte entre os dois continentes.

No entanto, o sistema de segurança mudou radicalmente após a Guerra Fria. Após o derramamento de sangue na região dos Balcãs, o governo britânico percebeu que a União Europeia (UE) deveria assumir uma maior responsabilidade pela segurança e defesa.

Além disso, a eleição de Tony Blair como primeiro-ministro marcou uma mudança fundamental na abordagem do Reino Unido em relação à Europa, favorecendo uma política de engajamento construtivo no seio das instituições europeias.

Como o Reino Unido, a França estava convencida de que a estabilidade doméstica e integração na UE pós-guerra fria já não bastava para garantir a segurança na Europa.

<sup>1</sup> **André E R S Aprigio** é doutorando em Ciência Política e Relações Internacionais pela Universidade do Minho (UMinho - Portugal), mestre e especialista em Relações Internacionais pela mesma instituição, membro colaborador do Centro de Investigação em Ciência Política (CICP) e pesquisador visitante do IRI/USP | andre.aprigio@gmail.com.

<sup>2</sup> **Isabel Estrada Carvalhais** é professora do Departamento de Relações Internacionais e Administração Pública da UMinho, diretora do Programa de Doutoramento em Ciência Política e Relações Internacionais da mesma instituição e membro integrado do CICP. É doutora em Sociologia pela Universidade de Warwick, mestre em Sociologia pela Universidade de Coimbra e graduada em Relações Internacionais pela UMinho | isabelestrada@eeg.uminho.pt.

Ademais, um objetivo central da política externa e de segurança francesa já não era, há muito, criar uma política de segurança e defesa europeia (relativamente) autônoma para contrabalançar os EUA e complementar a OTAN. A França também esperava que essa política conduzisse a uma parceria transatlântica mais equilibrada.

A Declaração de Saint-Malo<sup>3</sup> (1998, 1, tradução nossa), que levou à criação da Política Europeia de Segurança e Defesa (PESD), explicita que a UE deve adquirir a “capacidade de ação autônoma, apoiada em forças militares credíveis, de meios para decidir sobre sua utilização e de vontade para fazê-lo, a fim de responder a crises internacionais.”<sup>4</sup>. No entanto, esse compromisso não deveria desafiar o papel da OTAN, uma vez que a UE deve agir em consonância com as respectivas obrigações com a Aliança.

Do outro lado do Atlântico, porém, a Declaração de Saint-Malo foi recebida com um certo grau de ceticismo. Alguns tomadores de decisão política americanos, incluindo a então secretária de Estado Madeleine Albright, expressaram publicamente suas preocupações com a iniciativa Franco-Britânica, pois pensavam que poderia prejudicar a OTAN, e levar à duplicação desnecessária no tocante a questões de segurança e política.

A missão da OTAN como uma aliança de defesa parecia estar completa, uma vez que a União Soviética havia se desintegrado. Mas foi durante a década de 1990 que a OTAN passou a focar em sua transformação. Novos órgãos foram criados para garantir a lealdade dos Estados emergentes: O Conselho de Cooperação do Atlântico Norte (NACC), posteriormente chamado Conselho de Parceria Euro-Atlântica (CPEA) e da Parceria para a Paz (PfP) foram os mais importantes, além do Conselho OTAN-Rússia.

Na Conferência da OTAN em 1997 foi tomada a decisão pelo seu alargamento. A França iniciou o discurso que poderia ter significado a sua reintegração na estrutura de comando militar e a Espanha se juntou à estrutura de comando militar da OTAN.

A missão da OTAN também foi transformada, sendo adaptada para combinar com o novo ambiente estratégico. O quadro operacional da OTAN teve de ser alterado, de modo a implantar maior flexibilidade e eficácia. Na reunião de junho de 1999 do Conselho Europeu, em Colônia, na Alemanha, os chefes de Estado e de Governo ressaltaram que a PESD visa dotar a UE com os meios necessários para assumir as suas responsabilidades, mormente no que tange à capacidade de tomar decisões sobre a prevenção de conflitos e gestão de crises definidas no Tratado da União Europeia (TUE), ou seja, as tarefas de Petersberg.

Os chefes de Estado e de Governo chegaram a acordo sobre arranjos institucionais para assegurar o controle político e a direção estratégica das operações Petersberg lideradas pela UE (*EU-led operations*). Na Conferência de Helsinki, em dezembro de 1999 (e reuniões posteriores), o Conselho Europeu definiu os papéis dessas instituições

<sup>3</sup> Conferência de Saint-Malo, realizada entre os dias 3 e 4 de dezembro de 1998.

<sup>4</sup> Cf. texto original em inglês “capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises”, disponível em: [http://eeas.europa.eu/security-defence/index\\_en.htm](http://eeas.europa.eu/security-defence/index_en.htm).

de segurança e as suas novas atribuições. Assim, ficou decidido que essas instituições proporcionariam aos Estados-Membros da UE um processo de tomada de decisão eficaz em caso de crise.

Da Conferência de Helsinki resultou o chamado “*Headline Goal*”, pelo qual os Estados-Membros se comprometiam a criar um contingente de 60 mil homens mobilizável em até 60 dias e com capacidade sustentável de até um ano a fim de operacionalizar as tarefas de Petersberg. Assim, como a chave para o sucesso da IESD centra-se em capacidade (militar), restava-se evidente a intenção da UE.

As decisões então tomadas em Helsinki marcaram uma mudança significativa na evolução do regime de segurança da Europa, explicitando a real intenção europeia de se tornar ator principal (e não mais apenas um coadjuvante) no palco da segurança e defesa nos assuntos por muitos considerados como sendo do seu “próprio quintal”.

Com efeito, em novembro de 2000, os Estados-Membros da UE participaram da primeira *Capabilities Commitment Conference*, ou Conferência de Empenhamento de Capacidades, onde decidiram pelo “contributo voluntário para a realização do objectivo comum europeu prioritário da capacidade militar” (Ferreira-Pereira 2005). Ressalte-se, porém, que a PESD – que possui seu foco em operações de gestão de crises civis e militares, incluindo a resposta a catástrofes naturais, questões humanitárias, dentre outros –, é parte integrante da Política Externa e de Segurança Comum (PESC). Seus objetivos principais são as operações de gestão de crises e outras atividades, bem como o desenvolvimento de novos instrumentos e conceitos que visam alcançar os objetivos da PESC.

## 2. No início, uma questão de capacidades

O desenvolvimento da componente de gestão civil de crises começou com as conclusões do Conselho Europeu de 2000, em Santa Maria da Feira, e com a definição de atividades nos domínios da polícia, justiça, administração pública e proteção civil, com base no *2008 Civilian Headline Goal*<sup>5</sup>, ou Objetivo Global Civil 2008, de dezembro de 2004.

Já o desenvolvimento da componente militar da gestão de crises continuou em 1999 com a aprovação do *European Headline Goal*, ou Objetivo Comum Europeu Prioritário, e foi atualizado com o conceito de *battlegroup*<sup>6</sup> da UE (até ao nível de brigada), em 2004, que se tornou operacional em 2007, com a possibilidade de implantação em 5 -10 dias de 30-120 dias.

Por fim, o desenvolvimento das capacidades introduziu uma abordagem mais sistemática, com o reforço da cooperação com outros parceiros, bem como a criação

---

<sup>5</sup> Disponível em <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015863%202004%20INIT>.

<sup>6</sup> De forma geral, *battlegroups* significam o efetivo capaz de ser rapidamente implantado e de atuar de forma independente, ou como parte de fases iniciais de grandes operações, como se nota em [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/esdp/91624.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/esdp/91624.pdf).

de instituições para ajudar nesse desenvolvimento. A Agência Europeia de Defesa, por exemplo, é responsável por um desenvolvimento a longo prazo de políticas coerentes em defesa da indústria e dos mercados, pesquisa, desenvolvimento e de armamento.

### 3. A PESD em Campo

A crise na República Democrática do Congo foi o primeiro teste para a operação de *peacekeeping* (operações de paz) da UE sem o envolvimento da OTAN.

Em junho de 2003 as Nações Unidas pediram que a Europa interviesse. Aquela seria a primeira missão militar europeia fora da Europa, liderada pelos franceses, todavia sob a bandeira da Europa.

O sucesso da missão do Congo mostrou como a UE pode desempenhar o seu papel sem resultar em duplicação dos esforços da OTAN. A partir daí, surgiu um plano ambicioso de criar 13 *battlegroups* de até 1 500 soldados que poderiam ser enviados para estabilizar os pontos de conflito ou proteger as operações humanitárias em todo o mundo.

Desde que foi lançada, a PESD conta com um *acquis* de 23 missões. Dessas 23, lançadas entre 2002 (EUPM Bósnia e Herzegovina) e 2009 (EU NAVFOR Somália, desde 8 de dezembro de 2008), seis foram importantes operações militares, sendo a primeira delas, por exemplo, em 2004, denominada Operação Concórdia, na República da Macedônia.

Essas operações têm variado bastante em termos de escala, contando com algumas dezenas de observadores, policiais ou conselheiros civis chegando a possui até milhares de soldados.

Apesar de terem sido quase sempre em terra, a operação “Atlanta”, ao largo da costa da Somália, fez a primeira operação naval da UE.

### 4. A relação UE-OTAN

Mas onde a OTAN se encaixa enquanto a UE arquiteta suas próprias estratégias militares? Na realidade, a política de defesa da Europa está a se desenvolver em parceria com a própria Aliança Atlântica, e muitas das grandes operações da UE, tal como a da Bósnia, ainda compartilham as estruturas da OTAN, como por exemplo, comunicações e sistemas de satélite.

É certo que durante o desenvolvimento da PESD, um grande desafio foi o de determinar a relação e o nível de cooperação entre a UE-OTAN. Esta sempre foi uma tarefa difícil, porque alguns receavam que a criação da PESD enfraqueceria a OTAN.

Dada a complexidade do ambiente de segurança contemporâneo, os tomadores de decisão política consideram que uma relação mais harmoniosa entre UE-OTAN é essencial para efetivamente garantir a segurança no pós-guerra fria.

Neste sentido, Karl-Heinz Kamp (2009, tradução nossa), diretor da Divisão de

Pesquisa do *NATO Defense College*, afirma que: “Se, por exemplo, a OTAN e a UE não se orquestrarem no Afeganistão, pessoas morrerão [...] portanto nós não temos tempo a perder com essa competição que, por muitos, muitos anos, impediu uma cooperação mais eficiente entre essas instituições.”<sup>7</sup>

## 5. Tratado de Lisboa: um fôlego novo

Com relação à PESC e à PESD, o Tratado de Lisboa (TL)<sup>8</sup> pode ser considerado como o resultado de anos de prática institucional, reflexão estratégica e um compromisso entre diferentes perspectivas nacionais acerca da política externa e de segurança da UE.

O TL introduz novidade considerável. Por meio de avaliação geral, a reforma visa criar condições para aumentar o efetivo de decisão política, sem afetar as regras formais para a tomada de decisões no domínio da PESC e da PESD.

Ele modifica completamente o contexto institucional da PESD e introduz inovações mais específicas relativas à esta área política como tal. Em síntese, o novo Tratado enquadra pela primeira vez todos os aspectos da ação externa da UE, dentro de um conjunto comum de princípios e objetivos.

Com efeito, o TL altera a denominação da PESD para Política Comum de Segurança e Defesa (PCSD); expande o alcance das chamadas tarefas de Petersberg para incluir operações conjuntas de desarmamento, as missões de assistência, prevenção e estabilização pós-conflito, além das tarefas previstas no âmbito do atual Tratado, nomeadamente as humanitárias e de salvamento, missões de manutenção da paz e missões de forças de combate para a gestão de crises, incluindo operações de paz (*peacekeeping*).

Ademais, o novo Tratado traduz na área da segurança e da defesa o forte compromisso com a solidariedade dos Estados-Membros, por meio da cláusula de assistência mútua em caso de agressão armada no território de um deles.

Importante notar, porém, que a PCSD não avançou, substancialmente, desde a sua concepção no TL, em 2009.

## 6. O “mundo virtual” e seus “novos” desafios

O “mundo virtual” tornou-se, de fato, onipresente na vida da larga maioria dos cidadãos, mas como toda moeda, ele também possui dois lados.

As ameaças a Estados e indivíduos, hodiernamente, residem tanto no “mundo real” como “no virtual”, separadamente ou não, e possuem origens diversas, dentre elas

---

<sup>7</sup> Cf. entrevista original em inglês “If, for instance, NATO and EU don’t get their acts together in Afghanistan, people will die (...) so therefore we cannot afford these beauty contests anymore, which for many, many years, prevented a more efficient cooperation between these institutions.”, disponível em [http://www.nato.int/DOCU/review/2009/NATO\\_Change/EN/index.htm](http://www.nato.int/DOCU/review/2009/NATO_Change/EN/index.htm), minutagem 02”02’ de 05”35’.

<sup>8</sup> Assinado em 2007, com eficácia a partir de 1 de dezembro de 2009.

religiosas, políticas, etc., e muitas com alcance transnacional. Nesse sentido, os Estados devem ter em conta uma estratégia de defesa cibernética alinhada às demais estratégias existentes, trabalhando em sinergia e em tom uníssono.

Enquanto os primeiros usuários da Internet foram pesquisadores afiliados à Agência de Projetos de Pesquisa em Defesa Aplicada, do inglês *Defense Advanced Research Projects Agency* (DARPA) e ao Departamento de Defesa dos Estados Unidos da América, o uso do ciberespaço se alargou por todo o globo, transformando o conceito embrionário – de pesquisas – em apenas mais um dos objetos de sua utilização.

Nos dias atuais, não é raro encontrar ações de grupos terroristas desviadas para o ciberespaço, quer na forma de ameaças, quer na forma de apoio às suas operações, conforme advoga Abraham R. Wagner (2005, 18, tradução nossa) “há também uma quantidade substancial de evidências que terroristas estão, cada vez mais, usando a Internet para a logística relacionada com as suas operações.”<sup>9</sup>, na forma de pura propaganda, utilizando-se das ferramentas de mídia social, vide Figura 1.

Nesse mesmo sentido, Mette Eilstrup-Sangiovanni (2005, 10, tradução nossa) afirma que “a globalização do comércio, comunicação e transporte forneceu novos incentivos e oportunidades para a organização transnacional entre os criminosos e grupos terroristas.”<sup>10</sup>

Tem-se, como exemplo mais proeminente desses grupos, o ISIS, acrônimo do inglês *Islamic State of Iraq and Syria*, também conhecido como ISIL, *Islamic State of Iraq and Levant*, e Daesh, este último do acrônimo em árabe (Osborne 2015), e cuja origem remonta a 2002, quando o jordaniano Abu Musab al-Zarqawi criou o grupo radical Tawhid wal-Jihad, formado por insurgentes e apoiadores de Saddam Hussein, como consequência da invasão do Iraque.

Seu grupo foi inicialmente conhecido como Jama'at al-Tawhid wal-Jihad, antes de mudar para a forma mais simples al-Qaeda no Iraque (AQI), após prometer fidelidade à rede de Osama bin Laden em Outubro de 2004. Desde então, o grupo tem operado sob vários disfarces até o seu atual líder, Abu Bakr al-Baghdadi, declarar o Estado Islâmico no Iraque (ISI), em 2006, acrescentando o e “al- Sham” para criar “Isis”, em 2013. (Osborne 2015, tradução nossa)<sup>11</sup>

O ISIS tem ganhado território com ações de guerra e violência extrema. Porém, suas ações são mais coordenadas e integradas do que se poderia pensar. Nesse sentido, James P. Farwell (2014, 49, tradução nossa)<sup>12</sup> destaca:

<sup>9</sup> Cf. texto original em inglês “there is also a substantial amount of evidence that terrorists are increasingly using the Internet for logistics related to their operations”.

<sup>10</sup> Cf. texto original em inglês “the globalisation of trade, communication, and transportation has provided new incentives and opportunities for transnational organisation among criminals and terrorist groups”.

<sup>11</sup> Cf. texto original em inglês “His group was initially known as Jama'at al-Tawhid wal-Jihad, before changing to the simpler al-Qaeda in Iraq (AQI) after pledging allegiance to Osama bin Laden's network in October 2004. Since then, the group has operated under numerous guises until its current leader, Abu Bakr al-Baghdadi, declared it the Islamic State in Iraq (Isi) in 2006, adding the “and al-Sham” to make “Isis” in 2013”.

<sup>12</sup> Cf. texto original em inglês “the group's principal tool for expanding its influence has been brute force, but as it has attempted to build credibility and establish legitimacy, it has shown a deftness for propaganda,

A principal ferramenta do grupo para expandir a sua influência tem sido a força bruta, mas como ele tem tentado construir credibilidade e estabelecer legitimidade, ele tem mostrado uma destreza para propaganda, usando as mídias sociais e a tecnologia cibernética para recrutar combatentes e intimidar inimigos. (Farwell 2014, 49, tradução nossa)



Fonte: <https://www.zerofox.com/blog/islamic-state-isis-terror-has-gone-social-infographic/>.

A matéria do Portal Zerofox.com<sup>13</sup> aponta para o fato de o Estado Islâmico (ISIS) ter construído:

Uma ferramenta de propaganda on-line sofisticada e eficaz, explorando muitas redes populares como Facebook, YouTube, Twitter, Telegram, WhatsApp, Diaspora e LinkedIn. Seus esforços se assemelham a um departamento de marketing bem estruturado, empregando especialistas em RP e design para garantir uma aparência legítima. ISIS tem dominado a arte de fazer as vozes de poucos soarem como as vozes de milhões. (Zerofox.com 2015)

Conforme afirma Kevin Maney (2015, tradução nossa), a verdade é que o ISIS se vale da “tecnologia para envenenar as mentes de muçulmanos descontentes no Ocidente para recrutá-los”<sup>14</sup>. Assim, o grupo se utiliza de estratégias baseadas em **coordenação** e **comunicação**; criando e envolvendo entusiastas da “causa” em um verdadeiro grupo

using social media and cyber technology to recruit fighters and intimidate enemies”.

<sup>13</sup> Cf. texto original em inglês “A sophisticated and effective online propaganda engine, exploiting many mainstream networks such as Facebook, YouTube, Twitter, Telegram, WhatsApp, Diaspora and LinkedIn. Their efforts resemble a well-oiled marketing department, employing experts in PR and design to ensure a legitimate appearance. ISIS has mastered the art of making the voices of a few sound like the voices of millions”, disponível em: <https://www.zerofox.com/blog/islamic-state-isis-terror-has-gone-social-infographic/>.

<sup>14</sup> Cf. <http://www.newsweek.com/2016/01/08/wanna-fight-isis-weaponize-your-laptop-407168.html>.

de propagadores “*social bot armies*” de suas ideias e ideais; promovendo adequações das plataformas, quando as mesmas são bloqueadas “*network hopping*”; usurpando *hashtags*<sup>15</sup> e *trends*<sup>16</sup> ocidentais, direcionando sua propaganda para públicos de outros continentes e culturas; para além de publicar **revistas e filmes** de forma a apoiar suas ações de marketing (Zerofox.com 2015).

James N. Rosenau (2007, 92, tradução nossa) lembra que “as organizações estão, cada vez mais, capazes de informar e mobilizar seus adeptos, bem como recrutar outros novos.”<sup>17</sup>

Com efeito, Javier Lesaca (2015, tradução nossa) destaca exemplo da atuação do ISIS no ciberespaço e afirma ser imperativo compreender “o papel da comunicação audiovisual na radicalização de terroristas e definição de uma forma eficiente de combatê-lo.”<sup>18</sup> Isso, contudo, não significa que a mídia social seja um incentivo, mas, tão somente, um meio que deve ser compreendido de forma mais alargada.

Em 31 de outubro, catorze dias antes dos ataques em Paris, o ISIS divulgou um vídeo incentivando os jovens na França a se juntarem ao grupo terrorista. Algo semelhante aconteceu no dia 26 de junho, quando um terrorista inspirado pelo ISIS cometeu um ataque terrorista em Lyon. Um mês antes, o ISIS tinha publicado um vídeo nas mídias sociais incentivando os jovens cidadãos franceses a cometerem ataques terroristas. Finalmente, um mês antes do ataque de 7 de janeiro nos escritórios da Charlie Hebdo, o ISIS divulgou um vídeo onde um grupo de jovens cidadãos franceses pediam a seus pares para se alistarem ao grupo terrorista. Diante desses fatos, é mais importante do que nunca analisar e compreender o papel da comunicação audiovisual na radicalização de terroristas e definir uma forma eficiente de combatê-lo. (Lesaca 2015, tradução nossa)<sup>19</sup>

Nesse contexto, a comunidade internacional se vê diante do surgimento de (re)ações de grupos que, embora conhecidos igualmente pela instrumentalização de procedimentos ilegais (*hacking*) – porém não terroristas –, engajam-se em contraposição às ações terroristas de grupos como o ISIS. E embora essa assertiva soe de forma estranha,

<sup>15</sup> *Hashtag* é uma expressão utilizada entre os usuários das redes sociais, na internet, que consiste no uso de uma palavra-chave antecedida pelo símbolo #, conhecido popularmente no Brasil por “jogo da velha” ou “quadrado”, para incluir a respectiva publicação em um espaço comum de publicações análogas.

<sup>16</sup> Expressão em inglês que, de forma geral, significa “assuntos do momento” ou “assuntos mais comentados”.

<sup>17</sup> Cf. texto original em inglês “organizations are increasingly able to inform and mobilize their adherents as well as recruit new adherents.”

<sup>18</sup> Cf. texto original em inglês “*the role of audiovisual communication in the radicalization of terrorists and to define an efficient way to counter it*”, disponível em: <http://www.brookings.edu/blogs/techtank/posts/2015/11/19-isis-social-media-power-lesaca>.

<sup>19</sup> Cf. texto original em inglês “On October 31, fourteen days before the attacks in Paris, ISIS released a video encouraging young people in France to join the terrorist group. Something similar happened on June 26, when a terrorist inspired by ISIS committed a terrorist attack in Lyon. One month earlier, ISIS had released a video on social media encouraging young French citizens to commit terrorist attacks. Finally, one month before the January 7 attack on the offices of Charlie Hebdo, ISIS released a video where a group of young French citizens asked their peers to enlist in the ranks of terrorist group. Given these facts, it is more important than ever to analyze and understand the role of audiovisual communication in the radicalization of terrorists and to define an efficient way to counter it”.

as intenções desses “novos” grupos são, essencialmente, boas, no sentido de que passam a exercer um monitoramento contra as ações terroristas e em defesa do bem comum, em complemento às ações político-institucionais de Governos.

*Anonymous*, um grupo de *hackers* conhecido mundialmente, figura como exemplo desse “novo grupo” que passa a somar esforços na guerra contra o terror. Em matéria publicada no jornal *Mirror*, John Shammass explicita que os membros do *Anonymous* anunciaram guerra contra o ISIS. Deric Lostutter (2015, *apud* Shammass, 2015, tradução nossa), *hacker* e membro do grupo assim afirmou “o fato é, o ISIS pode recrutar pessoas em qualquer lugar, e ao romper essas comunicações, nós tornamos isso um pouco mais difícil de acontecer.”<sup>20</sup>. A partir de ações no ciberespaço, as investidas do *Anonymous* contra o ISIS ficaram conhecidas como *hack attack*.



Figura 2: *Anonymous* anunciam “guerra” digital contra o ISIS.

Fonte: <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-6931331>.

Nesse sentido, percebe-se um contraponto entre certas perspectivas das teorias de segurança, ou seja, como Estados – podem ser soberanos – frente à atuação de grupos terroristas, como o ISIS, em um contexto onde há, também, a participação de grupos internacionais de *hackers* que buscam intervir nesse processo, como o *Anonymous*? Esse cenário corrobora a ideia de que fatores outros são necessários na própria realização das proposições teóricas do campo da segurança internacional.

Assim, no contexto da Estratégia da *Europa 2020*, a Agenda Digital forma um dos sete pilares existentes, com vistas ao crescimento da Europa e, dentre eles, o objetivo em dar uma resposta europeia coordenada a ciberataques.

Aliás, esse movimento possui forte consonância com as discussões geradas no pós-Guerra Fria – que buscaram um alargamento da visão tradicionalista acerca dos estudos

<sup>20</sup> Cf. texto original em inglês “*the fact is, ISIS can recruit people anywhere, and by disrupting their communications, we make that a little bit harder*”, disponível em <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-6931331>.

de segurança –, ou seja, o cenário no qual Barry Buzan, Ole Waever e Jaap de Wilde (1998, 1, tradução nossa) descrevem como existindo “[...] dois pontos de vista dos estudos de segurança estão agora sobre a mesa, o novo, dos alargadores, e o velho, militar e centrado no Estado, dos tradicionalistas.”<sup>21</sup>

Adicionalmente, Hans G. Brauch (2011, 63, tradução nossa)<sup>22</sup> afirma:

O conceito de ameaça como base para o planejamento militar e para legitimação de programas militares – ao menos entre os países da OTAN – mudou muito depois de 1990. Com o alargamento do conceito de segurança da tradicional segurança militar e diplomática para suas novas dimensões econômicas, sociais e ambientais, o conceito de ameaça também se expandiu para se aplicar a uma série de novas ameaças, não só ao ‘Estado’, como também à outras referências dos novos conceitos de segurança, de seres humanos até segurança global.

Em fevereiro de 2003, portanto, em colaboração com a Alta Representante da UE para os Negócios Estrangeiros e a Política de Segurança, a Comissão Europeia (CE) tornou pública uma estratégia em matéria de cibersegurança, para além de uma proposta de diretiva da CE sobre a segurança das redes e da informação.

De forma coordenada, portanto, a UE busca, por meio da estratégia em matéria de cibersegurança “*An Open, Safe and Secure Cyberspace*”<sup>23</sup>, traduzir e por em prática essa sinergia e tom uníssono necessários no enfrentamento às ameaças e aos ataques, impondo “um nível de segurança mínimo para as tecnologias, redes e serviços digitais em todos os Estados-Membros”, (Comissão Europeia 2013a, tradução nossa) para além da “obrigatoriedade de comunicar a ocorrência de ciberincidentes significativos”<sup>24</sup>, quando ocorrerem em certas empresas e organizações.

Na prática, essa nova política define medidas para aumentar a resiliência sistêmica (informática), reforçando a política internacional da UE em caráter de cibersegurança, baseada em cinco pilares: (i) desenvolvimento da política e das capacidades no domínio da ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD); (ii) reforço dos meios de prevenção e oposição a ataques; (iii) desenvolvimento de recursos industriais e tecnológicos em matéria de cibersegurança; (iv) redução drástica da cibercriminalidade e (v) estabelecimento de uma política internacional harmônica no ciberespaço para a UE e promoção dos seus valores fundamentais.

A UE também criou, em 2013, o Centro Europeu de Cibercriminalidade (CEC), com o objetivo de “garantir uma melhor proteção dos cidadãos e das empresas europeias

<sup>21</sup> Cf. texto original em inglês “as a consequence, two views of security studies are now on the table, the new one of the wideners and the old military and state-centered view of the traditionalists”.

<sup>22</sup> Cf. texto original em inglês “the threat concept as the basis for military planning and legitimating military programmes – at least among many NATO countries – has fundamentally changed after 1990. With the widening of the security concept from the traditional military and diplomatic security, to the new economic, societal and environmental dimensions, the threat concept has also widened and been applied to a series of new threats not only to the ‘state’ but also to the other referents of new security concepts, from human beings to global security”.

<sup>23</sup> Cf. [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=1667](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667).

<sup>24</sup> Cf. <http://www.consilium.europa.eu/pt/policies/cyber-security/>.

contra a criminalidade informática.”<sup>25</sup>

Troels Oerting (2013, *apud* Comissão Europeia 2013b), então chefe do CEC, destacou:

No âmbito da luta contra a cibercriminalidade, tendo em conta a sua natureza transnacional e a grande habilidade dos criminosos para se esconderem, temos de reagir de forma flexível e adequada. O Centro Europeu da Cibercriminalidade foi concebido para fornecer essa especialização enquanto centro agregador de conhecimentos, nomeadamente para apoio operacional e de peritagem forense no quadro de investigações, bem como através da sua capacidade para mobilizar todos os recursos relevantes nos EstadosMembros visando mitigar e reduzir a ameaça dos criminosos informáticos, independentemente do local onde se encontrem. (Oerting 2013, *apud* Comissão Europeia 2013b)

Importante notar que o ciberespaço é um terreno vasto para a atuação de grupos terroristas e, por essa razão, deve ser protegido como fazendo parte das próprias fronteiras dos Estados, dentro de um conceito de governança da Internet.

Nesse sentido, têm sido constantes os esforços europeus em busca de um quadro de políticas de segurança, que incluem ações de cooperação com outras instituições, como a OTAN. Em fevereiro deste ano, a UE e a OTAN assinaram um “acordo técnico entre a Capacidade de Resposta a Incidentes Informáticos da OTAN (NCIRC) e da Equipe de Resposta a Emergências Informáticas da União Europeia (CERT -EU).”<sup>26</sup> (Europa 2016, tradução nossa).

O NCIRC faz parte do novo Conceito Estratégico da OTAN<sup>27</sup>, aprovado na Conferência de Lisboa, entre 19 e 20 de novembro de 2010.

O documento descreve o ambiente de segurança atual e identifica as capacidades e políticas que serão postas em prática para garantir a defesa e dissuasão da OTAN, bem como as capacidades de gestão de crises estão suficientemente bem equipadas para enfrentar as ameaças de hoje. Essas ameaças incluem, por exemplo, a proliferação de mísseis balísticos e armas nucleares, terrorismo, ataques cibernéticos e problemas ambientais fundamentais. O Conceito Estratégico também afirma como a OTAN objetiva promover a segurança internacional por meio da cooperação. (OTAN 2014, tradução nossa)

The document then describes the current security environment and identifies the capabilities and policies it will put into place to ensure that NATO's defence and deterrence, as well as crisis management abilities are sufficiently well equipped to face today's threats. These threats include for instance the proliferation of ballistic missiles and nuclear weapons, terrorism, cyber attacks and fundamental environmental problems. The Strategic Concept also affirms how NATO aims to promote international security through cooperation.

<sup>25</sup> Cf. [http://europa.eu/rapid/press-release\\_IP-13-13\\_pt.htm](http://europa.eu/rapid/press-release_IP-13-13_pt.htm).

<sup>26</sup> Cf. texto original em inglês “The European Union and NATO have today signed a Technical Arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU)”.

<sup>27</sup> Cf. *NATO 2010 Strategic Concept “Active Engagement, Modern Defence”*, disponível em: [http://www.nato.int/cps/en/natohq/news\\_68986.htm?selectedLocale=en](http://www.nato.int/cps/en/natohq/news_68986.htm?selectedLocale=en).

## 7. A governança da segurança

A respeito da importância de se pensar em governança da segurança, nos dias atuais, Weber et al (2004, 4, tradução nossa) afirmam que o termo “também engloba muitos dos temas centrais da segurança europeia: a importância das ideias, das instituições e ambas as estruturas formais e informais, de múltiplos atores propositadamente motivados.”<sup>28</sup>

Por outro lado, embora Rosenau (2007, 90, tradução nossa) acredite que o mundo é “demasiado complexo e diversificado para evoluir para um governo global, com uma única autoridade global”<sup>29</sup>, o autor acrescenta que “o critério de governança global como um mecanismo é plausível.”<sup>30</sup>

Os desafios de segurança que se apresentam nos dias atuais deixaram de ser desafios apenas regionais, como muitos vistos no passado. Assim, as abordagens teóricas centrais, ou clássicas, parecem carecer de argumentos e fundamentos outros, para que possam, de fato, explorar as variáveis de um mundo complexo, interdependente e, sobretudo, inseguro. As ameaças surgem, agora, em um *locus* mais alargado, com alcance transnacional.

A governança da segurança, estudada por inúmeros autores, também perpassa o “mundo virtual” e, por essa razão, cada vez mais estudos são voltados para esse tema e *locus*.

É com base na noção de que não há mais um inimigo interno e um externo que Didier Bigo (2000, 342, tradução nossa) afirma que a segurança interna possui uma “dimensão geográfica que se estende para além das fronteiras nacionais. Ela é Europeia, Ocidental, ou internacional no sentido de que ela é baseada em redes de colaboração entre agências de segurança.”<sup>31</sup>

Brandão (2011, 8) oportunamente destaca que “a natureza transnacional da ameaça suscitou a investigação sobre a relação entre segurança interna e a segurança externa (Eriksson e Rhinard 2009; Bigo 2006) e sobre os actores estaduais como fontes de insegurança.”

Elke Krahnemann (2003, 9, tradução nossa) afirma que as transformações estão “[...] afetando o modo como a segurança é definida na Europa e América do Norte, por quem faz as políticas de segurança e como elas são implementadas.”<sup>32</sup>

<sup>28</sup> Cf. texto original em inglês “also encompasses many of the central themes of European security: the importance of ideas, of institutions and both formal and informal structures, of multiple actors purposefully motivated”.

<sup>29</sup> Cf. texto original em inglês “too complex and diverse to evolve global government consisting of a single global authority”

<sup>30</sup> Cf. texto original em inglês “the criterion of global governance as a mechanism of coordination is plausible”.

<sup>31</sup> Cf. texto original em inglês “geographical dimension which extends beyond national borders. It is European, Western, or international in the sense that it is based on networks of collaboration between security agencies.”

<sup>32</sup> Cf. texto original em inglês “[...] are affecting the way in which security is defined in Europe and North

Outrossim, Eilstrup-Sangiovanni (2005, 8, tradução nossa) afirma que “a proliferação de redes transnacionais é, portanto, muitas vezes vista como causa de um declínio na capacidade do Estado de fornecer funções básicas, tais como a manutenção do direito civil e da ordem, defesa do território, etc. (e.g. Strange 1996).”<sup>33</sup>

Destaque-se que, tal como a missão da OTAN, em determinado momento, foi transformada – sendo adaptada para combinar com o novo ambiente estratégico –, talvez seja o momento de se (re)pensar uma nova transformação, visando a uma “atualização” mais contemporânea de seu papel, uma vez que a sociedade “está passando por uma transformação fundamental por meio do surgimento de novas formas de governabilidade no mundo ocidental. O transnacional está a esbater a distinção entre interno e externo, e a desestabilizar conceitos relacionados.”<sup>34</sup> (Bigo 2000, 320, tradução nossa).

Ademais, importante destacar a necessidade de se reconsiderar o próprio conceito de segurança, consoante destaca Bigo (2000, 343, tradução nossa), segundo o qual a “verdadeira” segurança “era a que dizia respeito à sobrevivência física da nação, e sua proteção contra a potencial agressão armada (Walt 1991).”<sup>35</sup>

Ainda, para o autor, “para além dessa aceitação de segurança como sobrevivência existencial, a segurança perdeu o seu propósito”<sup>36</sup>, surgindo o conceito de “segurança social”<sup>37</sup>, um termo guarda-chuva com vistas a definir os esforços para lidar com as ameaças de segurança modernas, as chamadas “novas ameaças” (Bigo 2000, 343, tradução nossa).

## Considerações finais

É verdade, além de compreensível, que os Estados-Membros da UE continuam avessos a qualquer perda de soberania em relação às políticas de segurança e de defesa e, por essa razão, muitas vezes a relação OTAN-UE pode parecer competitiva.

A PESD foi projetada para lidar com crises regionais semelhantes às das guerras dos Balcãs, e do seu enquadramento institucional e operacional reflete essa ambição.

Decerto que o futuro da PCSD depende se poderá contar com a concordância, por parte dos Estados-Membros da UE, pela busca comum de interesses estratégicos.

---

America, by whom security policies are made and how they are implemented.”

<sup>33</sup> Cf. texto original em inglês “the proliferation of transnational networks is therefore often forecast to cause a decline in the capacity of the state to provide basic functions such as the maintenance of civil law and order, defense of territory, etc. (e.g. Strange 1996).”

<sup>34</sup> Cf. texto original em inglês “is undergoing fundamental transformation through the rise of new forms of governmentability in the Western World. The transnational is blurring the distinction between the internal and external, and destabilising related concepts”.

<sup>35</sup> Cf. texto original em inglês “was that which concerned the physical survival of the nation, and its protection from potential armed aggression (Walt 1991).”

<sup>36</sup> Cf. texto original em inglês “*beyond this acceptance of security as existential survival, security lost its purpose*”.

<sup>37</sup> Cf. Barry Buzan, *People States and Fear*, 1991, Weaver, O., Buzan, B., Kelstrup, M. and Lemaitre, P. 1993. *Identity, Migration and the New Security Agenda in Europe*, London, Pinter. p.23.

Isto implicará, primeiramente, uma percepção da ameaça comum; em segundo lugar, a vontade política de aplicar diferentes instrumentos econômico-financeiros, diplomáticos e de gestão de crises de uma forma orientada e coerente; e, por último, uma melhoria das capacidades civis e militares atuais.

Contudo, os dias atuais não se apresentam mais como no passado. Há outras formas de ameaça, mormente as que ocorrem no ciberespaço, ou no chamado “mundo virtual”, que demandam atenção, planejamento e ações coordenadas, por parte de todos os Estados-Membros. De se notar, aliás, que as “novas ameaças” podem surgir (e/ou ocorrer) no mundo real, exclusivamente; no mundo virtual, exclusivamente; bem como de forma concomitante, conforme estratégia do ISIS, sejam elas complementares ou não.

O ISIS é uma realidade. Com ações coordenadas, apoiadas por um esforço de propaganda massiva, utilizando-se das mídias sociais, o grupo tem seu foco na persuasão.

Sua estratégia de comunicação visa persuadir todos os muçulmanos que lutar para restaurar um califado é um dever religioso. A narrativa do grupo retrata o ISIS como um agente de mudança, o verdadeiro apóstolo de uma fé soberana, um campeão de suas próprias noções perversas de justiça social, e uma coleção de vingadores empenhados em acertar contas para os sofrimentos percebidos dos outros. (Farwell 2014, 49-50, tradução nossa)<sup>38</sup>

Todavia, o ISIS não é a única ameaça e tampouco foi o primeiro grupo a se utilizar de propaganda para direcionar suas mensagens<sup>39</sup> (Farwell 2014). Por essa razão, este artigo não tratou de analisar suas investidas, ao longo do tempo. O interesse maior foi reforçar o que já afirmaram Buzan, Waeber e de Wilde (1998, 1, tradução nossa) “[...] dois pontos de vista dos estudos de segurança estão agora sobre a mesa, o novo, dos alargadores, e o velho, militar e centrado no Estado, dos tradicionalistas”.

Não se pode olvidar que a UE possui papel preponderante a ser desempenhado e que deve assumir, de fato e de direito, uma posição mais ativa e proativa no que concerne os assuntos de segurança e defesa na Europa. Tampouco se pode perder de vista o fato de que a UE tem tomado medidas, nos últimos anos, para se colocar em uma posição de vanguarda na proteção do ciberespaço. Aliás, as recentes políticas na área da segurança cibernética comprovam esse protagonismo.

Por outro lado, a insurgência do grupo *Anonymous*, contra a atuação terrorista do ISIS, coadjuvando em parceria (solicitada ou não) com instituições governamentais e Estados soberanos, parece ter sido uma resposta mais rápida e, por ora, mais eficaz, que a do Estado soberano. Muito há, ainda, que se estudar sobre o terrorismo, principalmente

<sup>38</sup> Cf. texto original em inglês “Its communication strategy aims to persuade all Muslims that battling to restore a caliphate is a religious duty. The group’s narrative portrays ISIS as an agent of change, the true apostle of a sovereign faith, a champion of its own perverse notions of social justice, and a collection of avengers bent on settling accounts for the perceived sufferings of others”.

<sup>39</sup> Vide considerações de Farwell, James P. 2014. The media strategy of ISIS. *Survival*, 56:6, 49-55, DOI: 10.1080/00396338.2014.985436.

em suas formas mais contemporâneas.

A estratégia “*An Open, Safe and Secure Cyberspace*”, ou “Um Ciberespaço Aberto, Seguro e Protegido” e a própria Agenda Digital são importantes complementos à PCSD e às ferramentas da UE em matéria de política de segurança. Embora não necessariamente simbolizando uma “militarização” do ciberespaço da UE, significa uma mudança fundamental em relação à postura da UE de outrora, frente os desafios e ameaças atuais e futuras.

Há, ainda, um longo caminho a ser percorrido, principalmente em razão do fácil acesso, pouca (ou ainda ineficiente) regulação, rápido fluxo de informação, dentre outras diversas e inúmeras características do ciberespaço que, ao mesmo tempo, são vantagens buscadas pelos grupos terroristas.

A certeza que se pode ter, até o presente, é o caminho sem volta do uso das Tecnologias de Informação e Comunicação (TICs) por grupos terroristas. Nesse sentido, oportuno ressaltar que, ainda em 2004, a *National Commission on Terrorist Attacks Upon the United States*, também conhecida com *The 9/11 Commission*, ou Comissão Nacional sobre Atentados Terroristas contra os Estados Unidos (Comissão de 11-9), divulgou relatório de 570 páginas, apontando para o uso de modernas tecnologias de comunicação e como os terroristas foram “[...] por sua vez, beneficiados por este mesmo desenvolvimento rápido das tecnologias de comunicação.”<sup>40</sup> (The 9/11 Commission 2004, 88, tradução nossa). Adicionalmente, o relatório afirma que:

O surgimento da World Wide Web deu aos terroristas um meio muito mais fácil de adquirir informações e exercitar comando e controle sobre suas operações. O líder operacional da conspiração do 11/9, Mohamed Atta, conectou-se online a partir de Hamburgo, Alemanha, para pesquisar escolas de voo dos EUA. Alvos de coleta de informações se tornaram mais sofisticados. Essas mudanças tornaram o aviso de vigilância e ameaça mais difícil. (The 9/11 2004, 88, tradução nossa)<sup>41</sup>

O olhar de Bigo (2000, 320, tradução nossa) acende e corrobora a imperativa necessidade de se pensar estrategicamente e, sobretudo, de forma articulada. Para o autor, “essa relação entre dentro e fora é central e mais importante que a necessidade de distinguir entre a segurança do Estado e da sociedade (Waeber et al., 1993).”<sup>42</sup>

Outrossim, segundo o autor, sobretudo após o fim da bipolaridade “as agências de segurança externa (o exército, o serviço secreto) estão procurando no interior das fronteiras, em busca de um inimigo de fora.”<sup>43</sup> (Bigo 2000, 320, tradução nossa).

<sup>40</sup> Cf. texto original em inglês “[...] in turn, have benefited from this same rapid development of communication technologies.”

<sup>41</sup> Cf. texto original em inglês “The emergence of the World Wide Web has given terrorists a much easier means of acquiring information and exercising command and control over their operations. The operational leader of the 9/11 conspiracy, Mohamed Atta, went online from Hamburg, Germany, to research U.S. flight schools. Targets of intelligence collection have become more sophisticated. These changes have made surveillance and threat warning more difficult.”

<sup>42</sup> Cf. texto original em inglês “this relation of inside and outside is central and more important than the need to distinguish between state and societal security (Waeber et al. 1993)”.

<sup>43</sup> Cf. texto original em inglês “external security agencies (the army, the secret service) are looking inside the borders in search of an enemy from outside.”

Com efeito, os estudos acerca da segurança e da governança da segurança possuem, ainda, vasto campo para reflexão e análise, sobretudo no que tange à perspectiva de uma “segurança cooperativa regional”<sup>44</sup>, apresentada por Knudsen (2001, 357, tradução nossa). Para o autor, segurança cooperativa “representa essencialmente a política, demonstrada na prática, de lidar pacificamente com conflitos, não apenas pela abstenção de violência ou ameaças, mas pelo engajamento ativo na negociação e busca de soluções práticas, e por um compromisso com medidas preventivas.”<sup>45</sup> (Knudsen 2001, 357, tradução nossa).

Dessa forma, desde o surgimento da PESD, perpassando pela PCSD que, agora tenta lidar com as “novas ameaças”, o debate sobre as teorias de segurança continua cada vez mais vivo.

Nesse contexto, portanto, torna-se natural que surjam alguns questionamentos que podem ensejar novas análises, investigações e críticas: i) Estaríamos, então, caminhando para uma realidade em que ciberexércitos serão, de fato, necessários? Ou já lá chegamos? ii) De que forma poderemos salvaguardar o uso das mídias sociais, sem bloquear ou diminuir os direitos dos cidadãos? iii) como os grupos terroristas conseguem manter suas conexões ativas, por tanto tempo, sem uma ação eficiente e proativa das instituições? iv) Qual a postura do Estado, frente ao engajamento de grupos outros, contra a articulação terrorista (*hack attacks*)?

Resta evidente que, esteja a ameaça onde estiver, no “mundo real” ou no “mundo virtual”, as guerras do século 21 devem ser travadas considerando as TICs como ferramentas importantes e como objetos de políticas de segurança e defesa, para além de considerar uma estratégia de defesa cibernética alinhada às demais estratégias existentes, trabalhando em sinergia e em tom uníssono com os demais atores, sejam eles estatais ou não. ■

## Referências

BIGO, Didier. 2000. When Two Become One: Internal and External Securitisations in Europe. In M. Kelstrup, & M. Williams (eds.), *International Relations Theory and The Politics of European Integration. Power, Security and Community*: 171-204. Routledge.

BRANDÃO, Ana Paula. 2011. As tendências internacionais e a posição de Portugal. In I Congresso Internacional do OBSERVARE. Disponível em: [http://observare.ual.pt/conference/images/stories/conference%20images%20pdf/S1/Ana\\_Paula\\_Brandao.pdf](http://observare.ual.pt/conference/images/stories/conference%20images%20pdf/S1/Ana_Paula_Brandao.pdf). Acesso em: 02 de março de 2016.

---

<sup>44</sup> Cf. texto original em inglês “regional cooperative security”.

<sup>45</sup> Cf. texto original em inglês “essentially represents the policy, demonstrated in practice, of dealing peacefully with conflicts, not merely by abstention from violence or threats, but by active engagement in negotiation and a search for practical solutions, and by a commitment to preventive measures”.

## ■ artigo

BRAUCH, Hans G. 2011. Concepts of Security Threats, Challenges, Vulnerabilities and Risks. In: Brauch, H.G et al. (Eds.). *Coping with Global Environment Change, Disasters and Security*. Berlin: Springer.

BUZAN, Barry, Waever, Ole e de Wilde, Jaap. 1998. *Security: a new framework for analysis*. Boulder: Lynne Rienner.

Comissão Europeia. 2013a. Comunicado de imprensa. “Centro europeu da cibercriminalidade (EC3) é inaugurado em 11 de janeiro. Disponível em: [http://europa.eu/rapid/press-release\\_IP-13-13\\_pt.htm](http://europa.eu/rapid/press-release_IP-13-13_pt.htm). Acesso em 02 de março de 2016.

\_\_\_\_\_, 2013b. Comunicado de imprensa. “Centro europeu da cibercriminalidade (EC3) é inaugurado em 11 de janeiro. Disponível em: [http://europa.eu/rapid/press-release\\_IP-13-13\\_pt.htm](http://europa.eu/rapid/press-release_IP-13-13_pt.htm). Acesso em 02 de março de 2016.

Conselho Europeu. 1998. Joint declaration issued at the British-French summit, Saint Malo, France, 3-4 December 1998. Disponível em: <https://www.consilium.europa.eu/uedocs/cmsUpload/French-British%20Summit%20Declaration,%20Saint-Malo,%201998%20-%20EN.pdf>. Acesso em 12 de março de 2016.

EILSTRUP-SANGIOVANNI, Mette. 2005. “Transnational Networks and New Security Threats”. *Cambridge Review of International Affairs* 18 (1): 7-13.

Europa. 2016. EU and NATO cyber defence cooperation. Disponível em: [http://eeas.europa.eu/top\\_stories/2016/100216\\_eu-nato-cyber-defence-cooperation\\_en.htm](http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm). Acesso em: 11 de julho de 2016.

FARWELL, James P. 2014. The media strategy of ISIS. *Survival*, 56:6, 49-55, DOI: 10.1080/00396338.2014.985436. Disponível em: <http://www.tandfonline.com/doi/pdf/10.1080/00396338.2014.985436>. Acesso em 13 de julho de 2016.

FERREIRA-PEREIRA, Laura. 2005. A Europa da Defesa: o Fim do Limbo. In *Revista Nação e Defesa*. Instituto da Defesa Nacional. No. 110, 3a Série. Lisboa.

KAMP, Karl-Heinz. 2009. Interview. In *Alone we fail*. *Video*: NATO. Disponível em: [http://www.nato.int/DOCU/review/2009/NATO\\_Change/EN/index.htm](http://www.nato.int/DOCU/review/2009/NATO_Change/EN/index.htm). Minutagem 02”02’ de 05”35’. Acesso em 13 de abril de 2016.

KRAHMANN, Elke. 2003. Conceptualizing security governance. In “Cooperation and

conflict". Journal of the Nordic International Studies Association. Vol. 38(1): 5-26. Sage.

KNUDSEN, Olav F. 2001. Post-Copenhagen security studies: desecuritizing securitization. In Security dialogue. Vol. 32. Sage.

LESACA, Javier. 2015. Fight against ISIS reveals power of social media. Disponível em: <http://www.brookings.edu/blogs/techtank/posts/2015/11/19-isis-social-media-power-lesaca>. Acesso em 29 de abril de 2016.

MANEY, Kevin. 2015. Wanna fight ISIS? Weaponize your laptop. Newsweek. Disponível em: <http://www.newsweek.com/2016/01/08/wanna-fight-isis-weaponize-your-laptop-407168.html>. Acesso em 29 de abril de 2016.

OSBORNE, Samuel. 2015. Isis vs Daesh vs Isil vs Islamic State: What do the different names mean and why are there so many? Independent. Disponível em: <http://www.independent.co.uk/news/world/middle-east/isis-vs-daesh-vs-isil-vs-islamic-state-what-do-the-names-mean-and-why-are-there-so-many-a6759106.html>. Acesso em 5 de julho de 2016.

OTAN. 2014. Strategic concepts. Disponível em: [http://www.nato.int/cps/en/natohq/topics\\_56626.htm](http://www.nato.int/cps/en/natohq/topics_56626.htm). Acesso em 11 de julho de 2016.

ROSENAU, J. N. 2007. Governing the ungovernable: the challenge of a global disaggregation of authority. In "Regulation & Governance" (1), 88-97.

SHAMMAS, John. 2015. Anonymous hacker reveals how they will destroy ISIS and its ability to carry out terror attacks. In Mirror. Disponível em: <http://www.mirror.co.uk/news/world-news/anonymous-vs-isis-hacker-reveals-6931331>. Acesso em 15 de abril de 2016.

The 9/11 Commission. 2004. The 9/11 Commission Report. Disponível em: <http://govinfo.library.unt.edu/911/report/911Report.pdf>. Acesso em: 04 de abril de 2016.

WAGNER, Abraham R. 2005. Terrorism and the Internet: use and abuse. In *Fighting terror in cyberspace*. World Scientific, ed. Mark Last e Abraham Kandel, v. 65.

WEBBER, Mark et al. 2004. The governance of European security. Review of international studies, 30 (1), 3-26.

Zerofox.com. 2015. ISIS: terror has gone social [infographic]. Disponível em: <https://www.zerofox.com/blog/islamic-state-isis-terror-has-gone-social-infographic/>. Acesso em 04 de abril de 2016.