Guerra cibernética precisa urgentemente de definição na doutrina

As cotidianas reportagens a respeito do que parece estar se consolidando como um novo tipo de conflito entre os países sugere que o tema não pode mais ser evitado ou menosprezado. Expressões como corrida armamentista virtual, guerra fria no ciberespaço, "*pearl harbor* eletrônico", "11 de setembro digital" e "*cibergedom*" deixam de parecer especulações para ocupar espaço entre as questões relevantes para todos os países.

Exemplo disso é o relatório[1] recentemente divulgado pela empresa de segurança da informação McAfee, do que supostamente seria a mais ampla série de ataques cibernéticos do mundo – o qual poderia ter um protagonista estatal na sua origem sem indicar qual – envolvendo espionagem de mais de setenta organizações, governos e empresas nos últimos cinco anos. Especialistas apontam para a China como possível responsável pelos ataques [2].

Em junho de 2011[3], diversos portais governamentais brasileiros, como da Presidência da República, da Receita Federal e da Petrobras, foram alvos de ataques cibernéticos assumidos pelo grupo Lulz Security Brazil, um braço do grupo internacional que também já teria invadido servidores da agência de inteligência e da polícia federal americanas, a CIA e o FBI, respectivamente. O grupo afirmou, no Twitter, que o ataque seria um protesto contra a corrupção e o aumento dos combustíveis. No mesmo período, o grupo Fatal Error Crew[4], que já havia atacado o portal da Presidência em janeiro de 2011, divulgou o endereço de 500 portais de prefeituras e câmaras municipais atacadas. Em audiência pública realizada em julho de 2009 pela Câmara dos Deputados[5], Raphael Mandarino Júnior, diretor de segurança da informação do Gabinete de Segurança Institucional da Presidência da República, relatou que uma quadrilha do Leste Europeu invadiu um servidor de computadores de um órgão público, trocou a senha e pediu um resgate de US$ 350 mil para devolver a senha antiga, o que não ocorreu porque o controle foi recuperado.

Em outubro de 2010, o vírus "stuxnet", supostamente desenvolvido pelos governos israelense e americano[6], foi infiltrado, possivelmente por um *pen drive*, nos sistemas do reator nuclear de Bushehr, no Irã, construído pela Rússia, com a finalidade de inutilizar centrífugas aumentando sua rotação enquanto sinais de normalidade eram enviados para o controle. O episódio afetou o projeto nuclear iraniano e por isso é amplamente noticiado como espécie de ataque de guerra cibernética.

Os ataques sofridos pela Estônia[7], país amplamente informatizado, em 2007, deflagrado pela remoção de um memorial de guerra da era soviética de uma praça da capital Tallinn, culminou com uma série de ataques cibernéticos dirigidos contra portais do governo, da imprensa e de empresas privadas, causando um "blackout" na internet estoniana por várias semanas. Levou meses para ser totalmente superado. Os ataques foram atribuídos à Rússia – que oficialmente negou a acusação -, mas tiveram origem em diversos locais, incluindo supostos provedores do governo russo. Razão pela qual o episódio é considerado a primeira guerra cibernética, embora não declarada. Tal episódio, sem precedentes, levou a OTAN – Organização do Tratado do Atlântico Norte a enviar especialistas em terrorismo virtual à Estônia para auxiliar nas investigações e a criar o Centro de Excelência para a Cooperação em Defesa Cibernética, em maio de 2008, na Estônia[8]. Ataques similares à Geórgia, em 2008[9], também

atribuídos e não reconhecidos pela Rússia, ocorreram poucas semanas antes e durante um conflito entre os dois países, também causaram um apagão cibernético, afetando agências governamentais e infraestruturas tecnológicas pouco antes da chegada dos russos.

Em setembro de 2007, Israel realizou ataque aéreo à Síria[10] para bombardear uma suposta usina nuclear que seria construída com a Coréia do Norte; o governo israelense teria se infiltrado no sistema de defesa aérea da Síria, porque os aviões israelenses não foram detectados por radares, o que possivelmente ocorreu em razão da utilização de programas específicos para burlar os sistemas sírios de controle de tráfego, que transmitiram sinais falsos.

Também em 2007, a China[11] foi acusada de atacar redes governamentais, instalando programas (*trojan horses*) no sistema de e-mails do Departamento de Defesa americano, no Pentágono, nos computadores do governo da Inglaterra, nos computadores dos ministros e da chanceler alemã Angela Merkel. A China negou as acusações, mas admitiu que seus programas contemplam a utilização de computadores em eventuais ações militares. Recentemente, em maio de 2011, hackers chineses afirmam ter invadido o sistema da rede elétrica da Letônia[12].

A Coreia do Norte é apontada como responsável pelos ataques realizados em julho de 2009 contra sites governamentais, de instituições financeiras e de imprensa nos Estados Unidos e na Coréia do Sul, manipulando aproximadamente 40 mil "computadores zumbis"[13].

Além dos poucos exemplos, aleatoriamente citados apenas para ilustrar os possíveis conflitos no espaço cibernético envolvendo governos, milhares de ocorrências similares ocorrem diariamente no mundo, o que explica porque o tema está nas prioridades da agenda mundial, com diversos países e organizações internacionais preocupadas com o assunto e implantando estruturas e estratégias de defesa e segurança cibernética.

O ambiente cibernético pode ser considerado um novo domínio ou palco de batalha, depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético. Os contornos da guerra cibernética, todavia, contemplam fatores e variáveis diversos que exigem novos raciocínios de defesa, pois as hostilidades no ambiente cibernético podem se desenrolar de formas distintas, que nem sempre permitem identificar o oponente e seus objetivos, a real origem, muito menos o momento e o impacto do ataque. Por isso, embora alguns conceitos da guerra cinética possam ser aplicados à guerra cibernética, outros chegam a ser antagônicos, embora seja certo que os efeitos de um ataque cibernético possam ser tão ou até mais nefastos quanto os de uma guerra convencional se afetarem as infraestruturas críticas de um país [14].

Em tal cenário, despontam intrincados desafios decorrentes do caráter transnacional e do entrelaçamento de diferentes ordenamentos jurídicos pelos mecanismos de funcionamento do espaço cibernético[15], cuja dinâmica nem sempre segue a lógica de fronteiras, território e soberania – conceitos a serem repensados particularmente para a solução de conflitos e para o combate aos crimes, as quais estão se multiplicando na medida em que as frestas e falhas sistêmicas estão sendo percebidas e utilizadas para a espionagem comercial e industrial e para a prática de crimes que o mundo inteiro conhece, mas tem dificuldade para definir e combater.

Se por um lado alguns países estão dialogando na tentativa de estabelecer normas internacionais para propiciar segurança jurídica e estabelecer regras de cooperação no combate e na investigação dos ilícitos cibernéticos, por outro, paradoxalmente, também estão aumentando as ameaças e ataques entre diferentes países com o emprego de tecnologias da informação, assim deflagrando um possível novo tipo de guerra que exige o desenvolvimento de novas estratégias de segurança, defesa e ataque.

De acordo com o glossário das Forças Armadas[16], guerra cibernética é "o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil." Trata-se, portanto, de operações defensivas ou ofensivas realizadas no espaço cibernético. É diferente da guerra eletrônica, definida como "o conjunto de ações que visam explorar as emissões do inimigo, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas."

Uma característica atribuída à guerra cibernética é a assimetria, pois um pequeno grupo de pessoas, ou mesmo um único indivíduo detentor de informações e conhecimentos específicos, com poucos recursos, pode representar uma grande ameaça a uma organização ou a um Estado, elos mais fortes, porém mais vulneráveis na medida em que seu gigantismo e complexidade podem dificultar um controle constante e efetivo de seus sistemas e ativos de informação. Além disso, pode ser difícil identificar o inimigo, porque além da relativização das distâncias, a lógica do espaço cibernético está vinculada a aspectos técnicos e não geográficos. Os bits podem percorrer grandes distâncias, passando por diversos territórios, em pouco tempo, dificultado o rastreamento e a identificação da origem e autoria de um ataque cibernético.

Existe uma corrente que não reconhece a existência da guerra cibernética, porque, em termos legais, o estado de guerra pressupõe uma declaração, não obstante seja reconhecida a necessidade das medidas de segurança para combater outros crimes e espionagem[17]. Richard Clarke[18], autor da obra *Cyber War: the next threat to national security and what to do about it*, responsável pela estratégia de combate ao terrorismo cibernético no Governo Bush e pelo estudo que levou Barack Obama a criar o comando de defesa cibernética, afirma que, se um país declarar guerra contra o outro, os ataques cibernéticos ocorrerão com a frequência de uma guerra comum e serão utilizados, por exemplo, para derrubar redes elétricas[19]. Na sua definição, "*cyber warfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls*."[20]

A guerra cibernética de que ora se trata, portanto, diz respeito aos conflitos que podem envolver diferentes países, algo diverso dos atos criminosos ou terroristas que podem ser praticados no espaço cibernético, não obstante seja bastante provável que qualquer país que pretenda realizar uma ofensiva contra outro busque camuflar suas ações como tais, razão pela qual os temas podem estar conectados,

embora sejam distintos.

O fato é que ainda não existem definições e doutrina consolidadas, muito menos normas jurídicas a respeito da guerra cibernética. Não obstante, o fato é que os países estão se mobilizando para desenvolver novas estratégias de defesa e segurança porque alguns eventos envolvendo o espaço cibernético já foram suficientes para evidenciar não apenas as vulnerabilidades, mas também o efetivo potencial das ameaças cibernéticas para colocar em risco a segurança dos países e estremecer as relações internacionais.

Desafios estratégicos e jurídicos

Com a crescente dependência tecnológica, é possível observar que a defesa e a segurança do espaço cibernético são questões cada vez mais estratégicas, sendo certo que nenhum país pode prescindir da capacidade de dissuasão, enfrentamento e neutralização das ameaças cibernéticas para preservar sua soberania e autodeterminação, o que é cada vez mais desafiador em razão da relativização das fronteiras e do território em tal contexto.

Para enfrentar adequadamente o problema, tão importante quanto aumentar os investimentos é desenvolver doutrinas e capacidade crítica suficiente para saber diferenciar as especulações e os oportunismos das efetivas ameaças e, assim, ser possível avaliar a real demanda, a confiabilidade da cadeia de fornecimento e a eficiência dos recursos investidos, discernimento que é fundamental para o adequado tratamento de cada situação, ainda que elas possam se confundir muitas vezes.

Além disso, é indispensável gerar sinergia entre as soluções tecnológicas com os componentes humanos, com a capacitação e adequada formação de agentes públicos, civis e militares, especialmente de servidores e fornecedores de produtos e serviços estratégicos, que são alvos de investigação bastante previsíveis na preparação de ataques cibernéticos.

Com base em tais premissas, os países estão organizando estruturas para aumentar a defesa e a segurança dos seus interesses e da sua soberania no espaço cibernético, desenvolvendo doutrinas militares e inteligência cibernética, até porque qualquer ataque é preparado com antecedência, como salienta Richard Clarke, segundo o qual “os países já estão se infiltrando nas redes uns dos outros, e instalando ‘portas dos fundos’, para terem acesso rápido a essas redes quando precisarem”, pois “para realizar um ataque cibernético é preciso fazer com que os trens parem, que a água deixe de ser bombeada, que oleodutos explodam, que a energia seja cortada. Para fazer essas coisas na hora em que você deseja, é preciso ter invadido as redes. Se o presidente disser a você que quer fazer tal coisa, não é possível começar naquele dia e tentar invadir as redes”.

No Brasil, o setor cibernético é definido como estratégico e essencial na Estratégia de Defesa Nacional, de 2008[21], segundo a qual as capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares e incluirão como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Além de enfatizar que, como decorrência de sua natureza, o setor cibernético transcende a divisão entre defesa

e desenvolvimento, civil e militar, também prevê a Estratégia Nacional de Defesa a necessidade de aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do Gabinete de Segurança Institucional da Presidência da República.

O encargo de coordenar e integrar as ações de defesa cibernética nas Forças Armadas foi atribuído ao Exército pela Diretriz Ministerial n° 14, de 2009. Em agosto de 2010 foi ativado o Núcleo do Centro de Defesa Cibernética (CDCiber). Iniciativas semelhantes já existem em diversos outros países, como os Estados Unidos (USCybercom), Alemanha, Reino Unido, Suíça, Suécia, China, Taiwan, Israel, Rússia, Estônia, Coréia do Norte, Coréia do Sul, Irã, etc.

O Livro Verde sobre segurança cibernética no Brasil[22], elaborado em 2010 pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, descreve o cenário atual e estabelece as diretrizes para a futura elaboração do Livro Branco da Política Nacional de Segurança Cibernética, sendo interessante destacar a proposta de fomentar articulação de acordos internacionais para potencializar a segurança cibernética no País e a capacidade de defesa e dissuasão, bem como a de elaborar a Política Nacional de Segurança das Infraestruturas Críticas, já existindo o Guia de Referência para a Segurança de Infraestruturas Críticas da Informação [23].

Diversos outros órgãos governamentais de alguma maneira interagem constantemente nas questões relacionadas à defesa e à segurança cibernética, tais como o Departamento da Polícia Federal, a Agência Brasileira de Inteligência, o Comitê Gestor da Internet, etc.

Mas, se por um lado, assim como o Brasil, os demais países estão elaborando estratégias de segurança e defesa cibernética, por outro, a comunidade internacional ainda está no estágio embrionário das discussões relativas às normas que devem reger a ameaça mundial do Século XXI, sendo certo que os desafios jurídicos são tão complexos quanto os estratégicos.

As dificuldades existentes na construção de um marco legal para a cooperação e combate ao terrorismo e aos crimes cibernéticos – tal como a Convenção de Budapeste, que está sendo rediscutida sob a coordenação do Embaixador brasileiro em Viena – são potencializadas na discussão das possíveis regras aplicáveis à guerra cibernética, na medida em que a questão envolve outras conseqüências no plano das relações internacionais.

Recentemente, o Departamento de Defesa dos Estados Unidos anunciou[24] sua primeira estratégia formal de defesa cibernética na qual um ataque cibernético oriundo de outro país, que comprometa estruturas críticas, cause mortes, prejuízos, destruição ou transtornos de algo nível, poderá ser interpretado como ato de guerra e, valendo-se do conceito da equivalência, motivar a resposta com a utilização de força militar convencional. A OTAN está alinhada com tal pensamento, justificando que um ataque cibernético contra uma infraestrutura crítica de um país membro pode ser equivalente a um

ataque armado e justificar a retaliação, inclusive medidas de defesa coletiva prevista na sua criação.

A guerra cibernética também foi debatida na última reunião do G8[25], e a Organização das Nações Unidas, além de elaborar uma nova Convenção de caráter global contra o crime cibernético, também já se manifestou favorável a um acordo internacional similar a um tratado para não proliferação de armas virtuais, um acordo de paz preventivo a uma guerra cibernética[26].

As constantes inovações tecnológicas e a dinâmica do espaço cibernético, no qual as distâncias e os conceitos de território, fronteiras e soberania são relativizados, bem como a assimetria que caracteriza a guerra cibernética, constituem desafios adicionais à dificuldade para estabelecer estratégias e regras para disciplinar não apenas a cooperação internacional nas investigações e no combate aos crimes e terrorismo cibernético, cuja regulamentação por si só já é complexa, mas também as regras que deverão reger os possíveis conflitos entre países no espaço cibernético, pois os conceitos da Carta da ONU a respeito da legitimidade ou não do uso da força em casos de legítima defesa ou da intervenção preventiva precisam de adaptação para a nova realidade das relações internacionais.

Por tais razões, é mais do que urgente e relevante estabelecer um consenso mínimo para a criação de regras dotadas de um mínimo de efetividade que estabeleçam parâmetros de ataque e defesa legítimos, ainda que seja difícil fazer tal diferenciação no espaço cibernético.

[1] http://www.nytimes.com/2011/08/04/technology/security-firm-identifies-global-cyber-spying.html, acesso em 04.08.2011.

[2] http://oglobo.globo.com/tecnologia/mat/2011/08/03/descoberta-maior-serie-de-ataques-hackers-da-historia-925053068.asp, acesso em 04.08.2011.

[3] http://www.teletime.com.br/22/06/2011/hackers-declaram-guerra-virtual-as-paginas-do-governo/tt/229147/news.aspx, acesso em 31.07.2011.

[4] http://www.istoe.com.br/reportagens/143548_BRASIL+SOB+ATAQUE+DE+HACKERS, acesso em 31.07.2011.

[5] http://www.conjur.com.br/2009-ago-23/redes-computadores-governo-sofrem-mil-ataques-hora, acesso em 31.07.2011.

[6] http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all, acesso em 30.07.2011.

[7] http://www.guardian.co.uk/russia/article/0,,2081438,00.html, acesso em 30.07.2011.

[8] http://www.ccdcoe.org/, acesso em 29.07.2011.

[9] http://georgiaupdate.gov.ge/doc/10006922/CYBERWAR-%20fd_2_.pdf, acesso em 30.07.2011.

[10] http://revistagalileu.globo.com/Revista/Common/0,,ERT198270-17773,00.html, acesso em

30.07.2011.

[11] http://veja.abril.com.br/120907/p_078.shtml, acesso em 31.07.2011.

[12] http://g1.globo.com/tecnologia/noticia/2011/05/hackers-chineses-dizem-ter-invadido-rede-eletrica-da-letonia.html, acesso em 31.07.2011.

[13] http://revistagalileu.globo.com/Revista/Common/0,,ERT198270-17773,00.html, acesso em 30.07.2011.

[14] Assim compreendidas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado, da sociedade e do mercado *www.gsi.gov.br/**infraestruturas–criticas**/conceitos, acesso em 31.07.2011*.

[15] Na definição de Raphael Mandarino JR, “a infraestrutura crítica da informação, à qual está vinculada a segurança da informação e comunicações, compreende, então, todos os hardwares, softwares e equipamentos que se interconectam, por fibras óticas ou pelo espectro eletromagnético. Compreende, também, os locais de armazenagem, processamento e transmissão de toda a informação, além da própria informação. As pessoas que interagem com a infraestrutura também são objeto de medidas de segurança da informação e comunicações. Esse todo forma um conjunto de partes virtuais ou partes físicas. O complexo virtual aí formado compõe o chamado cyberspace, ciberespaço ou espaço cibernético.” (Segurança e Defesa do Espaço Cibernético brasileiro. Recife: Editora Cubzac, 2010, pág. 64).

[16] Ministério da Defesa, Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007 (MD35-G-01, 4ª Edição/2007).

[17] http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/, acesso em 28.07.2011.

[18] http://www.richardaclarke.net/, acesso em 25.07.2011.

[19] http://www.conjur.com.br/2011-mar-11/ideias-milenio-ataques-ciberneticos-tornaram-armas-guerra , acesso em 25.07.2011.

[20] http://www.richardaclarke.net/cyber_war.php?ch=7#excerpts, acesso em 28.07.2011.

[21] http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf , acesso em 31.07.2011.

[22] http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf, acesso em 25.07.2011.

[23] http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf, acesso em 31.07.2011.

[24] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=rss_whats_n

, acesso em 31.07.2011.

[25] http://www.observatoriodaimprensa.com.br/news/view/a-guerra-fria-de-bits-e-bytes, acesso em 31.07.2011.

[26] http://www1.folha.uol.com.br/folha/informatica/ult124u687650.shtml, acesso em 28.07.2011.

No mesmo sentido, o Project of the International Convention on Prohibition of Cyberwar:

http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.

Date Created
06/08/2011