A ciberguerra como nova dimensão dos conflitos do século XXI

José Pedro Teixeira Fernandes

A importância crescente do ciberespaço e o aumento da relevância das questões de segurança neste não são surpreendentes. Há mais de um bilião de computadores pessoais, a maioria dos quais estão ligados à internet. No início de 2008, o número de proprietários de telemóveis ultrapassou a população (crianças incluídas) dos não proprietários. Cada telemóvel digital (em breve todos serão digitais), pode ser uma porta para o ciberespaço. A maioria dos utilizadores de computadores importa-se pouco com a segurança e sabem ainda menos desta. Uma consequência disto é que milhões, talvez até dezenas de milhões de computadores, são bots capazes de ser controlados por nefastos desconhecidos que os seus proprietários nem sabem que existem.

Martin C. Libicki[1]

RESUMO

Este artigo discute a tendência para que o ciberespaço se transforme em mais um campo de batalha dos conflitos internacionais. O artigo começa com uma análise do conceito de ciberguerra discutindo as dificuldades de estabelecer uma conceptualização rigorosa face ao direito dos conflitos armados / direito internacional humanitário. Em seguida são analisadas as capacidades e vulnerabilidades de alguns dos principais atores estaduais. O complexo papel dos atores não estaduais nos ciberconflitos é também objeto de uma análise e reflexão. O artigo termina com uma discussão sobre a dificuldade de avaliação do impacto económico dos ciberataques.

Palavras-chave: Ciberguerra, segurança, direito internacional humanitário, atores não estaduais

ABSTRACT

Cyber War: A New Dimension of the 21th Century Conflicts

The author discusses the progressive transformation of the cyberspace into one more battleground for international conflicts. The article begins with an analysis of the concept →

A (in)definição do conceito de ciberguerra

Todos os termos novos que, por uma razão ou por outra, se popularizam, tornando-se palavras de moda, acabam por trazer consigo uma utilização demasiado livre, tendencialmente proteiforme e confusa. É fácil constatar que isso está a acontecer atualmente com o termo ciberguerra. No seu uso mais comum e livre, 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,

of cyber war, and a discussion about the difficulties of establishing a rigorous conceptualisation within the framework of the Law of Armed Conflict/International Humanitarian Law. Then, the capabilities and vulnerabilities of great powers are also object of analysis, and the complex role of non-state actors in cyber conflicts. The article ends with a discussion about the difficulty of assessing the economic impact of cyber attacks.

Keywords: Cyberwar, security, International Humanitarian Law, non-state actors

então, ser protagonizadas por atores não estaduais. Sejam quais forem os contornos dados ao conceito é inquestionável que um uso livre, e, consequentemente, impreciso do termo é inadequado para um estudo académico-científico. Em tais circunstâncias de falta de rigor na conceptualização, também não existirá uma base para uma adequada atuação internacional nesta área. Basta pensarmos, por exemplo, numa análise da ciberguerra sob o prisma legal. Esta leva-nos, inevitavelmente, a ter de considerar o direito internacional humanitário[2] / direito dos conflitos armados. Aqui colocam-se curiosas questões, como, por exemplo, a de saber se os seus protagonistas poderão, ou deverão, ser tratados de forma similar aos combatentes ou se as ciberarmas poderão ser legalmente equiparadas a armas «físicas».

Quadro 1 > As fontes do direito internacional humanitário / direito dos conflitos armados[3]

Fonte	Título	Data	N.º de artigos
Convenção de Genebra	Melhoria das Condições dos Feridos no Campo de Batalha	1864	10
II Conferência de Haia	Leis e Costumes da Guerra em Terra	1899	60 (55 em Anexo)
IV Conferência de Haia	Leis e Costumes da Guerra em Terra	1907	64 (56 em Anexo)
Protocolo de Genebra	Para a Proibição do Uso na Guerra de Gás Asfixiante e dos Métodos de Guerra Bacteriológica	1928	–
I Convenção de Genebra	Para Melhoria das Condições dos Feridos e Doentes das Forças Armadas no Terreno	1864 (revista em 1949)	77 (13 em Anexo)
II Convenção de Genebra	Para Melhoria das Condições dos Feridos, Doentes e Náufragos das Forças Armadas no Mar	1949	63
III Convenção de Genebra	Relativa ao Tratamento dos Prisioneiros de Guerra	1929 (revista em 1949)	143
IV Convenção de Genebra	Relativa à Proteção de Civis em Tempo de Guerra	1949	180 (21 em Anexo)
Convenção de Genebra	Proibindo o Desenvolvimento, Produção e Armazenamento de Armas Bacteriológicas e Tóxicas e sobre a sua Destruição	1975	15
Protocolo I	Relativa à Proteção das Vítimas de Conflitos Armados Internacionais (amplia a definição dos mesmos às guerras de libertação nacional)	1977	102

Fonte	Título	Data	N.º de artigos
Protocolo II	Relativa à Proteção das Vítimas de Conflitos Armados Não Internacionais (completa o artigo 3 comum às quatro convenções de Genebra)	1977	28
Protocolo III	Relativa à Adoção de Um Emblema Adicional Distintivo	2005	17

A dificuldade de definir, no âmbito da rede, o conceito de ato de guerra, de combatente, etc., acresce a outros problemas com que atualmente se confronta o direito dos conflitos armados/direito internacional humanitário. De facto, se pensarmos em vários conflitos do passado recente verificamos que houve guerra – casos do Kosovo em 1999, do Afeganistão em 2001, do Iraque em 2003, do Líbano em 2006 –, sem declaração formal de guerra de Estado a Estado. Verificamos, também, que nem sempre as partes em confronto são estados – casos, por exemplo, da Al-Qaida e dos taleban no Afeganistão *versus* Estados Unidos/NATO, ou do Hezbollah no Líbano *versus* Israel. Isto levanta, desde logo, o problema da definição de quem pode, ou deve, ser considerado combatente. A ciberguerra insere-se nesta tendência, que já vem detrás, a qual evidencia algumas dificuldades na aplicação do direito internacional humanitário/direito dos conflitos armados aos conflitos atuais. Todavia, pelas implicações do que está em jogo – nomeadamente saber se um determinado ciberataque poderá ser considerado um ato de guerra –, é inevitável concordar-se que a clareza e o rigor do conceito são fundamentais não só para a segurança jurídica, como, também, para os decisores políticos poderem escolher a opção mais adequada em caso de um ciberconflito.

Uma vez efetuada esta nota prévia vamos proceder a uma revisão de literatura, com vista a identificar e avaliar alguns dos principais esforços de conceptualização já empreendidos. O objetivo será apresentar o que usualmente se designa pelo *state of the art*. Note-se que qualquer conceptualização rigorosa apontará, por um lado, para um fenómeno complexo e multifacetado, e, por outro, será sempre passível de alguma contestação. Pela natureza do fenómeno, esta implica articular aspetos estratégico-militares e político-legais com aspetos tecnológicos e até económico-empresariais. Por isso, vale a pena aqui relembrar uma reflexão sobre a definição de conceitos, efetuada num contexto de investigação jurídica, por Reinhold Zippelius. Como este explica, «os conceitos são, portanto, combinações de traços comuns a vários objetos. Mas saber quais dos aspetos comuns correntes pomos em evidência e abarcamos nos nossos conceitos, isso depende daquilo porque nos interessamos»[4]. Ou seja, «a formação dos conceitos orienta-se pela questão de se saber» qual a delimitação em que os «conceitos servem melhor os objetivos da investigação para que são formados»[5]. No caso da ciberguerra, vejamos algumas das mais relevantes propostas de conceptualização até agora efetuadas.

CONCEPTUALIZAÇÕES ESTRATÉGICO-MILITARES DE CIBERGUERRA

Em *Ciberwar is Coming!*, John Arquilla e David Ronfeldt procuraram traçar pioneiramente os contornos do conceito de «ciberguerra» (*cyberwar*). Estávamos, então, nos primórdios da sociedade em rede tal como hoje a conhecemos, em termos de uso da internet, da *web*, de comunicações móveis e de outras tecnologias digitais. Para clarificarem a sua conceptualização, estes procuraram destrinçar o conceito de ciberguerra de outros próximos, nomeadamente daquilo que estes designaram como «infoguerra» (*netwar*). Quanto a esta última, a infoguerra, foi definida como

> «um conflito relacionado com a informação a um grande nível, entre estados ou sociedades. Significa tentar desarticular, danificar ou modificar o que uma população "sabe", ou pensa que sabe, sobre ela própria e o mundo à sua volta. A infoguerra pode focalizar-se na opinião pública, ou na elite, ou em ambas. Pode envolver medidas de diplomacia pública, propaganda e campanhas psicológicas, subversão cultural e política, induzir em engano ou interferir com os média locais, ou infiltrações em redes de computadores e bases de dados e esforços para promover movimentos dissidentes e de oposição através das redes de computadores. Assim, conceber uma estratégia para a infoguerra significa reunir em conjunto, sob uma nova perspetiva, um conjunto de medidas que já foram usadas anteriormente, mas eram vistas de forma separada. Por outras palavras, a infoguerra representa uma nova entrada no espectro do conflito que abrange formas de "guerra" económica, política, social e militar. Em contraste com guerras económicas que têm como alvo a produção e a distribuição de bens, e as guerras políticas que têm como alvo a liderança e as instituições do governo, as infoguerras distinguir-se-ão por procurarem atingir a informação e comunicação. Como outras formas neste espectro, as infoguerras serão largamente não militares, mas poderão ter dimensões que se justapõem à guerra militar»[6].

Uma vez clarificado este conceito afim, John Arquilla e David Ronfeldt procuraram definir o conceito de ciberguerra propriamente dito. Na sua ótica, este

> «refere-se a conduzir e preparar para conduzir operações militares de acordo com os princípios da informação. Significa interromper, se não mesmo destruir, os sistemas de informação e de comunicação, definidos de forma ampla, de modo a incluir até a cultura militar, nos quais um adversário se apoia para se "conhecer" a si próprio: quem é, onde está, o que pode fazer quando, porque está a lutar, que ameaças contrariar primeiro, etc. Significa tentar saber tudo sobre um adversário, enquanto que se evita que este saiba muito sobre nós próprios. Significa modificar a "balança de informação e conhecimento" a nosso favor, especialmente se a balança de forças não é favorável. Significa usar conhecimento, pelo que menos capital e trabalho terão de ser gastos. Esta forma de guerra pode envolver diversas tecnologias – nomeadamente para C3I[7]; recolha de informação,

> posicionamento e identificação de amigos ou inimigos (IFF)[8]; e sistemas de armas "inteligentes" – para dar apenas alguns exemplos. Pode também envolver interferência eletrónica, falseamento, sobrecarga e intrusão nos circuitos de informação e comunicação de um adversário»[9].

Por tudo isto, a ciberguerra

> «poderá também implicar o desenvolvimento de novas doutrinas sobre o tipo de forças necessárias, onde e como deslocá-las, e saber com quê e como atacar no lado do inimigo. Como e onde posicionar determinados tipos de computadores e sensores relacionados, redes, bases de dados, etc., pode tornar-se tão importante como a questão que costumava ser efetuada sobre deslocação de bombardeiros e as suas funções de suporte. A ciberguerra pode também ter implicações para a integração dos aspetos políticos e psicológicos com os aspetos militares de fazer a guerra»[10].

Importa relembrar que esta conceptualização data de 1993, numa altura em que, como já referimos, a internet e a sociedade em rede estavam a dar os primeiros passos e era difícil discernir a evolução futura. Daí que Arquilla e Ronfeldt tenham sido também bastante cautelosos na sua formulação prospetiva. No seu texto original estes faziam notar que «como inovação na forma de fazer a guerra, antecipamos que a ciberguerra pode ser para o século XXI o que a *blitzkrieg* foi para o século XX. Mas, por agora, também acreditamos que o conceito é demasiado especulativo para uma definição precisa»[11].

O conceito de ciberguerra, tal com definido por Arquilla e Ronfeldt, tornou-se influente pelo prestígio dos autores e da Rand Corporation à qual estão ligados, bem como pelo seu caráter pioneiro e «futurista». Tal como ocorreu frequentemente no século XX, com muitas inovações em diferentes domínios, projetou-se rapidamente para fora dos Estados Unidos. Neste caso, naturalmente que interessou, em primeira linha, os meios estratégicos e militares de diferentes países. No universo lusófono encontramos, desde logo, essa influência de maneira evidente num Estado – o Brasil –, o qual tem sido crescentemente apontado como uma das principais potências em ascensão neste início de século XXI. Fazendo eco destas ideias, F. G. Sampaio, num *paper* elaborado para a Escola Superior de Geopolítica e Estratégia, referiu-se ao conceito de ciberguerra em termos bastante similares[12]. Segundo este, a «ciberguerra» derivaria do conceito estratégico-militar germânico de *leintenkrieg*[13], o qual data dos tempos da II Guerra Mundial. Na sua formulação atual, visaria «a paralisação de um adversário», o qual poderá ser um país, um bloco económico, ou uma aliança militar, «pela penetração das redes de computadores que regem as atividades vitais da economia, criando o caos e difundindo um estado de medo generalizado»[14]. Acrescenta ainda que «tal quadro permite o enfraquecimento das defesas convencionais, podendo-se, então,

por técnicas de infiltração, atacar o país, bloco ou aliança, por meio de ações terroristas, boatos (difundidos por agentes infiltrados), notícias falsas veiculadas pelos meios de informação de massa»[15]. Estas ações permitiriam destruir «a coesão, a capacidade de resistência e levariam a um colapso total, que seria a paralisação estratégica, elevada, porém, a um potencial muito maior do que o previsto até hoje»[16]. Quanto aos alvos preferenciais da ciberguerra, estes são, segundo o mesmo autor, «os computadores, individualmente ou em rede»[17]. Para os atingir, são invadidos os mais diversos «programas de controlo de operações, e, uma vez os mesmos penetrados», é aguardado o «momento propício para ativar a sabotagem»[18]. Por sua vez, «os alvos preferenciais para serem penetrados e desvirtuados são os programas de computador que controlam ou gerem»[19] os seguintes setores de atividade económico-empresarial e/ou de serviço público – as chamadas infraestruturas críticas: *i*) comando das redes de distribuição de energia elétrica; *ii*) comando das redes de distribuição de água potável; *iii*) comando das redes de gestão dos caminhos de ferro; *iv*) comando das redes de gestão do tráfego aéreo; *v*) comando das redes de informação de emergência (112, serviços de urgência médica, polícia, bombeiros); *vi*) comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registado em nome dos cidadãos; *vii*) comando das redes de comunicações em geral e em particular (incluindo as redes de estações de rádio e de televisão); *viii*) comando dos *links* com sistemas de satélites artificiais (incluindo fornecedores de sistemas telefónicos, de sinais para TV, de previsões de tempo e de sistemas GPS); *ix*) comando da rede do Ministério da Defesa (incluindo também outros ministérios-chave, como o do Interior e da Justiça, e o próprio Banco Central); *x*) comando dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral. Para o mesmo autor, os protagonistas típicos da ciberguerra seriam os *hackers*[20] e os computadores usados por estes.

Mas há outros desenvolvimentos mais recentes relevantes. Nos últimos anos, sobretudo desde os conflitos da Estónia (2007) e da Geórgia (2008) com a Rússia, tem-se assistido a um crescente interesse por este assunto e a uma maior sofisticação das abordagens teóricas. Verificamos, também, que têm surgido crescentemente análises mais aprofundadas e apuradas, quer da parte dos meios militares e de segurança, quer de organizações internacionais, de *think tanks* e de académicos ou de outros interessados. Por exemplo, para o Institute for Advanced Study of Information Warfare dos Estados Unidos, a ciberguerra define-se como

> «o uso ofensivo e defensivo da informação e dos sistemas de informação para negar, explorar, corromper, ou destruir a informação de um adversário, processos baseados na informação, sistemas de informação e redes baseadas em computadores, enquanto se protegem as próprias. Tais ações são projetadas para atingir vantagens sobre adversários militares»[21].

Recentemente, Peter Sommer e Ian Brown, num relatório elaborado para a Organização para a Cooperação e o Desenvolvimento Económico (OCDE) no âmbito do projeto «Choques Globais no Futuro» intitulado «Reduzindo o Risco Sistémico da Cibersegurança», voltaram a analisar esta importante questão concetual. No relatório, começaram por notar o problema já aqui referido, o qual decorre do facto de o termo tender a ser usado de forma livre, em sentidos bastante variáveis e pouco precisos[22]. Passando em revista alguns dos seus usos mais correntes, estes referem que, no âmbito do pensamento sobre segurança e estratégia, é frequente encontrarmos o termo utilizado no sentido de «uma guerra conduzida substancialmente no ciberespaço ou no domínio virtual»[23]. Aqueles que partilham de tal conceção «têm frequentemente em mente que as ciberguerras tendem a ser muito similares às guerras convencionais»[24] pelo que idênticas doutrinas de retaliação ou dissuasão poderão ser aplicadas. Todavia, Sommer e Brown consideram que é mais fácil definir «ciberguerra», se os critérios aplicáveis ao conceito forem os mesmos que são utilizados para qualquer guerra convencional ou «cinética». Desde logo, para a qualificação de uma ocorrência como guerra – e, por isso, também de ciberguerra –, será fundamental ter em conta as disposições contidas em alguns tratados internacionais, nomeadamente as convenções de Haia de 1899 e 1907[25], a Carta das Nações Unidas de 1945, a Convenção das Nações Unidas de 1948 sobre o genocídio e a Convenção das Nações Unidas de 1980 sobre armas convencionais excessivamente lesivas (ou cujos efeitos são indiscriminados) – ou seja, o normativo que integra o direito dos conflitos armados/direito internacional humanitário[26]. Assim, defendem estes, na sua essência, para se decidir se um ato deve, ou não, ser qualificado como ciberguerra, deverá submeter-se ao teste de verificar se pode ser considerado «equivalente» a um ataque convencional no seu objetivo, intensidade e duração. E, acrescentam Sommer e Brown, «há também uma distinção a fazer entre atos que procuram atingir alvos militares e atos destinados a alvos civis»[27]. Estes fazem notar que a

> «Carta das Nações Unidas requer uma justificação para a adoção de contramedidas por aqueles que afirmam ter sido atacados. No essencial, a vítima deve ser capaz de produzir provas fidedignas sobre quem a atacou (algo nem sempre fácil no cibermundo) e sobre os efeitos dos ataques. O objetivo das contramedidas deverá ser forçar o Estado atacante a acatar as suas obrigações nos termos da Carta das Nações Unidas. Todavia, como estes referem, entendido desta maneira o conceito apenas poderá, por princípio, aplicar-se aos estados e não a atores não estaduais. Face a estas dificuldades de definição dos contornos e da abrangência do conceito, pode-se argumentar que o foco da análise da ciberguerra deveria antes deslocar-se para a avaliação das capacidades das várias formas de (ciber) armamento. Nessa hipótese, a primeira preocupação deveria ser então tentar encontrar as razões pelas quais alguém pode querer fazer a guerra, ou iniciar uma atividade hostil em grau menor do que uma guerra em larga escala. Tipicamente, são disputas sobre o

> território, disputas para afirmar a hegemonia, disputas sobre o acesso a recursos e a matérias-primas, disputas sobre a religião ou disputas históricas e vingança»[28]

que levam ao conflito e à guerra. Uma vez que «estas hostilidades existem no mundo real, parece haver pouca razão para os estados se limitarem ao armamento "cinético"»[29]. O (ciber)armamento apenas fornece «meios adicionais através dos quais a hostilidade pode ser prosseguida».

CAPACIDADES E VULNERABILIDADES OFENSIVAS E DEFENSIVAS DOS ATORES ESTADUAIS

Quando se analisa a ciberguerra num plano estratégico, inevitavelmente nos ocorre efetuar um levantamento das capacidades ofensivas e defensivas dos diversos atores que se podem confrontar num hipotético cenário de conflito. Em termos modernos, quando pensamos a guerra pensamos, por inerência, nos estados. Esta tradição de considerar o Estado soberano (vestefaliano) como ator central das relações internacionais tem um profundo enraizamento histórico. A sua principal referência diplomática são os Tratados de Vestefália (1648), que puseram fim à Guerra dos Trinta Anos, na Europa do século XVII. Marcaram a ascensão progressiva do Estado soberano a forma primordial de organização política das comunidades humanas, primeiro na Europa, depois, por todo o mundo. Isto sobretudo por influência europeia ao longo do século XIX e primeira metade do século XX. Todavia, no mundo atual, como já referimos, a primazia dos estados vestefalianos sofre a competição de outros atores, com maior ou menor peso (OIG, ONG, empresas transnacionais, grupos subestaduais, etc.). No caso da ciberguerra, a questão da relevância dos atores não estaduais levanta-se com especial acuidade. Os exemplos dos ciberataques mais conhecidos – Estónia (2007) e Geórgia (2008), ao qual se poderá juntar o caso do ataque do vírus *Stuxnet* (2010), às instalações nucleares do Irão –, podem ser vistos como uma espécie de «guerras por procuração». De facto, o ponto comum é que ocorreram ciberataques contra esses estados, mas, oficialmente, não têm qualquer autoria de outros estados. Aparentemente, a responsabilidade caberia apenas a elementos da «sociedade civil»: *netizens*[30] («cibercidadãos»), ativistas ou «*hackers* patrióticos». Estes, teoricamente, atuariam de *motu* próprio, à margem e sem qualquer conhecimento dos estados dos quais são cidadãos. Vamos deixar esta questão para uma análise própria a efetuar mais à frente e, para já, concentrarmo-nos apenas nos atores estaduais.

Uma análise das capacidades e vulnerabilidades das principais potências militares mundiais foi efetuada recentemente por Richard Clarke e Robert Knake nos Estados Unidos. Estes colocaram uma especial ênfase no aspeto das capacidades defensivas e das vulnerabilidades, por considerarem que estas facetas estavam a ser subavaliadas pelos meios governamentais de segurança norte-americanos. Na sua abordagem, apresentaram uma estimativa das capacidades de ciberguerra dos Estados Unidos, bem

como de alguns do seus principais competidores ou inimigos. Segundo Richard Clarke e Robert Knake, qualquer avaliação (ainda que estimativa) dessas capacidades deve ter em conta três dimensões: i) a capacidade ciberofensiva, entendida como a capacidade de efetuar ciberataques a outros estados; ii) a capacidade ciberdefensiva configurada como «a medida da capacidade de adotar ações sob um ataque», ações essas que «irão bloquear ou mitigar esse ataque»; iii) a ciberdependência medida como «a extensão em que um Estado está ligado e assente sobre redes e sistemas que podem ser vulneráveis no caso de um ciberataque»[31]. Adotando estas três dimensões chegaríamos a um quadro estimativo dessas capacidades, como o que se apresenta em baixo.

Quadro 2 > Estimativa de capacidades globais de ciberguerra de alguns estados[32]

Estados	Capacidade ciberofensiva	Ciberdependência	Capacidade ciberdefensiva	*Score* total
EUA	8	2	1	11
Rússia	7	5	4	16
China	5	4	6	15
Irão	4	5	3	12
Coreia do Norte	2	9	7	18

Uma questão relevante é a de saber, em concreto, quais os dados que os autores usaram para chegarem aos *scores* que apresentam em cada uma destas três dimensões. Estes referem apenas que as pontuações atribuídas a cada uma destas dimensões e estados se baseiam numa «avaliação pessoal»[33]. O reparo óbvio é que remetendo os dados apenas para uma perceção subjetiva, não são verificáveis, nem comparáveis com outros, o que, naturalmente, lhes retira valor num uso estritamente científico. De qualquer maneira, apesar das limitações óbvias, não significa que sejam totalmente destituídos de interesse para a discussão e reflexão sobre as capacidades estaduais que aqui nos ocupa. Assim, vale a pena notar os comentários que Clarke e Knake fazem a este *ranking* de capacidades. Tal como os autores referem, «a China tem um elevado *score* na "defesa" em parte porque tem planos e capacidade para desligar as redes do país inteiro do resto do ciberespaço. A China pode limitar a utilização do ciberespaço numa crise desligando os utilizadores não essenciais»[34]. Já os Estados Unidos não têm a mesma possibilidade. Por sua vez, a Coreia do Norte tem um *score* elevado, quer para ciberdefesa, quer para a ciberdependência. Isto porque o país

> «pode desligar a sua limitada conexão ao ciberespaço ainda de forma mais fácil e efetiva do que a China. Para além disso, a Coreia do Norte tem tão poucos sistemas dependentes do ciberespaço que um grande ciberataque à Coreia do Norte praticamente não pro-

vocaria danos. Importa lembrar que a ciberdefesa não se refere ao número de habitações com banda larga, ou ao número de *smart phones* (telemóveis "inteligentes") *per capita*; refere-se à extensão em que infraestruturas críticas (rede elétrica, caminhos de ferro, gasodutos, cadeias de abastecimento, etc.), estão dependentes de sistemas em rede e não têm um *backup* efetivo»[35].

O PAPEL DOS ATORES NÃO ESTADUAIS NOS CIBERCONFLITOS

Num recente artigo publicado na revista *Survival* do International Institute of Strategic Studies (IISS) de Londres, Alexander Klimburg analisa a relevância dos atores não estaduais nos ciberconflitos[36]. O artigo incide especialmente nas situações em que estes são mobilizados e coordenados por estados, ainda que de forma não oficialmente assumida por estes. Klimburg começa por fazer notar os pontos de contacto que existem, nomeadamente quanto à base tecnológica e ferramentas usadas, entre o cibercrime, o ciberterrorismo e os atos de ciberguerra:

> «Cibercrime, ciberterrorismo e ciberguerra partilham uma base tecnológica comum, ferramentas, logística e instrumentos. Podem também partilhar as mesmas redes sociais e ter objetivos similares. As diferenças entre estas duas categorias de ciberatividades são frequentemente ténues, ou estão apenas nos olhos de quem as vê. Na perspetiva de um ciberguerreiro, o cibercrime pode oferecer uma base técnica (ferramentas de *software* e apoio logístico) e o ciberterrorismo a base social (redes pessoais e motivação) com as quais podem ser executados ataques às redes de computadores de grupos inimigos ou nações.»[37]

Assim, certos estados teriam interesse em manter, ou tolerar, aquilo que este designa como «organizações por procuração». Estas poderiam, quando oportuno, ser envolvidas em atividades de ciberataques (eventualmente, também, em atividades de ciberdefesa). Por exemplo, um ataque distribuído de negação de serviço poderá ser posto em prática por um utilizador médio de computadores, desde que disponha das ferramentas certas. Para os estados, uma vantagem, desde logo, é que os ataques de negação de serviço são, normalmente, mais difíceis de imputação de autoria do que os ataques de exploração da rede (tipicamente espionagem e roubo de informação sensível). Nestes últimos, a informação tem de viajar na rede até ao perpetrador, o que normalmente deixa rasto, e, tendencialmente, permite imputar a autoria[38]. Podendo ser o roubo de informação, em si mesmo, já bastante problemático, quer para a segurança nacional, quer para as empresas (consoante o que estiver em causa), este pode não ser ainda o pior problema. Klimburg chama a atenção para o facto de um ataque de exploração da rede, com o objetivo de espionagem e/ou roubo de informação ser, ao mesmo tempo, a base (técnica)

para um dos «mais perigosos tipos de ciberataques: a colocação, sem conhecimento, de "bombas lógicas" escondidas». Trata-se de «ficheiros ou de pacotes de *software* relativamente pequenos, escondidos, que, como não necessitam de comunicar, são extremamente difíceis de localizar. Uma vez acionadas as "bombas lógicas" podem ser massivamente destrutivas»[39]. Klimburg refere, como exemplo deste risco, o caso de um engenheiro de *software* indiano contratado pelo Fannie Mae – uma das instituições ligadas ao crédito hipotecário que esteve na origem do desencadear da crise financeira de 2008 nos Estados Unidos. Este, em litígio com a empresa, colocou uma «bomba lógica» na sua rede, a qual não chegou a ser acionada – por sorte, a programação da bomba lógica era defeituosa... –, mas poderia ter levado à paralisação, total ou parcial, do Fannie Mae durante uma semana, entre outros danos mais graves, como apagar toda a informação da empresa[40].

Algumas interrogações importantes colocam-se inevitavelmente aqui em matéria de imputação de responsabilidades: tendo em conta os meios técnicos necessários, que tipo de ciberataques é plausível que possam ocorrer por iniciativa de atores não estaduais e à margem dos estados? E, por similares razões técnicas, logísticas, de meios, etc., que tipo de ciberataques é plausível que só possam ocorrer com o apoio ou a anuência tácita dos estados, ainda que oficialmente estes neguem qualquer envolvimento? De acordo com Klimburg, ataques menos sofisticados do que a colocação de «bombas lógicas» mas mais visíveis do que estas, «como os ataques de negação de serviço ou os ataques que apagam páginas de um sítio na *web*[41] são empreendidos por grupos não estaduais atuando, pelo menos, com o seu suporte tácito»[42]. Note-se que Klimburg faz esta afirmação tendo em mente os casos concretos da Rússia e da China e ocorrências como as que tiveram lugar na Estónia em 2007 e na Geórgia em 2008. Todavia, em teoria, estes até poderão ocorrer apenas por *motu* próprio de atores não estaduais, dado o tipo de tecnologia, conhecimentos e recursos necessários estarem acessíveis a estes. Já a situação é diferente se considerarmos os ataques de exploração da rede, sobretudo nos casos mais sofisticados. Mesmo que executados por atores não estaduais, os ataques de espionagem mais avançados requerem largas centenas de horas de programação e têm, frequentemente, objetivos políticos subjacentes, trazendo consigo um benefício para um Estado. Um exemplo desta situação poderá ser o caso do vírus *Stuxnet*, que infetou computadores em, pelo menos, 11 países diferentes, o qual, tudo parece indicar, visava o programa nuclear iraniano. Todavia, este é também um bom exemplo dos «danos colaterais» que os ciberataques tendem a produzir. Tudo indica que o vírus terá sido concebido em diferentes módulos de forma a que a programação fosse feita por partes que não tinham conhecimento do projeto no seu conjunto. Para Klimburg este é um indício de que a execução do projeto poderá ter sido contratada a um certo número de indivíduos ou organizações envolvidas no cibercrime[43].

É na China, o Estado mais populoso do planeta, que existe também o maior número de utilizadores da internet a nível mundial, bem como de blogues, calculando-se que

o número destes últimos poderá atingir os 50 milhões[44]. Em valor absoluto, os utilizadores chineses ultrapassarão os 400 milhões, existindo, todavia, um enorme potencial de crescimento pois, em termos relativos, a população do país ligada à rede é ainda baixa (cerca de 30 por cento). Importa, por isso, reter que a liderança chinesa quanto ao número de utilizadores da internet tem tendência para se reforçar significativamente (ao longo deste século, provavelmente só a Índia, pela sua também enorme dimensão populacional, a poderá eventualmente disputar). Todavia, em abstrato, isto confere já à China a maior massa potencial de *hackers* ou *netizens*, os quais, eventualmente, podem ser «recrutados» ou mobilizados para objetivos estratégicos e de interesse nacional.

É NA CHINA, O ESTADO MAIS POPULOSO DO PLANETA, QUE EXISTE TAMBÉM O MAIOR NÚMERO DE UTILIZADORES DA INTERNET A NÍVEL MUNDIAL. DESDE 2003 QUE A CHINA INTEGRA NA SUA ORGANIZAÇÃO MILITAR UNIDADES PREPARADAS PARA ATIVIDADES DE CIBERGUERRA.

Desde 2003 que a China integra na sua organização militar unidades preparadas para atividades de ciberguerra. Por exemplo, «a milícia da cidade de Guangzhou criou um batalhão de guerra de informação organizado em torno das instalações da empresa de comunicações dessa província chinesa. Esse batalhão integra companhias de "guerra de redes de computadores" e de "guerra eletrónica"»[45]. Como faz notar Klimburg, é possível indivíduos «fazerem parte dessa milícia sem nunca terem usado um uniforme militar. Para muitos estudantes das universidades técnicas é uma condição de facto para a sua inscrição. Muitas instituições civis, especialmente as empresas detidas pelo Estado, também têm o seu papel nessa milícia»[46]. Em geral, nada disto é novidade. A sua existência é parte integrante da estratégia de defesa nacional chinesa e da organização das Forças Armadas desde a fundação da República Popular da China em 1949. Todavia, o que é novo é que essas organizações, que previamente eram uma espécie de «tigres de papel», adquiriram agora um novo fôlego, «tornando-se atores de ciberguerra proficientes». Aqui entra também em conta a enorme massa humana de que a China dispõe, e o facto de nas últimas décadas surgirem camadas da população com qualificações e conhecimentos tecnológicos importantes. Em 2007, «existiam mais de 25 milhões de estudantes em universidades estaduais. Milhões de pessoas são também empregadas nas empresas de informação-tecnologia detidas pelo Estado». Devido a estes números «e ao provável número de *hackers* patrióticos que podem fazer parte das estruturas militares, não é surpreendente que a maioria dos ciberataques aos Estados Unidos tenham origem na China»[47].

Ainda segundo Klimburg, não serão mais de mil a cinco mil os *hackers* que farão parte dessas estruturas ou programas paragovernamentais. Todavia, a afiliação informal poderá levar esse número a aumentar cerca de dez vezes. Muitos dos ataques são provavelmente encorajados de forma ativa para distrair os *hackers* de outras atividades. Assim, evita-se que «os seus talentos sejam direcionados para atividades antigovernamentais. Competições organizadas de *hackers* e outras ações desse género são não

apenas tentativas de identificar bons talentos, mas também de manter o talento ocupado de forma segura». A referida estratégia chinesa coloca aos analistas ocidentais, entre outros problemas complexos, o das múltiplas identidades dos seus intervenientes. Isto torna difícil, se não mesmo, em certos casos, impossível, a sua catalogação adequada: estamos perante atores estaduais ou não estaduais; as ações resultam de iniciativa «própria» ou são determinadas por organismos estaduais? Assim, «é possível, para uma mesma unidade de milícia de ações de ciberguerra ser, ao mesmo tempo, um departamento de tecnologias de informação numa universidade, uma agência de publicidade *online*, um clã de jogo *online*, uma equipa de *hackers* patrióticos e um sindicato do cibercrime local envolvido em pirataria informática»[48].

Outro caso interessante de atuação de atores não estaduais, direta ou indiretamente patrocinados pelo seu país de origem, é o caso da Rússia. A Rede de Negócios Russa é considerada a principal organização mundial no fornecimento de base logística para ciberataques e outras atividades, sem motivações políticas, que encaixam no perfil de cibercrime. É também identificada pela NATO como uma ameaça à cibersegurança dos seus membros. Entre outras acusações que lhe têm sido feitas, consta a da facilitação dos ciberataques à Geórgia, no verão de 2008. Como se explica esta atitude de benevolência das autoridades russas face a essa organização? Parecem existir duas grandes explicações. Uma primeira sugere a proximidade com os serviços de informações e segurança russos, que lhe permitiriam um «tratamento especial». Uma outra razão avançada prende-se com a maneira de encarar este tipo de atividades na sociedade russa. Uma parte significativa da população vê isso não como problemático para o país, mas antes para os países ocidentais – o alvo preferencial dessas atividades. Isto leva a que estes atos sejam vistos como uma espécie de «maus modos de cavalheiros», ou até em termos quase heroicos[49]. Tal como vimos no caso do «patrocínio» de atores não estaduais pela China – fenómeno que, naturalmente, não é exclusivo desse país, nem da Rússia.... –, os serviços secretos e de segurança procuram mobilizar «*hackers* patrióticos» que possam ser usados em ciberataques sem envolver diretamente, pelo menos na aparência, o Estado russo.

Mas serão estes usos, questionáveis do ponto de vista ético e legal, de atores não governamentais ou que supostamente têm esse perfil, um exclusivo de estados onde existem regimes autoritários ou semidemocráticos? Por razões ligadas aos valores democráticos e aos constrangimentos legais dos governos, a mobilização de atores não estaduais – que também se pode constatar nas democracias liberais –, não se verifica da mesma maneira. Não é típico destas, nem expetável face aos seus princípios, que organizem cibermilícias segundo o modelo chinês, ou direcionem organizações do cibercrime para esse efeito, como parece ser o caso da Rússia. (Não estamos com isto a querer dizer que os países ocidentais estejam totalmente «limpos» em matéria dessas estratégias). O que tipicamente os governos dos estados democráticos normalmente têm procurado fazer, é criar mecanismos de cooperação e de

estímulo à participação de elementos dos meios empresariais e da sociedade civil nos objetivos governamentais na área da cibersegurança. Por exemplo, no Reino Unido, existe um Centro para a Proteção da Infraestrutura Governamental, o qual desempenha um papel importante na ajuda à indústria britânica a defender-se do cibercrime. Nos Estados Unidos, as indústrias relevantes para a segurança nacional operam em proximidade com o governo federal. Como faz notar Klimburg, «as empresas privadas envolvidas diretamente em trabalhos de segurança e defesa podem estar tão estreitamente entrelaçadas com o Estado que, vistas do exterior, dificilmente se descortina qualquer distinção clara entre ambos»[50]. Para além disso, a forma mais relevante de mobilização de atores não estaduais passa pela identificação destes com os objetivos dos governos. Desde logo, há o papel desempenhado por numerosos *think-tanks* com propostas e contributos em matéria de cibersegurança, bem como outros grupos e organizações da sociedade civil. «É esse, por exemplo, o caso da Security Trusts Networks, a qual tem tido um papel relevante na análise de ciberataques (por exemplo, no caso dos ataques à Geórgia, no verão de 2008), algures entre o jornalismo de investigação e a informática forense»[51].

O PROBLEMA DA AVALIAÇÃO DO IMPACTO ECONÓMICO DOS CIBERATAQUES

Num estudo efetuado em 2004 e apresentado ao Congresso dos Estados Unidos, Brian Cashell e outros investigadores procuraram avaliar as consequências económicas que podem resultar de um ciberataque[52]. Apesar dos anos decorridos, esse estudo foi dos mais exaustivos até agora efetuados. Mostra também como a avaliação dos danos económicos de um ciberataque é um problema complexo e difícil de quantificar. Em primeiro lugar, «porque há fortes razões que desencorajam relatar as falhas de segurança informática»[53] (devida a receio de danos na imagem, perda de valor nos mercados bolsistas, perda de clientes, sanções legais por não observância de regras de segurança, inspirar outros ciberataques, etc.). Em segundo lugar,

> «porque as organizações são frequentemente incapazes de quantificar os riscos dos ciberataques que enfrentam, ou avaliar monetariamente o custo dos ataques que já tiveram lugar. Assim, mesmo que toda a informação confidencial e privada sobre ciberataques fosse tornada acessível e coligida numa base de dados, a mensuração do impacto económico continuaria a ser problemática»[54].

Mas a mensuração dos custos económicos de um ciberataque, ou de um ciberconflito, é também problemática por outras razões[55]. Como explicam Brian Cashell *et al.*

> «os custos associados aos ciberataques podem ser divididos em diretos e indiretos. Os custos diretos incluem as despesas relacionadas com a restauração do sistema original do computador, anterior ao ataque. A recuperação de um ataque irá, tipicamente, reque-

rer despesas extras em trabalho e materiais, sendo estes os custos mais fáceis de medir. Mas, mesmo a este nível básico de contabilização de custos, podem surgir complexidades. Se um ataque levar ao aumento das despesas em tecnologias de informação serão esses custos atribuíveis ao ataque? E se um *upgrade* no *hardware* ou no *software* for acelerado por um ataque, deve esse *upgrade* ser considerado como um custo de segurança? Um outro conjunto de custos indiretos deriva da interrupção dos negócios o que, numa linguagem mais jurídica, poderíamos designar como "lucros cessantes". Estes custos podem incluir perda de receita e perda de produtividade dos trabalhadores durante a interrupção. Receitas perdidas podem facilmente ser medidas por referência a um período pré-ataque, mas isto pode não resolver toda a questão. As receitas perdidas podem ser um fenómeno transitório, limitado ao período do ataque (e, possivelmente, também a um período posterior), ou podem ser de longo prazo, se, por exemplo, alguns mudarem permanentemente para empresas competidoras»[56].

Mas, para além das consequências ao nível microeconómico e empresarial, e da (já difícil) avaliação e quantificação desses danos, a questão das consequências de um ciberataque coloca-se, também, a nível macroeconómico, aumentando a dificuldade de avaliação. Neste contexto, Brian Cashell *et al.* fazem notar que «qualquer estimativa do potencial custo económico de um ciberataque será, em última instância, especulativa». Se imaginarmos um cenário em que toda a atividade económica é «temporariamente interrompida por um ciberataque, a única consideração na estimativa dos custos será a duração do evento. A percentagem do Produto Interno Bruto (PIB), produzida num dado dia é de cerca de 0,3 por cento do total do ano. Alguma da produção que poderia ser interrompida é improvável que fosse perda permanente. Seria simplesmente adiada até que os efeitos do ataque se dissipassem. Desde que uma considerável, ainda que desconhecida, fatia dos *ouptus* não esteja dependente dos computadores, o custo final será menor do que esse. Historicamente, a produção total anual de bens e serviços tem sido, em média, cerca de um terço do valor total de *stock* de capital físico. Em 2001, o equipamento informático e o *software* contavam cerca de 18 por cento do *stock* total de capital. Se for assumido que o equipamento e o *software* contribuem para o *output* da mesma maneira que outras formas de capital, a sua contribuição direta será cerca de 18 por cento da produção total anual. Se essa fatia do *output* fosse interrompida durante um único dia, isso representaria cerca de 0,05 por cento do PIB total anual. Desde que um ciberataque não seja abrangente e seja de duração curta, é provável que quaisquer consequências macroeconómicas sejam relativamente pequenas. Mas, seja qual for o âmbito do ataque, a capacidade de recuperar rapidamente é importante, pois a duração do período em que os computadores permanecem afetados é uma determinante importante dos custos. Pode ser quase tão importante para as empresas tratar das suas competências para restaurar as operações como trabalhar para isolar qualquer potencial ataque»[57].

CONCLUSÕES

A reflexão estratégica e legal sobre a ciberguerra e sobre as suas possíveis consequências ainda está nos primórdios. Este caráter incipiente deteta-se no próprio conceito de ciberguerra que não é objeto de um consenso internacional, sendo frequentes as suas utilizações «livres». A fronteira desta com o cibercrime e os atos de ciberativismo com motivações políticas também nem sempre é simples de traçar. O protagonismo que, tendencialmente, os atores não estaduais têm neste novo terreno, complica a análise, nomeadamente ao nível da atribuição de responsabilidades nos ciberataques. A avaliação das suas consequências microeconómicas e macroeconómicas levanta questões de mensuração de danos problemáticas, quer por falta de informação relevante, quer por dificuldade de estabelecer critérios adequados. Por outro lado, até agora, não tivemos nenhum ciberconflito em grande escala sustentado abertamente por atores estaduais. Aliás, em total rigor, os ciberataques até agora ocorridos, mesmo nos casos da Estónia e da Geórgia, não parecem configurar um ato de guerra face ao direito dos conflitos armados/direito internacional humanitário. Por isso, tudo o que se possa dizer sobre este assunto é, naturalmente, ainda um pouco especulativo e suscetível de revisão. Todavia, a revolução tecnológica e digital em marcha desde finais do século passado está, indiscutivelmente, a transformar a economia, a sociedade e a maneira de fazer a guerra. Tanto quanto é possível avaliar hoje, a tendência é para que o ciberespaço – entendido como a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores – se transforme, também, numa nova dimensão dos conflitos internacionais. Apesar das dificuldades de avaliação das reais consequências de uma genuína ciberguerra, é de recear que estas possam ser bem destrutivas para o normal funcionamento de sociedades complexas. R:I

NOTAS

1 LIBICKI, Martin – «Cyberdeterrence and Cyberwar», Rand Corporation, 2009, pp. 3-4. Disponível em: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

2 Para Michel Deyra, «apesar de as Nações Unidas utilizarem preferencialmente a expressão sinónima de "direito dos conflitos armados", a designação de direito internacional humanitário é a mais adequada, já que as disposições que integram esta disciplina constituem precisamente uma transposição para o direito das preocupações de ordem moral e humanitária. A expressão direito da guerra encontra-se atualmente abandonada a partir do momento em que caducou o conceito do estado de beligerância, ou pelo menos desde a adoção do princípio da proibição do recurso à força». In DEYRA, Michel – *Direito Internacional Humanitário*. Lisboa: Procuradoria-Geral da República, 2001, p. 15.

3 Adaptado de «Working towards rules for governing cyber conflict. Rendering the Geneva and Hague conventions in cyberspace». Nova York: The Eastwest Institute, 2011, p. 13.

4 ZIPPELIUS, Reinhold – *Filosofia do Direito*. Lisboa: Quid Juris, 2010, p. 23.

5 *Ibidem*, p. 23.

6 ARQUILLA, John, e RONFELDT, David – «Cyberwar is coming!». In *Comparative Strategy*. Vol. 12, N.º 2, 1993, p. 28.

7 Communications, Command, Control and Intelligence.

8 Indentification-Friend-or-Foe.

9 ARQUILLA, John, e RONFELDT, David – «Cyberwar is coming!», pp. 30-31.

10 *Ibidem*.

11 *Ibidem*, p. 31.

12 SAMPAIO, Fernando G. – *Ciberguerra. Guerra Electrónica e Informacional, Um Novo Desafio Estratégico*. Escola Superior de Geopolítica e Geoestratégia, 2001, pp. 3-4. Disponível em: http://www.defesanet.com.br/esge/ciberguerra.pdf

13 «A *leintenkrieg*, ou "guerra de controlo", é o mesmo que ciberguerra variando quanto ao uso do vocábulo alemão. Ambas as ideias, entretanto, estão relacionadas com um novo tipo de ope-

ração de guerra, que podemos chamar de uma variante da "guerra total" de Lundendorf, já que se trata de atacar não só as forças armadas mas também os civis. Talvez, até, a "ciberguerra" ou *leintenkrieg*, sejam a forma de "guerra total" que pode vir a ser aplicada ao século XXI, sendo que é evidente que o conceito abrange aquilo que os grandes teóricos da guerra, tanto Liddel Hart como Fuller, entendiam como "paralisação estratégica."» Cf. *Ibidem*.

14 *Ibidem*.

15 *Ibidem*.

16 *Ibidem*.

17 *Ibidem*.

18 *Ibidem*.

19 *Ibidem*.

20 O termo *hacker* é aqui usado no seu sentido mais corrente atual, o qual tem, conforme já referimos, uma conotação negativa. Refere-se a alguém mais ou menos, dotado para a informática, mas que usa o seu conhecimento especializado para ações abusivas e/ou ilegais de acesso a outros computadores e redes, bem como para praticar atos maliciosos que podem produzir danos de dimensão variável.

21 Citado em SINKS, Michael A. – «Cyber warfare and international law», Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements, Air Command and Staff College/ Air University, Maxwell, Al, 2008, p. 5.

22 SOMMER, Peter, e Brown, Ian – «Reducing systemic cybersecurity risk». Paris, OECD/IFP-International Future Program Department, 2011, p. 5. Disponível em: http://www.oecd.org/dataoecd/3/42/46894657.pdf

23 *Ibidem*.

24 *Ibidem*.

25 Nas Convenções de Haia de 1907 foram estabelecidas as leis e costumes de guerra, os direitos e deveres dos estados neutros, ao regime dos navios de comércio, à transformação de navios de comércio em navios de guerra, à colocação de minas submarinas automáticas de contacto, etc.

26 Sobre as fontes do direito dos conflitos armados / direito internacional humanitário, cf. DEYRA, Michel – *Direito Internacional Humanitário*, pp. 19-24.

27 SOMMER, Peter, e Brown, Ian – «Reducing systemic cybersecurity risk», p. 5.

28 *Ibidem*.

29 *Ibidem*.

30 Termo em língua inglesa criado a partir da junção das palavras *net + citizen*, e que, em língua portuguesa, poderia ser traduzido como «cibercidadão».

31 CLARK, Richard A., e KNAKE, Robert K. – *Cyber War. The Next Threat to National Security*. Nova York: Harper Collins, 2010, pp. 147-148.

32 Cf. *Ibidem*.

33 *Ibidem*.

34 *Ibidem*, pp. 148-149.

35 *Ibidem*.

36 KLIMBURG, Alexander – «Mobilising cyber power». In *Survival*. Vol. 53, N.º 1, fevereiro-março de 2011, pp. 41-60.

37 *Ibidem*, p. 41.

38 *Ibidem*, p. 42.

39 *Ibidem*.

40 Cf. RAGAN, Steve – «Fannie Mae logic bomb creator found guilty». In *The Tech Herald*, 7 de outubro de 2010. Disponível em: http://www.thetechherald.com/article.php/201040/6256/Fannie-Mae-logic-bomb-creator-found-guilty. Cf. também DVORAK, John C. – «The curious case of Rajendrasinh B. Makwan». In *Market Watch*, 30 de janeiro de 2009. Disponível em : http://www.marketwatch.com/story/the-curious-case-of-rajendra-sinh-b-makwana

41 Para o apagamento de páginas na *web* normalmente são exploradas falhas presentes na própria página ou nas aplicações da *web* , ou então é aproveitada uma falha de exploração do servidor onde a página está alojada. Na maioria dos casos, os sítios são afetados apenas na sua página inicial, sendo esta tipicamente totalmente apagada e/ou substituída por uma mensagem. Todavia, o apagamento da página em si mesmo não acarreta a perda dos dados. Para dados estatísticos sobre o apagamento de páginas *web* cf. ALMEIDA, Marcelo – «Defacements statistics 2008-2009–2010». In *Zone-h*, 27 de maio de 2010, Disponível em: http://www.zone-h.org/news/id/4735.

42 KLIMBURG, Alexander – «Mobilising cyber power», p. 42.

43 *Ibidem*, p. 43.

44 *Ibidem*, p. 45.

45 *Ibidem*.

46 *Ibidem*.

47 *Ibidem*, p. 46.

48 *Ibidem*.

49 *Ibidem*, p. 50.

50 *Ibidem*, p. 52.

51 *Ibidem*, p. 54.

52 CASHELL, Brian *et al*. – «The economic impact of cyber-attacks». crs Report for Congress, The Library of Congress, 2004. Disponível em: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

53 *Ibidem*.

54 *Ibidem*, p. 13.

55 *Ibidem*, p. 15.

56 *Ibidem*.

57 *Ibidem*, pp. 32-33.