Utopia, Liberdade e Soberania no Ciberespaço

José Pedro Teixeira Fernandes

Licenciado em Direito pela Universidade Católica, Mestre em Estudos Europeus, Doutor em Ciência Política e Relações Internacionais pela Universidade do Minho. Auditor do Curso de Defesa Nacional em 2003.

Resumo

Neste artigo são discutidos os desafios que o ciberespaço e o risco de ciberataques acarretam para a soberania do Estado e para a liberdade do cidadão. A utopia libertário-anárquica, que dominou nos primórdios da internet, está progressivamente a dar lugar a mecanismos de controlo e de afirmação da soberania estadual, nomeadamente através da criação de "fronteiras" no ciberespaço. Esta tendência, embora sob formas diferentes, pode detetar-se quer nos Estados autoritários, quer nas democracias liberais ocidentais. Encontra-se também na organização das forças armadas, através da criação de ciber-comandos, e nas OIG ligadas à segurança e defesa como a NATO, onde se passou a incluir ameaça de ciberataques no conceito estratégico.

Abstract
Utopia, Liberty and Sovereignty in Cyberspace

The author discusses the challenges that cyberspace and the risk of cyber attacks bring to statehood sovereignty and the freedom of the citizens. The libertarian-anarchic utopia, which dominated in the early days of the internet, is gradually giving way to mechanisms of control and affirmation of state sovereignty, including the creation of "borders" in cyberspace. This trend, albeit in different ways, can be detected both in authoritarian states and the western liberal democracies. It is also recognizable in the organization of the military by the creation of a cyber command. We also can find it in the IGO related to security and defense like NATO, which includes the threat of cyber attack in the new strategic concept document.

> "Governos do mundo industrial, vós sois uns gigantes enfadonhos de carne e aço, eu venho do ciberespaço, o novo mundo da mente. Em nome do futuro, peço-vos, a vós do passado, que nos deixem sós. Não são bem-vindos entre nós. Não têm soberania onde nos reunimos. Não temos governos eleitos, nem provavelmente iremos ter. Assim, eu dirijo-me a vós sem autoridade maior do que aquela que me dá a liberdade com que sempre falei. Eu declaro o espaço social global que estamos a construir naturalmente independente das tiranias que nos tentam impor. Não têm o direito moral de nos governar, nem têm métodos de coação que tenhamos verdadeira razão para temer."
>
> John Parry Barlow (1996)

Introdução[1]

No seu uso mais rigoroso, o termo "ciberespaço" – originalmente cunhado pelo escritor de ficção científica William Gibson na obra *Neuromancer* de 1984 (Till, 2011) –, designa hoje a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores. Num uso mais livre, a palavra tornou-se também uma designação conveniente para referir algo ligado à internet e às novas práticas sócio-culturais que lhe estão associadas. Pela sua própria natureza complexa e multifacetada, o ciberespaço, no referido sentido mais rigoroso do termo, é suscetível de uma abordagem multidimensional e de ser objeto de investigação a partir de disciplinas muito variadas. Para o seu estudo, convergem, entre outras, a perspetiva tecnológica, sociológica, jurídica, política, estratégica e de segurança. Este pode ser, também, objeto de estudo de forma mais geral, incidindo sobre questões transversais aos diferentes Estados, ou estudado, de forma mais focalizada, em questões específicas ligadas a uma realidade nacional. Neste artigo, a opção foi por uma ênfase numa perspetiva política – incluindo nesta aspetos estratégicos e de segurança –, associada a observações de enquadramento de tipo cultural-sociológico. Para além disso, a análise centra-se em aspetos transversais aos diferentes Estados, não considerando, especificamente, o caso português. Este é, sem dúvida, merecedor de uma análise própria que ultrapassa o âmbito limitado da abordagem que aqui nos propomos efetuar.

1 O autor agradece os comentários e sugestões efetuadas pelo *referee* anónimo, as quais contribuíram para valorizar a versão final do artigo.

Assim, o principal objetivo do artigo que a seguir se apresenta é avaliar em que medida a utopia libertário-anárquica dos primeiros tempos da internet está a dar lugar, a nível internacional, a crescentes mecanismos de afirmação da soberania estadual, nomeadamente à criação de "fronteiras" e de mecanismos de controlo do ciberespaço. O objetivo é também procurar avaliar em que medida a resposta securitária dos Estados ao crescente risco de ciberataques ou de uma ciberguerra, põe em causa a liberdade do cidadão. Para o efeito, são passados em revista casos de Estados autoritários (a China), mas também as tendências de domínio do ciberespaço que se encontram nas democracias liberais ocidentais, incluindo a sua principal organização de segurança e defesa coletiva (a NATO), onde a ameaça de ciber-ataques passou a ser parte integrante do seu último documento estratégico.

A Utopia Libertário-Anárquica[2] do Ciberespaço e os seus Críticos

Talvez nada exemplifique melhor a utopia libertária ou até de anarquia do ciberespaço, que o manifesto da autoria do ex-compositor de letras do grupo *rock* norte-americano, *Grateful Dead*, John Parry Barlow, *A Declaration of the Independence of Cyberspace* (1996). Nesse texto emblemático sustentou que os governos nacionais deveriam manter-se afastados do "novo mundo" acabado de criar. Estes não tinham o direito moral de o governar pelo que se deveriam abster de criar quaisquer imposições legislativas reguladoras do "espaço social global". Ainda segundo este, seria a própria comunidade *online* quem deveria formar o seu "contrato social" (numa alusão à ideia moderna de um contrato social, entre governantes e governados, teorizada por Locke e Rousseau no Iluminismo, a qual legitimaria o exercício do poder pelos governos). Nesta visão utópica, surgiria assim uma "nova civilização", mais humana e mais justa do que as criadas anteriormente, que eram dirigidas pelos governos.

Visto como lugar de realização do ideal libertário-anárquico, o ciberespaço tem, no supra citado manifesto de John Parry Barlow, uma proclamação imbuída de uma lógica "contracultural", no sentido que era dado à palavra nos anos 60 do século passado. Mas há outros protagonistas emblemáticos destes ideais, que adquiriram até maior notoriedade junto do grande público. No passado recente, embora por razões bastante diferentes, destaca-se o caso de Julian Assange, o principal criador do WikiLeaks (Leigh e Harding, 2011). Na ótica dos que se revêm

2 O título deste ponto (e do artigo) é livremente inspirado no livro de Nozick (1977) originalmente publicado em 1974.

nos ideais libertário-anárquicos este representa, provavelmente, não só um ativista carismático em prol de causas justas, como uma espécie de "mártir da transparência informativa", ou Némesis do secretismo, pela perseguição que os governos estaduais – sobretudo o dos EUA –, lhe têm movido.

Importa notar que a utopia libertário-anárquica do ciberespaço não gerou apenas uma onda de simpatia e a adesão entusiástica, difundindo-se através de "evangelizadores" carismáticos como Barlow ou Assange um pouco por todo o mundo. Como é normal nos fenómenos culturais e/ou políticos novos, deu origem, também, a dissidências e a algumas vozes críticas bastante cáusticas. Estas evidenciam os aspetos potencialmente negativos da revolução digital em curso. Neste contexto destaca-se Andrew Keen[3], um "evangelizador dissidente" da revolução digital que, de alguma maneira, condensa os principais argumentos dos críticos. Quais são, então, esses argumentos? Um primeiro é dirigido contra a própria utopia libertário-anárquica subjacente à internet, em especial à chamada Web 2.0., considerada como uma nova e perversa versão das clássicas utopias políticas dos séculos XIX e XX:

> "Desde a revolução francesa e russa até às revoltas contraculturais dos anos 60 e à revolução digital dos anos 90, temos sido seduzidos, repetidas vezes e texto após texto, pela visão de uma utopia política ou económica. Em vez de Paris, Moscovo, ou Berkeley, o grande movimento utópico na nossa época contemporânea situa-se em Silicon Valley, cuja grande sedução é verdadeiramente a fusão de dois movimentos históricos: o utopismo contracultural dos anos 60 e o utopismo técnico-económico dos anos 90. Aqui em Silicon Valley, esta sedução anunciou-se a si própria ao mundo como o movimento 'Web 2.0'."(Keen, 2006: 1).

Um segundo argumento crítico relaciona-se com o novo jargão associado à Web 2.0, que este considera ser uma linguagem absurda, herdada da contracultura *hippie* dos anos 60/70, agora embelezada e sofisticada numa fraseologia de tipo sociológico:

> "Termos de moda da antiga era dot.com – como *cool*, *eyeballs*, ou *burn-rate* – foram substituídos na Web 2.0 por uma linguagem que é, simultaneamente, ainda mais militante e absurda: conferir aos *media* dos cidadãos, democratizar radicalmente, esmagar o elitismo, redistribuição de conteúdos, comunidade autêntica… Este jargão sociológico, no passado uma preservação da contracultura *hippie*, é agora o léxico do novo capitalismo dos *media*." (Keen, 2006: 1).

3 Andrew Keen é um britânico ligado à nova economia que tem desenvolvido a sua atividade em Silicon Valley, na Califórnia, EUA.

Desenvolvendo as suas críticas, Keen argumenta que, em termos ideológicos, estamos perante uma fusão entre "o radicalismo dos anos 60 com a escatologia utópica da tecnologia digital". O resultado, ao contrário do que muitos supõem, poderá ser bastante negativo para a generalidade da sociedade. Isto porque a Web 2.0 está a abrir caminho àquilo que este chamou "o culto do amador"[4]. Desta forma estar-se-á a destruir o que usualmente se designa por "alta cultura"[5], bem como o conhecimento especializado, nas mais diversas áreas do saber. Este necessita de anos de formação e treino, não sendo compatível com a lógica "amadora" da Web 2.0. Keen (*ibidem*: 1) faz ainda uma curiosa comparação entre a atual utopia libertário-anárquica do ciberespaço e a bem conhecida utopia marxista da sociedade radicalmente igualitária, que marcou grande parte da luta política desde a segunda metade do XIX até finais do século passado:

> "Tal como Marx seduziu uma geração de idealistas europeus com a sua fantasia da autorrealização da utopia comunista, também o culto da autorrealização criativa da Web 2.0 seduziu toda a gente em Silicon Valley. O movimento faz a ponte entre os radicais da contracultura dos anos 60, como Steve Jobs, com a cultura contemporânea *nerd* do Google de Larry Page. Entre os extremos de Jobs e Page encontra-se o resto de Silicon Valley, incluindo comunitaristas radicais como Craig Newmark (da *Craigslist.com*), comunistas da propriedade intelectual como o professor de Direito da Universidade de Stanford, Larry Lessig, cornucopianos económicos como o editor da revista *Wired*, Chris "*Long Tail*" Anderson e novos mogóis dos *media* como Tim O'Reilly e John Batelle."

Ao contrário de distopias literárias bem conhecidas, como o *1984* de George Orwell, ou *Admirável Mundo Novo* de Aldous Huxley, onde a tecnologia permitia controlar a informação e a mente (era o caso do *Big Brother* no livro *1984*), o problema com a Web 2.0 poderá ser, paradoxalmente, o inverso. Keen configura um hipotético cenário de pesadelo provocado por uma superabundância de autores e de "informação". A consequência bizarra e extrema dessa hipotética ocorrência seria que, sendo todos autores, a audiência tenderia a desaparecer,

4 Estamos a referir-nos ao livro *The Cult of the Amateur: How Today's Internet Is Killing our Culture*, que Andrew Keen publicou no ano seguinte (2007).

5 A designação "alta cultura" refere-se normalmente a um conjunto de realizações culturais essencialmente no domínio das artes (arquitetura, pintura, escultura, música, literatura, etc.) tendencialmente consideradas os expoentes máximos de uma sociedade, de uma época histórica, de uma nação, ou até da própria humanidade. Supõe, implicitamente, a existência de realizações culturais mais elevadas do que outras, ou seja, a expressão só faz sentido por contraponto ao que não é "alta cultura". A conceção "elitista" que lhe está subjacente conflitua com a lógica pós-moderna do nivelamento dos saberes e com a ideia que "todas as culturas têm igual valor", difundida, sobretudo, pela via da antropologia cultural.

tornando-se o ato de não escrever, paradoxalmente, numa forma de rebelião quase kafkiana.[6]

O Controlo na Rede: a (im)Possível Realização da Distopia Orweliana?[7]

Em face das críticas anteriormente formuladas uma dúvida surge inevitavelmente: será plausível que a utopia libertário-anárquica da internet possa dar origem a uma espécie de distopia Orweliana? Será tal possibilidade um mero exagero especulativo, até por ser, em termos técnicos e políticos, algo inviável? Analisemos a questão nessa dupla faceta. Quando se fala de controlo e vigilância através da tecnologia, vem quase inevitavelmente ao pensamento a imagem do já referido sistema monstruoso imaginado por George Orwell. Neste, a liberdade e a privacidade do indivíduo eram completamente esmagadas e submetidas aos desígnios de um poder totalitário, que atuava como dono do corpo e da mente dos cidadãos. Quando este foi escrito, estávamos em 1948, numa era pré-internet, anterior à revolução digital das últimas décadas do século XX. Será que a evolução tecnológica posterior contribuiu para afastar o espectro do *big brother is watching you*, na famosa frase do *1984*? Ou, pelo contrário, a internet e a revolução digital potenciam (ainda) mais a implementação de mecanismos orwelianos de vigilância do cidadão? Conhecemos já a resposta de John Parry Barlow, secundada por outros, como por exemplo, Louis Rosseto, fundador da revista *Wired*, e a visão libertário-anárquica que lhes está subjacente. Estes encararam a internet e a Web como um promissor espaço de realização da utopia libertária, vendo a possibilidade de emergir no ciberespaço um "homem novo" e uma "civilização nova" à margem da "tirania" dos governos. Por outras palavras, algo à margem dos mecanismos tradicionais de poder e controlo do Estado.

Sejam quais tiverem sido as intenções dos criadores da internet – e, na grande maioria dos casos, estavam, de facto, próximas de ideais libertário-anárquicos que impregnavam a contracultura dos anos 60[8] –, quando olhamos para a evolução posterior deparamo-nos com uma imagem bastante mitigada. É inquestionável

6 *"In the Web 2.0 world, however, the nightmare is not the scarcity, but the over-abundance of authors. Since everyone will use digital media to express themselves, the only decisive act will be to not mark the paper. Not writing as rebellion sounds bizarre – like a piece of fiction authored by Franz Kafka. But one of the unintended consequences of the Web 2.0 future may well be that everyone is an author, while there is no longer any audience."* Keen (1996: 1-2).

7 Sobre a liberdade na internet e nos *media* digitais ver o relatório editado por Kelly e Cook (2011).

8 Sobre este assunto ver Turner (2006).

que o ciberespaço trouxe, de uma ou de outra forma, um espaço de liberdade, com alguns traços de anarquia à mistura. Na sua faceta mais benéfica, permite a expressão individual de gostos e preferências, facilita a troca de ideias, propicia o ativismo social e político. Esta é uma faceta facilmente observável, pelo menos nos Estados que se pautam por valores democráticos e admitem o pluralismo político e social. Todavia, em paralelo, existe também aquilo que pode ser designado como um "lado negro". Sob a capa do anonimato – por princípio possível nas sociedades democráticas –, o uso da internet tende a libertar também algumas das piores facetas do ser humano[9]. Para além disso, a própria difusão da internet e a digitalização da economia geram novas dependências, vulnerabilidades e riscos: o mais óbvio é o da possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de uma ciberguerra[10] envolvendo, direta ou indiretamente, atores estaduais (casos, por exemplo, da Estónia em 2007 e da Geórgia em 2008, envolvidas em conflitos com a Rússia)[11].

Neste contexto, importa notar que a possibilidade de aceder, sob anonimato, à rede, não é propriamente uma inevitabilidade ou fatalidade tecnológica, mas uma opção política e legislativa. Pelo contrário, utilizar a internet significa, quase sempre, deixar um "rasto", deixar uma "pegada" eletrónica. Esta pode ser usada comercialmente para detetar os gostos e preferências dos utilizadores por coisas mais ou menos inócuas como vestuário, comida ou vinhos; mas também por coisas que podem eventualmente já não ser tão inócuas como livros ou filmes dependendo, obviamente, do tipo de livros e filmes em questão; bem como outras, já muito menos inócuas, como gostos ou orientações sexuais, ou até nada inócuas como preferências político-ideológicas e causas sociais e políticas. Paradoxalmente, torna-se hoje mais fácil, e a custo mais baixo, fazer esse rastreio na internet do que no mundo real. Naturalmente que isto confere uma oportunidade de uso interessante, quer para as empresas, quer para os governos, sejam quais forem as intenções últimas desse rastreio.

9 O comentário insultuoso, a acusação gratuita e sem quaisquer provas, a opinião sem um conhecimento razoável, o rumor, a intriga, o plágio, a escrita de má qualidade, etc. ganharam igualmente um novo "espaço de liberdade" e de difusão.

10 No seu uso mais comum e livre, ciberguerra designa, vagamente, algum tipo de "ataque" ou "represália", intrusão ilícita numa rede e/ou computador ou uma situação de espionagem que ocorre usando meios informáticos. Tais situações poderão surgir, ou não, ligadas a conflitos políticos e/ou militares no mundo "real", ou seja, ocorrer em paralelo com uma conflitualidade "física" ou de forma totalmente autónoma (nesta última hipótese estaríamos perante uma ciberguerra "pura"). Por outro lado, poderão ter origem diretamente em Estados, ou, então, ser protagonizadas por atores não estaduais.

11 Sobre este assunto ver Klimburg (2011: 41-60).

O Caso da "Grande *Firewall* da China"

Em termos de seguir o "rasto" ou procurar a "pegada" eletrónica deixada pelos seus cidadãos o caso que, individualmente, mais chama à atenção é o da China, até pelo crescente impacto que o país está a ter na economia e na política mundial. Um curioso artigo de Oliver August (2007), publicado na revista *Wired*, retrata o *golden shield*/escudo dourado (também conhecido como *great firewall of China*/grande *firewall*[12] da China, num jogo de palavras com a grande muralha da China), que o país tem implementado internamente para vigiar o uso da internet. O seu objetivo é monitorar, filtrar e/ou bloquear conteúdos considerados sensíveis pelas autoridades chinesas. O sistema assenta num banco gigante de computadores e servidores a partir do qual se procura vigiar o tráfico gerado pelos 384 milhões de utilizadores[13] chineses da internet. Comentando a abordagem chinesa à revolução digital e os seus esforços de controlo e de vigilância na rede, Jack Goldsmith e Tim Wu (2006: 90), fazem notar que a visão típica da internet no Ocidente, como "espaço de liberdade", é apenas uma possibilidade, ou seja, é uma escolha social e política e não uma inevitabilidade que decorre da tecnologia[14]. Sobre a maneira como o sistema do *golden shield* foi posto em prática na China, estes mostram também o paradoxo de ter sido feito com a tecnologia de empresas norte-americanas – as quais, em teoria, se identificam com a democracia liberal e pluralista e atuam em respeito pelos seus valores:

> "A barreira de informação da China foi fundamentalmente construída pela Cisco, e empresa fornecedora de redes de Silicon Valley. No início dos anos 90, a Cisco e outras empresas desenvolveram produtos para deixar as empresas americanas filtrarem o acesso dos seus empregados à internet. As empresas queriam a internet, mas não queriam os seus empregados no ESPN ou na playboy.com, todo o dia. A Cisco demostrou há muito tempo às autoridades chinesas como os mesmos produtos poderiam ser usados para bloquear, de forma eficiente, materiais de entrarem na China. Mostrou como isso poderia ser feito de forma flexível, subtil e sem perda de *performance*. Por isso, a moderna "grande muralha China" é, com efeito, construída com tijolos americanos." (Goldsmith e Wu, 2006: 93)

12 Literalmente "parede corta-fogo".

13 Ver Internet World Stats (s.d.).

14 *"China is not only an extreme example of control; it is also an extreme example of how and why the internet is becoming bordered by geography. Only time will tell whether the China strategy will work, or whether the sheer volume of information will erode the government's influence and render the internet in China open and free. But so far, China is showing the opposite: that the internet enjoyed in the West is a choice – not fate, not destiny, and not natural law."* Goldsmith e Wu (1996: 90).

Para além disso, estes chamam também a atenção para o facto de o sistema de vigilância da internet da China não só ser subtil e sofisticado, como bastante mais eficaz do que se poderia pensar à primeira vista (*ibidem*: 94):

> "A censura chinesa é não só eficiente como também subtil. Não aparece nenhum écran a dizer "bloqueado pelo Estado Chinês." Em vez disso, o bloqueio assume a aparência de um erro técnico. Um utilizador que tente, por exemplo, aceder a free-china.net, encontrará um ecrã a dizer "*site* não encontrado", um écran de tempo de acesso de rede esgotado, ou um dos muitos códigos HTTP de erro. E pode ser difícil para um utilizador final (e investigadores) saber se o problema é de facto censura ou dificuldades técnicas. A lista mandatada de *sites* bloqueados muda à medida da evolução dos acontecimentos. Por exemplo, por vezes o *website* do *New York Times* está acessível nos computadores da China, outras vezes não está**.** Esta incerteza, ligada à falta de fiabilidade geral da internet, ajuda a mascarar os esforços de censura."

Quer dizer, o caso da China mostra claramente que a ideia da internet como espaço de (não) liberdade é, na sua essência, uma opção social e política e não uma "fatalidade" tecnológica. Não existe qualquer inevitabilidade de liberdade que decorra da própria tecnologia por esta utilizada. A consequência inevitável é que diversos cenários sobre a sua evolução futura, entre os quais o da perda de liberdade, estão necessariamente em aberto.

Rumo a uma Era de "Afirmação Vestefaliana" no Ciberespaço?

Uma das questões mais importantes sobre o futuro da internet é a de saber se os Estados vestefalianos irão afirmar, crescentemente, a sua soberania sobre o ciberespaço, ou se este se manterá um feudo libertário-anárquico, à margem poder do Leviatã[15] (Estado), como imaginaram muitos dos pioneiros. Será o referido caso da "grande *firewall* da China" a exceção constituída por um grande Estado

15 Referimo-nos, naturalmente, à obra de Thomas Hobbes, *Leviatã* (1651), cujo título evoca um monstro da mitologia da Antiguidade, dotado de uma força sobre-humana. Esta foi a metáfora usada por este pensador político britânico no século XVII para justificar a necessidade do poder do Estado. De facto, Hobbes via no estado de natureza não só um estado de máxima liberdade dos indivíduos, como também um estado de máxima insegurança e conflito. A nota dominante que o caracterizava era anarquia marcada pela "guerra de todos contra todos" (*bellum omnium contra omnes*). Por isso, Hobbes considerou que seria do interesse da generalidade dos indivíduos formar uma sociedade e aceitar uma espécie de "contrato social". Só através deste processo se poderia obter uma pacificação social e a segurança contra os inimigos internos e externos. Assim se justificava não só a existência do Leviatã (o Estado soberano) como, no contexto da época, o exercício de um poder tendencialmente absoluto.

capitalista autoritário[16]? Será antes revelador de uma tendência mais geral, de afirmação crescente do poder estadual, a qual ultrapassa a lógica do autoritarismo político? Em resposta a esta questão, Chris Demchak e Peter Dombrowski em *Rise of Cybered Westphalian Age* (2011), sustentam que está em marcha um processo de afirmação do poder dos Estados sobre o ciberespaço. Estes antecipam mesmo uma nova era de "afirmação vestefaliana" vista, em termos valorativos, como uma tendência necessária e desejável. Na sua ótica (2011: 32), estamos já hoje a assistir ao "início de um processo de criação de fronteiras". Este processo tem múltiplas facetas que vão desde "a tentativa chinesa de criar a sua própria internet, interna e controlada, até ao aumento dos filtros e das regras da internet nas democracias ocidentais". Isto denota uma tendência de os Estados estabelecerem "os limites do seu controlo soberano no mundo virtual, em nome da segurança e da sustentabilidade económica".

Demchak e Dombrowski consideram que o processo histórico que levou à afirmação do Estado soberano encerra uma analogia útil para se perceber a atual tendência de afirmação do poder de soberania sobre o ciberespaço. Assim, importa aqui recordar o conceito histórico de soberania, originalmente teorizado pelo francês Jean Bodin em finais do século XVI, numa obra intitulada *Les Six Livres de la République* (Bodin, 1993). A soberania foi apresentada como um poder, ou seja, a faculdade de impor aos outros um comando a que estes devem obediência. Tal poder revestia o caráter de um poder perpétuo, ou seja, sem limites de natureza temporal, dando substância ao princípio da continuidade do Estado que permanece para além das eventuais mudanças de regime político, ou de governo. Este poder era também absoluto, não estando a soberania sujeita a quaisquer condições ou limitações impostas por outrem. Quer dizer, o detentor da soberania não estava sujeito a instruções de ninguém nem era responsável perante nenhum outro poder[17].

Em termos de características, esta foi apresentada como sendo indivisível (de forma claramente contrastiva com a fragmentação política medieval); como sendo própria e não delegada (na conceção original de Bodin esse poder próprio não pertencia ao povo ou à nação – formulação que só apareceu mais à frente, no séc. XVIII –, mas ao monarca e não estava dependente nem de um processo eletivo nem de nomeação pelo Papa ou Imperador); como sendo irrevogável (nem o Papa, nem o Imperador, nem o povo ou nação poderiam retirar ao soberano esse poder político máximo). Além de tudo isto, a soberania era vista também como sendo suprema na ordem interna, quer dizer, representando um poder que

16 Ver o artigo do académico israelita Azar Gat (2007).

17 Na conceção original de Jean Bodin o poder de soberania pertencia ao monarca por direito próprio. Para mais desenvolvimentos sobre o pensamento político de Jean Bodin, ver Amaral (1998).

não podia admitir outra igual com o qual tivesse de partilhar a autoridade do Estado. Por sua vez, no plano internacional, era caracterizada como sendo uma expressão de plena independência, só lidando o Estado soberano com outros poderes iguais (no contexto da época, o Estado soberano só estaria vinculado pelas normas de Direito Internacional Público resultantes de tratados livremente celebrados com outros poderes soberanos iguais, ou de costumes internacionais voluntariamente aceites).

Obviamente que o conceito de soberania evoluiu bastante desde a teorização de Jean Bodin. Hoje, por um conjunto diversificado de razões – regime dos Direitos Humanos, organizações de integração económica e política para as quais são transferidas competências soberanas, etc. –, tende a ser entendido de forma bastante mais matizada e limitada. Em *Sovereignty: Organized Hypocrisy*, Stephen Krasner (1999) dá-nos uma panorâmica da sua evolução até ao mundo político contemporâneo. A análise foi efetuada numa perspetiva abrangente (histórica, política e jurídica) e colocou em evidência as múltiplas aceções em que este pode ser encarado (soberania interna, soberania interdependente, soberania legal internacional e soberania vestefaliana).

Quadro 1 – As Aceções do Conceito de Soberania segundo Stephen Krasner

Soberania interna	Soberania interdependente	Soberania legal internacional	Soberania vestefaliana
Organização da autoridade pública no seio de um Estado ligada ao controlo efetivo exercido pelos que detêm a autoridade	Capacidade de as autoridades públicas controlarem os movimentos transfronteiriços (de pessoas, bens, ideias, doenças, poluentes, etc.)	Estabelecimento do *status* de uma entidade política no sistema internacional através do reconhecimento mútuo dos Estados (regulação das relações interestaduais baseada no princípio da igualdade jurídica)	Exclusão dos atores externos da configuração e do exercício da autoridade interna (princípio da não ingerência externa nos assuntos internos dos Estados)

Fonte: José Pedro Teixeira Fernandes (2009: 103).

Krasner desmistificou também algumas ideias bastante em voga, não só no discurso mediático como na própria academia. Estas surgiram ligadas ao entusiasmo à volta da globalização, típico dos primeiros anos da última década do século passado, sugerindo, pelo menos até à crise financeira iniciada em 2007/2008, que estaríamos perante uma progressiva e inexorável perda de poder do Estado

soberano[18]. Naturalmente que há fenómenos contemporâneos que colocam sob tensão a ideia clássica da soberania do Estado, os quais não existiam na época em que Bodin teorizou. É inquestionável que estes desafiam, sob diversos moldes, o poder estadual soberano. Inserem-se aqui as já referidas convenções internacionais sobre os Direitos Humanos, o Direito Internacional Humanitário, a integração económica e política regional nas suas diferentes formas, e a incontornável globalização. Todavia, o estudo de Krasner acaba por evidenciar também uma certa fragilidade existente na argumentação da "inexorável" perda de poder do Estado soberano. Em parte esta baseia-se no pressuposto de que, em termos histórico-políticos, teria existido até à atual globalização uma espécie de "idade de ouro" das soberanias. Durante essa "época dourada", a soberania estadual teria sido respeitada pela generalidade dos atores estaduais (e não estaduais) e não teria enfrentado constrangimentos de relevo. A verdade é que essa ideia não tem uma base histórico-política sólida – apenas tem alguma consistência para as grandes potências. Não é difícil no período posterior aos Tratados de Vestefália de 1648 encontrarmos exemplos de "atropelos" à soberania estadual, por vias coercivas e de imposições – daí a "hipocrisia organizada" de que fala Krasner. Para além disso, não parece ser também este o destino do Estado vestefaliano no mundo pós-11 de setembro de 2001, e, sobretudo, pós crise financeira de 2008. Pelo contrário, o que se deteta é uma tendência geral para uma (re)afirmação do poder soberano, sendo provavelmente o ciberespaço, que nos ocupa nesta análise, uma nova frente dessa (re)afirmação de poder.

18 Ideia ventilada, por exemplo, no livro de Ohmae (1996).

Quadro 2 – Os Desvios à Soberania Legal Internacional e à Soberania Vestefaliana

Convenções (desvio voluntário)	Contratos (desvio voluntário)	Coerção (desvio involuntário)	Imposição (desvio involuntário)
Acordos através dos quais os Estados se comprometem a seguir determinadas práticas que envolvem relações entre governantes e governados no interior das fronteiras estaduais; permitem a atores externos exercer alguma influência interna (por ex.: a Declaração Universal dos Direitos do Homem, de 1948 e a Convenção Europeia dos Direitos do Homem, que entrou em vigor em 1953)	São atos negociados entre dois ou mais Estados, ou entre um Estado e uma organização internacional (por ex. um empréstimo do FMI), revestindo nos casos mais importantes normalmente a forma de tratados internacionais (por ex. o Tratado de Utrecht de 1713, no qual a França cedeu a Arcádia e a Baía de Hudson à Grã-Bretanha)	Ocorre quando um Estado (ou Estados) ameaçam impor sanções a outro Estado, a menos que o coagido aceite limitar a sua autonomia interna e praticar o ato pretendido (ou abster-se de uma determinada conduta); para ter credibilidade e eficácia pressupõe uma assimetria de poder entre as partes envolvidas. Os casos mais claros de coerção envolvem a ameaça de sanções económicas, ou sua efetiva aplicação (ex.: as sanções impostas pelos EUA a Cuba, na sequência da ascensão de Fidel Castro ao poder, em 1959; as sanções autorizadas pela ONU à África do Sul, para pôr fim ao *apartheid*, entre 1962-1994)	Tem sido empregue em casos associados aos direitos das minorias, aos empréstimos a Estados soberanos e às estruturas institucionais dos Estados mais fracos (a ação norte-americana em 1989, em território do Panamá, que levou à detenção do general Noriega, presidente da república, e ao seu envio para os EUA onde foi julgado e condenado por narcotráfico; a ação da NATO na província Sérvia do Kosovo, em 1999, para proteger a minoria albanesa)

Fonte: José Pedro Teixeira Fernandes (2009: 104)

Voltando à análise de Demchak e Dombrowski, em termos histórico-diplomáticos estes referem-se aos já mencionados Tratados de Münster e Osnabrücke (conhecidos como a Paz de Vestefália), celebrados em 1648 e que colocaram fim à Guerra dos Trinta Anos na Europa. Esses Tratados constituem o marco simbólico da progressiva afirmação da soberania territorial, a qual decorreu ao longo dos séculos subsequentes. Esta tem uma expressão visível na delimitação precisa e cartográfica das fronteiras[19] estaduais. Note-se que a pacificação das zonas limite entre diferentes comunidades políticas, bem como a segurança das respetivas populações, favoreceu a aceitação deste processo e a afirmação da soberania territorial nos moldes previstos nos Tratados de Paz de Vestefália. Para Demchak e Dombrowski (*idem*: 40), os desafios de segurança do mundo de hoje voltam a colocar similares circunstâncias, agora num terreno novo que é o ciberespaço. Assim, estes consideram que "uma ciberfronteira nacional é tecnologicamente possível, psicologicamente confortável, sendo também sistematicamente e politicamente gerível". Em reforço deste argumento, afirmam que "técnicos excecionalmente dotados discutem a necessidade de separação de sistemas críticos para os proteger de predadores da internet e atores hostis". Como resultado, mesmo se os políticos estão normalmente "inclinados a manter uma internet totalmente aberta, terão poucos argumentos técnicos para usar" na sustentação dessa posição.

Mas há outros argumentos relevantes a favor da instituição de fronteiras nacionais no ciberespaço. Desde logo, estes fazem notar que, ao contrário das teses de alguns "evangelizadores" dos primórdios da internet, não estamos perante uma realidade física que funcione fora da vontade humana, tipo força da gravidade – algo que já tivemos oportunidade de demonstrar quando assinalamos que não há qualquer inevitabilidade que torne automaticamente a tecnologia numa área de liberdade. Por outro lado, chamam ainda a atenção para uma distinção particularmente importante. Em Estados democráticos, a ênfase relevante em matéria de afirmação da soberania estadual é colocada nas "fronteiras". Ou seja, o que está em causa não é um "controlo" generalizado dos fluxos eletrónicos que ocorrem dentro do próprio Estado (a verificar-se algo deste tipo estaríamos a abrir a porta a formas de vigilância e controlo autoritárias) mas, por razões de segurança externa, afirmar "fronteiras" da comunidade política (*ibidem*: 40):

> "(...) as fronteiras físicas são conhecidas, aceites e desejadas pelos cidadãos nas modernas sociedades civis e esse conforto psicológico não será diferente na criação de fronteiras no ciberespaço. A ênfase relevante é nas "fronteiras", não no controlo universal de todos os fluxos na rede ocorrendo inteiramente dentro das fronteiras de um Estado-Nação democrático. Historicamente, os cidadãos aceitaram as fron-

19 Para uma visão histórica e geopolítica do problema das fronteiras estaduais ver Foucher (1991).

> teiras como uma necessidade de reforço da segurança contra incertezas externas que pusessem em causa regras aceites internamente de interação. Sem tais limites, o sentido coletivo de pertença é mais facilmente subvertido tal como as regras de comportamento civil."

Um terceiro argumento por estes avançado, é o de que as "fronteiras cabem na arquitetura existente de gestão dos sistemas nacionais". A maioria dos Estados faz uma distinção entre forças que defendem as fronteiras de um ataque externo (militares) e aquelas que protegem cidadãos individuais de um ataque interno, normalmente com origem criminosa (polícia). Esta distinção, que historicamente "é um dos resultados diretos da ascensão do Estado moderno após a Paz de Vestefália", tem sido "severamente posta em causa pelo caráter irrestrito da atual tipologia do ciberespaço". Entre outros problemas, confunde a separação entre a esfera interna e esfera externa da segurança. Para Demchak e Dombrowski (*ibidem*: 43), uma evolução para "fronteiras virtuais" no ciberespaço contribuiria positivamente para clarificar esta questão. Em defesa da sua posição, apontam o recente caso do vírus *Stuxnet* que afetou as instalações nucleares iranianas:

> "(...) Sem a legitimação e a clareza burocrática de uma fronteira virtual, por exemplo, disputas jurisdicionais entre nações, que respeitaram séculos de diferenciação entre crime e segurança nacional, as leis da sociedade civil ficam paralisadas na resposta. O vírus Stuxnet facilmente atravessou as fronteiras conforme pretendido por aqueles que o criaram. Se foi um ator não estadual, então a ação é criminal, invocando o poder das forças policiais. Se foi um ator de nível estadual, então os militares deverão atuar. Hoje, não é claro que grupos estiveram envolvidos, em grande parte porque o rasto eletrónico de possíveis atribuições move-se rapidamente através dos Estados. Estes não têm obrigação de sancionar um mau comportamento emanando de fora do seu território."

Estas zonas cinzentas e vazios podem trazer oportunidades a explorar por atores estaduais e não estaduais. Todavia, a verdade é que muitos Estados começam a ver esta "incerteza e a dificuldade em estabelecer a culpa e atribuir a responsabilidade do ataque como vulnerabilidades inaceitáveis". Como sublinham Demchak e Dombrowski, "em princípio, apenas de territórios não governados ou ingovernáveis podem grupos modernos lançar mísseis destrutivos, sem um apelo interestadual automático para sanções. Com fronteiras físicas, os Estados que querem ser aceites internacionalmente estão obrigados por lei e costume a parar o comportamento atacante dos seus residentes ou a permitir ao Estado ofendido atuar no seu interior para fazê-lo parar. Uma vez que os limites virtuais do poder soberano possam ser demarcados no ciberespaço global, os Estados que ignorem ou apoiem ataques massivos de negação de serviço a partir dos seus territórios serão inter-

nacionalmente responsáveis" (*ibidem*: 44). Mas a afirmação da soberania estadual, através de fronteiras virtuais no ciberespaço global, tem ainda outra vantagem que consiste em identificar "maus territórios não governados", ou seja, o equivalente a regiões físicas de Estados falhados ou em vias de se transformarem em tal.

Como estão a surgir e em que Estados se pode observar a implementação de fronteiras nacionais no ciberespaço? Desde logo, há a referir o já mencionado caso da China, que lidera a abordagem, mas numa lógica de Estado autoritário. Quer dizer, a sua atuação não se restringe a uma afirmação de soberania nas suas fronteiras externas do ciberespaço, mas prossegue, paralelamente, um controlo generalizado dos fluxos eletrónicos com origem nos seus próprios cidadãos. Ainda na década de 90, o Partido Comunista Chinês "declarou a internet como sendo uma quinta área de territorialidade" a ser objeto de segurança nacional. Para além disso, nos últimos anos a China tem estado a trabalhar na sua própria internet – no que é designada por "Internet da Próxima Geração Chinesa – onde o "limitado número de endereços da internet se expande enormemente (IPv6), fornecendo a cada computador ligado à internet o seu único endereço Web". Como fazem notar Demchak e Dombrowski (*ibidem*: 45), este novo sistema de endereços é mais "amigo da vigilância" permitindo ao governo chinês, ou a qualquer outro governo que o deseje, efetuar um controlo das suas fronteiras, sem ter de usar agentes ou recorrer a outras entidades".

Fora do contexto de Estados autoritários, encontramos diferentes formas de afirmação da soberania nacional sobre o ciberespaço. Uma das mais usadas no contexto das democracias liberais é o modelo da "empresa-chave". Este modelo impõe algumas obrigações legais às maiores empresas de telecomunicações, com o intuito de diminuir atividades maliciosas ou fraudulentas na rede. Encontra-se, por exemplo, na Austrália, e, em certa medida, também na Alemanha. Outro modelo – representado pela abordagem do Reino Unido –, assenta numa atuação coordenada de diversas agências governamentais em áreas económicas e sociais, com o objetivo de encorajar, monitorar e guiar as transações internas na internet. Há também outras abordagens com um enfoque mais securitário e que têm surgido nestes últimos anos em vários países. Por exemplo, em 2008, no contexto da aprovação de medidas antiterrorismo, a Suécia adotou uma legislação que permite aos serviços de informações da polícia nacional "monitorar todo o tráfico para dentro e para fora do país, tendo origem, ou não, em cidadãos suecos" (*ibidem*: 47).

O Ciberespaço na Organização Militar e no Conceito Estratégico da NATO

A tendência para a afirmação da soberania nacional no ciberespaço está também a ter implicações a outro nível. As forças armadas e de segurança nacionais – uma das expressões inquestionáveis da soberania do Estado –, estão a tentar

adaptar-se aos desafios do ciberespaço e aos riscos de uma eventual ciberguerra. Neste contexto assiste-se, sobretudo entre as principais potências mundiais e regionais, a uma tendência para instituir um cibercomando[20] no âmbito das suas forças armadas ou de segurança interna. A opção pela sua institucionalização no âmbito das forças armadas converte-o no "marcador singular mais óbvio de uma fronteira emergente". Trata-se de criar uma organização de tipo militar destinada "a proteger a nação de danos que, historicamente, só outro Estado, ou vizinho, poderia infligir". Por sua vez, o ato de "estabelecer tal unidade e publicamente declarar tê-lo feito" significa afirmar explicitamente que "existe um território a defender" e que a ameaça de ciberataques pode ser vista como uma "ameaça existencial". No plano simbólico, o estabelecimento de um cibercomando marca também o reconhecimento "de um espaço detido nacionalmente que a nação valoriza e vai proteger usando os recursos apropriados disponíveis". O facto de as "fronteiras não terem ainda sido reconhecidas por outros Estados – um resultado-chave do longo processo vestefaliano –, não diminui o significado desta declaração institucional de soberania a ser defendida, por inerência, no próprio ciberespaço." A afirmação do ex-primeiro ministro britânico, Gordon Brown de que "no século XIX tivemos de tornar seguros os mares para a nossa própria segurança e prosperidade nacional, no século XX tivemos de tornar seguro o ar, e no século XXI temos de tornar segura a nossa posição no ciberespaço de forma a dar às pessoas e aos negócios a confiança que estes necessitam para aí operar", é, provavelmente, a que melhor capta a tendência que descrevemos (*ibidem*: 47-48).

Uma outra área onde a crescente perceção da possibilidade de ciberconflitos ou de uma ciberguerra está a ter repercussões é a dos documentos estratégicos de segurança e defesa, quer nacionais, quer de OIG vocacionadas para essas tarefas. Pela sua importância, merece aqui uma referência especial o caso da NATO[21], que continua a ter na segurança (militar) dos seus membros o seu objetivo último. De facto, a garantia de assistência mútua entre os Estados signatários, em caso de agressão externa, consagrada pelo artigo 5.º do Tratado de Washington, o texto fundador da organização em 1949, mantém-se como elemento-chave. Nesse artigo afirma-se que "um ataque armado contra uma ou mais partes do Tratado, na Euro-

20 Ver "Meet USCybercom: Why the US is fielding a cyber army" em BBC News. Acessível em http://news.bbc.co.uk/2/hi/technology/8511711.stm (15/3/2010). Ver também U.S. Department of Defence/United States Cyber Command. Acessível em http://www.defense.gov/home/features/2010/0410_cybersec/. Sobre o caso alemão ver Fischer e Reissmann (2011).

21 North Atlantic Treaty Organisation (NATO), na sigla em língua inglesa. Esta organização intergovernamental é designada tradicionalmente por Aliança Atlântica, evidenciando o facto de o Tratado de Washington reunir numa aliança militar a generalidade dos Estados da Europa Ocidental e da América do Norte.

pa ou na América do Norte será considerado como um ataque dirigido contra todas as partes". Verificando-se tal situação "cada uma delas, no exercício do direito de legítima defesa, individual ou coletiva, reconhecida pelo artigo 51.º da Carta[22] das Nações Unidas, assistirá a parte, ou as partes, atacadas". Consequentemente serão adotadas "individualmente e de acordo com as outras partes", as ações julgadas necessárias incluindo o "uso da força armada para restabelecer e assegurar a segurança na região do Atlântico Norte" (NATO, s.d.).

Naturalmente que o objetivo da inicial de segurança militar que tinham em mente os fundadores da NATO – a ex-URSS e os seus aliados do extinto Pacto de Varsóvia –, se tornou obsoleto com final da Guerra Fria. Várias transformações e adaptações ocorreram entretanto, procurando dar resposta às circunstâncias e necessidades de segurança no mundo da Guerra Fria (alargamentos a novos membros, alterações na identificação de ameaças e área geográfica de atuação, etc.). Neste contexto evolutivo, múltiplos documentos estratégicos foram adotados nos últimos 20 anos, o último dos quais foi aprovado na Cimeira de Lisboa, ocorrida em finais de 2010. Sobre o atual ambiente de segurança e as ameaças que lhe estão subjacentes, diz-se o seguinte no novo documento estratégico:

> "Os ciberataques estão a tornar-se mais frequentes, mais organizados e mais custosos nos danos que infligem às administrações governamentais, negócios, economias e potencialmente também às redes de transporte e fornecimento, bem como a outras infraestruturas críticas; podem atingir um patamar que ameaça a prosperidade nacional e Euro-Atlântica, a segurança e a estabilidade. Serviços militares e de informações estrangeiros, organizações criminais, grupos terroristas e/ou extremistas podem ser fonte de tais ataques." (NATO, 2010).

Quanto às capacidades de defesa e dissuasão este documento prevê que a NATO, "deve assegurar a totalidade das capacidades necessárias para dissuadir e defender contra qualquer ameaça à segurança das populações". No caso específico da ameaça de ciberataques – os quais, pela primeira vez, são mencionados ao nível do conceito estratégico –, foi estabelecido que a organização deverá "desenvolver

22 O Artigo 51.º da Carta das Nações Unidas tem o seguinte teor: "Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais." Acessível em http://www.fd.uc.pt/CI/CEE/pm/Tratados/carta-onu.htm, consultado em 10/07/2011.

mais a capacidade de prevenir, detetar, defender e recuperar de ciberataques, incluindo através do uso do processo de planeamento". Acrescenta-se, ainda, que deverá reforçar e coordenar "as capacidades de ciberdefesa nacionais, colocando todos os organismos da organização sob uma ciberprotecção centralizada, e integrando melhor a ciberconsciencialização, aviso e resposta com os Estados-membros (NATO, 2010).

Reflexões Finais

A emergência do ciberespaço durante os anos 90, ligada à explosão do uso da internet – tornada possível, sobretudo, pela invenção da World Wide Web e pela progressiva difusão das comunicações móveis e de banda larga –, mostrou os limites da visão idealista ou utópica dos fundadores da internet. Em vez de um "novo mundo" de liberdade e autorregulado, funcionando com base numa lógica de solidariedade e comunitária, emergiu, essencialmente, um domínio marcado por interesses económicos-comerciais e por um crescente uso profissional feito por múltiplos organismos públicos e privados. No caso dos grandes Estados autoritários, de que a China é o exemplo mais evidente, o ciberespaço foi, desde o início, um novo "território" não só de afirmação de soberania estadual como de controlo das atividades dos cidadãos, através de um sofisticado sistema tecnológico de vigilância. Ao contrário de uma opinião muito comum no Ocidente, a internet, como espaço de liberdade, não é uma inevitabilidade da própria tecnologia, mas, fundamentalmente, uma opção política. Nas democracias capitalistas liberais, nomeadamente nos EUA e na Europa, o próprio sucesso da internet e a crescente digitalização da economia acarretaram novas dependências, vulnerabilidades e riscos. O mais óbvio é o da possibilidade de ciberataques a organismos públicos ou empresas privadas ou até de uma ciberguerra, envolvendo atores estaduais e/ou não estaduais, causando sérios prejuízos e afetando o normal funcionamento de uma economia e sociedade. Assim, o crescente uso e dependência das economias nacionais da internet e das infraestruturas de comunicação (e outras) levaram também as democracias liberais a afirmar a sua soberania sobre este novo "território", adotando, paralelamente, medidas securitárias de diversos tipos. A NATO, a principal organização de segurança e defesa coletiva das democracias capitalistas liberais, denota esta tendência que podemos designar como uma espécie de "regresso do Leviatã". A questão em aberto é a de saber se a afirmação de soberania e a tendência para "securizar" o ciberespaço, não só vai dar um golpe fatal à utopia libertário-anárquica inicial, como asfixiar o território de liberdade que o cidadão tinha ganho, com ou sem a vontade dos Estados.

Referências Bibliográficas

Amaral, Diogo Freitas do (1998). *História das Ideias Políticas.* (Vol. 1). Coimbra: Almedina.

August, Olivier (2007). "The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online". *Wired* (23/10/2007). Disponível em http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all. Data de acesso 10/07/2011.

Barlow, John Perry (1996). *A Declaration of the Independence of Cyberspace.* Acessível em http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration. Data de acesso 10/07/2011.

Bodin, Jean (1993). *Les Six Livres de la République.* Acessível em http://classiques.uqac.ca/classiques/bodin_jean/six_livres_republique/bodin_six_livres_republique.pdf. Data de acesso 10/07/2011.

Demchak, Chris e Dombrowski, Peter (2011). "Rise of Cybered Westephalian Age". *Strategic Studies Quarterly*, vol 5, n.º 1, p. 32.

Fernandes, José Pedro Teixeira (2009). *Teorias das Relações Internacionais: da Abordagem Clássica ao Debate pós-Positivista* (2ª edição). Coimbra: Almedina.

Fischer, Sebastian e Ole Reissmann (2011). "Germany Arms Itself for Cyber War". *Der Spiegel Online International*, Acessível em http://www.spiegel.de/international/germany/0,1518,768764,00.html. Data de acesso em 10/07/2011.

Foucher, Michel (1991). *Fronts et Frontières. Un Tour du Monde Géopolitique*. Paris: Fayard.

Gat, Azar (2007). "The Return of Authoritarian Great Powers". *Foreign Affairs*, julho/agosto. Disponível em http://www.foreignaffairs.com/articles/62644/azar-gat/the-return-of-authoritarian-great-powers. Data de acesso 10/07/2011.

Hobbes, Thomas (1978). *Lheviatan or the Matter Form and Power of a Commonwealth Ecclesiastical and Civil*. Oxford: Oxford University Press.

Internet World Stats (s.d.). *Internet in Asia – 2009. Top Ten Countries.* Acessível em http://www.internetworldstats.com/stats3.htm. Data de acesso 10/07/2011.

Keen, Andrew (1996). "Web 2.0 – The second generation of the internet has arrived. It's worse than you think". *Weekly Standard.* Acessível em http://www.weeklystandard.com/Content/Public/Articles/000/000/006/714fjczq.asp. Data de acesso 10/07/2011.

Keen, Andrew (2007). *The Cult of the Amateur: How Today's Internet is Killing our Culture. London:* Nicholas Brealey Publishing.

Kelly, Sanja e Sara Cook (2011). *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media.* Washington DC: Freedom House/The United Nations Democracy Fund.

Klimburg, Alexander (2011). "Mobilising Cyber Power". *Survival: Global Politics and Strategy,* vol. 53, nº 1, pp. 41-60.

Krasner, Stephen (1999). *Sovereignty: Organized Hypocrisy*. Princeton-New Jersey: Princeton University Press.

Leigh, David e Luke Harding (2011). *WikiLeaks: Inside Julian Assange´s War on Secrecy*. London: Guardian Books.

NATO (2010). *Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation (Adopted by Heads of State and Government in Lisbon, 2010).* Acessível em http://www.nato.int/lisbon2010/strategic-concept2010-eng.pdf. Data de acesso 10/07/2011.

NATO (s.d). *The North Atlantic Treaty* (4/04/1949). Acessível em http://www.nato.int/cps/en/natolive/official_texts_17120.htm. Data de acesso 10/07/2011.

Nozick, Robert (1977). *Anarchy, State and Utopia*. New York: Basic Books.

Ohmae, Kenichi (1996). *The End of Nation-State: The Rise of Regional Economics*. New York: The Free Press.

Till, Scott (2011). "March 17, 1948: William Gibson, Father of Cyberspace" em *Wired*. Acessível em http://www.wired.com/thisdayintech/2011/03/0317cyberspace-author-william-gibson-born/. Data de acesso 2/10/2011.

Turner, Fred (2006). *From Counterculture to Cyberculture*. Chicago: The University of Chicago Press.