

TECNOLOGIA 5G — POR QUE COMPETEM USA E CHINA?

Antônio Raimundo

Texto entregue em Novembro de 2021

A TECNOLOGIA É HOJE E SERÁ CADA VEZ MAIS no futuro, parte integrante da vida das pessoas, das organizações e do modo como as sociedades estão organizadas. Essa presença vai aumentar não apenas em volume ou importância operacional, mas transformando o modo de vida, a forma como a sociedade se organiza e funciona e consequentemente, os modelos de relacionamento.

As sociedades modernas “alimentam-se” de inovação e de tecnologia. A tecnologia de comunicações e internet móveis é hoje um “must” dos 8 aos 80.

Populações existem onde coexistem a par das carências mais básicas, taxas de penetração de telemóveis elevadas. A tecnologia torna-se assim fator “estruturante ou desestruturante”, mas sempre acelerador da transformação do funcionamento das sociedades, fazendo estas saltarem etapas de desenvolvimento.

Nos países mais desenvolvidos a penetração tecnológica faz-se de forma quase “invisível”. O acesso aos serviços – do supermercado a outros produtos correntes, da relação com o Estado à aquisição de conhecimento/educação/informação ou ao relacionamento com a saúde ou a cultura, alteraram modos operativos e comportamentais, de forma contínua.

Menos conhecida, apesar do crescente número de notícias, é o campo da cyber-segurança, da espionagem, do crime organizado, do controlo remoto e da tecnologia espacial. O topo desta cadeia de inovação aplicada é a tecnologia/engenharia militar e de segurança, mas as tecnologias base são duais e suportadas pela mesma investigação científica de base.

No passado próximo a competição pela liderança mundial esteve centrada no confronto entre os EUA e a União Soviética – arsenal nuclear, zonas de influência, modelo de sociedade – mas esses fatores, continuando a ser relevantes, foram sendo progressivamente relativizados pela afirmação da geoeconomia e do comércio internacional e pela competição pela liderança tecnológica e científica.

A competição é hoje entre os EUA e a China, dado o crescente posicionamento desta na economia mundial, nos organismos multilaterais, no domínio militar, na agenda política e na investigação e desenvolvimento, em áreas como as telecomunicações (5G), a robótica, a Inteligência Artificial (IA), as nanotecnologias ou a gestão de dados.

Obviamente que neste confronto a questão ideológica está sempre presente. Carlos Gaspar afirma mesmo: “Para Xi e para a legitimidade do PCC é essencial demonstrar a superioridade do regime comunista em comparação com os regimes de democracia pluralista” (Gaspar, 2019). Todos os confrontos

entre as superpotências, mesmo os aparentemente de pura base tecnológica, são, sempre, processos ideológicos, de propaganda e projeção de poder (Economy, 2020).

Na União Europeia (UE), a Presidente da Comissão pretende que a Europa seja uma referência para o mundo, compatibilizando ética e inovação e com isso projetar uma imagem de superioridade civilizacional e equidistância entre as superpotências, mas as contradições entre os Estados membros e o próprio modelo de funcionamento – uma união comercial forte, mas uma fraca união política, não permitem a afirmação no contexto da competição mundial. Nem mesmo em temas relacionados com os valores que suportam a EU esta consegue ter uma voz única, com decisões relevantes a serem bloqueadas por parte de Estados membros. A vontade de afirmação na investigação científica e na política tecnológica, consideradas como estrategicamente relevantes e apesar dos enormes programas de apoio financeiro que são colocados no terreno, não apresenta resultados significativos.

“
Em todo o mundo os países
começam a programar
ou mesmo a lançar concursos
para a implementação
da tecnologia 5G.”

A China não é, ainda, uma forte potência militar quando comparada com os EUA, quer na dimensão do arsenal nuclear quer no domínio das armas convencionais, mas investe de forma sustentada, tem um potencial humano apenas rivalizado pela Índia e avança muito rapidamente nas questões científicas e tecnológicas (Economy, 2018).

Uma tecnologia hoje universalmente aceite e que a sociedade como um todo já não dispensa, prende-se o “direito” a estar contactável e informado – exigindo-se mesmo “real-time” sobre os acontecimentos relevantes – mesmo que o critério de relevância não seja nem unívoco nem objetivo. As notícias pessoais/sociais, o acesso a informações do dia a dia, o complemento/ajuda de memória ou o apoio a todo o tipo de atividade ou desafio, são ferramentas que a dinâmica quotidiana dos grupos já não dispensa.

Com cada vez mais sistemas digitais a partilharem informações aumenta a pressão funcional quer para a sincronização e partilha de dados, entre sistemas, quer para o “diálogo” entre estes. A pressão por maiores larguras de banda,

maior velocidade e melhores coberturas, face ao aumento do número de objetos conectados, e a conectar, é enorme.

As redes 5G e futuras evoluções, são a resposta a este tipo de procura.

Mas a quantidade de informação gerida é proporcional ao risco de manipulação, intrusão ou roubo. Se as redes são críticas, os grandes repositórios de informação são tanto ou mais críticos. As tecnologias de intrusão, roubo e espionagem por meios automáticos, através de tecnologias de penetração e clonagem de sistemas, estão bastante banalizadas, e são já hoje uma ameaça para as empresas e para os governos.

As redes de quinta geração - 5G

As redes móveis de quinta geração – 5G, anunciam um “mundo” mais conectado possibilitando a IoT (Internet das coisas).

Todos temos uma boa noção no contexto doméstico sobre o que significa IoT – do “laptop” ao frigorífico, do alarme ao ar-condicionado, da máquina da louça aos “robôs” de cozinha, mas quando falamos de sistemas empresariais a rarefação é maior – dos “brokers” de mercado à contabilidade, do economato ao sistema de atendimento automático ou de aconselhamento comercial ou mesmo de vendas. Mas o universo de objetos a conectar não se confina ao domínio doméstico e empresarial. Quando pensamos em gestão de uma cidade – controlo dos sistemas vitais de energia, água, esgotos, recolha de lixo ou gestão de tráfego humano ou automóvel, controlo das pessoas (comportamentos e decisões), veículos autónomos, segurança de pessoas e instalações, sistemas de controlo – de centrais de energia a centrais nucleares – o contexto fica mais complexo e essa complexidade aumenta ainda mais se juntarmos a segurança física, os sistemas de saúde ou o sistema judicial.

Se numa cidade a dimensão e complexidade já é significativa, numa região ou num país, tudo se torna mais sensível porque falamos também em segurança interna e externa, sistemas de defesa ou gestão política ao nível estratégico e operacional.

Potencialmente, todos os sistemas geridos de forma automatizada podem vir a estarem ligados e a serem geridos e controlados remotamente a partir de algoritmos. Estes necessitam de redes de alto débito de modo a garantir velocidade de acesso e grandes volumes de informação, associados a operação em *real-time*, que são essenciais às funções de gestão. No campo militar podemos ter como exemplo, os “drones” ou os mísseis hipersónicos.



5G – COMPETIÇÃO PARA QUÊ?

O techno-nacionalismo como ideologia e prática política, afirmou-se como o fundamento e suporte da geopolítica e da geoeconomia da China do século XXI, suportando o aumento da capacidade militar regional e global.

ESTAÇÕES BASE 5G – QUOTAS DE MERCADO

Fornecedor	2019 Quota de mercado	2020 Quota de mercado
Ericsson	30%	26,5%
Huawei	27,5%	28,5%
Nokia	24,5%	22%
Samsung	6,5%	8,5%
ZTE	6,5%	5%
Other	5%	9,5%

Fonte: TrendForce 2020 in www.trendforce.com

O trânsito nas redes, desta tipologia de informações permite, potencialmente, que as mesmas sejam filtradas e indevidamente apropriadas por terceiros.

A tecnologia 5G abre o caminho a todo este tipo de utilizações na medida em que as suas características técnicas isso potenciam, em particular, o significativo aumento da largura de banda, a baixa latência, número de “dispositivos” conectados por Km² e menor consumo de energia. A Huawei é líder mundial na tecnologia 5G seguida da Nokia e da Ericsson.

Por estas razões objetivas e outras de carácter mais político, os EUA lançaram uma campanha diplomática de alerta sobre a segurança das redes 5G e em particular para a tecnologia da Huawei.

O foco da campanha são os fornecedores e equipamentos de origem chinesa e, com foco particular, os riscos para os países aliados dos EUA, nomeadamente os membros da NATO. De acordo com o ponto de vista dos EUA, licenciar redes que utilizam equipamentos com essa origem, coloca em risco a segurança estratégica.

A questão da segurança, pese embora os especialistas se mostrarem tranquilos porque não foram ainda comprovadas falhas de segurança, não é, no entanto, consensual, porque sendo uma questão política e geopolítica, não pode ser discutida no restrito âmbito técnico. Mas mesmo do ponto de vista estritamente técnico a questão não parece pacífica.

No contexto europeu, as preocupações da agência nacional de cibersegurança britânica (NCSC) que identificou falhas nos processos de engenharia da Huawei, que expõem as redes de telecomunicações a riscos como um ataque cibernético, parecem relevantes.¹

Mas também do ponto de vista político, a UE, pela voz da Vice-Presidente da Comissão Europeia, Margarethe Vestager, lembra que “as redes 5G são a espinha dorsal do setor industrial pelo que é importante que não estejam abertas para espionagem, cyberataques ou bloqueios”². Sem mencionar a Huawei, a UE aprovou uma recomendação sobre a seguran-

ça das redes 5G³ e promoveu um conjunto de recomendações dirigidas aos Estados membros,⁴ sobre regras a serem seguidas, do ponto de vista de segurança, pelos fornecedores e pelos operadores.

Já a posição dos EUA é mais política, e decorre de um relatório elaborado por uma comissão da Câmara dos Representantes (2012) sobre o assunto, onde se recomenda às empresas norte-americanas que evitem fazer negócios com as duas companhias chinesas (Huawei e ZTE). “Com base em várias informações – sigilosas e públicas –, não podemos considerar que a Huawei e a ZTE estejam livres da influência de um Estado estrangeiro e, portanto, constituem uma ameaça à segurança dos Estados Unidos e aos nossos sistemas”. Estas duas empresas, das mais representativas no contexto mundial neste tipo de tecnologia, são assim “acusadas” não apenas de falhas de segurança, mas de potencialmente poderem disponibilizar informações para os serviços secretos chineses.

“

O confronto EUA/China é global. Em causa está a liderança política, económica, civilizacional e tecnológica.

”

A questão é política e geopolítica, pelo que na argumentação sobre os riscos apontados por americanos e europeus, citam uma lei da China que requer às empresas a cooperação com os serviços secretos. A afirmação – “Queremos garantir a integridade de toda a cadeia de fornecimento do 5G e vemos como uma ameaça à segurança nacional que um governo tenha uma lei que obriga qualquer pessoa ou entidade a colaborar com os serviços de informação”, alude à Lei Nacional de Inteligência da República Popular da China, aprovada em Junho de 2017. O artigo sétimo dessa lei determina que “todas as organizações e cidadãos devem apoiar, ajudar e cooperar com o Estado em matéria de Inteligência Nacional”. O artigo 20.º, por seu lado, diz que durante ações de contraespionagem as “organizações e indivíduos relevantes” devem “fornecer informação” e “não devem recusar” a colaboração com o governo de Pequim⁵.

A questão poderá, pois, colocar-se entre o que a China considera os seus “interesses estratégicos” e o que os países ocidentais possam considerar como “uma questão de direitos fundamentais, de princípio ou de segurança”. A determinação legal que fornece cobertura para eventuais acessos indevidos a dados configura-se como um risco político que ultrapassa em muito o risco tecnológico. “A segurança

nacional é o cimento que sustenta a estabilidade da China” afirmou Zhang Yesui no Congresso Nacional Popular Chinês de 2020 sobre o Padrão de Segurança da China.

O fundador da Huawei – Ren Zhengfei, já negou as acusações de espionagem e de controlo por parte do Partido Comunista Chinês – “Eu era um técnico de uma empresa das forças militares, mas tornei-me vice-presidente de um pequeno instituto de investigação em construção, com um pouco mais de 20 pessoas”, explicou Zhengfei.

Fundada em 1987, por um ex-engenheiro das forças armadas chinesas, a Huawei rejeita assim as acusações de que é controlada pelo Partido Comunista Chinês (PCC), ou que desenvolve equipamentos que facilitam a espionagem chinesa. Importa ter presente que, de acordo com o relatório de 2013, em 120 incidentes envolvendo cyber-espionagem, 96% eram de origem chinesa (Timberg, 2013).

Por outro lado, parecem existir evidências que alguns funcionários da Huawei são, em simultâneo, funcionários dos Serviços públicos de Segurança chineses e do serviço de espionagem. Estão também reportadas situações, nomeadamente em África, em que funcionários da Huawei, forneceram dados sobre adversários de regimes políticos autocráticos, permitindo assim a localização e mesmo o silenciamento dos mesmos (McMaster, 2020).

Em todo o mundo os países começam a programar ou mesmo a lançar concursos para a implementação da tecnologia 5G. O assunto não é, no entanto, fácil de analisar e decidir face a estas questões geopolíticas, mas também a questões tecnológicas, de custo, de imagem e interesses económicos e políticos.

Um exemplo vem da Alemanha, onde Angela Merkel referiu que a RFA tem adotado, até agora, uma abordagem cautelosa em relação à Huawei, mostrando algum ceticismo perante a ideia de um boicote ao gigante chinês, já que, na opinião de Berlim, faltam provas concretas de abusos por parte da empresa. No entanto, Pequim “deve garantir que a empresa não transmita dados ao Estado chinês e que existam salvaguardas”, disse. Com entendimento diferente, menos flexível, estão a Austrália, o Reino Unido e a Nova Zelândia, que proibiram as redes 5G da Huawei, por motivos de segurança nacional. Para além destes, os Estados Unidos da América e Taiwan, que mantêm restrições mais amplas à empresa, adotaram a mesma medida. Também o Japão, cuja agência para a segurança no ciberespaço classificou a firma chinesa como de “alto risco”, banindo as compras à Huawei por departamentos governamentais.

A Huawei é o primeiro fornecedor chinês do sector tecnológico – 180 mil empregados e mais de 100 mil milhões de US\$ de vendas, tornando a empresa politicamente cada vez mais relevante, à medida que o PCC tenta transformar as firmas do país em importantes

competidores em tecnologias de alto valor agregado, como a inteligência artificial, as energias renováveis, a robótica, os veículos elétricos ou os veículos autónomos.

A questão coloca-se assim no plano geopolítico e de liderança tecnológica mundial. Importa ter presente que a liderança tecnológica é ainda mais determinante a partir do momento em que as tecnologias de ponta – 5G, IA, robótica, ciberespaço, veículos autónomos, etc., são de utilização dual (civil e militar). A tecnologia do veículo autónomo é na base, a mesma do “drone” ou do satélite hipersónico.

Importa também recordar que as redes 5G, porque irão transportar grandes quantidades de informação, de origens e criticidades diversas (pessoais e profissionais), são, objetivamente, “terreno fértil” para as atividades de espionagem e contraespionagem (Hannas, 2013).

Sob a liderança de Hu Jintao, a China assumiu o tecno-nacionalismo como instrumento de projecção geopolítica em que a inovação tecnológica, em particular na área da defesa, aparece como elemento crítico de sucesso. O tecno-nacionalismo como ideologia e prática política, afirmou-se como o fundamento e suporte da geopolítica e da geoeconomia da China do século XXI, suportando o aumento da capacidade militar regional e global (Cunha, 2016).

Conclusões

A China é uma sociedade fechada. A censura na China é um “jogo de sombras” em que a aparente tolerância é mitigada com as contínuas “burocracias”, dificuldades e se necessário, ações “musculadas”, mas tentando transmitir a ilusão de liberdade.

Neste contexto a abordagem política e de apoio aos projectos que requerem grandes volumes de dados aparecem muito interligados, quer sejam no domínio da IA – civil ou militar, no domínio da segurança ou no da saúde. Poder-se-á argumentar que a China possui uma base imensa para recolha de dados no seu contexto interno, mas, a riqueza de qualquer algoritmo depende da diversidade de informação com que é confrontado.

É neste contexto político e estratégico que se desenvolve a discussão sobre a segurança nas redes 5G. Como já se afirmou, a questão não é apenas técnica até porque se assim fosse seria “simples” de solucionar. As questões de segurança na Huawei não são novas, sendo claro que, apesar de estarem documentadas fragilidades, não foram reportadas quebras de segurança com as redes 4G de fabricação chinesa, apesar de os técnicos referirem que o código existente nas mesmas ser pouco estruturado (60% corrige erros e melhora eficiência) e por isso mais difícil de ser auditado. Em bom rigor e até agora, as redes não tinham a criticidade que agora passam a ter. Talvez por isso alguns países que decidiram bloquear a tecnologia da

Huawei no 5G, optaram mesmo por mandar retirar os equipamentos da tecnologia 4G, sobre os quais a solução 5G poderia vir a ser montada.

O caso da tecnologia 5G mostra bem a diferença entre a abordagem liberal seguida nos EUA e uma abordagem política centralizada seguida na China. Enquanto nos EUA a inovação tem uma fortíssima componente de responsabilidade individual e das empresas, a abordagem à inovação na China é objeto de planeamento em função dos interesses definidos pelo PCC (Simon, 2009).

O confronto EUA/China é global. Em causa está a liderança política, económica, civilizacional e tecnológica. A competição em torno do 5G não é um tema menor porque condiciona a liderança militar. A China parece mais interessada em dominar as tecnologias militares do futuro do que competir nas do presente. Nesta perspectiva a inovação é estratégica. ■

Notas

¹ NCSC – Annual Report 2019

² Jornal Expresso – 30/10/2020

³ Recomendação (UE) 2019/534

⁴ Secure 5G networks: the EU toolbox, Bruxelles Oct. 2020

⁵ Padrão Nacional “Cybersecurity” da China

Referências

- Cunha, Luís (2016). *China's Techno-Nationalism in the Global Era*. Lisboa. Instituto Internacional de Macau.
- Economy, E. (2018). *The Third Revolution*. New York. Oxford.
- Economy, E. (2020). *The United States, China and the Great Values Game in Covid-19 and World Order*. (Eds.) Hal Brands and Francis Brands. Baltimore. John Hopkins.
- EU's Cybersecurity for the Digital Decade. www.europa.eu
- Gaspar, C. (2019). *O Regresso da Anarquia*. Lisboa. FFMM.
- Hannas, William, et al. (2013). *Chinese Industrial Espionage – Technology Acquisition and Military Modernization*. New York. Routledge.
- McMaster, H. R. *Battlegrounds – The Fight to Defend the Free World*. London. HarperCollins.
- National Cyber Security Centre (2019). Annual Report. ncsc.gov.uk
- Simon, Denis & Cao, Cong. (2009). *China's Emerging Technological EDGE – Assessing the Role of High-End Talent*. New York. Cambridge.
- Timberg, Craig. 2013. *Vast Majority of Global Cyber-Espionage Emanates from China, Report Finds*. Washington Post. April 22.