Ciberataques em tempos de guerra

Miguel Godinho
CCA Law Firm

1- Introdução

Quando no início do ano um grupo de *hackers* atacou um dos maiores grupos de comunicação social em Portugal, grande parte da população portuguesa experienciou pela primeira vez a disrupção que um ataque organizado no mundo virtual pode causar. A este ataque seguiram-se múltiplos outros publicamente divulgados a empresas e entidades públicas portuguesas, tendo inclusivamente afetado o *website* da Assembleia da República.

As motivações para estes ataques no ciberespaço são bastante variadas, podendo assumir a forma de (i) intervenção social (*ciberhacktivismo*); (ii) ações criminosas (*hacking*, *cracking*, cibercrime, ciberespionagem ou ciberterrorimo) ou mesmo (iii) atos de guerra ("ciberguerra" - *para quem admita a sua existência*)[1].

Quando os diferentes atores intervenientes procuram atacar a disponibilidade, a integridade, a autenticidade e a confidencialidade da informação que circula em rede com o objetivo de afetar as infraestruturas críticas e a segurança de um Estado, estamos já perante uma nova e complexa realidade de ataque à soberania, podendo ser enquadrada na terceira forma de intervenção mencionada.

Nesta senda, é importante entender e fazer a destrinça entre os termos "ciberataque", "uso da força" e "ciberguerra", muitas vezes indistintamente usados. A acrescer à complexidade da ausência de fronteiras no mundo virtual, ao anonimato dos agentes e à inerente dificuldade de imputação aos mesmos, os próprios conceitos de ciberataque e de ciberguerra não são consensuais, dividindo a doutrina há mais de trinta anos. Esta distinção não se apresenta apenas como mais um despiciendo debate doutrinário, mas acarreta verdadeiras consequências, tanto a nível de conduta dos Estados como de aplicação de normas legais nacionais e internacionais.

Tipos de ataques e ações utilizados

Focando no tipo de atos agressivos utilizados, são mais frequentemente identificados os seguintes métodos:

a. ***Ransomware***: tipo de *malware* que impede os utilizadores de aceder ao seu sistema ou ficheiros pessoais, exigindo um pagamento para restaurar o acesso.

b. ***Denial-of-service* (DoS) ou ataque de negação de serviço**: impede os utilizadores legítimos de aceder a um *website* ao sobrecarregá-lo com pedidos falsos e forçando-o a processar os mesmos. Este tipo de ataques pode ser utilizado para perturbar operações e sistemas críticos, bloqueando o acesso a *websites* sensíveis. É favorecido por certos Estados pela dificuldade de imputação da sua autoria, uma vez que poderá ser posto em prática por qualquer utilizador de computadores mediano, desde que fornecido das ferramentas corretas.[2][3]

c. **Ataque de exploração de rede, através de vírus, *phishing*, *worms* ou outro *malware*:** considerado um dos mais perigosos tipos de ciberataques[4] por envolver a colocação de ficheiros ou outros, elementos pequenos e escondidos, extremamente difíceis de localizar até que sejam ativados.

Ciberguerra – será mesmo uma realidade?

Como adiantado supra, a definição de guerra cibernética ou ciberguerra não é consensual, sendo discutida na literatura há várias décadas.

Em 2021, Ashraf, da análise que fez à literatura acerca da ambígua definição de ciberguerra[5], identificou e isolou três sentidos interpretativos: alarmistas, realistas e céticos. Em termos genéricos, entende como alarmistas os autores que consideram a ciberguerra como uma ameaça iminente, céticos aqueles que afirmam que a ciberguerra não existe e realistas os que procuram encaixar o conceito de ciberguerra dentro das normas e leis existentes.

Quando Arquilla e Ronfeldt procuraram encontrar uma definição de ciberguerra em 1993, fizeram-no por referência à ideia de conhecimento: ataques através da interrupção dos sistemas de informação e conhecimento nos quais o adversário se apoia para se conhecer[6].

Outros autores, céticos, consideram que o conceito de ciberguerra não existe, tratando-se de uma realidade delimitada a pequenos eventos e atos isolados de sabotagem ou espionagem, não podendo estes ataques ser classificados como atos de guerra[7].

Grande parte do debate doutrinário, contudo, foca-se na perspetiva realista de ciberguerra e na aplicabilidade do direito internacional e nacional ao ciberespaço.

1. Viegas Nunes Paulo, 'Ciberespaço, ciberviolência e o uso organizado da força' [2014] JANUS 2014 - Metamorfoses da violência 146
2. José Pedro Teixeira Fernandes, "A Ciberguerra como Nova Dimensão dos Conflitos Internacionais" [2012] (33) Relações Internacionais 53-69
3. Alexader Klimburg, "Mobilising Cyber Power" [2011] 53(1) Survival 41-60
4. Ibid.
5. Cameran Ashraf, 'Defining cyberwar: towards a definitional framework' [2021] 37(3) Defense & Security Analysis 274-294
6. John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!' [1993] 12(2) Comparative Strategy 141-165
7. Thomas Rid, 'Cyber War Will Not Take Place', [2012] 35(1), Journal of Strategic Studies 5–32

Um ciberataque poderá ou não configurar um uso efetivo de força, sendo um ataque armado a mais grave forma de uso de força. Assim, se um ciberataque causar uma interrupção momentânea de serviços não essenciais, não será de afirmar que houve um ataque armado ou uso de força. Por outro lado, se desencadear consequências e estragos graves a infraestruturas críticas para a sobrevivência de um Estado, estaremos já perante um verdadeiro ataque de guerra[8].

De acordo com esta perspetiva, estes ataques assim configurados terão de ser avaliados no âmbito do *jus ad bellum*, que determina os critérios em que é legítimo o recurso à força por parte de um Estado para agir em legítima defesa – regendo-se pela Carta das Nações Unidas. A partir do momento em que seja de considerar que a ciberguerra teve início, os ciberataques e as suas justificações terão de ser já abrangidos pelo *jus in bello* e pelas regras de condução de conflitos armados – plasmadas na Convenção de Genebra e demais normas de direito humanitário internacional.

Ciberataques no âmbito do conflito ucraniano de 2022

O número de ciberataques de grandes dimensões tem aumentado significativamente, tendo a Microsoft afirmado, num relatório publicado a 22 de junho de 2022[9], que detetou, desde o início da guerra, esforços russos para intrusão em redes de 128 organizações em 42 países fora da Ucrânia.

Frequentemente, os ataques cibernéticos surgem coordenados com os ataques físicos (cinéticos) – ataques híbridos –, o que também se verificou no conflito a decorrer entre a Rússia e a Ucrânia, tendo-se assistido a uma intensificação de tentativas de ataques no primeiro dia da invasão, com a aparente intenção de criar distúrbios e sobrecarregar as defesas ucranianas, procurando interromper serviços e instalar *malware* destrutivo nas redes[10].

Mais recentemente, os ciberataques com origem atribuída à Rússia têm sido coordenados com ataques de mísseis e visaram os sistemas e vias ucranianas de transporte de armas e material militar – por exemplo, quando as subestações ferroviárias em Lviv foram atingidas a 3 de maio já o grupo militar Iridium estava ativo dentro das redes digitais destas agências[11].

Porém, alguns peritos têm manifestado surpresa com a relativa ausência de ciberataques russos destrutivos neste conflito. Este impacto menos significativo está a ser atribuído a diversos fatores, nomeadamente a preparação da Ucrânia, que se tem vindo a familiarizar com estes ataques desde 2014, e o auxílio que o país tem tido de outras nações.

Poderá o Direito ter uma resposta definitiva?

A União Europeia tem tido uma resposta importante a estas ciberameaças desde 2016, tendo nesse ano entrado em vigor a Diretiva (UE) 2016/1148 (Diretiva SRI), que foi transposta para o ordenamento jurídico português pela lei n.º 46/2018. Nos anos seguintes, mais significativamente em 2022, impulsionada pelo conflito ucraniano, tem adotado um conjunto de medidas no sentido de reforçar a segurança cibernética europeia, sobretudo em setores críticos como energia e infraestruturas digitais. Em maio de 2022 foi anunciado um acordo relativamente à nova legislação destinada a substituir e reforçar a Diretiva SRI, procurando, desta forma, alcançar regras mínimas comuns entre os diferentes Estados-membros e mecanismos para uma cooperação eficaz entre as autoridades nacionais. Esta Diretiva SRI 2 vê alargada a sua aplicabilidade a entidades de média e grande dimensão de um maior número de setores críticos para a economia e para a sociedade, incluindo os prestadores de serviços públicos de comunicações eletrónicas, os serviços digitais, a gestão das águas residuais e dos resíduos, o fabrico de produtos essenciais, os serviços postais e de correio rápido e a administração pública, a nível central e regional[12].

Mais recentemente, a 21 de junho de 2022, adotou também o Conselho conclusões sobre o conjunto de instrumentos da UE contra as ameaças híbridas (*Hybrid Toolbox*), introduzindo uma série de princípios sob os quais se devem reger as respostas a estas ameaças.

Urge, por último, fazer uma distinção relativamente ao enquadramento jurídico relevante, dividindo os ataques entre aqueles atos que são imputáveis a um ou mais Estados e os que não são imputáveis a Estados[13]. Apenas relativamente aos primeiros são aplicáveis as normas internacionais respeitantes a conflitos entre Estados, na vertente do *jus ad bellum* e do *jus in bellum*.

Por sua vez, aos atos não imputáveis a Estados poderão ser aplicáveis todas as normas do panorama jurídico nacional em matéria de responsabilização pelos atos praticados por meios eletrónicos[14].

8. Viegas Nunes Paulo, 'Ciberespaço, ciberviolência e o uso organizado da força' [2014] JANUS 2014 - Metamorfoses da violência 147
9. Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War' (Microsoft on the Issues, 22-06-2022) <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>
10. James Andrew Lewis, Relatório sobre 'Cyber War and Ukraine' [2022], Center for Strategic & International Studies
11. Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War' (Microsoft on the Issues, 22-06-2022) <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>
12. Comunicado de Imprensa de 13 de maio de 2022, disponível em <https://ec.europa.eu/commission/presscorner/detail/pt/ip_22_2985>
13. Sofia de Vasconcelos Casimiro , Quadro Legal para a Cibersegurança e a Ciberdefesa. in Contributos para uma Estratégia Nacional de Ciberdefesa (Instituto da Defesa Nacional 2017) 47-63
14. Ibid.