O Poder da Informação no Poder Militar

Contra-almirante
António Gameiro Marques

Vivemos numa sociedade hiperconetada, onde cada vez existem mais dispositivos ligados à internet. As cidades, as instituições, as casas das pessoas, os veículos, estão cada vez mais repletos de sensores que, em tempo real, recolhem dados e metadados, para coletarem enormes quantidades de informação e assim construírem e coligirem conhecimento sobre cada um de nós, e para, em princípio, incrementarem a qualidade das nossas vidas. No entanto, fazem-no, amiúde, com fins maliciosos, que nos prejudicam enquanto seres humanos que temos a privacidade como direito fundamental.

Um veículo moderno tem mais de 30 endereços IP. Um ar condicionado tem um endereço IP para ser controlado remotamente pelo seu utilizador a partir da Internet. O mesmo se passa com vários equipamentos que podemos ter nas nossas casas. Mas, da mesma maneira que nós os podemos controlar a partir da Internet, outros também poderão, interferindo, desta forma, com a nossa vida e até com a nossa segurança, se esta não for acautelada desde o princípio, numa lógica de *security by design*.

Num contexto de guerra cinética, uma *smartbomb* moderna possui um endereço IP. Um navio de guerra tem vários e uma aeronave, seja ela tripulada ou não, também. Um carro de combate moderno está em rede com a força terrestre a que pertence e um soldado, projetado no terreno, tem associado um endereço IP da rede tática onde a operação se desenvolve. Por isso, podemos imaginar o que poderá ser feito por alguém que, mal-intencionado, ganhe acesso à rede ou a um destes dispositivos.

A informação que permanentemente é recolhida sobre o nosso comportamento enquanto seres humanos, sem que nós nos demos conta disso, é imensa, estando cada vez mais na ordem do dia os assuntos relacionados com a privacidade e o respetivo equilíbrio com a segurança. Ciente deste facto, a União Europeia publicou o Regulamento Geral de Proteção de Dados[1] que entrará em vigor em maio de 2018 em toda a União, e que tem como enfoque a proteção dos dados pessoais de todos as pessoas que vivem na Europa.

Estamos numa *Knowledge Intensive Society*, em que o conhecimento, providenciado pela informação que decorre da combinação dos dados com os respetivos metadados, tem um valor capital, sendo, hoje em dia, exfiltrada de grandes bases de dados para depois ser vendida ilegalmente ou encriptada e, posteriormente, ser exigido ao seu autor avultadas somas para recuperar o acesso à informação. A edição de maio de 2017 da prestigiada revista "The Economist"[2], refere que os dados são o recurso mais valioso do século XXI.

Figura 1 – "The Economist", edição de maio de 2017.

Mas, por causa de tudo isto, os predadores abundam, são cada vez mais sofisticados e

complexos e usam as mesmas aplicações e os mesmos segmentos de comunicação que nós utilizamos, só que para fins ilegítimos. Paralelamente, desenvolveu-se um sofisticado sistema de compra e venda de "armas cibernéticas" na *Dark Web*, levando a que aqueles predadores possam adquiri-las, mesmo que não as saibam utilizar. Basta que saibam em que é que as querem usar.

Com toda esta envolvente, e como o número de dispositivos ligado à rede é cada vez maior, a potencial superfície de ataque é também cada vez maior. E isso deve preocupar-nos, quer como cidadãos quer como militares, designadamente no contexto das operações que poderemos ser chamados a cumprir, em prol da defesa dos interesses de Portugal. É que, ainda que os registos de ataques deste tipo com efeitos cinéticos sejam de baixo número, a tendência será para o seu aumento. E se ocorrerem nas infraestruturas críticas que fornecem serviços essenciais às sociedades, então poderemos vir a ter problemas graves e bem tangíveis.

Feita esta introdução, centremo-nos, então, no tema fulcral desta reflexão: O poder militar – Poder Naval, Terrestre, Aéreo e da Informação, tentando responder à pergunta: qual a relevância do poder da informação na construção do poder militar?

John Collins define Poder Militar, no seu livro *Military Strategy* (tradução livre), como a "capacidade percecionada de dissuasão e de combate, que resulta de um equilíbrio de atributos existentes nas forças armadas de um determinado país ou coligação de países. Esses atributos estão associados com as características qualitativas e quantitativas das respetivas forças armadas, designadamente o número de efetivos, e de meios materiais, a forma como estão organizados e treinados, o moral, a disciplina, e a respetiva lealdade, a prontidão do pessoal e do material, a capacidade de sustentação e ainda a liderança e a estrutura e meios de C2". Refere o autor que o Poder Militar é inútil se não acompanhado da Vontade Nacional para o utilizar (Poder = Capacidade X Vontade) (poder é a capacidade dos que querem e podem agir sobre aqueles que não podem nem querem).

Por outro lado, a OTAN, no seu documento doutrinário "NATO INFORMATION MANAGEMENT POLICY", define o termo "Informação" como (tradução livre) "Qualquer comunicação ou representação de conhecimento, tais como factos, dados ou opiniões, apresentados em qualquer formato compreensível, incluindo a forma textual, numérica, gráfica, verbal ou audiovisual". Num contexto mais genérico, define-se informação como tudo o que decorre da contextualização dos dados que lhe dão origem.

A informação é, assim, um recurso intangível sem o qual não se tomam decisões. Como qualquer recurso, tem um ciclo de vida que importa gerir para melhor retirar o devido partido. Quanto melhor e mais atempada for a informação, maior é a probabilidade da mesma ser transformada em conhecimento relevante e acionável. Para que tal aconteça, é importante desenvolver uma cultura de partilha no seio de uma comunidade de interesse, com quem lhe possa acrescentar valor, e com quem tem necessidade de conhecer, o que viabiliza, num ciclo recorrente, o incremento do conhecimento dessa comunidade. No ciberespaço, a partilha da informação atempada e acionável é determinante para o sucesso de qualquer operação.

Na verdade, as operações militares sempre dependeram em muito do recurso informacional, quer na fase que antecede a entrada das forças nos teatros de operações (TO) quer nas fases subsequentes. Há mesmo evidências de conflitos[3] cujo centro de gravidade residiu eminentemente no domínio da informação, tendo a componente física ou cinética sido diminuta ou mesmo inexistente. No entanto, com o avassalador incremento da capacidade das tecnologias de informação e de comunicação que temos vindo a presenciar, desde o início da década de 1990, e que têm a particular característica de incrementar significativamente a velocidade com que os processos se realizam, observou-se um acréscimo da complexidade dos TO, que passaram a ter uma natureza multidimensional.

Para além da dimensão física e humana já existentes no contexto clássico, passou a ter especial importância a dimensão virtual, consubstanciada na informação existente no ciberespaço relevante para a missão, e que liga toda a comunidade de interesse, dando, neste contexto, maior grandeza à dimensão humana. De facto, esta é a mais complexa das três, porque contempla os aspetos sociais, morais e cognitivos de todos os atores envolvidos que fazem parte da comunidade de interesse específica, uma vez que, cada pessoa, dada uma mesma peça informacional, produz juízos diferenciados e assim perceciona a realidade envolvente de maneira distinta, dependente do seu quadro de valores e do conhecimento tácito que já possui sobre o assunto. A dimensão humana é, também ,a que mais beneficia ou mais se prejudica com a já referida hiperconectividade que caracteriza o ciberespaço .Por esta razão, o TO de hoje é em rede, e um dos seus centros de gravidade é a informação que circula e é partilhada no respetivo ciberespaço de interesse e o conhecimento que daí advém.

O ciberespaço representa, assim, um domínio de natureza transversal e transnacional, que o tornam num espaço de interação social de características únicas. Caracterizado por desafios próprios, que combinam a existência de ameaças provenientes de agentes estatais e não estatais, expõe vulnerabilidades transversais às sociedades, exigindo, por essa razão, respostas multidimensionais nos domínios civil-militar e um alto nível de cooperação bilateral e multilateral. O anonimato, a inexistência de fronteiras físicas, a facilidade e a habilidade em se ser virtualmente ubíquo em qualquer parte ou lugar do ciberespaço, o custo relativamente reduzido em que podem importar as designadas *computer network operations* (CNO) e o seu potencialmente elevado impacto (material e reputacional) que pode causar aos interesses dos estados, deram oportunidade a pequenos atores de se baterem com estados ou atores de maior dimensão física, demográfica, económica e militar de "igual para igual", ou mesmo com vantagens. Esta última particularidade potencia a assi-
metria e a natureza híbrida dos conflitos atuais.

As evidências de ciberataques contra Estados Soberanos – Estónia (abril/maio de 2007), Geórgia (agosto de 2008) e Ucrânia (no âmbito do conflito na Crimeia) –, perpetrados por pequenos grupos de atores, muitas vezes ao serviço de estados, fez com que muitas das maiores potências mundiais (EUA, China e Rússia), já detentoras de uma capacidade militar convencional de dimensão significativa, tenham vindo a criar, ao longo dos últimos anos, não só os mecanismos necessários para evitarem ser atacadas, mas

também a capacidade para projetar poder neste novo domínio operacional. Neste contexto, com a criação do *U.S. Cyber Command*, em 2010 (que atingiu a *Final Operating Capability* em 3 de novembro de 2010), os EUA passaram a assumir doutrinariamente o ciberespaço como um novo domínio operacional. Ao nível europeu, esta decisão foi, entretanto, seguida pela Alemanha, Reino Unido, Espanha e França, que anunciaram a criação de comandos responsáveis pela condução de operações militares no ciberespaço.

Demonstrando grande preocupação com o impacto crescente do ciberespaço no ambiente de segurança internacional, na Cimeira de Varsóvia (7-9 de julho de 2016), a Aliança Atlântica reconheceu o ciberespaço como um quarto domínio operacional, a par do mar, da terra e do ar, estando em curso todo o processo que levará à concretização desta decisão. Ainda que sujeito a confirmação, existem indicações que fazem supor que o *Allied Command Transformation* possa vir a assumir no futuro a função de *Cyber Command* da Aliança Atlântica.

Face ao que antecede, podemos afirmar que o ambiente do moderno TO se apresenta cada vez mais multidimensional, constatando-se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações defensivas, de exploração e ofensivas, centradas nas redes de computadores e na informação que lá circula, juntando, de forma transversal, o ciberespaço aos tradicionais domínios ou espaços de atuação. O reconhecimento formal do ciberespaço como domínio operacional por parte de um estado, traduzindo o empenhamento nacional na proteção e salvaguarda da sua liberdade de ação no espaço cibernético de interesse, suscita, neste contexto, uma mudança da tradicional abordagem militar com enfoque na garantia da informação (defesa das comunicações e sistemas de informação), para uma postura centrada no impacte dos ciberincidentes e ciberataques no cumprimento das missões das forças armadas. Por outras palavras, o paradigma operacional transita, assim, naquele contexto, da garantia da informação (*Information Assurance*) para a garantia do cumprimento da própria missão (*Mission Assurance*), refletindo o papel central que o ciberespaço e o próprio ambiente de informação assumem hoje no moderno campo de batalha. O ciberespaço é, assim, hoje em dia, um espaço estratégico de potencial confrontação, no qual se pode utilizar a informação e todos os artefactos que o constituem (infraestrutura e ativos de redes, computadores, e outros dispositivos) como forma de coação[4]. Julgo que é possível afirmar que, hoje em dia, o poder da informação no ciberespaço condiciona de sobremaneira o poder naval, terrestre, e aéreo, sendo determinante para a consecução do estado final desejado das operações de natureza cinética, desenvolvidas no âmbito naval, terrestre e aéreo.

Em Portugal, e no que se refere à Ciberdefesa, na sequência do Despacho n.º 13692/2013, de 28 de outubro, do Ministro da Defesa Nacional, foi criado o Centro de Ciberdefesa (CCD), na dependência da Direção de Comunicações e Sistemas de Informação do EMGFA, tendo iniciado o seu funcionamento no final de 2014. Destaca-se a sua importância, nomeadamente, como ponto de coordenação operacional da segurança das redes e dos sistemas de informação das Forças Armadas e da Defesa Nacional. No entanto, julgo que o ainda número reduzido dos efetivos existentes e a sua capacidade mitigada para conduzir operações militares no ciberespaço, decorrente da atual inserção

organizacional do CCD (julgo que deveria estar na dependência de um Comando Operacional), aconselha uma revisão do constructo organizacional existente, face ao reconhecimento doutrinário do ciberespaço como quarto domínio operacional da guerra.

Relativamente à cibersegurança, Portugal conta, desde 7 de outubro de 2014, com o Centro Nacional de Cibersegurança, que funciona na estrutura do Gabinete Nacional de Cibersegurança e que desde então tem vindo a edificar a respetiva capacidade operacional, incluindo a do ponto focal da rede CSIRT[5] nacional. Desde agosto de 2017, faz parte do *Forum of Incident Response and Security Teams*.

Vejamos agora o problema numa perspetiva um pouco diferente, mas não menos relevante: tal como os domínios físicos (mar, terra e ar), o ciberespaço, o único criado pelo ser humano, existe, entre outras, para proteger e desenvolver os interesses económicos dos estados no contexto da economia digital, perpetuando o binómio mais segurança mais desenvolvimento. Todos os domínios possuem pontos de confluência e de concentração, os quais, nos domínios físicos, se consubstanciam nos pontos de convergência associado às linhas de comunicação e fluxos de pessoas e bens (marítimo, terrestre e aéreo), mas que, no ciberespaço, atenta as suas características mais significativas acima enunciadas (ubiquidade, inexistência de fronteiras, dispersão e descentralização), conduzem à identificação de vários pontos de concentração que importa caracterizar e relacionar no contexto geoestratégico:

– o primeiro, é a infraestrutura física que existe à escala global e cujos ativos[6] são predominantemente provenientes de um só fabricante, a norte-americana *CISCO*.

Ciente deste facto, a China, com a Huawei, está a ganhar terreno, havendo mesmo evidências fundamentadas que, nalguns países dos Balcãs e do Cáucaso estão a "oferecer" toda a infraestrutura de rede dos edifícios governamentais. Refira-se que as poucas empresas europeias com estas competências (*e.g.*, Ericsson, Nokia, Alcatel) quase que desapareceram, deixando a Europa sem qualquer relevância estratégica neste contexto. De igual modo, os cabos submarinos mais importantes têm todos pontos de amarração nos EUA[7];

– o segundo ponto de concentração estratégico refere-se aos sistemas operativos (SO). O predominante, com 92% de penetração à escala global, é o *Windows* da *Microsoft*. O seguinte, com 6% é o *MAC OS* da *Apple*. Ambos norte-americanos. No caso dos SO móveis, o *Android* da *Google* e o *IOS* da *Apple* contam, no conjunto, com mais de 63% do mercado. Assim, neste particular, uma clara dominância de um só estado.

– o terceiro, refere-se às redes sociais e aos motores de busca. Não há muito a dizer: a *Google*, com os seus algoritmos de procura, tem 91% deste mercado. É de relevar que os motores de busca exercem um poder enorme sobre as ideias das pessoas, porque determinam o que é importante e o que não é, através do que colocam nos cinco primeiros lugares da lista dos resultados da pesquisa (1ª página). E a *Goolge* faz isto mais de mil milhões de vezes por dia. Se, na era da informação e do conhecimento, isto não é poder, então o que é ter poder? Ciente deste potencial estratégico, a China envidou

esforços para erradicar a *Google* do seu território, que teve que se instalar em Hong Kong, a partir de 2010. Hoje, o motor de busca chinês *Baidu* possui cerca de 81% de quota de mercado, de mais de 400 milhões de internautas chineses. Na Europa, com mais habitantes do que os EUA, nada existe também neste contexto.

– o quarto ponto de concentração estratégico refere-se aos sistemas de armazenamento na nuvem (*cloud computing*). Também aqui o panorama a predominância e das empresas dos EUA. Ainda que algumas possuam centros de dados no continente europeu, são empresas norte-americanas e guardam a larga maioria da informação existente à escala global em formato digital. Finalmente, o último ponto de concentração estratégico é constituído pelos fóruns de governação do ciberespaço. Devido à sua génese na comunidade académica, tendem a ser predominantemente espaços de partilha de conhecimento, em vez de *fora* de controlo. No entanto, a I&D nestes e noutros domínios encontra-se muito desenvolvida nas universidades norte-americanas e, por isso, os EUA continuam a exercer aqui também o seu poder de influência (*soft power*) e de predominância.

É ,por isso ,e por ora, evidente que os EUA dominam os pontos de concentração estratégicos do ciberespaço e detêm, assim, uma hegemonia sobre ele, que importa acompanhar no contexto do que se está a passar naquele estado federal e no resto do Mundo. Em que é que a Europa ou um país se pode diferenciar? O recentemente anunciado *EU Cyber security Act*[18] poderá fazer alguma diferença.

Relativamente ao futuro, daria nota que a Inteligência Artificial (IA) é considerada um dos mais promissores (e inquietantes) desenvolvimentos tecnológicos da nossa era e que a cibersegurança é uma das áreas que já hoje mais beneficia dessa nova tecnologia. Novos algoritmos, novas técnicas, e novas ferramentas e empresas, que disponibilizam serviços baseados em IA, estão a surgir no mercado global de cibersegurança. Em comparação com as soluções convencionais de cibersegurança, estes sistemas são mais rápidos, mais flexíveis, mais adaptáveis e mais robustos, contribuindo assim para melhorar a segurança do ecossistema em que se encontram inseridos e protegendo, de um modo mais eficaz, um cada vez maior e mais sofisticado conjunto de ciberameaças. Através da IA é já possível prever ciberataques com antecedência e assim agir atempadamente, em vez de apenas investir na prevenção e na reação tendente a mitigar dos mesmos.

Todavia, apesar das melhorias que a IA tem trazido para este domínio, os sistemas associados ainda não são capazes de se ajustar completa e automaticamente às mudanças no ambiente em que operam, aprendendo todas as ameaças e tipos de ataque e escolhendo e aplicando autonomamente contramedidas específicas para a proteção contra esses ataques.

Consciente dos aspetos de natureza ética, nomeadamente quanto à privacidade dos cidadãos, à ausência de um quadro moral para a tomada de decisão autónoma e à inexistência de um enquadramento legislativo para a utilização desta promissora tecnologia, algumas entidades consideram, mesmo assim, que a sua utilidade, quando

aplicada à cibersegurança, pesa mais do que os riscos que lhe estão associados. Julgo que esta consideração merece uma reflexão mais cautelosa e mais profunda.

Por todas estas razões, e com o atual nível de maturidade, é necessária uma forte interdependência entre os sistemas de IA (ou outros quaisquer) e os seres humanos para incrementar a maturidade da cibersegurança das organizações. Uma visão holística relativamente a estes assuntos é determinante para o sucesso, pois a cibersegurança é muito mais do que apenas uma questão tecnológica. Neste contexto, os mais altos dirigentes, que no caso das Forças Armadas são os comandantes, diretores ou chefes, devem ter um papel determinante no incrementar da resiliência digital das suas organizações, fomentando proactivamente uma cultura que minimize o ciber-risco através da intervenção pró-ativa no fator humano:"*People matter as much, if not more than, technology. We have to get beyond focusing on just a technological piece. It's about ethos. It's about culture. It's about how you train your men and equip your organization, how you structure it and the operational concepts you apply*"[9].

Conclusões

A título de conclusão, diria que a informação, que sempre foi determinante para o exercício do Poder Naval, Aéreo e Terrestre, tem um valor que, hoje em dia, é exponenciado pelo ciberespaço, constituindo-se este como o quarto domínio operacional, a par do mar, da terra e do ar.

O Poder da Informação está intimamente ligado ao domínio do ciberespaço como espaço estratégico de potencial confrontação, sendo, por isso, decisivo para a boa prossecução das operações militares, em quaisquer dos outros domínios. Do ponto de vista geoestratégico, releva-se a posição quase hegemónica dos EUA no controlo de todos os pontos de confluência estratégica do ciberespaço à escala global, da ausência quase completa da Europa neste contexto e da emergência da China nalguns pontos fulcrais de convergência. Apesar do desenvolvimento significativo da IA aplicada à cibersegurança, é cada vez mais evidente que esta não é apenas uma questão de natureza tecnológica, sendo cada vez mais importante instituir nas organizações uma cultura que minimize o ciber-risco através da intervenção pró-ativa no fator humano, como forma de incrementar a resiliência digital das organizações e, assim, mitigar os efeitos que a utilização ilegítima do ciberespaço pode aportar para a vida de todos nós. Esta ação deve começar pelos líderes, porque todos sabemos que a maneira mais eficaz de liderar é pelo exemplo.

---

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[2] https://www.economist.com/printedition/2017-05-06.

[3] Vários episódios da Guerra Fria, do qual se destacaria a crise dos mísseis em Cuba.

[4] Coronel Viegas Nunes, Competitive Intelligence and Information Warfare Association (CIIWA).

[5] Computer Security Incident Response Team.

[6] Equipamentos e sistemas responsáveis por todas as comunicações na Internet, incluindo a respetiva gestão.

[7] Recentemente, foi do conhecimento público que Portugal está a assumir um papel bastante relevante neste contexto, com o lançamento de um cabo submarino que ligará a Europa a África.

[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505290611859&uri=COM:2017:477:FIN.

[9] Almirante Michael Rogers, USA Cyber Command