E se...?

Cenários para 2021
Futuros para 2024

Colectânea de textos a partir dos relatórios:

What if...? Scanning the horizon: 12 scenarios for 2021 (Chaillot Paper 150)
What if...? 14 Futures for 2024 (Chaillot Paper 157)

Editados por Florence Gaub, directora do European Union Institute for Security Studies (EUISS).

Tradução
Conclusão das Letras

Selecção dos Textos
Pedro Fonseca

Paginação
Sara Dias

Fotografias
Capa: Lizzet Ortiz/Unsplash
Separador "Cenários para 2021": Leonard von Bibra/Unsplash
Separador "Futuros para 2024": Junior Moran/Unsplash

Produção
Conclusão das Letras
Versão online em TICtank.pt

Data de Publicação
Setembro de 2020

Patrocínio

Cenários para 2021

Futuros para 2024

E se...?

Cenários para 2021

Introdução: Regresso ao Futuro - Novamente

Florence Gaub (directora, EUISS)

Existem muitas maneiras de pensar sobre o futuro - mas algumas são mais produtivas do que outras. Horóscopos, profecias e interpretações de sonhos antigos, por exemplo, não são exactamente úteis: enquanto horóscopos e sonhos são muito vagos, as profecias são muito apocalípticas para dar uma ideia clara do que pode ser feito para moldar o futuro.

É disso que trata a previsão: escolha, decisão e acção - e não, como é repetido tantas vezes, prever o futuro e errar. É um exercício intelectual e criativo concebido para ajudar os decisores a desenvolver e fazer escolhas, a desafiar antigas crenças e/ou ortodoxias, a concentrar os seus recursos e atenção e a prevenir e antecipar certos desenvolvimentos.

Este é um exercício contínuo por duas razões: a primeira é, de modo algo óbvio, que o futuro pode mudar a cada dia, assim como a maneira como pensamos sobre ele. É justamente por essa razão que relatórios sobre o futuro são publicados regularmente, substituindo os anteriores. Na verdade, relatórios futuros desactualizados raramente são lidos novamente, após o lançamento dos novos. A segunda razão é que a maioria das nossas instituições não foi concebida para planear o futuro de médio a longo prazo. O entendimento implícito da burocracia dominante do futuro é linear - essencialmente, que o amanhã será mais do hoje. Isso é lógico: as nossas instituições não se podem desafiar permanentemente, pois deixariam de estar operacionais.

Portanto, a previsão estratégica, embora conduzida para a tomada de decisão, é feita principalmente por entidades ligeiramente afastadas da gestão do dia-a-dia. Afinal, o seu papel é justamente desafiar as premissas das instituições, procurar e detectar sinais fracos, fiscalizar os contornos externos dos acontecimentos e investigar áreas que não fazem necessariamente manchetes. O European Union Institute for Security Studies (EUISS) é um dos organismos criados para esse fim.

Como acontece com outros actores envolvidos na previsão, o EUISS usa uma série de métodos para pensar sobre o futuro de uma forma construtiva. No passado, consultámos especialistas (chamado de método Delphi), produzimos análises de tendências e impactos e desenvolvemos vários tipos de cenários. Na maioria das vezes, usámos dois ou mais métodos consecutivamente. E há muito mais técnicas a serem exploradas, que vão desde crowdsourcing a inquéritos, visão e simulações [1].

A escolha do método de previsão nunca é aleatória mas depende de vários factores: estamos a olhar para um futuro próximo, a médio ou a longo prazo? É para quem, exactamente? Que desenvolvimentos estamos a tentar entender, têm de ser analisados ou interpretados? Que tipo de dados são necessários e disponíveis? O que acontecerá com os resultados? Começamos com o fim em mente (criar um futuro preferível) ou reagimos às coisas que acontecem ao nosso redor (futuros prováveis)?

Nesta publicação, pretendemos alertar os decisores sobre desenvolvimentos potenciais com impacto estratégico significativo enquanto eles ainda se podem preparar ou até evitá-los. Fazemos isso usando dois métodos combinados: "horizon scanning" e também a criação de um cenário único. Juntos, produzem eventos plausíveis a ocorrer em 2021 - com ramificações estratégicas muito para lá disso.

O "horizon scanning" é um método que visa aumentar o alcance da visão. Claro, o conceito é uma referência etimológica a um tempo em que o horizonte e a distância até ele eram vitais, especialmente para a navegação no mar: indicava os próximos portos seguros possíveis, mas também os encontros potencialmente perigosos com fenómenos meteorológicos ou navios hostis. De modo mais geral, fazer "scanning" ao horizonte expressa o facto de que o olho humano não consegue capturar todo o horizonte com um olhar; em vez disso, precisa de se mover para acumular informação. Em previsão, esta informação pode ser quantitativa (dados sobre preços de alimentos ou dados demográficos, por exemplo), mas também qualitativa (como medir o descontentamento com um determinado desenvolvimento numa determinada população).

Este método opera com uma mente aberta, ao invés de procurar confirmar uma visão específica: ele identifica mudanças, mas também constantes.

Por defeito, o "horizon scanning" é uma monitorização contínua e sistemática e uma interpretação de um ambiente específico, em vez de um evento ad hoc. Isto, em essência, é o que os analistas do EUISS fazem continuamente.

Para esta publicação, os analistas do EUISS foram convidados a criar um cenário com base nos desenvolvimentos que eles identificaram nas suas respectivas áreas de especialização - algo que ilustre as consequências potenciais dos factores observados durante o processo de "horizon scanning".

Os cenários são um método de previsão que é muito mais narrativo e estreito do que a "horizon scanning" - essencialmente, são histórias. A vantagem de contar histórias na previsão é dupla: primeiro, permite-nos destacar relacionamentos e tendências que os dados quantitativos nunca podem capturar. Eles são, portanto, particularmente adequados para casos em que os seres humanos moldam os eventos, pois os cenários podem incorporar valores, motivações e comportamentos que os dados em bruto não reflectem.

Em segundo, eles podem gerar a emoção necessária para superar a negação - em si mesma um dos mais fortes obstáculos para a mudança de percepções sobre um assunto. A melhor maneira de fazer isso é tirar vantagem de uma característica humana, a "suspensão voluntária da descrença" que ocorre quando ouvimos ou assistimos uma história de ficção. Um cenário vívido pode capturar a atenção e a imaginação dos decisores com mais facilidade do que tendências vagas, precisamente porque pode superar a negação e gerar emoção [2].

Para ser útil, um cenário deve cumprir certos critérios: precisa de ser, obviamente, plausível e dentro dos limites do que pode acontecer. Por exemplo, um cenário pode ser possível - como um enorme asteróide atingir a Terra - mas não é muito plausível. Os cenários apresentados aqui não são, portanto, como os agora (in)famosos "Black Swans" ou "Wild Cards" - eventos altamente improváveis com implicações estratégicas igualmente sérias - mas sim "Grey

Swans" [3]. Os "Grey Swans" partilham com os "Black Swans" um elevado nível de impacto estratégico, mas há mais provas a apoiar a ideia de que eles são realmente possíveis. Assim, embora haja mais dados para os "Grey Swans", eles ainda são frequentemente considerados improváveis de acontecer e frequentemente considerados fantásticos - simplesmente porque os humanos, como as burocracias que construíram, não podem funcionar com pensamentos catastróficos o tempo todo.

Mas esta é precisamente a razão pela qual esses desenvolvimentos potencialmente estratégicos são concretizados neste Chaillot Paper. Afinal, se esses eventos fossem mais previsíveis (um pouco como a previsão meteorológica), não fariam parte da previsão. Nesse sentido, a imaginação é para a previsão o que o génio criativo é para um pintor: sem ele, o exercício é mais ou menos fútil. Sem imaginação, as informações recolhidas no "horizon scanning" são apenas isso: dados secos sem implicações para o futuro. É a imaginação, e não apenas os factos, que pega nos desenvolvimentos, os reúne e os projecta no futuro. Esta é, por exemplo, a razão pela qual a comissão do 11 de Setembro afirmou que o fracasso em antecipar os ataques a Nova Iorque e a Washington D.C. foi antes de mais "uma falta de imaginação" [4].

Os factos estavam na sua maioria disponíveis: ligá-los de uma forma criativa é que não foi feito. Um cenário elaborado não deve, portanto, ser desqualificado devido à sua natureza inesperada - o que importa é que ele está enraizado em provas e construído numa coerência lógica de pensamento.

Todos os cenários neste Chaillot Paper reflectem a experiência e a imaginação dos investigadores que os escreveram: alguns exploram potenciais conflitos,

enquanto outros olham para desenvolvimentos políticos disruptivos ou mesmo para crises com ramificações significativas. Dito isto, todos são concebidos para os decisores europeus, na esperança de chamar a sua atenção para aspectos da política externa e de segurança que são potencialmente esquecidos, e todos são extrapolados de desenvolvimentos em curso e recentes.

Assim como o primeiro EUISS Report "What if… Conceivable crises: Unpredictable in 2017, unmanageable in 2020?" [5], os cenários seguem a mesma estrutura, apresentando três instantes estratégicos no tempo: o momento em que o próprio evento ocorre (2021), os anos seguintes (2021-2025) e o momento em que os desenvolvimentos que levaram até lá estão a ocorrer (2019).

Simplificando, viajamos para o futuro a fim de ver o que podemos mudar hoje para evitar que esses eventos se tornem realidade ou para nos preparar para o seu impacto. A analogia com o filme "Regresso ao Futuro" de 1985 é pura coincidência, obviamente - mas, assim como no filme, às vezes precisamos de fazer uma viagem ao futuro para sustentar uma decisão tomada hoje.

---

[1] Rafael Popper, “Foresight Methodology”, in Luke Georghiou et al. (eds.), The Handbook of Technology Foresight (Cheltenham: Edward Elgar, 2008): pp. 44-88.

[2] Peter Schwartz, "The Art of the Long View: Planning for the Future in an Uncertain World" (New York: Currency Doubleday, 1996): pp. 29-43.

[3] Anthony J. Masys, “Black Swans to Grey Swans: Revealing the Uncertainty”, Disaster Prevention and Management: An International Journal, 21, no. 3 (2012): pp. 320-335.

[4] National Commission on Terrorist Attacks Upon the United States, “The 9/11 Commission Report” Julho 2004: p. 339.

[5] Florence Gaub, “What if... Conceivable crises: unpredictable in 2017, unmanageable in 2020?”, EUISS Report no. 34 (Junho 2017).

E se… um submarino estrangeiro fosse atacado em território da UE?

Daniel Fiott (editor de segurança e defesa, EUISS)

Às 04h44 de 17 de Maio de 2021, as autoridades governamentais da República de Zirta receberam uma comunicação do grupo terrorista New Petra Circle (NPC) de que um submarino a diesel (classe Kilo), pertencente à marinha da República Federal de Parousia, foi sequestrado na cidade portuária de Plimsolla, em Zirtia.

Oficiais parousianos confirmaram às autoridades zirtianas que haviam perdido a comunicação directa com o capitão do submarino PK216 (classe Skulla). O NPC, que estava baseado em Parousia e era conhecido por se opor violentamente ao governo deste país, afirmou que 20 tripulantes a bordo do PK216 eram membros do grupo e os 30 submarinistas restantes foram colocados numa zona segura.

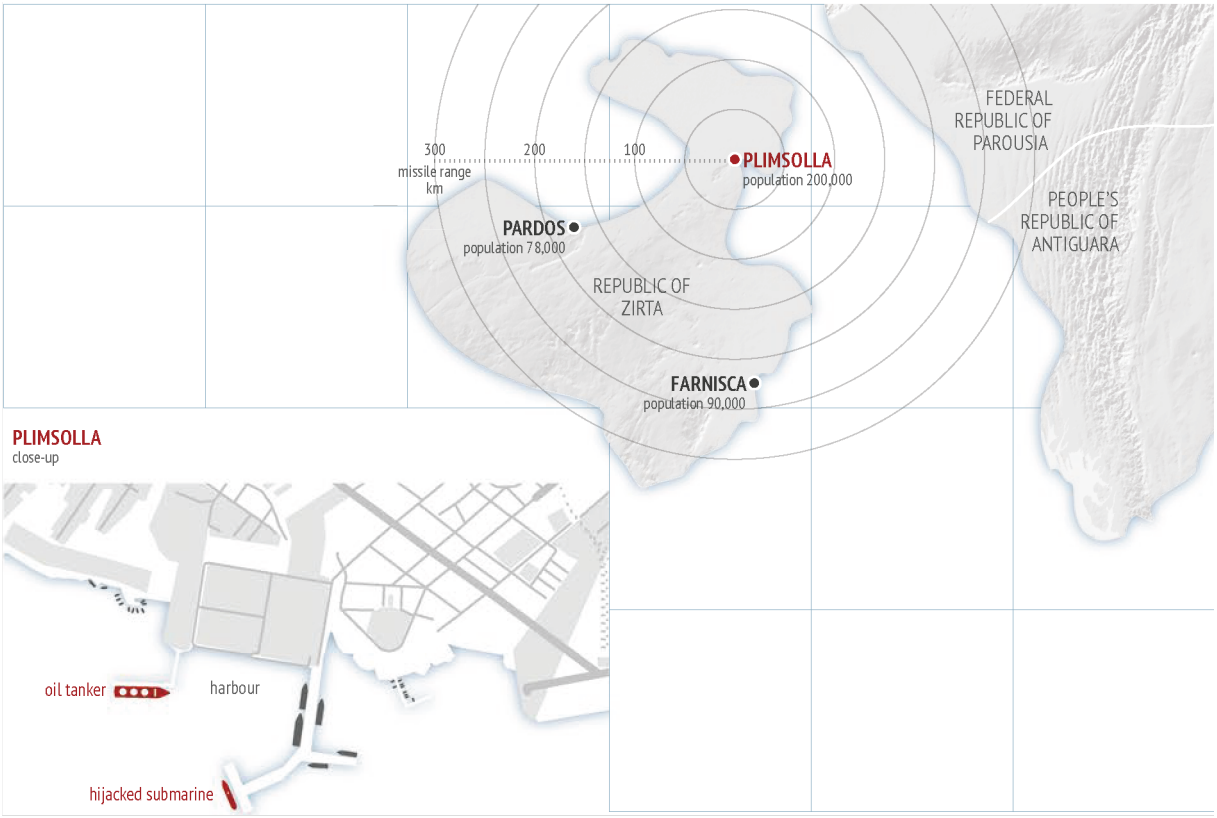
O NPC ameaçou começar a assassinar membros da tripulação e disparar mísseis de cruzeiro Excalibur a bordo contra as cidades de Zirtia caso Parousia ou outras partes tentassem recapturar o navio. Dado que o PK216 carregava no máximo quatro mísseis com um alcance de 300 quilómetros, as cidades de Plimsolla (população: 200 mil), Farnisca (população: 90 mil) e Pardos (população: 78 mil) estavam todas a essa distância.

Embora incapaz de levar o PK216 para o mar com a tripulação reduzida, o NPC ameaçou torpedear três grandes navios comerciais e um petroleiro ancorados no porto de Plimsolla se Parousia não libertasse os membros do NPC detidos ou organizasse a sua passagem segura para obter asilo na UE.

Apesar desses avisos, às 23h37 de 17 de Maio a marinha de Parousia tentou sem sucesso desactivar os torpedos do PK216 e os tubos de mísseis de cruzeiro utilizando forças especiais. Em retaliação, o NPC torpedeou o petroleiro ancorado em Plimsolla. O porto foi abalado por uma grande explosão e, devido ao risco de que o incêndio resultante pudesse ter submergido outras

partes de Plimsolla, os zirtianos moveram-se para apagar o incêndio.

Nas redes sociais, começaram a circular "fake news" provenientes de Parousia, que afirmavam que as forças da OTAN eram responsáveis pela explosão do petroleiro. Os nacionalistas em Parousia apelaram posteriormente a medidas contra a UE e a OTAN. Por sua vez, "bloggers" de Zirta afirmaram que o sequestro foi encenado por Parousia para justificar uma intervenção militar na ilha e fomentar divisões dentro da UE.



As consequências

Nem Parousia nem Zirta eram membros da OTAN. No entanto, Zirta era um Estado-Membro da UE e, após o ataque do torpedo, invocou o artigo 222 [1] do Tratado sobre o Funcionamento da União Europeia (TFUE) - a "cláusula de solidariedade" - para obter o apoio das instituições da UE e dos outros Estados-Membros. Entretanto, Parousia afirmou veementemente que este não era

um assunto da OTAN e que a aliança não se deveria intrometer. A vizinha e rival de Zirta, a República Popular de Antiguara (um membro da UE mas não da OTAN) apoiou Parousia e bloqueou qualquer discussão sobre a crise no Conselho do Atlântico Norte. Zirta considerou primeiro a possibilidade de invocar o artigo 42.7 do Tratado da UE [2] (a "cláusula de assistência mútua") antes de optar pelo artigo 222, embora tenha sido advertida de que ao invocar estes artigos poderia legitimar o NPC. Ficou claro para Zirta que, para garantir uma resposta abrangente à crise, o artigo 222 era mais adequado.

Como esta foi a primeira vez que o artigo 222 foi invocado por um estado-membro da UE, Zirta argumentou que o fracasso da UE em responder à crise abriria um precedente negativo. As implicações jurídicas da crise eram vastas, dado o potencial recurso ao uso de meios militares ao abrigo do artigo 222. Na sequência de um pedido para explorar opções militares, os peritos jurídicos da UE ficaram divididos entre aqueles que consideravam que o artigo 222 determinava o envio de meios militares para o território de um estado-membro da UE, e os que argumentaram que o Artigo 42.1 dos tratados da UE só permitia destacamentos militares da UE fora da União.

As instituições da UE tentaram neutralizar a crise através da diplomacia: os líderes condenaram tanto o ataque com o torpedo como o NPC e decidiram que não negociariam directamente com o grupo terrorista.

Bruxelas também fez contactos bilaterais com a OTAN e Parousia e pediu moderação para evitar uma escalada militar.

Com base na gestão de crises da UE e nas estruturas de protecção civil, foi decidido planear potenciais evacuações das principais cidades de Zirta para diminuir o risco representado pelos mísseis de cruzeiro Excalibur. A UE também enviou meios de protecção civil e assistência humanitária a Zirta para lidar com a explosão do porto.

Após essas acções, Parousia reclamou publicamente que a UE não estava a agir como um intermediário honesto. Argumentou que Zirta violou o artigo 24 da Convenção das Nações Unidas sobre o Direito do Mar (UN-

CLOS) [3] porque não protegeu o PK216 após as autoridades zirtianas terem concedido o direito de passagem ao submarino.

Contrariando esse argumento, Zirta afirmou que Parousia violou o seu território soberano ao tentar retomar o PK216 à força. Perante essa discordância, Parousia decidiu levar o assunto ao Conselho de Segurança da ONU (CSNU), onde alegou que a UE não tinha mais qualquer papel legítimo a desempenhar no impasse.

O único membro permanente da UE no CSNU, a França, e dois membros não permanentes, a Finlândia e a Espanha, apoiaram Zirta (assim como o Reino Unido), embora Parousia tivesse o apoio da China e dos membros não permanentes Antiguara, Irão e Venezuela.

Diplomatas de Parousia redigiram uma Resolução para o CSNU condenando as ações do NPC e, com referência à Resolução do CSNU 1950 [4] (2010) que autoriza os estados a intervir em caso de pirataria, argumentaram ter base legal para novas acções militares para apreender o PK216.

Os Estados membros da UE vetaram o projeto de resolução, argumentando que a Resolução 1950 era específica para a situação na Somália. Furioso com a rejeição, o embaixador paroussiano abandonou o UNSC em Nova Iorque, jurando que Parousia retomaria o seu submarino pela força, mesmo sem uma Resolução do UNSC.

Apesar desta situação, às 9h00 de 20 de Maio, membros da tripulação foram vistos a sair do PK216. Os primeiros relatórios afirmavam que a tripulação leal a Parousia havia conseguido retomar o controlo do navio.

Como aconteceu isto?

Esta foi a primeira crise do Artigo 222 com a qual a UE teve de lidar, apesar de antes ter realizado vários estudos internos e simulações. Embora Zirta tenha cumprido com as suas obrigações de segurança portuária da UE ao abrigo do Regulamento (CE) n.º 725/2004 [5] e da Diretiva 2005/65/CE [6], esta legislação não se aplica a navios de guerra (da UE ou outros). Além disso, enquanto o Plano de Acção da Estratégia de Segurança Marítima da UE [7], revisto em 2018, instava os Estados membros a melhorar a resiliência da infra-estrutura de transporte marítimo até 2020, Zirta tinha uma marinha relativamente pequena e um Ministério da Defesa com poucos recursos. Coube à guarda costeira e ao Ministério do Interior elaborar a estratégia de segurança do porto de Zirta - as considerações de defesa estavam notavelmente ausentes. A legislação relevante da UE em matéria de segurança portuária não acompanhou as considerações do artigo 222 e a UE não trabalhou em estreita colaboração com as autoridades civis nacionais para garantir que os aspectos de defesa fossem integrados nas estratégias de segurança dos portos.

Além disso, alguns estados membros reclamaram que Zirta se tinha aproximado economicamente de Parousia com investimentos internos, o que tornava difícil para o primeiro negar o direito de passagem ao PK216. Outros estados-membros sublinharam a importância de uma diligência prévia ("due diligence") quando submarinos estrangeiros entram nos portos da UE, incluindo a necessidade de uma lista mais abrangente dos membros da tripulação. Zirta rebateu essas afirmações, afirmando que os fluxos de investimento interno são uma questão soberana e que, mesmo que uma lista completa da tripulação do PK216 estivesse disponível, eles não teriam a capacidade de realizar verificações de inteligência. As instituições e os estados membros da UE não apoiaram Zirta nos seus procedimentos de verificação de inteligência. Isto, em última análise, foi um erro, dada a importância do planeamento para quaisquer contingências relacionadas com o Artigo 222.

---

[1] Artigo 222 do Tratado sobre o Funcionamento da União Europeia define que "A União e os seus

Estados-Membros actuarão em conjunto, num espírito de solidariedade, se um Estado-Membro for alvo de um ataque terrorista ou vítima de uma catástrofe natural ou de origem humana. A União mobiliza todos os instrumentos ao seu dispor, incluindo os meios militares disponibilizados pelos Estados-Membros".

[2] O artigo 42.7 do Tratado da UE afirma: "Se um Estado-Membro vier a ser alvo de agressão armada no seu território, os outros Estados-Membros devem prestar-lhe auxílio e assistência por todos os meios ao seu alcance, em conformi¬dade com o artigo 51 da Carta das Nações Unidas. Tal não afecta o carácter específico da política de segurança e defesa de determinados Estados-Membros".

[3] O artigo 24 da UNCLOS afirma que "O Estado costeiro dará a devida publicidade a qualquer perigo de que tenha conhecimento e que ameace a navegação no seu mar territorial".

[4] A Resolução 1950 refere-se à situação na Somália.

[5] O Regulamento (CE) n.º 725/2004 diz respeito ao reforço da protecção dos navios e das instalações portuárias.

[6] A Directiva 2005/65/CE respeita ao reforço da segurança portuária.

[7] Council of the EU, “Council Conclusions on the Revision of the European Union Maritime Security Strategy Action Plan,” 10494/18, June 26, 2018.

E se… um país criasse lixo espacial de propósito?

Gustav Lindstrom (director, EUISS)*

No final de 2021, um país que permanecerá sem nome decidiu levar os limites das ameaças assimétricas e híbridas para novas alturas - literalmente. No início, quando a ideia de introduzir detritos espaciais na órbita terrestre baixa (160 quilómetros a 2.000 quilómetros acima da superfície da Terra) foi apresentada aos dois assessores seniores do líder do país, ela foi descartada sem qualquer cerimónia [1].

Nenhum dos conselheiros a levou a sério, mesmo que tal movimento pudesse supostamente perturbar os serviços de satélite, desferindo um golpe nos arqui-inimigos no Ocidente. Um dos conselheiros até troçou da proposta, observando que a ideia era de alguém que "viu muitos filmes de Hollywood" ou que "levou a posição do líder para pensar fora da caixa um pouco longe demais".

Mais tarde e após uma reflexão mais aprofundada, no entanto, a ideia começou a ser apoiada.

Os assessores aprenderam que o desafio representado pelos detritos espaciais era real. Se os satélites fossem atingidos por destroços ou tivessem que mudar periodicamente o seu posicionamento para evitar colisões com destroços, as suas capacidades poderiam ser degradadas, tendo impacto em serviços como os de observação da Terra ou nas comunicações.

E, embora todos na Terra sofressem com as consequências, isso afectaria os países ocidentais de forma desproporcional, dada a sua maior dependência desses serviços.

Os assessores também souberam que várias entidades monitorizam a trajectória dos destroços para minimizar os riscos de colisão. Eles ficaram surpreendidos ao saber que só o Comando Estratégico dos EUA rastreou mais de 20 mil peças maiores do que 10 centímetros. Antes de 2021, um novo

sistema baptizado de Space Fence permitiria o rastreamento de aproximadamente 200 mil objectos com 5 a 7 centímetros.

Certamente, isto tinha que ser um assunto sério!

Com a confiança renovada, os planos começaram a tomar forma. Três semanas depois, os assessores encaminharam a ideia ao líder para sua consideração. O plano dependia do aproveitamento da tecnologia rudimentar de mísseis e satélites do país para colocar um satélite em órbita terrestre baixa (LEO). Uma vez em órbita, o satélite seria destruído por uma carga explosiva no seu interior - criando uma quantidade significativa de destroços.

Eles já tinham avisado o líder de que a ideia era incomum, mas prometia. A espera ansiosa por uma resposta durou pouco: após dois dias, o líder apoiou a ideia com entusiasmo. Na sua mente, essa acção não apenas poderia desferir um golpe desproporcionalmente grande ao Ocidente mas também poderia abrir a porta para um estilo de vida mais simples, onde a tecnologia não ocupava mais o centro do palco ou se mostrava fiável. Se feito correctamente, eles provavelmente conseguiriam provar a sua inocência ou, pelo menos, serem capazes de alegar de forma plausível tratar-se de um acidente.

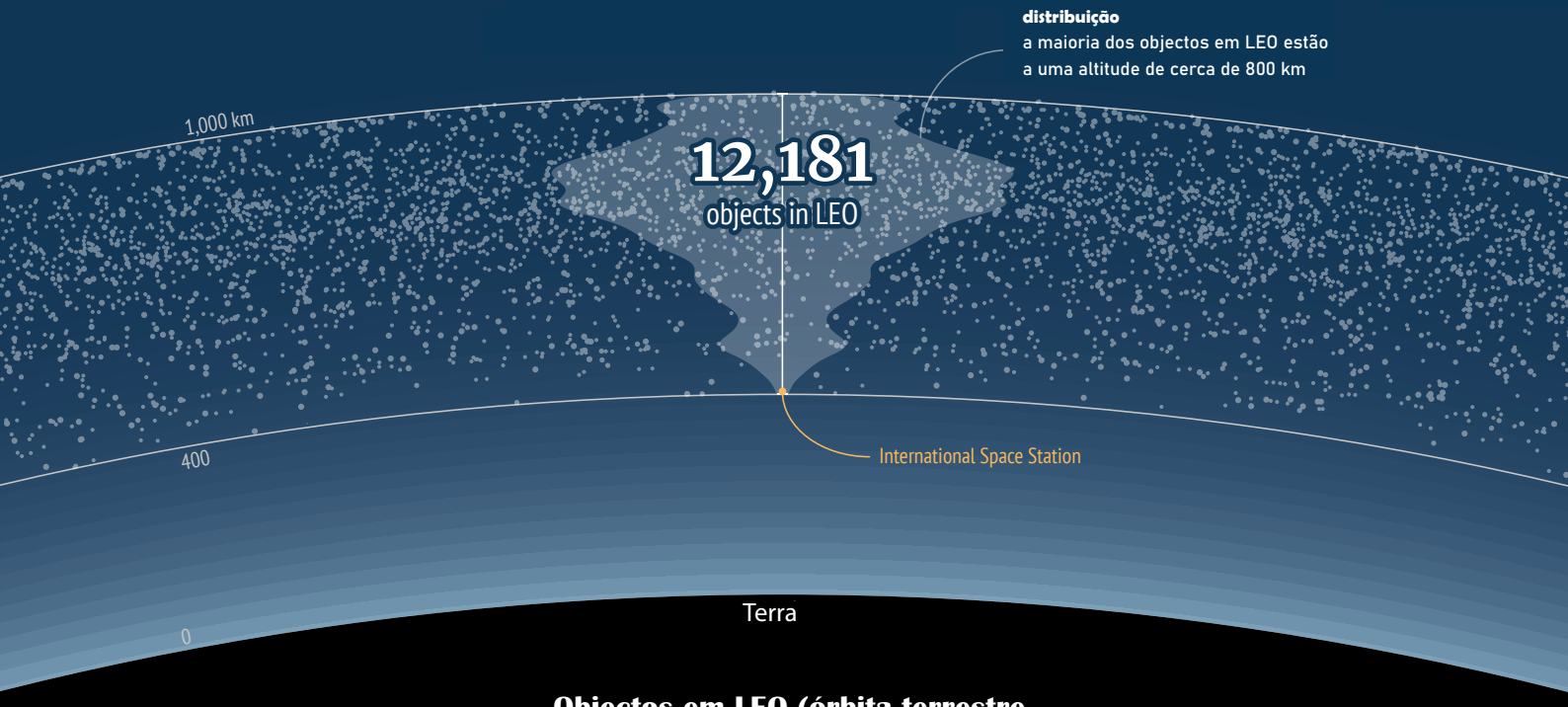
Na segunda-feira, 15 de Novembro de 2021 - três anos após a ideia ter sido apresentada pela primeira vez - o plano foi posto em prática. Naquela manhã, um veículo espacial foi lançado carregando um satélite de tamanho considerável. Depois do lançamento, o satélite entrou em órbita a aproximadamente 800 quilómetros acima da Terra.

Após cerca de uma hora em órbita, o explosivo explodiu, destruiu o satélite e enviou destroços em todas as direcções. Seguindo as ordens do líder, foi feito um anúncio afirmando que a tentativa do país de colocar um satélite de comunicações no espaço tinha falhado inesperadamente.

Independentemente da explicação, havia agora pelo menos 10 mil novos pedaços de lixo numa parte particularmente congestionada da LEO. Se os pedaços muito pequenos fossem contabilizados, incluindo os pequeníssimos

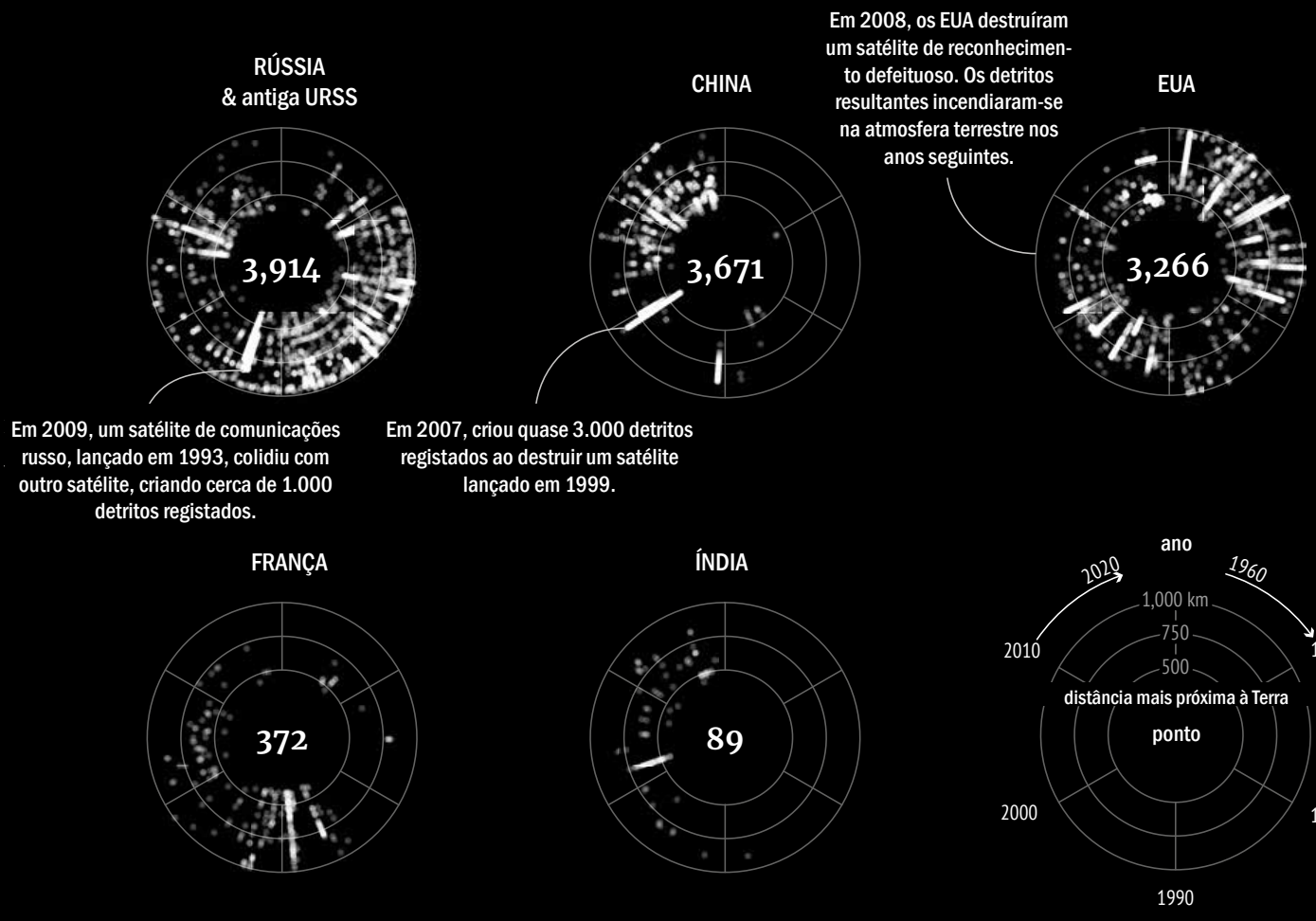
03

Objectos em órbitra terrestre baixa a 8 de Outubro de 2018



Objectos em LEO (órbita terrestre baixa) por data de lançamento

top 5 dos países com mais satélites em LEO



Dados: space-track.org, 2018

objectos, o número era muito mais elevado.

As consequências

O evento, que foi rapidamente noticiado, surpreendeu a comunidade internacional.

Além de tentar entender o que acabara de acontecer, havia a preocupação com as possíveis consequências para outras infra-estruturas espaciais.

A atenção inicial concentrou-se na segurança da Estação Espacial Internacional (ISS).

Felizmente, a ISS, que normalmente opera a uma altitude orbital de 408 quilómetros, tem várias medidas de protecção, como escudos de detritos, um sensor de detritos espaciais e a possibilidade de realizar manobras de evasão [2]. Em circunstâncias extremas, e se o tempo o permitir, os astronautas podem até abrigar-se na cápsula Soyuz - como aconteceu antes - para esperar pela passagem dos destroços.

Um minuto após a explosão, a ISS começou a notar alguns efeitos. Vários micro-objectos chocaram contra os painéis solares da estação, danificando-os. Suspeitou-se que alguns apoios de mão, que ajudam os astronautas durante as caminhadas espaciais, poderiam ter sido impactados. Embora uma avaliação completa dos danos demorasse dias ou mesmo semanas, três dos oito painéis solares apresentavam defeitos. Em resultado disso, o uso de energia a bordo da estação foi racionado e as caminhadas espaciais temporariamente canceladas por receio de que as luvas de protecção se rasgassem nos corrimãos danificados. A estação espacial também precisaria de reparações para garantir que as suas baterias pudessem ser carregadas adequadamente.

Em breve, as preocupações focaram-se noutro lugar. Cinco minutos após a explosão, um satélite de observação da Terra viajando numa órbita sincronizada com o Sol foi atingido por detritos soltos.

As agências de notícias explicaram rapidamente as forças em causa. Citando a Administração Nacional de Aeronáutica e Espaço (NASA), explicaram que um pedaço de destroços de 10 centímetros viajando a 10 quilómetros por segundo atingiria uma força comparável de 7 quilos de TNT [3].

A destruição do satélite resultou num efeito em cascata, em que os novos destroços destruíram outro satélite passados três minutos. Ninguém teve tempo para reagir ou efectuar acções evasivas. Para muitos, esta foi uma demonstração clara da síndrome de Kessler em funcionamento: uma quantidade cada vez maior de detritos espaciais aumenta a probabilidade de os detritos colidirem com outros detritos, resultando numa quantidade cada vez maior de lixo espacial.

O resultado final foi a perda de dois satélites, uma estação espacial danificada e um LEO substancialmente mais congestionado. Os operadores de satélite tinham agora que fazer ajustes de posicionamento mais frequentes para manter os seus satélites fora de perigo. Além disso, várias operadoras [de telecomunicações] mudaram os seus satélites para órbitas mais altas para evitar os destroços, degradando alguns dos seus serviços. Elas também tiveram que aceitar uma redução na vida útil de alguns satélites, devido à necessidade de usar combustível a bordo para reposicionar os satélites. Olhando para o futuro, surgiram questões se futuras missões espaciais poderiam ser comprometidas devido a um anel de destroços em expansão na LEO. Havia o temor de que a comunidade internacional deixasse de ter o mesmo acesso ao espaço que tinha antes.

Como aconteceu isto?

Não houve um ponto claro de origem ou combinação de eventos que levaram a este incidente - mesmo com alguns a apontar para o precedente estabelecido pelos testes anti-satélite, a tendência para a militarização do espaço, ou a falta de medidas de mitigação de detritos espaciais nos tratados da ONU que lidam com o espaço sideral.

Em vez disso, o evento colocou três questões para consideração posterior. Primeiro, que havia uma necessidade de entender melhor os riscos de segurança representados pelos detritos espaciais, especialmente numa LEO já congestionada. Esta questão vai provavelmente aumentar em importância à medida que novos actores, em particular do sector privado, entram no mercado dos satélites. Alguns observadores apontam para a indicação inicial de que milhares de pequenos satélites podem ser lançados na LEO na próxima década para aumentar o acesso à Internet de banda larga [4].

Uma segunda consideração foi o reconhecimento de que o desafio dos detritos espaciais dificilmente irá melhorar com o tempo sem medidas pró-activas. A acção necessária pode variar dos esforços para recolher fisicamente os detritos de grande porte até à implementação das directrizes existentes que definem como se descartar dos satélites no final da sua vida útil.

Por último, houve o reconhecimento de que quanto mais o mundo depende de serviços baseados no espaço, mais vulnerável está para a disrupção. Embora os efeitos de tais disrupções sejam sentidos em todo o mundo, eles variam entre os países, dependendo da sua dependência de tais serviços. Essa divergência no uso poderia, por sua vez, encorajar actores a considerar atingir a infra-estrutura espacial - directa ou indirectamente - para alcançar efeitos assimétricos adicionais. Na verdade, alguns começam a questionar-se se foi isso que aconteceu neste caso em particular.

** O autor expressa os seus agradecimentos ao EU Satellite Centre bem como a Laurent Muhlematter, consultor de segurança espacial no Geneva Centre for Security Policy, pela sua útil revisão deste capítulo.*

- - - - - - - - - -

[1] Matt Williams, "What is Low Earth Orbit?", Universe Today, 6 de Janeiro, 2017.

[2] European Space Agency, "Where is the International Space Station?", 18 de Dezembro, 2018.

[3] NASA, "Micrometeoroids and Orbital Debris (MMOD)", 14 de Junho, 2016.

[4] Caleb Henry, "LEO and MEO Broadband Constellations Mega Source of Consternation", 13 de Março, 2018.

E se… o Sol levasse a uma ciberguerra?

Patryk Pawlak (responsável executivo em Bruxelas, EUISS)
Nathalie van Raemdonck (analista associada, EUISS)

A 26 de Junho de 2021, o povo de Karenia, Timbabu, Sorea e Norea acordou de uma noite de comemorações após a assinatura do Pacto de Não-Agressão entre essas grandes potências. Mas alguns foram acordados mais cedo: o gabinete de Timbabu reuniu-se às 06h35, após dois comboios de alta velocidade entre as principais cidades do país, Noronha e Xica, colidirem no seguimento de uma falha no sistema de controlo de tráfego. As quedas de energia dificultaram o funcionamento dos serviços de emergência e a resposta às chamadas. Com a ligação à Internet aparentemente interrompida, até mesmo os serviços vitais com geradores de electricidade de "backup" tentaram fornecer serviços essenciais. Além disso, as operadoras de telemóveis não podiam fornecer serviços de comunicações, tornando difícil às equipas de gestão de crises coordenar esforços.

Vários outros acidentes foram relatados - ironicamente agravados pela dependência da Internet das Coisas (Internet of Things ou IoT) e a adopção de tecnologias inteligentes. Ambas transformaram Noronha na primeira verdadeiramente Smart City, com uma ampla dependência de inteligência artificial e de robôs para interacções básicas de serviço público (por exemplo, responder a chamadas, marcar compromissos, etc.) que re-afirmou a liderança de Timbabu neste domínio.

Mas sem a Internet, tudo isso se tornou num problema: com a rede inteligente desactivada, os metros sem condutores pararam de circular pelos túneis e os acidentes de trânsito aumentaram. O número de vítimas registado às 10h30 era de 654, com mais de 700 outras pessoas feridas. A economia do país também sofreu um forte golpe, com a perturbação a resultar em perdas económicas significativas para o mercado bolsista.

Com informações limitadas disponíveis, o Grupo de CiberDefesa do país concluiu que esta crise só poderia ser resultado de um ataque distribuído de nega-

ção de serviço (DDoS) em larga escala que incapacitou centrais eléctricas, desactivando redes de eletricidade em grandes regiões e paralisando o tráfego da Internet. Relatórios prévios de inteligência sugeriram que pequenos ataques DDoS testando as redes de energia poderiam ser atribuídos à Norea.

Com os Estados Unidos (o principal aliado regional de Timbabu) a recusar envolver-se, no dia seguinte o gabinete decidiu lançar um ataque aéreo contra a infra-estrutura militar de transportes e de telecomunicações de Norea - a primeira vez que tal acção foi realizada desde a guerra que dilacerou toda a região, excepto nas décadas de 1930 e 1940 - num esforço para impedir o que acreditava ser um ciberataque originado de Norea. A Operação "Paz Eterna" resultou em 132 mortes.

As consequências

O ataque armado de Timbabu à Norea gerou uma crise diplomática internacional. Quando a rede eléctrica de Timbabu permaneceu desligada por mais quatro dias, Karenia convocou uma sessão de emergência do Conselho de Segurança da ONU, o que levou a uma Resolução da ONU pedindo um diálogo e uma cessação imediata de quaisquer hostilidades. Na ausência de uma resposta militar de Norea - agindo sob conselho de Karenia - e uma rápida suspensão de novas operações em Timbabuan, a diplomacia teve uma hipótese quando Marja Selin, uma diplomata finlandesa, foi nomeada chefe da Comissão Especial de Inquérito da ONU para Timbabu.

O processo liderado por Selin - e implementado com total cooperação do governo de Timbabu - chegou a várias conclusões importantes. Em primeiro, parecia que as ciberoperações anteriores e que os serviços de inteligência de Timbabuan atribuíram à Norea foram, na realidade, conduzidas pelo grupo hacktivista soreano Cyberian Tiger. No passado, o grupo expressou o seu descontentamento com a negociação do Pacto de Não-Agressão, ao qual se opôs devido à sua suposta "negligência dos anos de injustiça causada pelo regime noreano ao povo de Sorea".

Usando "bandeiras falsas" - uma técnica que permite a um invasor esconder a

sua identidade e deixar para trás provas a apontar para outra entidade -, o grupo enganou os serviços de inteligência japoneses para atribuírem erradamente as operações à Norea. Ao que parece, o grupo também examinou e testou a resistência das subestações de transformadores de energia em Noronha e Xica nos meses anteriores ao incidente.

No final, no entanto, descobriu-se que nem a Norea nem o grupo hacktivista foram responsáveis pelo "ciber-terramoto" - nome dado à crise pelos media. Uma verdade ainda mais preocupante emergiu: as quebras de energia e o subsequente mau funcionamento da infra-estrutura que durou entre 26 de Junho e 1 de Julho foram causadas não por um ciberataque, como se acreditava, mas por explosões solares. Essas correntes induzidas geomagneticamente que o sol liberta esporadicamente danificaram as subestações transformadoras de energia e afectaram as redes de energia, de maneira semelhante ao que ocorrera no Quebeque em 1989.

Parece que relatórios sobre as explosões solares iminentes (e indicações sobre os danos que poderiam causar) foram transmitidos ao centro de gestão de crises uma semana antes, mas o seu impacto foi subestimado pela liderança política de Timbabu. Além disso, constatou-se que cenários semelhantes foram simulados pelo governo de Timbabu em 2020, antes dos Jogos Olímpicos de Noronha, mas as lições identificadas não foram incorporadas nos procedimentos da gestão de crises do país. Com essas provas nas mãos, a resposta militar - em violação ao Artigo 9 da constituição de Timbabu - levou a uma crise constitucional e à renúncia do primeiro-ministro de Timbabu.

Os resultados da investigação encorajaram a Norea a procurar compensação de Timbabu no Tribunal Internacional de Justiça (TIJ). Em 2025, o TIJ emitiu a sua decisão apoiando a Norea. A sentença concluiu que o ciberataque de Timbabu constituiu uma violação dos artigos 2(4) e 51 da Carta das Nações Unidas, relativos à proibição do uso da força e ao direito à legítima defesa. O TIJ reconheceu que, apesar do facto de que "a escala e os efeitos dos danos sofridos por Timbabu poderiam ter constituído o uso da força" e "equivaler a um ataque armado", se realmente tivesse sofrido um ciberataque, o governo de Timbabu não teve "suficientemente em consideração todas as circunstâncias

04

Maiores tempestades solares com impacto nos sistemas eléctricos terrestres

eventos extremos do clima espacial desde a medição da actividade solar

1859
EVENTO DE CARRINGTON
A primeira erupção solar disruptiva registada com a maior actividade geomagnética nos últimos 160 anos. Inutilizou o uso das linha de telégrafo em todo o mundo.

1940
ERUPÇÃO DO DOMINGO DE PÁSCOA
As comunicações a longa distância foram danificadas com mais de 2,600 volts registados num cabo atlântico.

1946
"BLACKOUT" DA RÁDIO
Uma erupção solar causou um quase completo apagão dos sinais de rádio no hemisfério norte.

1989
"BLACKOUT" DO QUEBEQUE
Uma erupção solar danificou uma estação de transmissão eléctrica no Quebeque, colapsando a distribuição de energia na região.

2000
TEMPESTADE DO DIA DA BASTILHA
Curto-circuitos em satélites e "apagão" de rádios nos EUA.

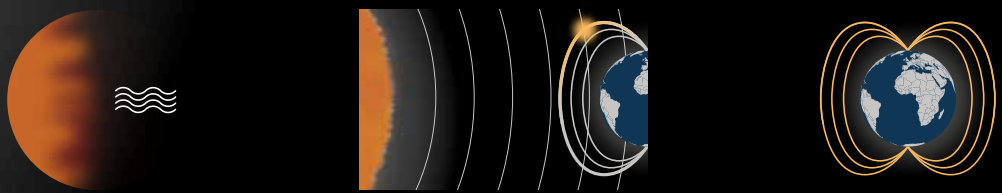
2006
TEMPESTADE GEOMAGNÉTICA
Na erupção solar registada mais rapidamente a atingir a Terra, ocorreram problemas nas comunicações de satélites para as estações terrestres.

1921
A GRANDE TEMPESTADE
Erupção solar incendiou estação telefónica na Suécia e desactivou o sistema de comutação ferroviário de Nova Iorque.

1958
MÁXIMO SOLAR
Registo do número mais elevado de erupções solares, com perturbações nos sinais de rádios durante vários dias.

1972
TEMPESTADE DA IDADE ESPACIAL
A primeira vez que se previu que uma erupção solar atingiria a Terra, a comunicação telefónica a longa distância foi afectada durante horas.

2003
TEMPESTADE DO "HALLOWEEN"
Problemas técnicos em satélites e falta de energia eléctrica na Suécia.



ERUPÇÕES SOLARES...

As explosões solares e as ejecções de massa coronal (denominadas em conjunto de tempestades solares) surgem de erupções solares, que ocorrem a diferentes frequências durante os 11 anos do ciclo solar.

...ATINGEM O CAMPO MAGNÉTICO DA TERRA

Quando ocorrem as tempestades solares, nuvens de radiação electromagnética atingem o campo magnético da Terra em horas, o que por vezes resulta em auroras boreais.

...CAUSANDO PERTURBAÇÕES

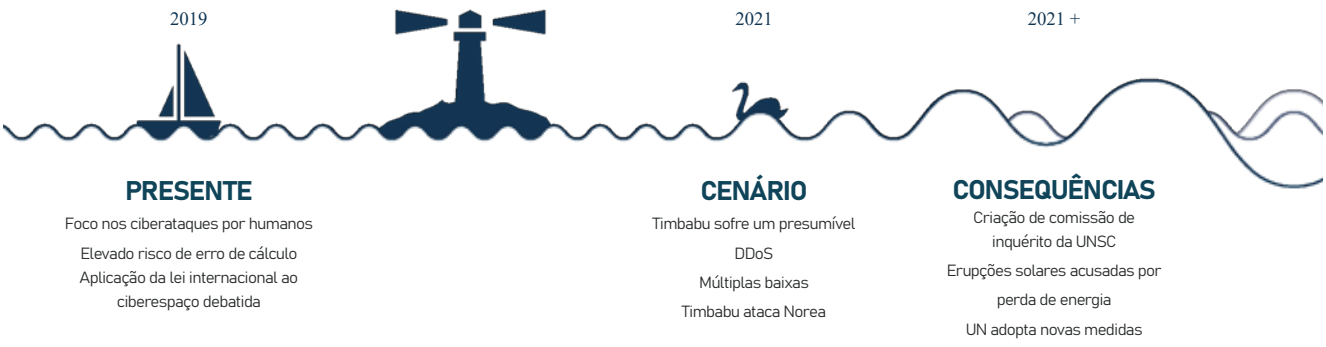
Isto pode afectar a ionosfera terrestre (perturbando as comunicações satélite/rádio) e atingir a superfície da Terra, levando a corrente geomagneticamente induzida para os sistemas eléctricos.

Dados: Royal Observatory of Belgium, Sunspot Index and Long-term Solar Observations, 2018

que envolveram o incidente".

Embora uma resposta militar possa ser considerada necessária e proporcional no caso de um ciberataque realizado por outro estado, o caso em questão claramente não atendia a esses critérios.

Com base nesse julgamento e reconhecendo os desafios crescentes de atribuição de actividades maliciosas no ciberespaço, a Resolução 1979/25 do Conselho de Segurança da ONU apelou a todos os Estados para se absterem do uso do ciberespaço para fins militares e declarou-o uma "zona livre militar" afim de prevenir qualquer conflito decorrente do uso das tecnologias de informação e comunicação (TICs). A fim de assegurar uma implementação adequada da Resolução 1979/25 do CSNU, a ONU adotou um conjunto de Medidas de Fortalecimento da Confiança vinculativas, incluindo um mecanismo de consulta compulsório. Também criou o Órgão de Solução de Conflitos para o Ciberespaço da ONU.



Como aconteceu isto?

Embora a maioria das discussões sobre cibersegurança se tenha concentrado em ataques maliciosos feitos pelo ser humano, a investigação mostrou que a maioria dos incidentes foi realmente causada por desastres naturais. Estudos têm mostrado que correntes induzidas geomagneticamente - por uma erupção solar ou uma tempestade geomagnética – estão entre as causas de possíveis choques globais futuros devido à sua capacidade de desligar redes condutoras, como redes de transmissão de energia eléctrica, oleodutos e gasodutos, cabos

submarinos não-ópticos de comunicações e redes telefónicas e telegráficas não-ópticas e ferrovias [1].

Uma série de ataques de alto perfil, como as botnets Mirai, WannaCry e NotPetya em anos anteriores, levou a um maior foco nas ciberactividades maliciosas e ao seu potencial impacto na estabilidade do ciberespaço. Ao mesmo tempo, a aplicação do direito internacional existente para o ciberespaço, normas de comportamento responsável do Estado e Medidas de Reforço de Confiança continuaram a ser discutidas nas Nações Unidas, na Organização para a Segurança e Cooperação na Europa (OSCE), na Organização dos Estados Americanos (OEA), e noutros formatos não governamentais, como a Comissão Global de Estabilidade no Ciberespaço. A adoção da Ciber Diplomacy Toolbox levou a uma maior reflexão sobre a possível resposta da UE, mas os desafios associados à atribuição de ciberactividades maliciosas ainda limitam as opções para uma dissuasão eficaz [2].

Apesar do progresso significativo feito pelo Grupo de Especialistas Governamentais da ONU em 2013 e 2015, questões como a diligência prévia ("due diligence ") dos estados e o uso de contramedidas ainda não foram abordadas. Em 2018, apenas um punhado de países - incluindo os EUA, o Reino Unido e a Austrália - tinham declarado publicamente as suas posições sobre a aplicação do direito internacional ao ciberespaço, o que significa que o risco de erro de cálculo e conflito permaneceu elevado, quando nenhum regime global foi aplicado.

- - - - - - - - - -

[1] OECD, Geomagnetic Storms, OECD/IFP Futures Project on “Future Global Shocks”, Janeiro 2011.

[2] Erica Moret e Patryk Pawlak, “The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?”, EUISS Brief no. 24, (Julho 2017).

E se… houvesse uma nova Primavera Árabe?

Florence Gaub (director, EUISS)*

Em 2021, o mundo do futebol começou a preparar-se para o Mundial de Futebol da FIFA em 2022 no Qatar, assim que começaram as eliminatórias. A competição foi muito aguardada pelos fãs árabes de futebol, principalmente porque três países árabes se classificaram para o torneio anterior e houve duas candidaturas árabes para ser a sede do evento em 2030 (o Egipto sozinho e uma candidatura conjunta da Argélia, Tunísia e Marrocos) [1].

Para o jogo inaugural, a selecção egípcia foi sorteada para jogar contra o Gana. Poucos minutos após o apito inicial, o impensável aconteceu: o craque Mohammed Salah foi brutalmente abordado e caiu no chão em agonia. De forma polémica, o culpado guarda-redes ganês recebeu apenas um cartão amarelo do árbitro argelino. Quando Salah foi levado para fora do campo, os fãs egípcios reagiram com fúria - principalmente online, já que apenas 10 mil pessoas puderam assistir ao jogo ao vivo (o Egipto proibiu a participação em jogos de futebol após 2012 devido a confrontos regulares entre fãs e forças de segurança e só gradualmente começou a permiti-lo a partir de 2018) [2]. Apenas alguns segundos depois, as redes sociais - Facebook, Twitter e Instagram - explodiram com imagens de Salah chorando a sair de campo. Tal como em 2009, quando fãs argelinos e egípcios se confrontaram após um jogo de qualificação, as emoções aumentaram [3].

Em duas horas, #justiceforMo já era uma tendência online, com quase um milhão de tweets e mais de meio milhão de "posts" no Instagram - a maioria originalmente do Egipto, mas a "hashtag" espalhou-se rapidamente pela Tunísia, Jordânia, Arábia Saudita e, em seguida, para o Reino Unido, Alemanha, Itália e França. A comunidade mundial do futebol estava em alvoroço e, quando os fãs egípcios se reuniram em frente à embaixada da Argélia na Ilha Gezira, no Cairo, as autoridades não intervieram inicialmente, pois consideraram a indignação uma expressão saudável de nacionalismo. Mas quando os manifestantes se dirigiram para a Praça Tahrir gritando "ele quer justiça, nós queremos justiça", e #justiceforMo se transformou em #justiceforMasr (*Egip-*

to em árabe), o governo começou a entender que a agitação relacionada com o desporto estava a tomar um rumo político.

Forças de segurança foram enviadas e começaram a reprimir violentamente os fãs.

O Twitter e o Facebook foram bloqueados, mas demorou nove horas para fazer o mesmo ao Instagram - uma rede de media social vista anteriormente como apolítica. As forças policiais tentaram dispersar as multidões cada vez maiores mas, apesar do apagão forçado da Internet, as redes dos ex-fãs dos clubes de futebol do Cairo, os Ultra White Knights e os Ultras Ahlawy, rapidamente encontraram métodos alternativos de mobilização [4].

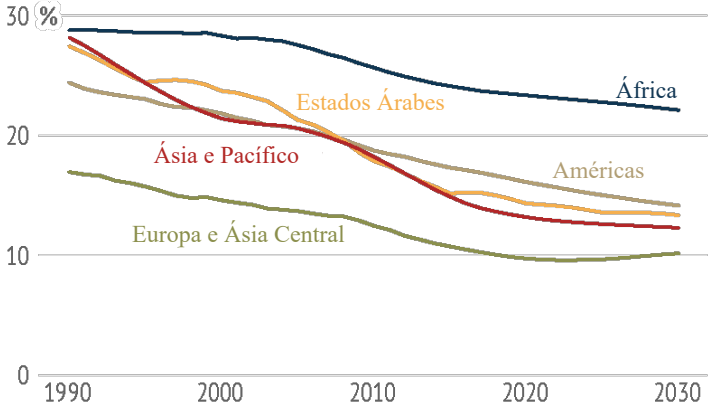
As consequências

24 horas após o incidente, milhares de manifestantes reuniram-se nas ruas do Cairo, bem como em Tunes, Amã e Beirute.

Antes do pôr do sol, #justiceforMiddleEast e #justiceforME eram virais. Em face dos protestos em massa, as forças de segurança recorreram à violência ou desapareceram. Enquanto observadores internacionais - incluindo jogadores de futebol e comentadores - pediam moderação, hackers atacaram sites do governo do Egipto e da Arábia Saudita, cobrindo-os com imagens de Salah e a legenda "Cartão vermelho para este governo". Uma mensagem de vídeo de Mohammed Salah, na qual ele pedia aos seus fãs para manterem a calma, só piorou as coisas - o rumor de que as autoridades o forçaram a gravá-la espalhou-se mais rapidamente do que qualquer outro elemento da história, e #FreedomforMo começou a ser uma tendência online.

Tendências e projecções da força de trabalho jovem

Quota dos 15 aos 24 anos no total da força de trabalho por regiões



Dados: International Labour Organization, 2018

Os governos da região reagiram de forma diferente à eclosão de distúrbiosem grande escala, mas nenhum conseguiu contê-la; o aumento da violência fez crescer uma maior resistência. Na Tunísia, as forças policiais confrontaram-se repetidamente com os manifestantes, com quatro pessoas mortas na primeira semana. No Egipto, tanto a polícia como as forças militares usaram de violência excessiva e tentaram manter esta postura perante os protestos recorrentes; no final da primeira semana, o Egipto lamentou mais de 300 vítimas. No final da segunda semana, quando ficou claro que a escalada de violência não resolveria o problema, os apelos do presidente Sisi para o diálogo não foram ouvidos. Mesmo na Líbia, onde partes do país permaneceram fora do controlo do governo, os cidadãos foram para as ruas exigir o desarmamento das milícias. Na Síria, os insurgentes encheram ruas inteiras com bolas de futebol, interrompendo fortemente o tráfego, e hackers atacaram o site do governo, colocando uma foto de Abdul Baset al-Sarout (um jogador sírio que se juntou à oposição durante a guerra civil) ao lado das palavras "Cada jogo tem duas metades".

Uma série de carros-bomba explodiu na Síria, matando pelo menos 21 soldados russos e iranianos. Também ocorreram manifestações em Argel e Bagdade, mas não foi registada nenhuma vítima.

Quando a violência entrou na sua terceira semana e as forças de segurança se mostraram incapazes de lhe pôr fim, os decisores regionais e europeus entenderam que não se tratava de algo efémero. A escolha dos decisores regionais foi clara: recorrer a mais violência e repressão e lançar a região para uma década ainda pior de instabilidade, crise económica e insegurança - ou reformar.

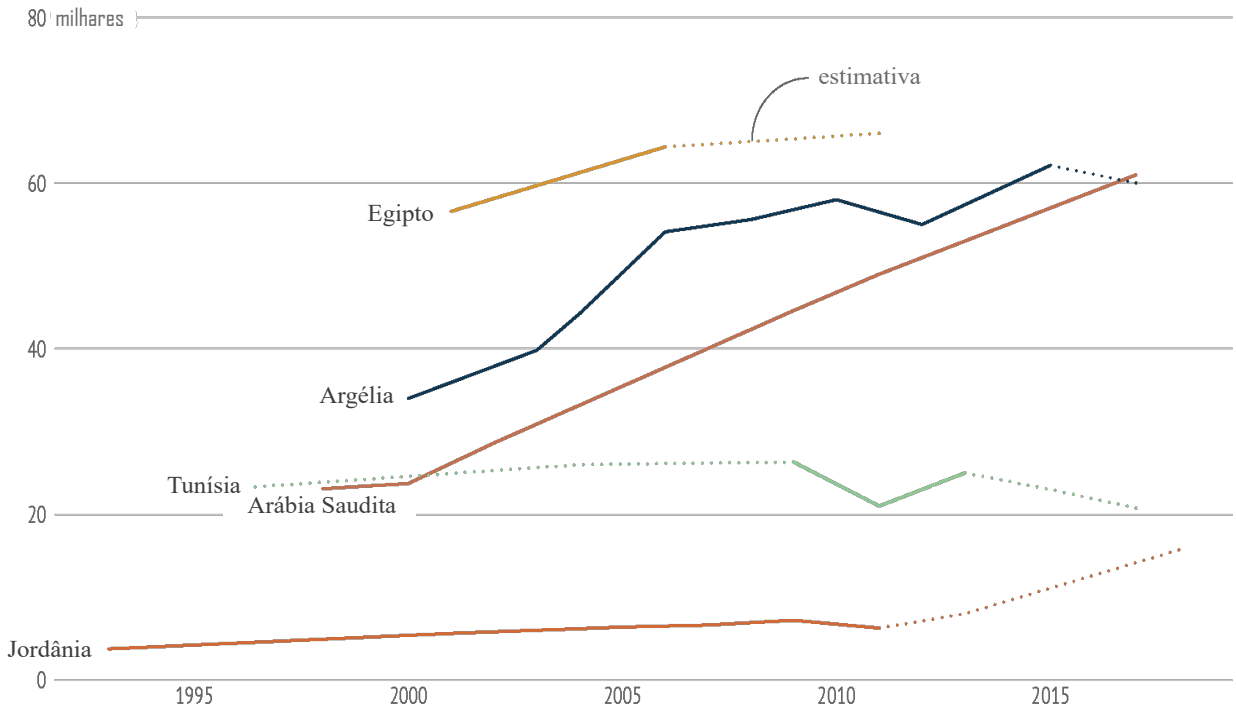
Como aconteceu isto?

A repressão prolongada nos anos após a Primavera Árabe criou a ilusão de que os protestos na região não seriam possíveis de repetir; em 2018, apenas no Egipto, mais de 60 mil activistas estavam presos, mais de 500 sites bloqueados e entidades colectivas - de grupos de fãs de futebol a associações de farmacêuticos - foram colocadas sob vigilância do governo ou dissolvidas [5].

O fim das operações militares na Síria em 2019 só aumentou a percepção de que, pelo menos temporariamente, a democracia estava paralisada na região.

Está a ficar lotado

População prisional nalguns países do Médio Oriente e África do Norte (MENA), 1998-2018



Dados: World Prision Brief, 2018

Os decisores regionais não viram assim nenhuma necessidade premente de reformar o mercado de trabalho, promover um ambiente de negócios que encorajasse a criação dos 27 milhões de empregos necessários ou empenharem-se em políticas inclusivas. A actividade económica dos militares egípcios, por exemplo, sufocou o sector privado, contribuindo para níveis ainda mais baixos de criação de empregos do que os conseguidos antes da Primavera Árabe. Na Tunísia, os monopólios que foram criados no governo do presidente Ben Ali mantiveram-se, causando problemas semelhantes. Um ambiente internacional que frequentemente se concentrava miopicamente no terrorismo e na migração em detrimento da democracia e da reforma económica pouco fez para reverter essa dinâmica regressiva [6].

Entretanto, todos os principais factores que desencadearam a Primavera Árabe em 2011 pioraram progressivamente. O desemprego juvenil, por exemplo, aumentou de 28% em 2010 para 34% em 2017 no Egipto, de 29% para 35% na Tunísia, de 30% para 39% na Jordânia e de 22% para 24% na Argélia [7]. Crucialmente, a disparidade dos rendimentos também piorou: 10% da população da região possuía 61% da riqueza, tornando-a a área menos igualitária do mundo. Ao mesmo tempo, o crescimento dos jovens na região prosseguiu - nos dez anos após a Primavera Árabe, a população do Egipto cresceu 20 milhões, com 57% da população a ter menos de 24 anos até 2021. O grupo entre os 15 e os 29 anos (também chamada de "idade da luta") atingia os 24 milhões - um número demasiado grande para controlar. Para manter os grupos descontentes sob controlo, a maioria dos governos da região aumentou o seu domínio sobre os media; o Egipto caiu 34 lugares no Freedom of Press Index entre 2010 e 2018, por exemplo [8].

No entanto, os governos da região não conseguiam impedir o acesso à Internet por completo: 35% da população do Egipto eram utilizadores da Internet em 2011, crescendo para 55% em 2019, enquanto metade do país tinha uma conta no Facebook [9]. E a incontrolabilidade da Internet era especialmente visível quando se tratava do Instagram, que ultrapassou o Twitter e o Facebook como a rede de media social favorita dos egípcios. Os fãs de futebol, em particular, acharam esta como uma saída ideal para a sua paixão, após terem sofrido com a pressão política após a Primavera Árabe. Mais de 21% dos utilizadores do Instagram (cerca de 146 milhões de pessoas) eram fãs de futebol, mas as autoridades da região percebiam o canal de media social como um meio não ameaçador devido à mistura predominante de "posts" de moda, viagens e desportos

- enfatizando o facto que as autoridades estarão sempre um passo atrás no que diz respeito ao policiamento do mundo online [10].

Em última análise, foi uma mistura de descontentamento e falta de progresso sócio-económico, combinado com as fortes redes sociais online e offline, que inevitavelmente levaram aos eventos de 2021.

** O autor agradece a Jakob Penner, do We Play Forward, Sascha Hahn, da Sport1, bem como a Christian Dietrich, Daniel Fiott e John-Joseph Wilkins, do EUISS, pela sua contribuição para este capítulo.*

---

[1] "Egypt Planning Bid to Host 2030 World Cup Despite Economic Woes", The New Arab, 11 de Julho, 2018; Ramy Allahoum, "Algeria Mulls Joint 2030 FIFA World Cup Bid with Morocco, Tunisia", Al Jazeera, 4 de Julho, 2018.

[2] Hend El-Behary, "Egypt Football Fans Gradually Allowed to Return to Stadiums", Egypt Independent, 7 de Agosto, 2018.

[3] Abigail Hauslohner, "The Political Fallout of Egypt's Soccer War", Time Magazine, Novembro, 2009.

[4] James Dorsey, The Turbulent World of Middle East Soccer (London: Hurst, 2016); John Duerden, "Football and the Arab Spring", ESPN, 4 de Fevereiro, 2012.

[5] Arabic Human Rights Network, "There is Room for Everyone… Egypt's Prisons Before & After January 25 Revolution", Setembro 2016; Arabic Human Rights Network, "The Battle is not Over... Internet and the Arab Governments", Setembro 2017.

[6] Andrew England, 'Middle East Jobs Crisis Risks Fueling Unrest, IMF Warns", Financial Times, 12 Julho, 2018.

[7] Arjun Kharpal, "'Alarming Scale' of Youth Unemployment in Middle East, OECD Official Warns'", CNBC, 12 de Fevereiro, 2017; Stratfor, "Youth Unemployment: The Middle East's Ticking Time Bomb", 28 de Fevereiro, 2018.

[8] Reporters without Borders, "Freedom of Press Index 2018", 2018.

[9] Mohamed Alaa El-Din, "Egypt is the Largest Arab Country Using Facebook with 17 Million Users", Daily News Egypt, 12 de Outubro, 2018.

[10] Andrew Hutchinson, "How Facebook and Instagram Users Engaged with the World Cup", Social Media Today, 17 de Julho, 2018.

E se...?

Futuros para 2024

Introdução

Qualquer apreciador de ficção científica sabe que o género parece ser surpreendentemente bom a prever o futuro: satélites, alunagem, telemóvel, impressão 3D e até antidepressivos foram todos apresentados em romances, filmes e séries de TV, várias vezes muito antes de realmente se materializarem [1]. Isso significa que os autores de ficção científica são melhores a prever do que outros? Claro que não.

Um mecanismo diferente está presente: quando os humanos vêem a possibilidade de inovação, eles inadvertidamente se inspiram nela. (Por uma razão ainda desconhecida, este é ainda mais o caso hoje do que no passado) [2]. A ficção científica não é, portanto, um mecanismo de previsão extraordinariamente preciso, mas em vez disso actua como um ciclo de "feedback": porque as pessoas vêem filmes de ficção científica, elas entendem ideias sobre como podem moldar o futuro.

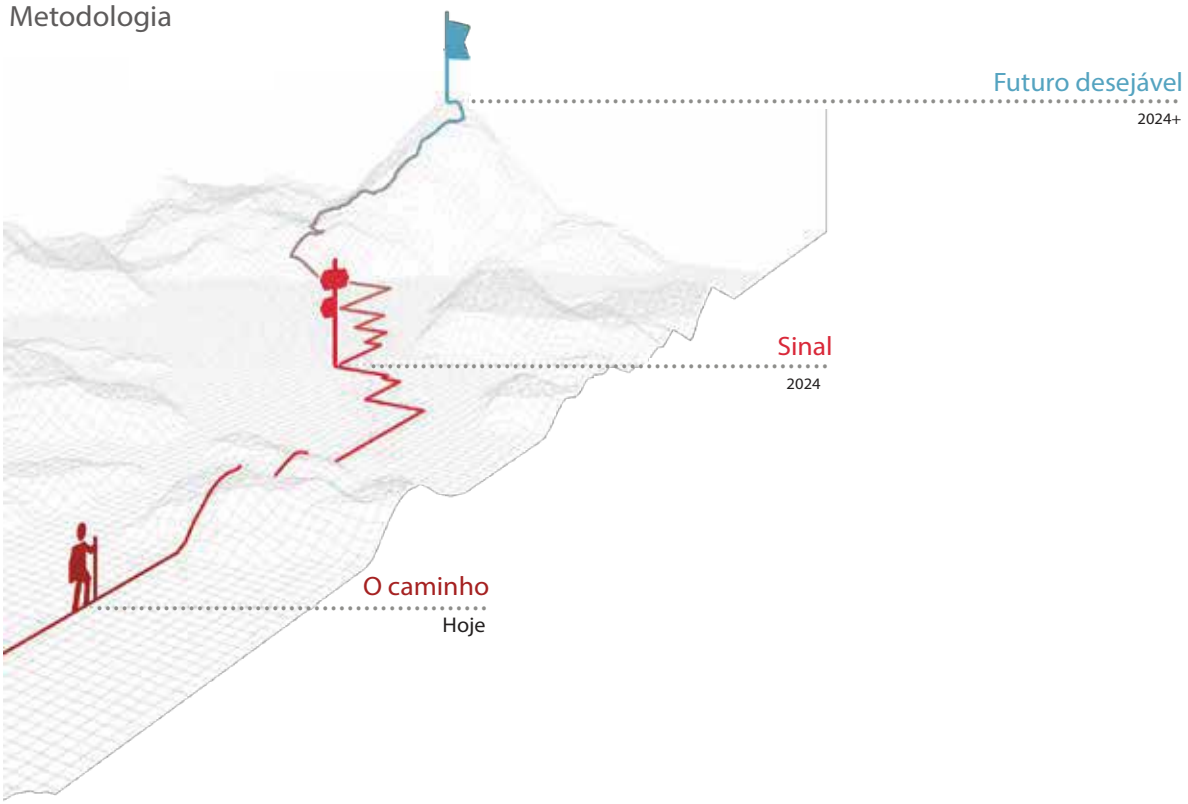
Este "loop" não se aplica apenas à ficção mas a todos os tipos de domínios voltados para o futuro. Veja-se a ciência, por exemplo: no século XVII, o cientista Robert Boyle escreveu uma lista de 24 inovações que ele esperava resolvessem uma série de problemas humanos, incluindo o "prolongamento da vida, a arte de voar, a arte de estar muito tempo debaixo de água, a cura de feridas e doenças por transplante, a aceleração da produção de coisas a partir de sementes e medicamentos para apaziguar a dor" [3]. Mais de 300 anos depois, a grande maioria dos itens da lista de Boyle tornou-se realidade - não porque ele tivesse uma bola de cristal, mas porque ele e a sua lista de desejos influenciaram como a Royal Society, e uma série de outros cientistas após ele, concentraram os seus esforços de investigação. Nesse sentido, visões e utopias não são ingénuas: podem servir de inspiração para a ciência, mas também para a formulação de políticas.

Os cenários também podem ter esse efeito: ferramentas populares que dão vida a um futuro distante, os cenários são essencialmente histórias para adultos, que ajudam a suspender a descrença e a orientar os nossos decisores.

Mas eles podem contar diferentes tipos de histórias: nos nossos dois anteriores Chaillot Papers ""What If..." (2017 e 2019), os cenários eram avisos de futuros possíveis, inspirando acções para os evitar.

Neste Chaillot Paper - como sempre, um verdadeiro esforço de equipa do EUISS - mudámos de direção, seguindo o exemplo da ficção científica, ao propor cenários desejáveis em 2024. No entanto, em contraste com Star Trek et al., não exibimos simplesmente futuros possíveis mas também se incluem os caminhos que nos podem levar até lá.

Esse tipo de metodologia é denominado de "backcasting". Onde a previsão olha para o futuro a partir do presente, o "backcasting" olha para o presente a partir do futuro. Escolhe-se um futuro preferido e definem-se os caminhos e marcos que podem levar a ele [4]. Devido à sua natureza de resolução de problemas, o "backcasting" é uma ferramenta particularmente adequada para a formulação de políticas. (Talvez por isso, surgiu primeiro no sector da energia com estudos pioneiros e a codificação do método no final dos anos 1970 e início dos anos 1980) [5].



Tal como a previsão, o "backcasting" é mais uma arte do que uma ciência: não existe uma metodologia rígida sobre como projectar o caminho a partir do futuro. É claro que, para ser mais do que uma fantasia incrível, deve incluir obstáculos e oportunidades; idealmente também define objectivos provisórios e o que alguns chamam de "sinais", designando um evento futuro potencial reconhecível que sinaliza uma mudança significativa no caminho para o futuro desejado [6].

Os cenários neste Chaillot Paper seguem todos a mesma estrutura, levando-nos não apenas numa viagem ao futuro, mas também de volta ao presente: eles começam com a sinalização definida em 2024, descrevem o futuro desejável nos anos para lá dessa data, e traçam o caminho que liga essa situação aos dias de hoje.

A razão para essa estrutura não linear é que todos os cenários giram em torno de uma mudança de política que provavelmente não será alcançada em apenas um ciclo político - portanto, é crítico conseguir a continuidade entre eles. Mas se forem dados os passos recomendados, os sinais, indicando a mudança estratégica, serão visíveis em 2024 - o ano em que termina o mandato desta geração de líderes da UE. Isto não é para os distrair das muitas outras tarefas que terão de enfrentar durante o seu mandato mas é uma contribuição para lidar com as profundas mudanças que estão a ocorrer.

Nesse sentido, esses cenários podem ser lidos como recomendações de política disfarçadas, pois trazem à vida uma situação em 2024 que poderia ser o resultado positivo do trabalho desta geração. Mas os cenários de "backcasting" não são apenas recomendações; uma vez que giram em torno de uma ideia clara - e até normativa - de um determinado futuro, eles exigem um forte entendimento de que tipo de futuro é realmente desejável num determinado contexto. Se houver incerteza sobre o futuro preferido, o "backcasting" pode, assim, servir como um plano para formar a opinião pública antes de realmente servir como um mapa para a formulação de políticas.

Por fim, cenários, visões partilhadas para o futuro e etapas telescópicas acor-

dadas são úteis na jornada que levará de uma visão newtoniana do mundo (onde este é essencialmente mecanicista, compreensível e, portanto, gerível) para uma visão quântica do mundo (onde tudo é ligado, complexo e requer mais do que apenas conhecimento para resolver um problema). Neste mundo, teremos que desacelerar, adoptar perspectivas mais longas e procurar soluções mais criativas na formulação de políticas. Ciclos eleitorais, tecnologia moderna e estilos de vida estão a empurrar-nos para tomar decisões cada vez mais rápidas, e não apenas na formulação de políticas - executivos de negócios e organizações não governamentais (ONGs) também são forçados a pensar em termos trimestrais. Estudos mostram que o ritmo de vida aumentou 10% em todo o mundo desde meados da década de 1990 – e até 30% na Ásia. Os estudos históricos também sofrem com essa compressão do tempo: nas últimas duas décadas, a investigação encolheu para examinar intervalos de tempo de no máximo 50 anos, perante mais de 75 no início do século XX. A arte de adoptar uma visão a longo prazo, "la longue durée", está a desaparecer ao mesmo ritmo que os problemas se tornam mais complexos - em detrimento da formulação de políticas visionárias [7].

A prospectiva e os seus primos podem ajudar nisso: por design, ela é orientada para um futuro mais distante (como arte, é notoriamente míope; quanto mais próxima do futuro, menos visível se torna). Pode alertar, mas também propor futuros positivos para os quais queremos trabalhar. Assim como a [revista] New Scientist pediu uma nova lista de desejos semelhante à de Robert Boyle para alcançar uma inovação positiva, esta publicação oferece uma série de futuros desejáveis pelos quais vale a pena lutar [8]. Na ausência de exercícios como este, a ficção científica e os pessimistas manterão o monopólio sobre as visões do futuro.

- - - - - - - - - -

[1] Peter Kotecki, "Here are 15 wild sci-fi predictions about future technology that actually came true", Business Insider, 12 de Janeiro, 2019.

[2] "When science fiction inspires real technology", MIT Technology Review, 5 de Abril, 2018.

[3] Ian Sample, "Robert Boyle: wishlist of a Restoration visionary", The Guardian, 3 de Junho, 2010.

[4] Karl Dreborg, “Essence of backcasting”, Futures, vol. 28, 1996, pp. 813-28.

[5] Amory B. Lovins, "Soft Energy Paths: Towards a Durable Peace" (New York: Harper & Row, 1979); John Robinson, “Energy backcasting: a proposed method of policy analysis”, Energy Policy, vol. 10, 1982, pp. 337-44.

[6] Ray Strong et al., “A new way to plan for the future”, Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS’07) 2007, IEEE Computer Society.

[7] Fernand Braudel, “La longue durée”, Réseaux, vol. 5, no. 27, 1987, pp.7-37; Jo Guldi & David Armitage, The History Manifesto, (Cambridge: Cambridge University Press, 2014).

[8] David Cannadine, “Longer life, flying, mind-bending drugs: Dreams that science made real”, New Scientist, 9 de Outubro, 2019.

E se… a UE lançasse a sua primeira cibermissão civil?

Patryk Pawlak

O Global Forum on Digital Security for Prosperity organizado pela Organização para Cooperação e Desenvolvimento Económico (OCDE) em Junho de 2024 não foi como qualquer outra edição anterior. Pela primeira vez, a conferência atraiu líderes de todo o mundo. A União Europeia foi representada pelo Comissário para o Mercado Interno e pelo Representante Especial para a Política Internacional do Ciberespaço.

A declaração deste Representante Especial foi clara: "Com o lançamento das ciberunidades civis (CCUs) sob a [Common Security and Defence Policy] CSDP em Janeiro de 2024, a UE provou mais uma vez o seu papel como fornecedor de segurança global apontado ao futuro". As CCUs, sublinhou, são o primeiro passo no esforço de adaptar os conceitos, ferramentas e instrumentos da UE aos novos desafios colocados pela gestão de conflitos e crises no ciberespaço.

Na verdade, em linha com as conclusões do Conselho dos Negócios Estrangeiros anteriores, a UE estava a preparar-se para lançar as suas primeiras cibermissões civis (CCMs da UE) em Outubro de 2024. Com o objectivo de fortalecer a resiliência do Estado e da sociedade, a CCM UE Vietname e a CCM UE Indonésia pretendiam enviar um sinal claro a todos os agentes maliciosos: a UE não iria tolerar violações das normas internacionais e utilizará todos os instrumentos à sua disposição para apoiar os países parceiros onde as ciber-operações maliciosas causam perturbação e instabilidade e aumentam o risco de conflito.

Em Novembro de 2023, a UE activou pela primeira vez a Cláusula de Defesa Mútua (Art. 42.7 TUE) na sequência de um pedido da França, que sofreu um ataque de ransomware significativo que paralisou as operações de vários contratantes responsáveis pela preparação dos Jogos Olímpicos de 2024, os sistemas de controlo de aviação nos aeroportos de Orly e Charles de Gaulle, bem como os sistemas de controlo de tráfego da rede de metro de Paris. A escala do

ataque aos contratantes levantou preocupações significativas sobre a capacidade da França ser a sede dos Jogos e resultou na decisão do Comité Olímpico de permitir que o evento acontecesse em vários locais de França, incluindo Bordéus e Nice. Uma investigação sobre os ciberataques mostrou que eles foram montados em vários países do Sul Global. Com o objectivo de fortalecer a capacidade de outros países para prevenir ou interromper ciberataques, a contribuição dos Estados membros da UE foi fundamental para a decisão da OCDE de actualizar o Official Development Assistance (ODA) Casebook on Conflict, Peace and Security Activities para reconhecer oficialmente as despesas em cibercapacidades como assistência oficial ao desenvolvimento.

O conceito de CCU baseou-se na experiência da UE com o desenvolvimento de cibercapacidades relacionadas. As CCMs no Vietname e na Indonésia forneceram provas de que a ideia das CCUs como meio concreto de estabelecer uma ponte entre o desenvolvimento e os instrumentos de política externa e de segurança funcionava. No final de 2025, especialistas da UE de Computer Emergency Response Teams (CERTs ou equipas de resposta a emergências de segurança informática), centros de resposta a crises, unidades de crime e juízes ministraram mais de oito sessões de formação para uma ampla gama de actores da reforma do sector de segurança (SSR) nesses países e ajudaram com reformas institucionais e legislativas em outros nove países.

Embora as decisões tomadas pela UE para reforçar a protecção dos interesses da União através do reforço da resiliência dos países parceiros tenham tido um impacto positivo na percepção da UE como um ciberactor verdadeiramente global, não impediram nem reduziram significativamente as ciberactividades maliciosas dirigidas à UE e aos seus estados membros. Muito pelo contrário: o número de ciberataques multiplicou-se, com vários ataques realizados contra a UE e a agências dos estados membros que implementam projectos da UE em países parceiros ou funcionários com acesso a informações confidenciais (por exemplo, vários projectos da UE financiados através do programa Digital4Development). O maior número de incidentes comunicados pela equipa de resposta a emergências informáticas das instituições, organismos e agências europeias (CERT-UE) incluiu campanhas de ciberespionagem.
Ao mesmo tempo, a experiência da UE na defesa de ataques sofisticados -

principalmente devido à implementação da Directiva de Segurança de Redes e Informações (NIS) de segunda geração em 2025 - e a capacidade de impor consequências a agentes mal-intencionados aplicando sanções específicas e sectoriais, foi cada vez mais apreciada pelos países parceiros, especialmente em África. Com o aumento da população online de 19 milhões em 2005 para quase 400 milhões em 2025, o continente africano tornou-se um dos maiores mercados de plataformas digitais, mas também um campo de testes [1] para as ciberactividades maliciosas. Dada a potencial utilização de campanhas de desinformação online para alimentar conflitos e minar os frágeis acordos de paz em certas partes do continente, aumentaram os pedidos de assistência abrangente à UE, incluindo através de projectos de desenvolvimento e cibermissões civis da CSDP (Civilian CSDP Cyber Missions).

A contribuição da UE para a prevenção de conflitos foi reconhecida na Joint Declaration on EU-UN Cooperation in Cyber Conflict Management, assinada à margem do segundo UN Summit on Digital Cooperation em 2026. No mesmo ano, elementos de ciber-resiliência foram integrados na CSDP e todos os outros instrumentos relevantes da Política Comum Externa e de Segurança (PESC), bem como da cooperação para o desenvolvimento e dos instrumentos de liberdade, segurança e justiça (FSJ) com a adopção da Comunicação Conjunta "Elements for an EU-wide strategic framework for supporting Security Sector Reform (SSR) in the digital age".

Contrariamente ao cepticismo inicial sobre as novas iniciativas empreendidas no âmbito da CSDP, em 2029 a UE tinha concluído quatro cibermissões civis com outras três planeadas (UE CCMs Argélia, Tunísia e Camarões). Além disso, todas as 12 operações da CSDP a decorrer incluíam uma ciberdimensão civil, com foco particular no desenvolvimento da competência do sector de segurança [2]. Esses desenvolvimentos foram possíveis graças ao forte compromisso dos estados-membros em estabelecer CCUs. Em 2029, a UE tinha 20 dessas unidades, cada uma contando com 15 especialistas de diferentes disciplinas e nacionalidades e estabelecidas por meio de contribuições dos estados-membros e de países como o Reino Unido, Austrália, Nova Zelândia, Canadá, Singapura, Jordânia, Japão e Coreia do Sul, com quem a UE assinou um Framework Participation Agreement (FPA ou Acordo-Quadro de Partici-

pação). Em consonância com a declaração UE-ONU sobre gestão de ciberconflitos, as CCMs também desempenharam cada vez mais um papel complementar em relação às missões da ONU.

Durante muito tempo, a ciberdiplomacia da UE careceu de uma visão estratégica. Isso mudou com a adopção da Estratégia da UE para a CiberPolítica Internacional durante a presidência alemã em Dezembro de 2020. O documento reconheceu a urgência de definir como a ciberdiplomacia contribui para a realização dos objectivos mais amplos da política externa e de segurança da UE. O Plano de Acção anexo à Estratégia indicou a necessidade de um único ponto de contacto para parceiros internacionais em todas as questões "ciber" e propôs a nomeação de um Representante Especial para a Política Internacional do Ciberespaço. Além disso, com base nos documentos anteriores [3], a Estratégia sublinhou o papel fundamental do desenvolvimento de cibercapacidades em países e regiões parceiros para a promoção e protecção dos valores e interesses da UE, tal como estabelecido nos Tratados da UE.

Perante um ambiente internacional cada vez mais hostil e competitivo, o Civilian CSDP Compact [4], adoptado em 2018, cumpriu a maioria dos seus compromissos antes do prazo final do Verão de 2023. O Civilian Annual Report on Capabilities by the European External Action Service (EEAS) de 2022 identificou as cibercapacidades como uma das principais lacunas na panóplia existente de capacidades civis da UE e propôs a criação de CCUs. A primeira dessas unidades foi instalada em 2024 como parte do novo Pacto Civil.

Muitos obstáculos [5] que comprometeram os esforços anteriores para melhorar a cooperação a nível da UE foram evitados. Por exemplo, o desafio da uniformização da formação e dos currículos foi superado graças aos esforços desenvolvidos pela ciberplataforma de educação, formação, avaliação e exercício (ETEE) coordenada pelo European Security and Defence College, o projecto European Defence Agency's Cyber Ranges Federation [6] ajudou a melhorar as capacidades de formação de ciberdefesa e projectos da Permanent Structured Cooperation (PESCO) como o EU Cyber

Academia and Innovation Hub (EU CAIH) [7].

Relativamente à criação de CCUs, dois projectos específicos revelaram-se particularmente relevantes para a superação das lacunas que impediram as tentativas anteriores de criar uma reserva permanente de especialistas no domínio ciber a nível da UE. No final de 2022, a EU CyberNet estabeleceu uma rede funcional de especialistas que podia ajudar e fornecer "expertise" a países dentro e fora da Europa. Além disso, lições aprendidas com o destacamento de Cyber Rapid Response Teams (CRRTs ou equipas de ciber-resposta rápida) [8] para lidar com ciberataques do United Cyber Caliphate que paralisaram as comunicações das missões e operações da CSDP da UE no Iraque, Mali, Níger, Somália e Mediterrâneo em Dezembro de 2020, ajudaram a identificar ferramentas e métodos para detectar, reconhecer e mitigar ciberameaças.

O efeito humilhante desses ciberataques coordenados - lançados por uma coligação multinacional de hackers em resposta a novas listas no regime de ciber-sanções da UE em 2021 visando ramificações do Lazarus Group da Coreia do Norte e entidades associadas ao United Cyber Caliphate - mobilizou a atenção política. A necessidade de abordar a falta de capacidades nacionais, institucionais e organizacionais adequadas que ajudaram a estabelecer esses países como portos seguros a partir dos quais grupos criminosos e terroristas pudessem operar livremente tornou-se uma prioridade do Representante Especial para a Política Internacional do Ciberespaço - um cargo criado em Fevereiro de 2021.

Em Junho do mesmo ano, como sinal de apoio ao Group of Governmental Experts da ONU, todos os estados membros da UE publicaram a sua interpretação do direito internacional no ciberespaço, o que contribuiu para fortalecer uma abordagem conjunta para responder a ciberatividades maliciosas. O "Secret Cyber Santa" da Europa - como o ataque de 2020 contra as missões da UE foi apelidado pelos media - também acelerou a revisão dos regulamentos da UE relativos à classificação de documentos [9], que subsequentemente levou a novos acordos de cooperação entre a UE e a OTAN em 2023, incluindo uma cooperação mais estreita entre o EU INTCEN e o Cyberspace Opera-

tions Centre (CYOC) da OTAN [10].

No final de 2024, a UE tinha feito progressos significativos para se tornar um verdadeiro "ciberactor apontado ao futuro", conforme previsto na Estratégia Global da UE de 2016. Infelizmente, não foi uma visão política clara, mas sim a pressão de eventos externos que mais uma vez levou os líderes europeus a agirem.

- - - - - - - - - -

[1] Council on Foreign Relations, "Disinformation, Colonialism and African Internet Policy", Blog Post, 21 de Novembro, 2019.

[2] European External Action Service (EEAS), "Rule of Law also in the Cyber Environment: EUPOL trains Palestinian judges", 3 de Setembro, 2019.

[3] Council of the European Union, "Council conclusions on EU external capacity building guidelines", 10496/18, Bruxelas, 26 de Junho, 2018.

[4] Council of the European Union, "Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on the establishment of a Civilian CSDP Compact" 14305/18, Bruxelas, 19 de Novembro, 2018.

[5] Nicoletta Pirozzi, "The Civilian CSDP Compact: A success story for the EU's crisis management Cinderella?", EUISS Brief no. 9, Outubro, 2018.

[6] European Defence Agency, "Cyber Ranges: EDA's first ever cyber defence pooling & sharing project launched by 11 member states", Bruxelas, 12 de Maio, 2017.

[7] Projectos da PESCO, "EU Cyber Academia and Innovation Hub (EU CAIH)".

[8] O CRRT é um projecto da PESCO lançado em 2018 para apoiar os estados membros, instituições da UE, operações da CSDP, bem como parceiros para garantir um nível mais elevado de ciber-resiliência e responder colectivamente a ciberincidentes. Informação adicional aqui.

[9] Council of the European Union, "Council Decision on the security rules for protecting EU classified information", 23 de Setembro, 2013.

[10] Alexandra Brozowski, "NATO sees new cyber command centre by 2023 as Europe readies for cyber threats", Euractiv, 19 de Outubro, 2018.

E se… a Europa criasse uma plataforma social/de notícias internacional?

Nathalie van Raemdonck

Era uma tarde de segunda-feira, 12 de Dezembro de 2024. A recém-nomeada HR/VP da UE, Eva Gizvel, tinha terminado a sua sessão de Discutons na NovaWeb, onde respondeu a perguntas de cidadãos europeus. A Strategic Communications Division convenceu o serviço da porta-voz "techsavvy" a experimentar uma sessão de perguntas e respostas online na NovaWeb, a nova plataforma europeia social/de notícias, e ela estava curiosa por participar após a sua nomeação ser aprovada pelo Parlamento Europeu. A equipa de comunicação de RH/VP estava a preparar-se para isso há semanas e parecia satisfeita com os resultados; com 70 mil comentários, foi a maior interacção registada na história de qualquer sessão de perguntas e respostas online e até ultrapassou o histórico "Ask Me Anything" com o presidente Barack Obama em 2014 no Reddit, o primeiro feito por um líder mundial [1]. A equipa de RH/VP conseguiu responder aos 587 comentários mais votados pelos participantes nas 8 horas em que a sessão esteve aberta e deu cerca de 15 respostas em vídeo. As perguntas iam desde questões muito técnicas sobre reformas orçamentais e missões da CSDP a questões filosóficas sobre o futuro da UE e até a perguntas sobre como a RH/VP se sentia a viver em Bruxelas. Pela primeira vez na história da NovaWeb, também houve um elevado nível de interação de não-europeus, representando um quinto do tráfego.

Moderadores de dezenas de subnovas - as comunidades baseadas em interesses da NovaWeb - ofereceram-se para ajudar a subnova europeia a moderar o enorme fluxo de comentários. Eles excluíram cerca de 1% dos comentários sinalizados por outros utilizadores, baniram 325 utilizadores e admoestaram cerca de 5.000 utilizadores. As intervenções foram baseadas nas directrizes da comunidade do site, onde o comportamento criminoso, discurso de ódio e desinformação deliberada foram sistematicamente excluídos. No entanto, os comentários que criticavam a política europeia não foram eliminados, de

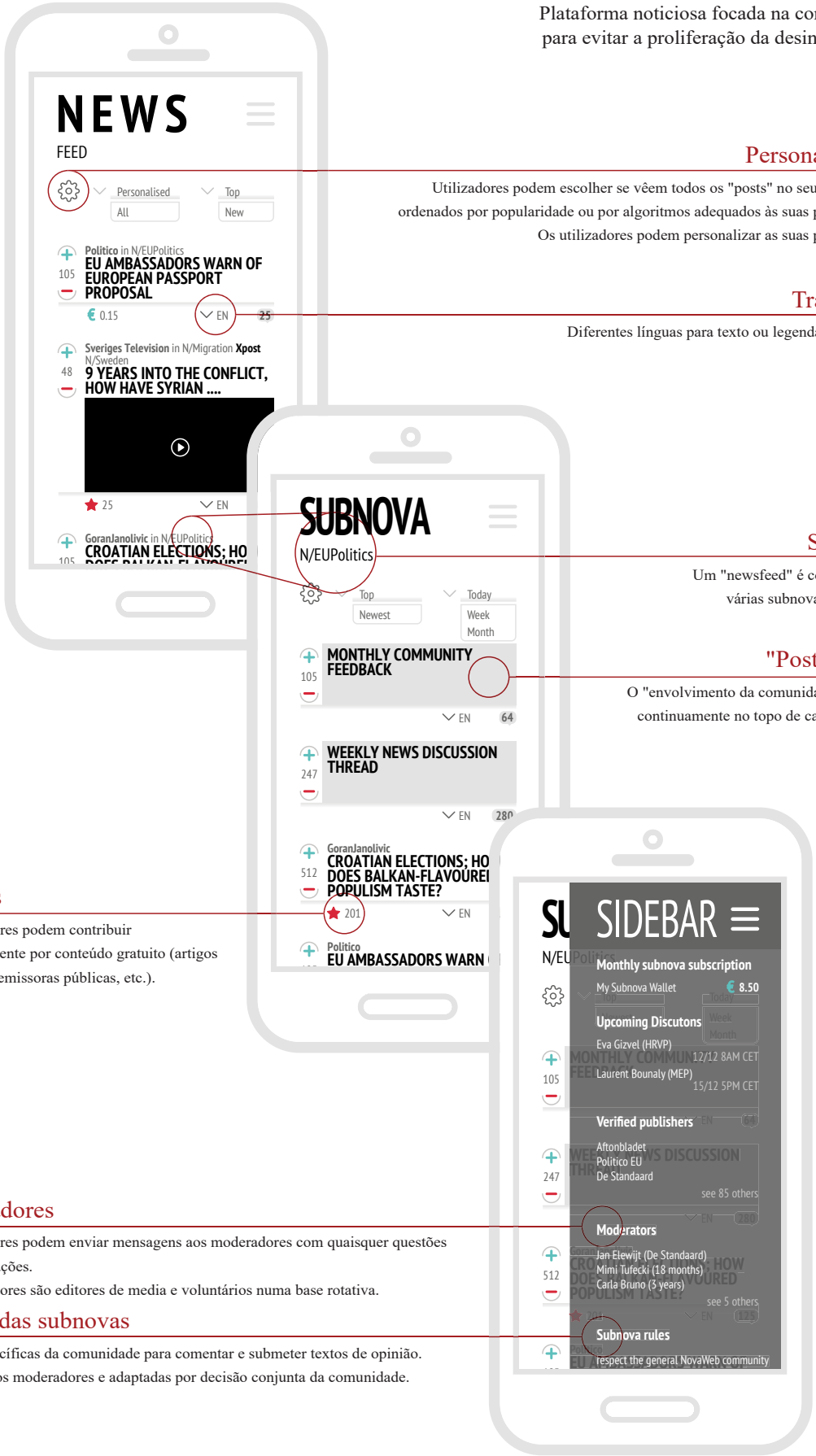
acordo com os regulamentos do site relativos à cobertura de tópicos políticos. Aqueles que não foram construtivos nos seus comentários naturalmente ganharam menos visibilidade, pois foram reprovados por outros utilizadores. Alguns comentários particularmente críticos, mas relevantes, receberam muita visibilidade na sessão Discutons, instando o HR/VP em exercício a responder. As suas respostas capazes às perguntas contundentes marcaram-na como alguém da nova geração de decisores europeus que não contornavam as críticas às políticas e instituições da UE.

Como a NovaWeb foi inicialmente criada com o objectivo principal de distribuição activa de notícias e envolvimento, ela estabeleceu uma comunidade que valorizava uma elevada qualidade de interacção. Isso foi evidente na sessão de perguntas e respostas, na qual foram feitas várias perguntas esclarecidas e informadas. Também validou o crescente sucesso da plataforma híbrida social/de notícias. Moderadores das maiores subnovas viram a plataforma e a sua comunidade crescerem ao longo dos anos como um canal informativo caracterizado pelo debate e interacção saudáveis. A expansão da NovaWeb numa constelação cada vez maior de subnovas atraiu novos utilizadores de todos os tipos de origens e diversificou o ecossistema online.

A sessão de perguntas e respostas online do HR/VP teve um impacto de longo alcance. Não só recebeu atenção considerável nos meios de comunicação de todo o mundo, mas as suas respostas também foram amplamente discutidas nas subnovas relevantes da NovaWeb. Os jornalistas verificaram e investigaram a pertinência de certas respostas e "opinion makers" e académicos europeus analisaram os planos políticos. Algumas subnovas ficaram um pouco decepcionadas com o nível de conhecimento sobre questões específicas, especialmente sobre tecnologia. As subnovas específicas de tecnologia convidaram os decisores relevantes da UE a comparecerem em sessões calendarizadas de "chat" no Discutons, sugestões que também foram bem recebidas pelos próprios políticos. Quando o HR/VP revelou uma nova Estratégia Global alguns meses depois, os participantes de várias subnovas dedicadas à política externa e à política mundial redigiram um relatório de recomendações com base nos comentários mais votados feitos por participantes verificados da sub-

Plataforma social de notícias

Plataforma noticiosa focada na comunidade para evitar a proliferação da desinformação



Personalização

Utilizadores podem escolher se vêem todos os "posts" no seu "newsfeed" ordenados por popularidade ou por algoritmos adequados às suas preferências.
Os utilizadores podem personalizar as suas preferências.

Traduções

Diferentes línguas para texto ou legendas em vídeo.

Subnova

Um "newsfeed" é composto por várias subnovas temáticas.

"Posts" fixos

O "envolvimento da comunidade" aparece continuamente no topo de cada subnova.

Moedas

Os utilizadores podem contribuir voluntariamente por conteúdo gratuito (artigos de opinião, emissoras públicas, etc.).

Moderadores

Os utilizadores podem enviar mensagens aos moderadores com quaisquer questões ou preocupações.
Os moderadores são editores de media e voluntários numa base rotativa.

Regras das subnovas

Regras específicas da comunidade para comentar e submeter textos de opinião.
Criadas pelos moderadores e adaptadas por decisão conjunta da comunidade.

nova. No geral, isso acrescentou uma camada de participação dos cidadãos que a UE se tem empenhado há anos por meio das consultas públicas da Comissão Europeia. A NovaWeb também teve um efeito positivo na redução da desinformação e da radicalização online. As sociedades de informação paralelas começaram a surgir na era em que a NovaWeb viu a luz pela primeira vez. O sistema engenhoso, mas simples, de editores de notícias verificados da NovaWeb e moderação da comunidade de baixo para cima e de cima para baixo provou ser um antídoto poderoso contra essa degradação do espaço da informação.

O modelo chamou a atenção de outros países fora da Europa. Sociedades em todo o mundo têm lutado com os efeitos colaterais prejudiciais não intencionais das plataformas de Silicon Valley. Editores e a sociedade civil da América Latina e da África aventuraram-se na NovaWeb, e um vibrante ecossistema de subnovas com foco na América do Sul e África encontrou o seu lugar na rede. Os seus decisores políticos também tomaram nota e saudaram a influência positiva da plataforma nos seus países. Outros países viram a NovaWeb como uma ameaça e bloquearam o acesso. O controlo rigoroso de conteúdo era, no entanto, um assunto muito caro para a maioria dos estados com recursos limitados [2]. A falta de abertura atrofiou o seu desenvolvimento e fê-los ficar para trás na digitalização e na inovação. Alguns regimes nos países árabes foram derrubados violentamente no final de 2025, após políticas cada vez mais draconianas e a deterioração das condições económicas causarem uma agitação social generalizada. O programa de desenvolvimento europeu Cyber4Dev foi convidado para países que provavelmente terão o mesmo destino e partilhou a experiência da NovaWeb. Alguns governos gradualmente permitiram à sua população mais liberdade de informação e criaram uma versão descentralizada da NovaWeb. Com o tempo, a maioria desses governos permitiu que toda a NovaWeb ficasse acessível no seu país, e uma política de adesão foi criada para que as plataformas locais se unissem à rede global da NovaWeb.

O que correu bem?

Quando um inquérito em 2020 mostrou que 18% da população europeia

acreditava que havia alguma verdade na conspiração do "plano Kalergi" [3], também conhecida como a conspiração do "genocídio branco", os legisladores perceberam que algo precisava de ser feito. 65% dos crentes indicaram ter visto um meme viral do plano Kalergi nas suas páginas de media social no início de 2020. Os dedos apontaram para as plataformas de media social de Silicon Valley, que lutavam contra a disseminação de desinformação nos seus serviços. Embora quatro deles já tivessem concordado em cumprir o Código de Prática Europeu contra a Desinformação em 2017 [4], isso não impediu a disseminação de algo como a conspiração Kalergi. A aplicação das regras, no entanto, obteve pouco apoio numa Europa que valorizava uma Internet livre e aberta. Algumas verificações de factos intensivas foram realizadas por organizações de notícias, mas os resultados pareciam ter apenas um efeito limitado sobre aqueles que acreditavam na teoria da conspiração. Um relatório do Conselho da Europa tinha antes concluído que injectar simplesmente mais "informações factuais" no ecossistema de media não impediria a desordem da informação. "Os elementos emocionais e ritualísticos da comunicação devem ser tidos em consideração" [5].

Uma nova iniciativa foi assim lançada no final de 2020. A versão piloto da plataforma NovaWeb foi criada por nove agências europeias de media de financiamento público [6]. Após anos de esforços para fazer um canal de radiodifusão europeu decolar, numa sociedade cada vez mais digital uma abordagem diferente foi tentada para lançar uma plataforma online. A colaboração entre as emissoras públicas foi facilitada pelo Mercado Único Digital Europeu e pela Divisão de Comunicações Estratégicas do EEAS [Serviço Europeu de Acção Externa], que também forneceu financiamento parcial para a plataforma. Parceiros de media comercial juntaram-se alguns meses depois, e um sistema foi criado para verificar os editores participantes por meio da Federação Europeia de Jornalistas. Um modelo de "pay-per-view" facilitaria a receita de financiamento do

trabalho jornalístico e evitaria a necessidade dos algoritmos de publicidade que atormentavam as plataformas de Silicon Valley.

Os utilizadores podem criar uma carteira NovaWeb e facilmente efectuar micropagamentos por cada artigo lido. Entretanto, o conteúdo da emissora pública permanecia gratuito, já que esse material era financiado pelos contribuintes. Como a NovaWeb era estruturada em subcomunidades chamadas subnovas, os utilizadores encontrariam os seus interesses agrupados em comunidades específicas, e os utilizadores intensivos e especialistas teriam uma assinatura mensal por todo o conteúdo pago fornecido numa subnova.

Além do modelo de receitas, a novidade da NovaWeb é que valoriza a interação saudável da comunidade tanto quanto o conteúdo de qualidade. O objectivo da NovaWeb era envolver os utilizadores além do consumo passivo de notícias e ter em consideração a influência das emoções e dos sentimentos tribalistas na maneira como as pessoas processam as notícias [7]. Para esse propósito, as subcomunidades foram concebidas para terem o seu próprio espaço autogerido sob directrizes gerais da comunidade NovaWeb e, assim, permitindo criar a sua própria identidade e destacar itens de notícias que considerassem interessantes e importantes, ou desinteressantes ou indesejáveis, por meio de um sistema de votação. O facto de os moderadores serem membros reais das comunidades de notícias também foi essencial para a atracção da NovaWeb. As regras de moderação foram claramente delineadas, criadas como parte de um processo de tomada de decisão conjunto na comunidade e flexíveis a mudanças. Os editores de media da Novaweb seriam obrigados a designar moderadores da comunidade em tempo integral para a plataforma, dependendo da receita que obtivessem com a NovaWeb. Os participantes da comunidade também podiam voluntariar-se como moderadores numa base rotativa, mas nenhuma subnova poderia ser criada sem dois moderadores certificados. Em meados de 2021, um curso de formação foi criado para auxiliar os moderadores da NovaWeb nesta tarefa de gerir uma comunidade online. À medida que a NovaWeb inaugurava um ambiente social novo e inovador para o consumo de notícias, estava a formar-se uma nova estrutura política online.

- - - - - - - - - -

[1] "I am Barack Obama, President of the United States", Reddit, 29 de Agosto, 2012.

[2] Em 2016, as paralisações da Internet e as restrições a conteúdos custaram aos países globalmente 2,4 mil milhões de dólares, de acordo com a Brookings Institution.

[3] Richard Von Coudenhove-Kalergi foi um político austro-japonês do século XX, diplomata e filósofo, que desempenhou um papel central na integração europeia. A teoria da conspiração afirma que os seus planos de reunir o continente mascaram a intenção de encorajar um processo de mistura racial forçada. Ver: Sophia Gaston (com Joseph E. Uscinski), "Out of the Shadows: Conspiracy Thinking on Immigration", Henry Jackson Society, Centre for Social and Political Risk, November, 2018.

[4] Comissão Europeia, "Code of Practice against Disinformation", Bruxelas, 29 de Janeiro, 2019.

[5] Claire Wardle e Hossein Derakhshan, "Information Disorder: Towards an Interdisciplinary Framework for Research and Policymaking" Council of Europe Report DGI(2017)09, Setembro, 2017.

[6] Hossein Derakhshan, "Why Europe should build its own social platform for news", The Guardian, 2 de Julho, 2019.

[7] Op.Cit., "Information Disorder: Towards an Interdisciplinary Framework for Research and Policymaking".