Ciberespaço, ciberviolência e o uso organizado da força

Paulo Viegas Nunes

O CIBERESPAÇO, tendo como porta de acesso a internet, tornou-se um verdadeiro mediador das relações sociais e um motor do desenvolvimento económico dos países mais desenvolvidos. Assumindo-se como *global common*, o ciberespaço não tem fronteiras definidas. O espaço físico perde significado e a comunicação entre os homens passa a ser dirigida pelo tempo de interação, num espaço virtual onde a informação está disponível *online*, independentemente do local e da hora do dia.

Num mundo hiperconectado, o ciberespaço é hoje palco de ataques lançados contra indivíduos, empresas, redes públicas ou privadas, infraestruturas críticas ou mesmo contra os sistemas de governação eletrónica do Estado.

Ciberameaças e gestão do risco social

Apesar do inegável valor associado ao ciberespaço e à internet, diferentes atores têm vindo a explorá-los de forma maliciosa para atacar a disponibilidade, integridade, autenticidade e confidencialidade da informação que circula em rede. Só a análise das capacidades dos atacantes e a avaliação da probabilidade de um ciberataque permitirá perceber como este pode afetar as infraestruturas de informação, quer individualmente, quer de forma agregada. Dependendo do impacto estimado, estes ataques podem configurar um risco social e colocar em risco as infraestruturas críticas, consideradas vitais para a sobrevivência do Estado.

Entre as fontes de ciberameaças, identificam-se funcionários insatisfeitos, amadores, *hackers*, *crackers*, cibercriminosos, espiões de segredos industriais, hactivistas, terroristas e até Estados. As motivações dos atacantes são bastante variáveis e estão associadas aos objetivos a atingir. Por sua vez, estas ciberameaças (Denning, 1999; Nunes, 2010) podem assumir a forma de intervenção social (ciberativismo, ciberhacktivismo), ações criminosas (*hacking*, *cracking*, cibercrime, ciberespionagem ou ciberterrorismo) ou mesmo a forma de atos de guerra (ciberguerra).

Devido ao impacto estratégico das ciberameaças, a gestão do risco social associado ao ciberespaço influencia cada vez mais a segurança e defesa dos Estados. Os ciberataques podem vir a configurar uma situação de uso da força e até um potencial ato de guerra.

Moderna conflitualidade e a militarização do ciberespaço

Os ciberataques podem ter origem em qualquer parte do mundo, são baratos, fáceis de lançar e apresentam grande eficácia, sem que muitas vezes seja possível detetar a verdadeira identidade do atacante. Os ciberataques têm ainda como vantagem estratégica o facto de apresentarem um impacto menor na opinião pública que as tradicionais formas cinéticas de conflito ou guerra.

Se um ataque cibernético atingir exclusivamente recursos e sistemas de informação, podemos dizer que estamos perante um ataque não cinético. No entanto, a maior parte destes ataques afeta também sistemas e infraestruturas físicas. Neste caso, apesar de lançado de forma virtual (não cinética), o ciberataque pode ser considerado um ataque cinético, uma vez que origina, em maior ou menor grau, a disrupção e/ou destruição de sistemas físicos.

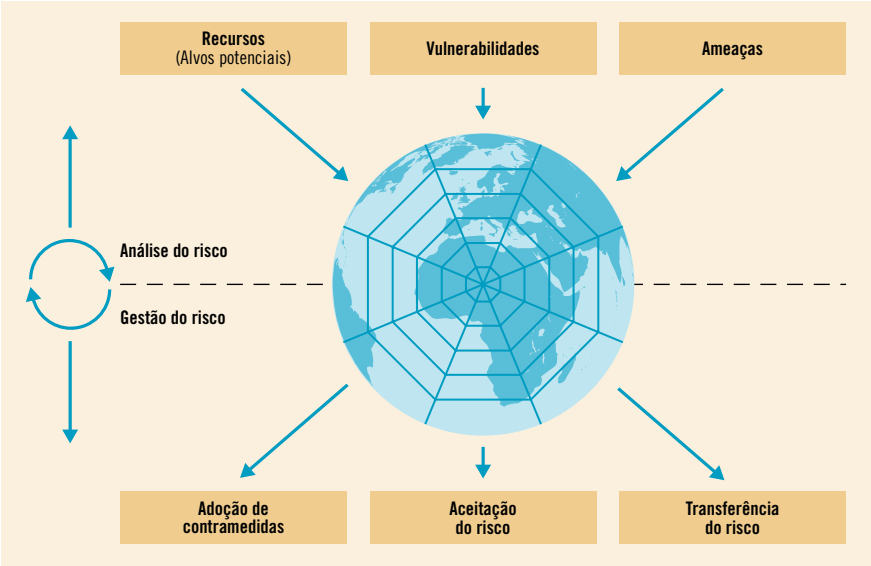
As estratégias de poder de alguns Estados têm vindo a ser contrariadas, cada vez mais frequentemente, por operações de "contraestratégia" conduzidas por atores não-Estado. Em linha com esta visão, a internet tem vindo a constituir um autêntico campo de batalha digital, sendo palco de constantes ações de retaliação entre *hackers* associados a diversos países e atores estratégicos. Ainda que estas atividades não configurem, na maior parte dos casos, um envolvimento direto dos mesmos, são vários os casos já detetados de redes de *hackers* associadas a atores Estado.

A recente ocorrência de ciberataques lançados contra Estados soberanos fez com que muitas das grandes potências mundiais tenham desenvolvido capacidades de recolha e análise de informações à escala global, nomeadamente com a justificação de que estas se tornam imprescindíveis à segurança e defesa nacional. O programa PRISM[1], tornado recentemente público por Edward Snowden (ex-funcionário da NSA), constitui um bom exemplo deste tipo de sistemas. O caso "*WikiLeaks*"[2], em que foram revelados documentos secretos é apontado como uma motivação para o seu levantamento.

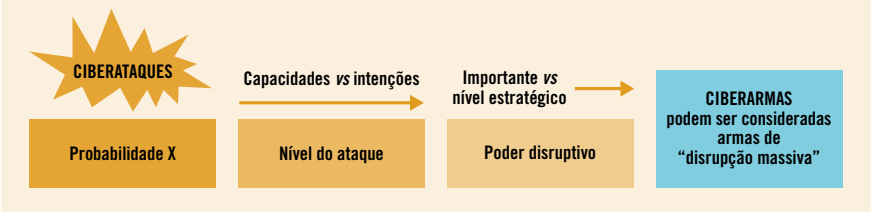
Um ciberataque poderá ser lançado para criar as condições ideais ou para maximizar os efeitos de um ataque militar convencional, como aconteceu em 2008 no caso da Geórgia. Este tipo de ações militares levaram os EUA à recente criação do *US Cyber Command*, passando a assumir o ciberespaço como um novo domínio operacional, onde podem vir a ser conduzidas operações militares[3]. A crescente militarização da internet suscita assim uma preocupação redobrada, pois não é possível ignorar que os ciberataques lançados ou patrocinados por Estados são os que apresentam um maior poder disruptivo.

Alguns autores (Rid, 2011) assumem a ciberconflitualidade como algo permanente, encarando-a não como atos de guerra, mas como atos de sabotagem, espionagem ou subversão, afirmando que a "ciberguerra não terá lugar". No entanto, apesar de tendermos a concordar que as "ciberameaças vieram para ficar", teremos de atribuir à ciberguerra, no mínimo, a mesma probabilidade de ocorrência que a qualquer outro conflito cinético.

No ambiente estratégico atual, nenhuma guerra



Modelo de análise e gestão do risco. Fonte: Autor.



Impacto estratégico das ciberarmas. Fonte: Autor.

poderá ser ganha exclusivamente com a utilização militar do ciberespaço (ciberguerra pura). No entanto, também é certo que nenhuma campanha militar conduzida noutro qualquer domínio operacional poderá ser ganha sem o ciberespaço.

Conflitos armados no ciberespaço

Um ataque cibernético é uma ação de contornos agressivos, cujos efeitos se fazem sentir tanto no mundo virtual como real. Um ciberataque pode consubstanciar um uso efetivo da força e constituir, por essa razão, um ato de violência. Neste âmbito, importa reconhecer que um ataque armado é a forma mais grave de uso da força, mas que nem todo o uso da força constitui um ataque armado. Desta forma, um ciberataque que cause uma interrupção pontual de serviços não essenciais não pode ser considerado um ataque armado. No entanto, se este originar estragos sérios e de longo prazo em infraestruturas críticas ou serviços essenciais para a sobrevivência de um Estado, considera-se que estamos perante um ataque armado no ciberespaço. Constituindo um conflito armado no ciberespaço, para todos os efeitos, uma guerra conduzida no ciberespaço, a legislação que rege os conflitos armados (*jus in bello*) também terá que ser aplicada.

> “Os ciberataques podem vir a configurar uma situação de uso da força e até um potencial ato de guerra.”

Neste tipo de situações, o direito à legítima defesa e a possibilidade de retaliação por parte do Estado atingido confronta-se com o problema da atribuição, nomeadamente porque um ataque armado no ciberespaço poderá constituir um *causus belli*. Neste contexto, importa clarificar quem exerce o ónus da prova, qual o grau de probabilidade existente quanto à identidade do atacante e como será possível provar que um determinado Estado se encontra por trás de um ciberataque.

O princípio da distinção (militar ou civil) e o princípio da neutralidade também constituem fatores importantes a considerar nos ciberataques. Se, à luz do direito que rege a guerra, os ataques só podem ser dirigidos contra combatentes e ter por alvo objetivos militares, no caso dos ciberconflitos muitos dos atacantes não são militares e os recursos utilizados pelas Forças Armadas são hoje de duplo-uso civil-militar. A existência de um nexo de causalidade entre uma ação e o seu potencial impacto negativo poderá conferir o estatuto de beligerante a indivíduos ou grupos civis que conduzam operações no ciberespaço.

O princípio da neutralidade poderá também vir a ser desafiado pelos ciberconflitos pois estes são conduzidos num espaço aberto e sem fronteiras físicas, onde não é possível aplicar os princípios tradicionais de jurisdição e exercício de soberania. Se um Estado neutral não conseguir impedir que um dos beligerantes lance um ciberataque através do seu território e esse ataque constituir uma ameaça séria e eminente para outro Estado, poderá perder o seu estatuto de neutralidade e ver-se envolvido diretamente no conflito.

Todos os Estados terão assim que ter uma cibercapacidade credível para poderem assegurar o direito a afirmar a sua neutralidade. A incapacidade poderá, neste caso específico, ser assumida como um sinal de favorecimento de uma das partes, comprometendo o estatuto de neutralidade que se pretende assumir e afirmar.

Visão estratégica para um futuro digital mais seguro

A persecução violenta de objetivos políticos utilizando exclusivamente o ciberespaço não se coloca atualmente mas não poderá deixar de ser perspetivada no futuro, sob pena de se vir a comprometer a estabilidade do sistema político internacional. Para reduzir a conflitualidade e aumentar o nível de proteção das infraestruturas críticas de informação, os países têm que rever o atual quadro legal, criar novas doutrinas, estruturas e meios para implementar a sua estratégia nacional de cibersegurança e ciberdefesa.

Atendendo às dinâmicas competitivas e conflituais que têm lugar no ciberespaço, importa construir os fundamentos de uma base geradora de confiança e de um código de conduta, de forma a potenciar um modelo de utilização do ciberespaço cada vez mais livre e aberto, mas também mais seguro e protegido. Só assim será possível aproximar as diferentes legislações nacionais e convergir para a criação de uma base jurídica comum, facilitando o combate ao cibercrime e a redução da ciberconflitualidade, tanto num plano nacional, como internacional. Uma vez que o ciberespaço constitui um domínio estratégico prioritário de defesa de valores e interesses nacionais (não alienável), a construção de um futuro digital para Portugal passa inevitavelmente por explorar sinergias nacionais e a cooperação internacional de forma a garantir em permanência a segurança e defesa do ciberespaço. Nesse sentido, atentos às estratégias emergentes de projeção de poder e aos novos vetores de uso da força no ciberespaço, importa avaliar as implicações da ciberviolência e da ciberguerra na sociedade pós-moderna, aprofundando assim uma cultura de cibersegurança e ciberdefesa. ■

ENQUADRAMENTO LEGAL DA CIBERVIOLÊNCIA E DO USO DA FORÇA

As referências legais que regulam os conflitos entre Estados desde a II Grande Guerra Mundial são a Carta das Nações Unidas (ONU,1945) e a Convenção de Genebra (CG,1949). A Carta das Nações Unidas, legitima o recurso ao uso da força por parte dos Estados (o *jus ad bellum*) ao passo que a Convenção de Genebra, a principal fonte de direito humanitário internacional, regula a condução dos conflitos armados e é vista como a Lei da Guerra (o *jus in bello*).

Como ação de contornos agressivos, um ciberataque pode refletir um uso efetivo da força e constituir, por essa razão, um ato de violência. Para caracterizar uma situação de uso da força no ciberespaço, o Manual de Tallinn (CCD COE, 2013) aponta oito critérios de eligibilidade: severidade, imediatez, direcionamento, capacidade invasiva, mensurabilidade dos efeitos produzidos, carácter militar, envolvimento de Estados e presumível legalidade.

O ciberataque à Estónia em 2007 não pode, à luz destes critérios, ser considerado um uso efetivo da força devido tanto às suas consequências (não letais) como à identificação do seu originador[1] (só foram identificados atores não-Estado). No caso do código malicioso *Stuxnet*, que em 2010 afetou o programa nuclear iraniano, a aplicação destes critérios aponta para o uso efetivo da força, se for provado que na sua origem esteve um Estado. No entanto, a menos que em autodefesa, a ação conduzida por esse Estado (não identificado) será considerada ilegal devido à ausência de autorização do Conselho de Segurança da ONU.

Quando um ciberataque constituir um “perigo grave e iminente” e ameaçar a sua soberania, um Estado pode invocar a necessidade de defesa para justificar a adoção de contramedidas. Neste caso, o Estado vítima poderá, de forma a poder defender-se, violar os direitos de outros Estados. A necessidade desta ação não requer a atribuição do ataque a outro Estado, podendo apenas ser invocada em circunstâncias excecionais e desde que não prejudique os interesses essenciais de outros Estados[2].

[1] A autoria deste ataque não foi oficialmente assumida mas tem vindo a ser atribuída à Rússia, supostamente em retaliação pela retirada da estátua de um soldado russo de um dos Jardins de Tallinn em 2007. [2] Aplica-se neste contexto o artigo 2º (4) e o artigo 51º da Carta das Nações Unidas (1945) que enquadra e legitima o direito à autodefesa individual e coletiva de um Estado membro da ONU (o *Jus ad Bellum*).

Notas

[1] PRISM é o nome de código atribuído a um programa secreto de vigilância eletrónica massiva lançado em 2007 pela *National Security Agency* (NSA), contando também com a participação da Agência Britânica GCHQ.

[2] WikiLeaks é uma organização internacional que, no seu *site* se intitula, *online*, não-lucrativa e jornalística, publicando informação secreta, notícias e fugas de informação provenientes de fontes anónimas. O *website* da organização foi fundado em 2006, na Islândia, pela organização ativista *Sunsbine Press*.

[3] A criação do *U.S. Cyber Command* foi anunciada em Junho de 2009. Este novo Comando Militar declarou ter adquirido a sua plena capacidade operacional em 03NOV10. As operações no ciberespaço podem atingir objetivos tanto no ciberespaço como nos outros domínios (mar, terra, ar ou espaço).

Referências

CCD COE (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*, NATO Cooperative Cyber Defense Centre of Excellence (CCD COE), Cambridge University Press, ISBN: 9781107613775, Abril 2013.

CG (1949). Convenção de Genebra (ratificada a 12 Agosto de 1949), tradução disponível em http://www.abong.org.br/final/download/DH.pdf, consultada em 18Dez13 às 20H17.

DENNING, Dorothy E., (1999). “*Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*”, Washington D.C., disponível por via electrónica em http://www.nautilus.org/info-policy/workshop/papers/denning.htm.

NUNES, Paulo (2010). “*Mundos Virtuais, Riscos Reais: Fundamentos para a definição da Estratégia da informação Nacional*”, Atas do I Congresso Nacional de Segurança e Defesa, Editora Diário de Bordo, Dezembro.

ONU (1945). Carta da Organização das Nações Unidas (ratificada a 26 Junho de 1945), tradução disponível em http://docentes.por.ulusiada.pt/rmmarr/CNU2003.pdf, consultada em 18Dez13 às 19H36.

RID, Thomas (2011). “*Cyber War Will Not Take Place, Journal of Strategic Studies*” 2011, pp. 1–28.

VIHUL, Liis (2013).“*Cyber Conflict and International Law – The Tallinn Manual*”, Conferência proferida em 04Dez13, ESDC, Bruxelas.