Ciberguerra: uma palavra (mal)dita no século XXI

João Carlos Relvão Caetano[1], *Alexandra Ferreira Martins*[2]

Resumo

O espaço é uma arena de conflitos. Onde existem dois ou mais seres vivos, existe competição pelo espaço. É assim com os animais ditos irracionais, mas também com os animais ditos racionais, ou seja, os seres humanos, desde o início da história. Paradoxalmente, por racionalidade ou por falta dela, os seres humanos estão dispostos a lutar pelo domínio do espaço – outros dirão, do seu espaço vital – até ao limite das suas forças e inteligência, recorrendo à guerra. Neste trabalho, é feita uma incursão sobre as principais teorias da guerra e a sua relação com a política por forma a melhor compreender a atualidade e a nova realidade que é a ciberguerra.

Palavras-chave: Ciberguerra. Política. Guerra. Território.

1 Licenciado em Direito e doutor em Ciências Políticas. É Professor Auxiliar do Departamento de Ciências Sociais e de Gestão da Universidade Aberta de Portugal, onde exerce funções como Pró-Reitor para o Desenvolvimento Institucional e os Assuntos Jurídicos. Investigador do CEPESE, CLEPUL e CEMRI. Foi membro do Conselho de Administração da Agência Europeia dos Direitos Fundamentais, com sede em Viena.

2 Licenciada em Comunicação Social e Mestre em Ciência Política no ISCSP da Universidade de Lisboa. Está neste momento a terminar o doutoramento em Ciência Política na mesma instituição. É tutora na Universidade Aberta e investigadora no Instituto do Oriente, Observatório Político e CLEPUL.

1. Da origem e consequências da guerra como fenômeno humano

O espaço é uma arena de conflitos. Onde existem dois ou mais seres vivos, existe competição pelo espaço. É assim com os animais ditos irracionais, mas também com os animais ditos racionais, ou seja, os seres humanos, desde o início da história.Paradoxalmente, por racionalidade ou por falta dela, os seres humanos estão dispostos a lutar pelo domínio do espaço – outros dirão, do seu espaço vital – até ao limite das suas forças e inteligência, recorrendo à guerra.

A guerra pode ser justificada, sublimada, reduzida nos seus efeitos destrutivos, mas, como luta pelo poder que é, é uma realidade própria da existência humana. Não esqueçamos pois esta ideia acabada de introduzir: a guerra (em todas as suas aceções, reais ou metafóricas), é sempre uma luta pelo poder!

Referimos há pouco que as guerras ocorrem no espaço. Ora, o espaço é uma categoria prevalecente no século XXI, dado o elevado grau possível de mobilidade humana. Nunca como neste século foi tão fácil e acessível viajar ou mudar de país ou território. Não significa isso porém uma diminuição da conflitualidade humana, dado que muita da mobilidade humana é indesejada. Pensemos, já neste século, nos fluxos migratórios massivos, por razões políticas, sociais e ambientais, assim como nos conflitos pelo domínio de países e cidades, que estão na base da emergência de movimentos políticos e sociais e também da guerra. É assim, por exemplo, nas nações europeias que rejeitam a presença de migrantes ou refugiados, provocando graves dissídios no seio da União Europeia, na Palestina, onde cada palmo de espaço é diariamente disputado por israelitas e palestinianos, ou na Catalunha, em que parte significativa da população pretende criar um Estado independente, por razões identitárias. Segunda ideia a reter: assiste-se, no século XXI, a uma intensificação da luta pelo espaço, por razões várias, que podem conduzir à guerra, tanto pela força armada quanto por formas mais sutis.

Realidade tão tangível quanto o espaço físico é o espaço cibernético. O cientista político italiano Marco Revelli (REVELLI, 2014) (ver também CAETANO, 2014: 744) defende que no século XXI se está a produzir

uma nova e profunda desigualdade nas sociedades entre as elites que circulam nos espaços digitais e as outras pessoas, que necessitam de se mover fisicamente para sobreviver. Longe de querer desvalorizar a importância do espaço físico, o autor italiano destaca a relevância do domínio das tecnologias digitais como forma de se ter poder nas sociedades contemporâneas, que são tipicamente sociedades em rede.

Qualquer conceito estratégico de segurança e defesa de um país desenvolvido no século XXI inclui a dimensão tecnológica entre os seus fundamentos, dado que, sem capacidade tecnológica, é-se vulnerável. Note-se que quando, no tempo a que nos referimos, se fala de segurança e defesa nacional, não se pressupõe apenas a capacidade militar, mas a capacidade generalizada de resistir às ameaças de qualquer tipo e de promover os interesses próprios, num contexto de globalização. Para o efeito, é necessário que o país em questão tenha, por exemplo, uma situação financeira equilibrada e um forte desenvolvimento econômico e social. Mais ainda, é preciso que o país seja capaz de se posicionar proativamente em relação ao mundo, com uma adequada capacitação das suas elites e das pessoas em geral, que devem ter elevados níveis de formação.

É este o contexto da política contemporânea, em que as dimensões de ação nacional e internacional estão profundamente interligadas, por força da utilização de tecnologias digitais de aplicação generalizada. É em ambientes de altíssima complexidade que os Estados e as organizações de Estados no século XXI defendem os seus interesses e fazem guerras, por certo de tipos diferentes das guerras clássicas, mas que não deixam de ser guerras, ou seja, conflitos pela conquista ou exercício do poder.

Na apresentação do seu livro "Em caso de guerra", António de Sousa Lara escreve, logo no primeiro parágrafo, duas coisas fundamentais para se compreender o estado da arte em matéria de guerra, nos inícios do século XXI: já não vivemos em paz no mundo; estamos numa fase, por natureza transitória, em que focos de guerra coexistem, unidos por adversários coincidentes, quer direta quer indiretamente (LARA, 2015, p.11).

Podemos classificar a situação em apreço como sendo de guerra permanente, não no sentido de que há sempre guerras em curso, mas no sentido de que a guerra é inerenteao sistema político e social vigente.

Em "A Rebelião das Massas" ORTEGA Y GASSET, 1987 [1929]), o filósofo e literato espanhol Ortega y Gasset notou que a guerra foi uma extraordinária invenção humana, comparável à ciência e à administração, para resolver certos conflitos. Notou ainda que tendo a guerra constituído um progresso na história da civilização humana, atendendo porém aos seus efeitos catastróficos, haveria que substituí-la, de forma inteligente, por outra instituição política mais justa e eficiente. Julgou o filósofo, que era um democrata, ver nas saudáveis controvérsias de ideias o fator de modernização política e cultural da sua amada Espanha. Infelizmente, outras guerras venceram os debates e diálogos entre adversários que propunha. Recordamos que grande parte da obra de Ortega y Gasset foi escrita antes da instauração da República em Espanha e da consequente Guerra civil, que antecederam a Segunda Guerra Mundial, em que os fanatismos e a força das armas prevaleceram contra os desejos de paz.

Ao falarmos de guerra permanente, referimo-nos ao fato de que no atual estádio de evolução dos sistemas políticos, sociais e econômicos num tempo de globalização, dadas as contradições dos interesses em jogo, a guerra é inevitável. Aproximamo-nos assim da posição defendida pelo papa Francisco desde 2016 a propósito da guerra. Com efeito, em julho desse ano, estando o papa a bordo do avião que o conduziria às Jornadas Mundiais da Juventude, na Polónia, surpreendeuos jornalistas presentes e, posteriormente, a opinião pública mundial com a afirmação de que o mundo vivia em guerra. Citamos Francisco (2016): "Quando falo em guerra, falo numa guerra de interesses, por dinheiro, pelos recursos da natureza, pelo domínio dos povos. Mas não é uma guerra de religiões. Todas as religiões querem a paz, são os outros que querem a guerra". Referindo-se concretamente ao assassinato do padre francês Jacques Hamel, de 85 anos, que fora degolado, poucos dias antes, num ataque perpetrado pelo grupo extremista Estado Islâmico, numa igreja nos arredores de Rouen, no noroeste de França, o pontífice romano explicitou a que tipo de guerra se referia: uma guerra fragmentada, não orgânica, ou seja, uma guerra não declarada, mas organizada, que provoca a

morte de muitos inocentes. Assim como o padre francês – continuou Francisco, na sua explicação – foi morto quando rezava, muitos outros cristãos, crianças e pessoas inocentes são atacadas no mundo, como se comprova pelo que então ocorria na Nigéria, com a perseguição violenta dos cristãos por parte dos fundamentalistas islâmicos.

No livro acima referido, António de Sousa Lara(2015) diz, sobre a guerra, que há várias possibilidades alternativas, com maior ou menor verosimilhança, para procurar resolver os conflitos contemporâneos: deixar apodrecer as situações, por inação; provocar ruturas que levem à subversão indireta, por exemplo, pelo desmoronamento da União Europeia; ou ainda provocar o aparecimento de novos focos de conflito internacionais, o aumento de intensidade de outros e o desenvolvimento de fenômenos de guerra intermitentes.

Na verdade, todas as possibilidades enunciadas são formas de guerra. A guerra é o modelo político mais subversivo que existe, tendo sido causa de ascensão e queda de muitos poderes ao longo da História. Com as suas ideologias específicas, as guerras destruíram muitas vidas humanas, por vezes de forma massiva. O que importa perceber, no século XXI, é que as novas guerras, processadas a partir ou com apoio em sistemas informáticos, não são guerras clássicas, antes operam num "sistema instável, fluído, policêntrico, modular, de intensidades variáveis, assimétrico, multifinanciado, lentamente convergente" (LARA, 2015, p.11), que é o sistema capitalista, tanto na sua forma liberal como autoritária.

A ciberguerra é o nome geral desta nova realidade, que é preciso perceber com recurso ao trabalho de equipes interdisciplinares de acadêmicos e especialistas em várias áreas do conhecimento.

Como já fora intuído por Ortega y Gasset, a humanidade saída da Segunda Guerra Mundial percebeu as consequências nefastas da guerra e a necessidade de que esta nunca se voltasse a repetir. Trata-se de um tema abordado por vários autores e que foi sintetizado na célebre frase de João Paulo II, em vésperas do início dasegunda guerra do Iraque[3], em 2003: "Guerra nunca mais!".

3 Também conhecida por 2.ª Guerra do Golfo, teve como designação militar "Operação Liberdade Iraquiana". Iniciou-se em 20 de março de 2003.

É porém uma ilusão pensar que já se criaram as instituições políticas capazes de pôr termo à guerra, apesar de, como se disse, após as grandes tragédias do século XX, a comunidade política internacional ter percebido que era necessário regular a guerra em novos moldes e ter procurado evitá-la a todo o custo. Prova disso é a miríade de instituições internacionais que foram criadas para garantir uma efetiva aplicação da justiça a criminosos de guerra – caso exemplar do julgamento de Nuremberga, em 1945/1946 – e o desenvolvimento e aplicação de novas formas políticas visando garantir o mútuo entendimento entre Estados e povos desavindos, com destaque para as Nações Unidas e as convenções que foram aprovadas no seu âmbito.

Não sendo ainda possível culturalmente afastar a guerra da história humana, por esta ainda poder ser vista como necessária e justa, pensou-se e têm-se procurado formas de diminuir a sua intensidade. Segundo Sousa Lara (LARA, 2015, p.13-14), a "guerra justa" passou, já no século XXI, a ser "guerra *light*", "guerra limitada" e "guerra cirúrgica". E a nova "guerra dos drones" vai ainda mais longe, ao procurar criar uma guerra sem mortos do lado contra-atacante e uma adaptação ao cenário econômico – leia-se, com diminuição de custos associados.

Não serão esta leveza ou desinteresse pela guerra uma realidade falsa? Com efeito, as situações de tensão motivadas, por exemplo, pela aprovação, em diferentes partes do mundo, de novas leis anti-imigração ou de exclusão de determinados grupos étnicos ou religiosos aumentaram. Igualmente aumentou a tensão entre Estados outrora rivais e que supostamente se entenderiam após a queda do "maléfico" bloco comunista. Contra os frêmitos defensores da globalização tecnológica, econômica e cultural que afirmaram o fim das fronteiras e uma nova era de paz, Putin, o vitorioso líder russo, e os seus sequazes reafirmaram a existência, ainda que com uma nova configuração, da sociedade internacional das fronteiras, com estas a serem defendidas, se necessário, pelo uso da força das armas. Para estes últimos, políticos realistas ao modo clássico, as novas tecnologias digitais que operam na sociedade em rede, longe de poderem ser rejeitadas ou de ser utilizadas com parcimônia, devem ser aproveitadas para as finalidades de domínio de sempre, com a vantagem de poderem operar em terreno não regulado

pelo direito internacional ou de serem de mais difícil controle ou detecção.

Com o dealbar do novo século, assistimos, com efeito, não ao fim da guerra, mas a uma mutação no esquema de colaboração/confrontação global entre Estados. Continua a haver uma divisão entre Estados fortes e fracos, distinção fundamental da política internacional clássica, em que a ideologia justifica a nova ordem das coisas e explica tanto o descontentamento quanto as formas de atuação dos diversos atores.

Na preparação e ativação da guerra, continuam a ter primazia os Estados nacionais e os blocos militares, sejam eles permanentes (p. ex., a OTAN) ou *ad-hoc* (p. ex., as coligações de Estados que fizeram as duas guerras do Golfo). Já vimos que os conteúdos da guerra não mudaram, mas tão-só a sua aparência. Há menos soldados, tanques, fardas, coreografias, mas o objetivo é o mesmo: derrubar, vencer ou eliminar o inimigo, por forma a exercer o poder, da forma mais ampla possível.[4]

Vemos assim que, em matéria de guerra, mudaram muitas coisas nas últimas décadas, mas que não mudou o essencial, o que, nalguns casos, é estranho, particularmente no que respeita à perceção que as pessoas comuns têm do fenômeno. Com efeito, falando-se da utilização das novas tecnologias ao serviço de objetivos militares, poder-se-ia pensar que as pessoas comuns, que fazem, pelo menos nos países desenvolvidos, um uso massivo da internet, estariam bem informadas dos perigos das tecnologias para a segurança das sociedades, o que não é verdade. Vive-se no primeiro quartel do século XXI o que se viveu no primeiro quartel do século precedente: a sensação de que se vive no melhor dos mundos e de que a paz é um dado adquirido. Puro engano. É o papa Francisco, paladino da justiça e da paz no novo século, que denuncia, como vimos, o sistema de guerra fragmentada em que vivemos, bem como os criadores da situação, o que é um interessantíssimo caso de realismo político, embora de outro tipo que não o de Putin. A situação denunciada é, de fato, grave,

4 Pelo menos idealmente, o poder pode ser comparado ao direito de propriedade no direito romano clássico, ou seja, à "plena in repotestas", que exclui todos os outros do gozo de um mesmo bem. Sabemos que, de acordo com a teoria democrática, o poder deve ser partilhado e que tal também ocorre na política internacional, mas, em política, ainda que inconfessadamente, almeja-se sempre o poder pleno, sem constrangimentos, que é o que normalmente se tenta ao empreender-se a guerra.

como os fatos o demonstram, com a particularidade de as tecnologias e as redes digitais serem um campo privilegiado de guerras no século XXI.

Vejamos, com alguns exemplos, aquilo de que falamos. Entre 2003 e 2005, um grupo associado ao governo chinês promoveu vários ataques cibernéticos contra agências dos governos norte-americano e britânico, que ficaram conhecidos como o "TitanRain". Tratou-se do primeiro caso confirmado publicamente de espionagem cibernética levada a cabo pela China. O *Councilon Foreign Relations* (CFR), que analisa a política externa dos Estados Unidos, publicou em 2017 uma lista de 187 ciberataques publicamente conhecidos cujas suspeitas recaem sobre os governos de 16 países. Os referidos ciberataques da China contra os Estados Unidos e o Reino Unido constam em primeiro lugar na lista, dado o seu volume e impacto. De resto, a China é suspeita de ter perpetrado 76 ataques constantes nessa lista, seguida da Rússia (40) e do Iran (19). Mas outros países levam a cabo o mesmo tipo de atividades, como são os casos dos Estados Unidos, Reino Unido, França, Índia, México, Cazaquistão, Espanha, Coreia do Sul, Coreia do Norte, Emirados Árabes Unidos, Israel, Vietname e Formosa.

Segundo Paulo Veríssimo (2017), especialista em cibersegurança, citado pelo jornal português Público, o número de Estados com poder cibernético está a aumentar, sendo que, nas suas palavras, "há pelo menos meia dúzia de países com grande poder" (VERÍSSIMO, 2017). Esta matéria não está regulada pelo direito internacional, advogando o autor português que se proceda urgentemente a uma extensão cibernética das Convenções de Genebra de 1949 e seus Protocolos Adicionais, que estabelecem as principais regras em matéria de direito internacional humanitário.

Em causa no relatório estão ataques a sistemas e dados informáticos, vitais para as nações atingidas. A Convenção de Budapeste de 2001[5]

5 A Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, é um tratado internacional estabelecido no âmbito do Conselho da Europa e que define a tipologia dos crimes praticados por meio da internet e as formas de investigação e perseguição criminal dos infratores. O tratado incide especialmente sobre questões de direito autoral, crimes informáticos, pornografia infantil e violação da segurança das redes. A Convenção e o seu Relatório Explicativo foram aprovados pelo Comitê de Ministros do Conselho da Europa em 8 de novembro de 2001. A assinatura do tratado

procurou estabelecer condições de cooperação internacional visando a investigação deste tipo de crimes, mas tem-se revelado insuficiente.

Está provado que os ataques cibernéticos são feitos de acordo com os interesses de quem ataca, sendo que, em última instância, os alvos são escolhidos pelos Estados nacionais, que definem também a estratégia. Ao olharmos para as entidades que são atacadas, verificamos que 52% dos ataques da China têm como alvos organizações dos Estados Unidos de natureza variada como, por exemplo, laboratórios de pesquisa científica, empresas de telecomunicações e campanhas de políticos estadunidenses.

Já a Coreia de Norte procurou atingir fundamentalmente a Coreia do Sul (11 em 14 ataques, no período referido), mas a sua atuação é planetária. Suspeita-se que a Coreia do Norte tenha estado na origem do WannaCry, um ataque cibernético de grande escala que, em 2017, atingiu vários países, entre os quais Portugal.

A variedade de ataques promovidos por iniciativa ou com o apoio do Governo russo é significativa. Entre os alvos atingidos contam-se Estados e instituições políticas ou militares como a Estônia, o Parlamento alemão e o Pentágono, empresas como a Yahoo ou ainda a bolsa nova-iorquina Nasdaq.

A maior parte dos ataques (82%) é classificada como espionagem. Os ataques distribuídos de negação de serviço (DDoS, em inglês), em que se paralisam as redes de computadores com sobrecarga de informação, são 8% das ocorrências. Há ainda casos classificados como sabotagem (4%), destruição de dados (4%), descaracterização de sítios na internet (2%) e divulgação de dados privados de pessoas individuais (0,5%).

O estudo tem algumas limitações, reconhecidas pelos seus próprios autores: só relata casos de ataques em que os autores têm ligações a governos de países; e a maior parte dos casos relatados incide sobre países de língua inglesa ou onde se fala inglês – Estados Unidos, Reino Unido, Canadá, Austrália e Índia. Apesar destas limitações, o estudo dá a conhecer grande parte da realidade existente, incluindo todos os Estados mais poderosos do mundo, deixando ainda claro que o poder destes é militar, mas também econômico, científico e tecnológico.

---

teve lugar em Budapeste, em 23 de novembro de 2001, tendo o tratado entrado em vigor em 1 de julho de 2004.

Se, por um lado, é difícil dizer com absoluta certeza qual é a potência que realiza mais ciberataques, não há dúvidas de que a maior parte dos Estados não dispõe de infraestruturas adequadas ou suficientes para garantir a sua segurança. De notar que temos de considerar nesta matéria não apenas os Estados mas todos os potenciais alvos de ciberataques, como é o caso das grandes empresas, normalmente associadas simbolicamente ao poder dos Estados onde estão sediadas. Ora, assim como os Estados não estão suficientemente protegidos de ciberataques, também as empresas não estão,sendo que os efeitos dos ataques podem ser catastróficos.

2. A política da guerra

O que define a política é o poder para alcançar fins específicos, como aceder ou permanecer no exercício de um cargo público, trabalhar ou dirigir uma organização política, aconselhar ou assessorar quem exerce funções públicas ou ainda influenciar as decisões políticas. Procuramos então sistematizar tudo o que se disse até agora, acrescentando alguns elementos classificatórios.

A política foi criada pelo homem em tempos imemoriais para regular a convivência entre pessoas que, querendo viver juntas ou tendo de coexistir umas com as outras, têm interesses potencialmente conflitantes.

A política visa assim garantir a sobrevida com bem-estar (DAMÁSIO, 2003) dos membros da comunidade política, preferentemente de modo pacífico mas, se necessário, com recurso à guerra.

As principais definições de guerra continuam válidas, mas precisam de ser atualizadas, para contemplarem o que de novo comporta a realidade da ciberguerra, no século XXI. Vejamos, sumariamente.

Clausewitz define guerra como "um ato de violência com que se pretende obrigar o nosso oponente a obedecer à nossa vontade" (CLAUSEWITZ, 1997, p.29). Por sua vez, Huntington define guerra como "ação recíproca violenta entre dois grupos políticos organizados" (HUNTINGTON, 1966, p.1) Já Pedro Silva diz que a guerra é "um ato de violência sistemática e organizada entre duas ou mais unidades políticas,

com o objetivo de atingir objetivos políticos" (SILVA, 2015, p.29). E Cabral Couto define-a como "violência organizada entre grupos políticos, em que o recurso à luta armada constitui, pelo menos, uma possibilidade potencial, visando um determinado fim político" (COUTO, 1988, p.148) (apud SILVA, 2015, p. 28-29).

Elemento comum às várias definições de guerra apresentadas é a existência de uma ação violenta perpetrada pelos seus autores com objetivos políticos. Refere-se ainda que a guerra é levada a cabo por pelo menos duas entidades ou grupos políticos em confronto.

A definição de Cabral Couto (1998) tem a particularidade de destacar a possibilidade de existir guerra sem luta armada, como aconteceu durante a chamada "guerra-fria", em que dois grandes blocos militares, OTAN (ou NATO) e Pacto de Varsóvia, se confrontaram. Referimo-nos ao período que decorreu entre o fim da Segunda Guerra Mundial até à queda, em finais da década de 1980 e princípios da década de 1990, dos regimes de socialismo real na Europa, a que se seguiu a desintegração do Pacto de Varsóvia. Específico da guerra-fria é que foi uma guerra que existiu sem ter sido declarada. Temos aqui uma ideia muito importante: uma guerra pode existir, de forma latente, mesmo sem ter sido formalmente declarada, por razões táticas ou até por impossibilidade jurídica. É o caso típico da ciberguerra, nas sociedades tecnológicas pós-modernas (fundamentalmente os países ocidentais) ou de modernidade tardia (casos da China ou da Índia), no século XXI. Nunca uma guerra cibernética foi formalmente declarada, mas existem guerras cibernéticas. Trata-se de guerras latentes, como referimos há pouco, embora esta afirmação precise de ser clarificada. Assim como a guerra-fria, que não se traduziu no uso da força armada, se apoiava em atos sistemáticos de espionagem e sabotagem de Estados e blocos militares em relação a outros Estados e blocos militares, também a típica guerra cibernética, podendo dispensar o uso da força militar, se apoia em atos de espionagem, sabotagem, destruição, etc. Claro está que pode existir uma diferença não despicienda entre as duas situações, que se prende com o potencial destrutivo associado, que agora é muito maior. Com efeito, com uma ciberguerra pode parar-se ou diminuir-se

significativamente o funcionamento de um Estado ou de uma empresa. Basta pensar nos efeitos decorrentes de se deixar um país sem acesso às fontes energéticas ou de telecomunicações. Podemos mesmo admitir que o uso de palavras ou expressões antigas prejudica o avanço que é necessário efetuar em matéria de regulação dos novos fenômenos de ciberguerra, porque, e para dar apenas um exemplo, um ato de espionagem, por definição, não pode ser regulado, dado que existe sempre à margem do direito. Ou seja: precisamos de inventar palavras para os novos fenômenos sociais e políticos.

Estamos agora em condições de poder definir o conceito de ciberguerra. Ciberguerra ou guerra cibernética é a violência organizada entre grupos políticos de vários tipos (Estados, organizações de Estados, unidades fixas ou móveis especializadas, de natureza estadual ou outra, com níveis de autonomia variáveis), visando fins políticos determinados, em que a confrontação entre os oponentes se faz primordialmente com recurso a meios eletrônicos e informáticos, no chamado ciberespaço, sem excluir a possibilidade de ser complementada com o recurso à força armada.

Como todas as guerras, as ciberguerras visam resolver conflitos políticos, econômicos ou militares no mundo real. O conceito de ciberguerra é usado para designar ataques, represálias ou a intrusão ilícita em computadores ou redes de terceiros. Incluem-se na definição os ataques a todo o tipo de infraestruturas críticas, designadamente as unidades militares e de pesquisa científica avançada, as redes de energia elétrica, de gás e de água, a serviços de transportes e a serviços de saúde e financeiros.

A ciberguerra assumeformas distintas da guerra clássica, sendo ou não um complemento a esta. Pode ocorrer em conflitos de alta intensidade e em conflitos de baixa intensidade com o envolvimento de forças militares, mas também pode operar por si só.

Apesar de o fenômeno ser recorrente e muito relevante nas relações internacionais, é difícil falar em ciberguerra porque o fenômeno não foi ainda regulado pelo Direito Internacional Humanitário ou Direito dos Conflitos Armados.

É discutível se se pode falar de ciberguerra quando em causa estão ataques a empresas privadas ou quando o móbil é apenas privado. Do que dissemos decorre que existem nesta matéria preocupações relativas não apenas à defesa mas também à segurança dos Estados. Com efeito, se no século XXI há ponto claramente assente nos conceitos estratégicos de defesa nacional é que eles cobrem matérias muito mais extensas do que no passado, o que se compreende no mundo global em que vivemos, no qual, por força das novas tecnologias digitais e de locomoção humana, as sociedades atingiram o nível máximo de conexão conhecido. Entre os instrumentos de direito internacional que referimos, está a Convenção de Budapeste de 2001, que, visando a proteção de interesses privados, na verdade, não protege só interesses privados, porque o dever principal dos Estados, e a razão por que existem, é a defesa da segurança das pessoas. Existindo uma continuidade entre as preocupações de defesa e segurança dos Estados, vistos que os valores e interesses em jogo são fundamentalmente os mesmos, comungamos do entendimento de que é apropriado o uso do conceito de ciberguerra relativamente a todas as situações de ataque a infraestruturas relevantes, independentemente de serem públicas ou privadas.

3. Conclusão

A título de conclusão, pretendemos destacar três pontos, que se prendem com o enunciado que dá título ao presente trabalho: "Ciberguerra: uma palavra (mal)dita no século XXI".

Em primeiro lugar, é preciso dizer que, desde que existe humanidade, existem conflitos e existe guerra. Essa é a razão porque também existem a política e o direito. Num mundo sem conflitos, não seria necessário poder de mando, nem regras jurídicas, com a inerente possibilidade de estas, pelo menos teoricamente, serem aplicadas pela força, em caso de incumprimento. Como forma de regular as relações entre indivíduos e entidades com interesses potencialmente conflitantes, criaram-se, ao longo da história humana, constituições, principados, estados, parlamentos, tribunais, forças armadas, etc. Se repararmos, verificamos

que praticamente todas estas entidades têm historicamente intervenção na deflagração das guerras. As constituições definem os termos em que o Estado pode declarar a guerra e por intermédio de quem. As forças armadas fazem a guerra, etc. A verdade é que a realidade muda e exige mudanças ao próprio modo de exercer o poder e dizer o direito. Durante a guerra-fria, que foi uma guerra real, não houve intervenção de forças armadas em campo aberto, assim como não houve declaração de guerra. E, no entanto, as peças do jogo político acompanharam mutuamente os movimentos umas das outras. Fez-se outra guerra. Também agora podemos afirmar que existe um novo tipo de guerra, também não formalmente declarada, mas cujos efeitos são reais, denominada ciberguerra.

Em segundo lugar, há que realçar que mesmo sendo estudada nas instituições de ensino superior e referida pelos meios de comunicação social, a ciberguerra não é ainda compreendida pela maioria das pessoas comuns, que desconhecem os perigos decorrentes deste fenómeno para as suas próprias vidas. Sendo pois referida e sabendo-se que os seus efeitos podem ser catastróficos, não existe uma suficiente explicação do conceito, por parte de quem tem obrigação de fazê-lo. Estamos, por isso, perante um conceito mal dito, mas que precisa de ser bem dito.

Em terceiro lugar, pretendemos destacar a relevância da definição que damos do fenômeno, que, como atualização de definições de guerra anteriormente feitas e que estão corretas, incluem elementos novos: a possibilidade de colaboração efetiva, que a realidade evidencia, entre diferentes tipos de atores, públicos e privados, de um mesmo ou de diferentes países, na efetivação da guerra cibernética; a possibilidade de as ameaças se efetivarem sem recurso à força armada; e, por último, mas não o menos importante, a necessidade de se regular internacionalmente este tipo de conflitos, o que se afigura particularmente difícil no tempo em que escrevemos, dadas as tensões existentes entre Estados, que preferem a não-cooperação à cooperação.

É ainda a guerra cibernética uma invenção humana. Que podemos esperar? "Com mãos se faz a paz se faz a guerra / Com mãos tudo se faz e se desfaz / Com mãos se faz o poema — e são de terra. / Com mãos

se faz a guerra — e são a paz" – escreveu o poeta português Manuel Alegre (ALEGRE, 1979, poema "As mãos"). Mãos que redigem ideias e as transformam em tecnologia poderosa, que pode ter um propósito de construção ou de destruição. Mãos ainda que podem firmar acordos sobre questões essenciais. É esta fundamentalmente uma questão de educação, porque uma coisa é certa: sem o esforço cultural de elevação das pessoas acima dos seus sentimentos e interesses primários, a humanidade corre o sério risco de desaparecer.

Referências Bibliográficas:

ALEGRE, M. **O Canto e as Armas.** Mem Martins: Europa-América, 1979.

CAETANO, J. C. R.Da Democracia na Europa. **Revista Portuguesa de Filosofia.** Publicações da Faculdade de Filosofia, n. 70:4. p.743-764, 2014.

CLAUSEWITZ, C. **Da guerra**. 2.ª ed. Mem Martins: Europa-América, 1997.

COUTO, A. C. **Elementos de Estratégia.** Lisboa: Instituto de Altos Estudos Militares, 1988.

DAMÁSIO, A. **Looking for Spinoza**: Joy, Sorrow, and the Feeling Brain. Harcourt, 2003.

FRANCISCO. Reportagem LUSA. Papa Francisco diz que o "mundo está em guerra". **TSF**. Lisboa, 26 jul. 2016. Disponível em<https://www.tsf.pt/sociedade/interior/papa-francisco-diz-que-o-mundo-esta-em-guerra-5308864.html>. Acesso em 26 de julho de 2016.

LARA, A. S. **Ciência Política**: Estudo da ordem e da subversão. Lisboa: ISCSP, 2005.

LARA, A. S. Apresentação. In: LARA, A. S. (coord.): **Em Caso de Guerra.** Lisboa: Edições MGI, 2015. p. 11-12.

ORTEGA Y GASSET, J.. **A Rebelião das Massas**. São Paulo: Martins Fontes, 1987. [Edição original: ORTEGA Y GASSET, J. **La rebelión de las masas.** Barcelona: Espasa Lobros, 1929].

REVELLI, M. **Post-Sinistra: Cosa resta dellapolitica in un mundo globalizzato.** Roma:EditoriLaterza, 2014.

SILVA, P. **Entre Ceres e Marte.** A segurança e defesa na Europa do séc. XXI. Lisboa: Imprensa Nacional-Casa da Moeda, 2011.

SILVA, P. Sobre a Guerra. In: LARA, A. S. (coord.): **Em Caso de Guerra.** Lisboa: Edições MGI, 2015. p. 27-37.

VERÍSSIMO, P. em entrevista a: LOPES, Francisco. China é acusada de metade dos ciberataques dos últimos 12 anos. **Público.** Lisboa, nov. 2017. Disponível em <https://www.publico.pt/2017/11/28/infografia/teste-teste-teste-200>. Acesso em 30 de novembro de 2017.