A Barragem de Eventos e a Morte da Inteligência de Fontes Abertas no Nível Tático

Cap Michael J. Rasak, Exército dos EUA

Os não combatentes utilizam, cada vez mais, as mídias sociais para informar a disposição e composição de forças militares, o estado da infraestrutura e os detalhes de acontecimentos locais em curso, representando um grande risco para as atividades militares de forças amigas e adversárias. Estados-nação e grupos adversários já demonstraram a capacidade e a intenção tanto de mitigar quanto de explorar esse fenômeno. No futuro próximo, os comandantes e analistas das forças amigas provavelmente enfrentarão uma "inundação" digital de uma série de fatos exagerados ou totalmente forjados nas mídias sociais, que ameaçarão diretamente as operações táticas em andamento ou no curto prazo, o que se denomina "barragem de eventos". Em meio a uma barragem de eventos, e devido à iminência das operações no nível tático, os comandantes são obrigados a escolher entre duas opções indesejáveis: corroborar sistematicamente cada um deles ou ignorar completamente as mídias sociais como uma plataforma para observar as atividades das forças adversárias. As ramificações subsequentes da barragem de eventos, apropriação ou sequestro de tendências (*trend hijacking*) e esforços de desinformação precisamente direcionados poderiam, então, desorganizar o processo decisório dos EUA no nível tático; sobrecarregar os meios de inteligência, reconhecimento, vigilância e aquisição de alvos (IRVA) de forças amigas; e reduzir a utilidade das informações de fontes abertas (*open-source information*, OSIF). Os Estados-nação ou grandes grupos poderiam incentivar suas populações a participarem de barragens de eventos, acabando por comprometer a integridade da inteligência de fontes abertas (*open-source intelligence*, OSINT) como disciplina em geral.

O Cap Michael J. Rasak, do Exército dos EUA, é oficial de inteligência da 4ª Brigada de Cavalaria, Divisão Leste, Primeiro Exército. Possui bacharelado pela Michigan State University. Serviu em duas missões no Afeganistão, uma como comandante de pelotão de infantaria na 101ª Divisão Aeroterrestre (Assalto Aéreo) e outra como oficial de inteligência de regimento na 3ª Divisão de Infantaria.

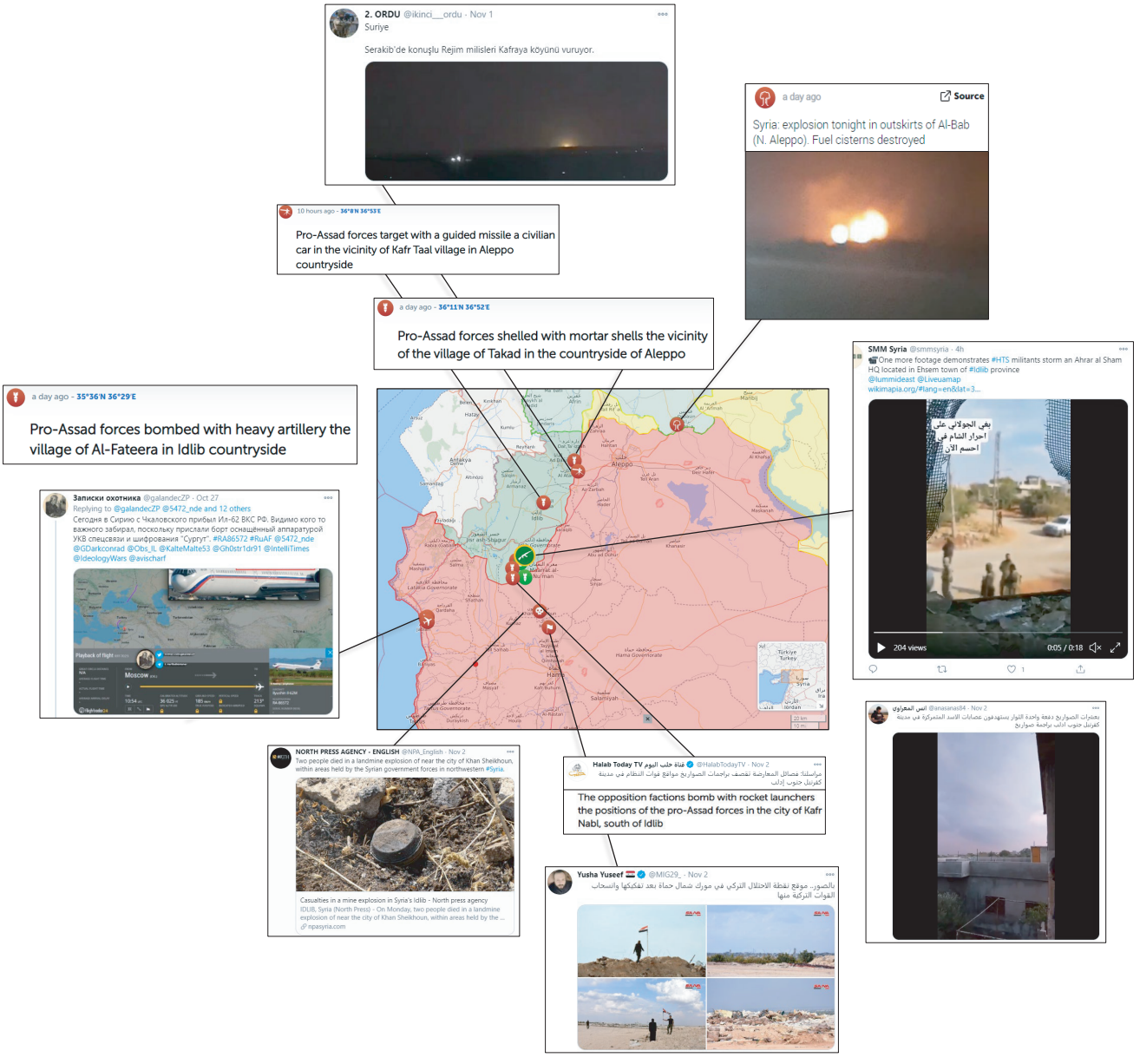
Inteligência de fontes abertas no nível tático

Apesar do título soturno deste artigo, a OSINT provavelmente não morrerá como disciplina. O enorme volume de informações existentes no campo das fontes abertas oferece aos analistas um conjunto de dados disponíveis valiosos demais para serem totalmente deixados de lado. Basta considerar as observações perspicazes de profissionais experientes procedentes de toda a comunidade de inteligência e das fileiras das Forças Armadas. O Gen Div Samuel V. Wilson, ex-Diretor da Agência de Inteligência de Defesa (Defense Intelligence

Técnico de inteligência de todas as fontes (à direita), do 2º Batalhão, 34º Regimento Blindado, 1ª Brigada de Combate Blindada, assiste o oficial de inteligência do batalhão durante o Exercício *Allied Spirit X* em Hohenfels, na Alemanha, 8 de abril de 2019. (Foto: 3º Sgt Thomas Mort, Exército dos EUA)

Agency), afirma que a OSINT fornece cerca de 90% das informações utilizadas pela comunidade de inteligência.[1] Robert Cardillo, Diretor da Agência Nacional de Inteligência Geoespacial dos EUA (National Geospatial-Intelligence Agency), declarou que "as informações não classificadas já não devem ser consideradas como complementares às fontes classificadas, e sim o inverso".[2] Mesmo aqueles que não têm um interesse especial na segurança da nação, como o canal Vice News, comentaram a gama ilimitada de valiosas informações militares a serem obtidas a partir de fontes publicamente disponíveis.[3] O conjunto de OSIF disponíveis em decorrência da ascensão das mídias sociais só veio a estimular ainda mais entusiasmo: *geotagging* (marcação geográfica), georreferenciamento, *web scraping* (raspagem de dados), análise de sentimentos e análise léxica são algumas das tecnologias e técnicas que vêm surgindo. A OSINT oferece aos comandantes do nível tático ao estratégico revelações valiosas e aprofundadas sobre ambientes não permissivos, que só eram obtidas anteriormente por meio de esforços clandestinos. Munidos desse maior grau de "resolução", os comandantes ficam mais aptos a entender e visualizar o campo de batalha, o que lhes confere uma vantagem quando precisam descrever, dirigir, liderar e avaliar as operações.

No nível tático, a OSINT oferece aos comandantes de forças terrestres informações quase em tempo real que são essenciais para a tomada de decisões. As mídias sociais, em especial, proporcionam aos analistas a oportunidade de colher, monitorar e avaliar rapidamente os acontecimentos dentro da área de operações de um comandante. Inúmeros cidadãos comuns munidos de smartphones, dispositivos internos de GPS e contas de Twitter divulgam, sem saber, informações sobre a disposição, composição e efetivo das forças inimigas, estado da infraestrutura, acontecimentos em curso e opinião geral da população. Além disso, a iminência inerente às operações no nível tático (ao contrário das operações nos níveis operacional ou estratégico) faz com que as



(Figura criada pelo autor com capturas de tela do site Live Universal Awareness Map)

Figura 1. Exemplo do site Live Universal Awareness Map: Síria, 3 de novembro de 2020

informações obtidas a partir da coleta de OSINT sejam de uma importância ainda maior. Suponha, por exemplo, que um pelotão de infantaria conduz um patrulhamento, operando a apenas alguns quilômetros de uma aldeia. Se um oficial de inteligência de batalhão ou brigada observar um grande volume de tuítes indicando uma concentração de combatentes inimigos na aldeia, ele terá a obrigação de confirmar essa informação na medida do possível e transmiti-la para o comandante do pelotão no terreno. Caso contrário, ele poderia expor o pelotão a uma emboscada ou levá-lo a perder a oportunidade de engajar o inimigo em condições mais vantajosas.

Estudiosos, profissionais militares e membros da comunidade de inteligência comentaram a eficácia da OSINT no nível tático. Em "Operationalizing OSINT Full-Spectrum Military Operations" ("Operacionalização de Operações Militares no Amplo Espectro de OSINT", em tradução livre), o *Senior Chief*

Petty Officer Ron Penninger apresentou um excelente exemplo da eficácia da OSINT no nível tático e mostrou como a análise de sentimentos e o georreferenciamento podem contribuir diretamente para o processo decisório dos comandantes de forças terrestres.[4] A empresa RAND Corporation também comentou os efeitos de mudança de paradigma produzidos pela "OSINT de segunda geração". Heather J. Williams e Ilana Blum afirmam: "Os analistas [...] podem usar uma combinação de Google Maps, Wikimapia, tuítes disponíveis publicamente, postagens no Facebook e vídeos do YouTube para identificar os locais exatos de ações militares em curso".[5]

O aproveitamento da OSINT para a aplicação tática é muito mais que mera retórica ou elogio falso. Forças Armadas, agências governamentais, organizações não governamentais e empresas já a exploram. A empresa Live Universal Awareness Map (Liveuamap) talvez seja um dos melhores exemplos. Em seu site, a Liveuamap explica que ela consiste em um "site independente de notícias e informações globais", que tem por objetivo ajudar as pessoas a "tomarem decisões conscientes sobre sua segurança".[6] Baseando-se principalmente em postagens nas mídias sociais, o site fornece informações quase em tempo real sobre a movimentação de pessoal e equipamentos militares, distúrbios civis, violência e outras atividades, justapondo esses eventos em um mapa interativo (veja a Figura 1). Por exemplo, quando da redação deste artigo, um dos eventos mais recentes na Líbia (extraído com base na contribuição colaborativa, ou *crowdsourcing*, no Twitter) indicava que "[seis] viaturas com sistemas antiaéreos Pantsir, de fabricação russa, chegaram a Sirte".[7]

Os manifestantes em Hong Kong que usaram o "HKMap Live" durante os enormes protestos do final de 2019 e início de 2020 oferecem outro exemplo claro de como não combatentes sem nenhum treinamento podem ser eficazes em rastrear o movimento de forças governamentais. Por meio da contribuição colaborativa e das mídias sociais, os manifestantes acompanharam a composição e disposição de forças policiais, comunicaram sua intenção e concentraram pessoal nos locais e horários de sua escolha. Os manifestantes de Hong Kong afirmaram que seus esforços de rastreamento tinham por objetivo evitar as forças policiais, enquanto o governo chinês declarou que as ações deles visavam a facilitar emboscá-las. Independentemente de qual argumento seja mais verdadeiro, as mídias sociais facilitaram, claramente, a execução de doutrina tática, ou seja, obter e manter o contato, romper o contato ou conduzir uma emboscada.

Forças Armadas em todo o mundo têm, cada vez mais, utilizado as mídias sociais como primeiro passo no processo de busca de alvos — ou seja, "localizar" ou "detectar" o que, posteriormente, será "finalizado" ou "engajado". Conforme explicado por Williams e Blum, "muitos analistas de inteligência de todas as fontes começam com a OSINT e, em seguida, acrescentam materiais de fontes classificadas", reduzindo rapidamente, assim, o tempo e a energia necessários para facilitar as operações de busca de alvos.[8] Os batalhões, brigadas e divisões estariam sendo negligentes caso não mostrassem feeds pertinentes das mídias sociais ao lado dos mapas nas paredes de seus postos de comando. A consciência situacional que as OSIF proporcionam na era moderna é importante demais para ser ignorada. O campo de batalha se transformou em um ambiente onde há olhos e ouvidos por toda a parte, que tanto as forças amigas quanto adversárias podem consumir e utilizar como quiserem. Parece que pelo menos uma das características da ofensiva foi completamente sobrepujada: a surpresa.

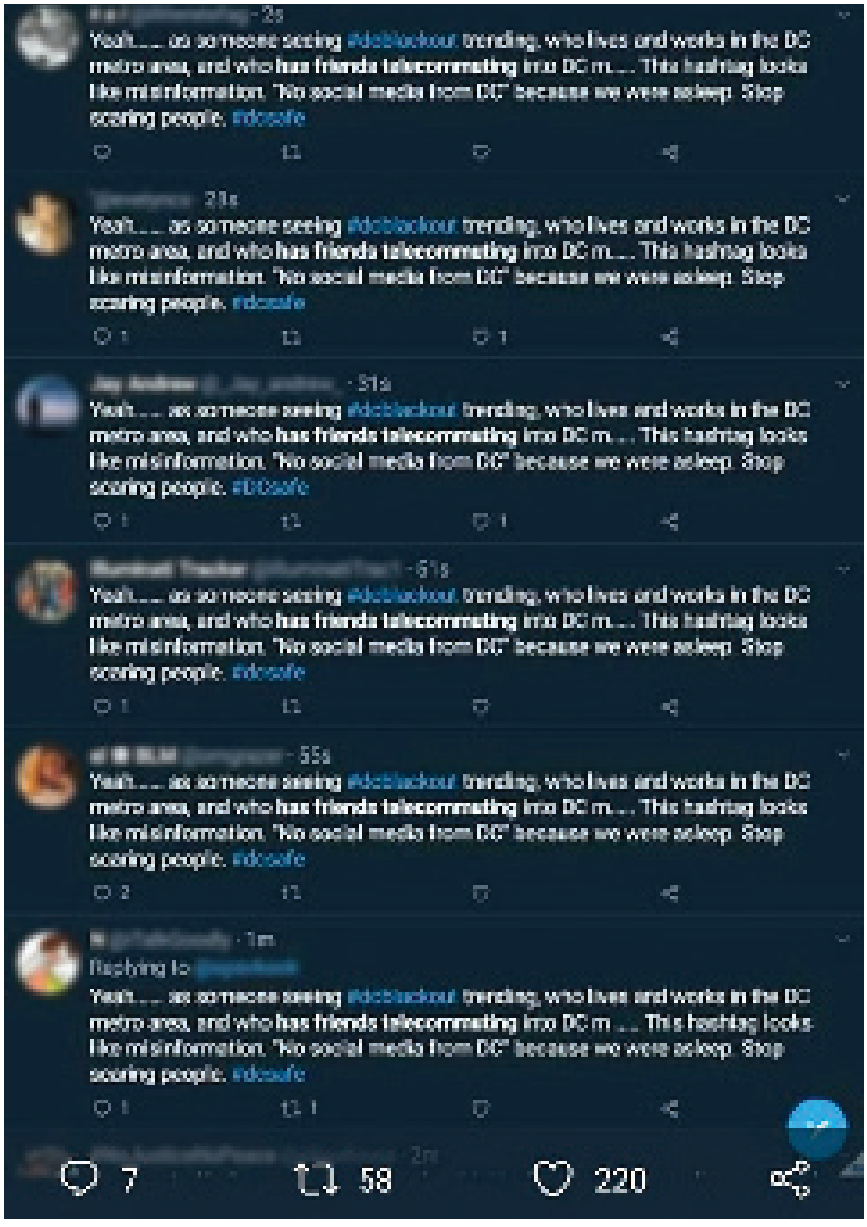
Compreender que "todo cidadão agora é um sensor" levanta duas importantes questões: "como isso pode ser mitigado?" e "como isso pode ser utilizado como arma?" O resto deste artigo explorará essas perguntas e abordará algumas de suas implicações.

Barragem de eventos

Os profissionais de OSINT treinados são aconselhados a questionar a autenticidade e credibilidade das OSIF oriundas das mídias sociais devido à predominância de dissimulação e vieses. Contudo, como, exatamente, um profissional pode verificar a credibilidade e autenticidade de um tuíte? A resposta habitual é corroborar essa informação com as de pelo menos uma outra disciplina de inteligência e, subsequentemente, convertê-la de dados brutos questionáveis de uma única fonte em um produto analítico acabado e fidedigno, de múltiplas fontes. Embora seja o padrão-ouro, esse processo pode ser difícil ou excessivamente trabalhoso, especialmente quando os analistas estão apoiando o rápido ritmo das operações no nível tático. Muitas vezes, os analistas se apoiam na corroboração por meio de múltiplas tentativas de coleta por um mesmo (ou semelhante) sensor. Um exemplo disso fora da OSINT poderia ser a utilização de duas

fontes separadas de inteligência humana para confirmar uma informação ou o uso de dois feeds separados de vídeo *full-motion* de sistemas aéreos não tripulados para corroborá-la.

Os profissionais de OSINT frequentemente podem e, de fato, se apoiam na agregação de OSIF de muitas fontes para realizar um processo semelhante. Williams e Blum explicam que "[um] único tuíte que reflita a perspectiva de uma pessoa aleatória sobre o Estado Islâmico do Iraque e do Levante (EIIL) não tem quase nenhum valor de inteligência; entretanto, sintetizar todos os tuítes com opiniões sobre o EIIL em uma área geográfica é de grande valor de inteligência".[9] Penninger oferece outro exemplo, recomendando uma raspagem de dados de uma área geográfica (no caso, uma aldeia) antes de uma missão, para determinar a linha de base de sentimentos da população, observando mudanças relevantes, à medida que as forças estadunidenses executam sua operação. Nesse caso, diz ele, as mudanças de opiniões na aldeia podem ajudar os comandantes de forças terrestres a "tomar decisões bem informadas" e "moldar suas ações para alcançar, da melhor forma, o resultado pretendido pelo comando superior".[10]



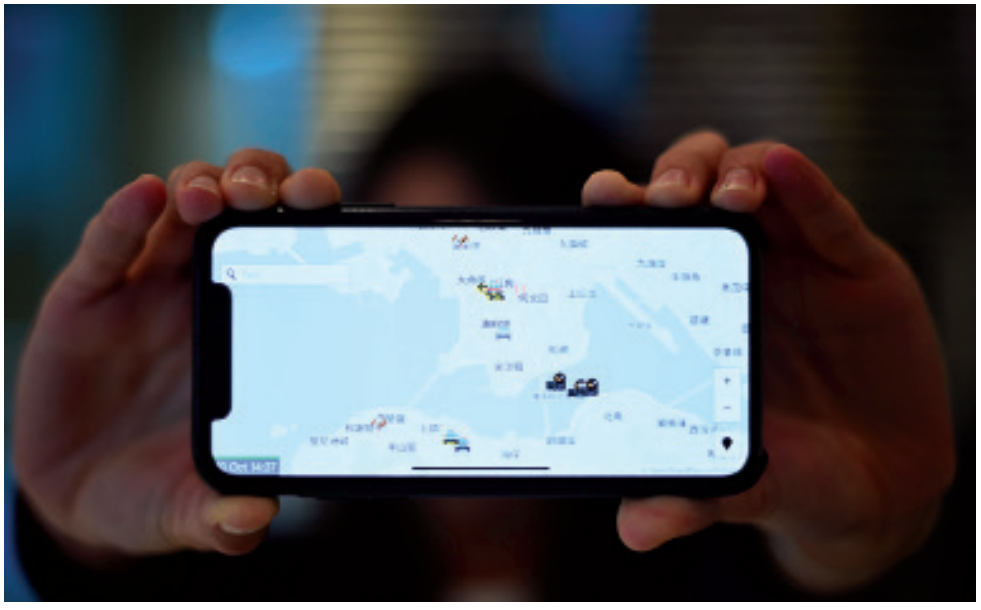
(Captura de tela do autor, via Twitter)

Figura 2. Exemplo de uma *botnet* no Twitter

Com o uso crescente de *bots* (programas automáticos), inteligência artificial e aprendizado de máquina, surge o potencial de que os adversários falsifiquem completamente, ampliem artificialmente ou disfarcem tendências, padrões, ideias, acontecimentos ou ações existentes. O artigo "Commanding the Trend" ("Comandando a Tendência", em tradução livre), de Jarred Prier, descreve a sofisticação e eficácia cada vez maiores da "apropriação de tendências" nas mídias sociais. Ele explica que "contas de *bot* são contas não humanas, que tuitam e retuitam automaticamente com base em um conjunto de regras programadas", que ampliam, subsequentemente, uma determinada narrativa (veja o exemplo da Figura 2).[11] Observa, ainda, que, em 2017, o Twitter estimou que quase 15% de suas contas eram contas de *bot*.[12] Indivíduos, grupos ou até Estados-nação inteiros podem dedicar seus recursos à apropriação de tendências para a finalidade que desejarem. Por exemplo, um grupo supremacista branco anunciou, em junho de 2020, que iniciaria o projeto SOCH (Solar Orbiting Casaba Howitzer), que tem por objetivo a construção de "um sistema de

automação [...] capaz de gerar, rapidamente, contas nas mídias sociais com o clique de um botão, fazendo com que seja mais fácil [...] manter uma presença em plataformas fortemente censuradas".[13] Embora pesquisadores como Prier investiguem as implicações da apropriação de tendências para o nível nacional e estratégico, as mesmas preocupações também podem chegar até o nível tático.

Além de *bots*, os adversários também podem empregar a alteração de dados (*spoofing*) de GPS para gerar georreferências falsas ligadas às suas postagens nas redes sociais. Não só os Estados-nação ou grupos sofisticados são capazes da falsificação de GPS, como os não combatentes comuns podem fazer o mesmo. Aplicativos disponíveis comercialmente, como "Fake GPS Location–GPS Joystick", permitem que qualquer pessoa cancele o sistema interno de GPS de seu smartphone com pouco esforço. A falsificação de GPS também pode ser organizada e direcionada para locais designados. Janus Rose explica que, em 2016, um grupo "varr[eu] os perfis de 60 redes de Wi-Fi nas proximidades [...], retransmit[iu] essas redes", capacitando, assim, qualquer pessoa com acesso à internet a fazer com que seus telefones parecessem estar localizados na embaixada equatoriana.[14] Assim, os adversários não apenas estão munidos da capacidade de produzir acontecimentos falsos, mas também de direcioná-los para regiões geográficas específicas.



Depois de Pequim ter intensificado a pressão sobre empresas estrangeiras que, a seu ver, estavam prestando apoio ao movimento pró-democracia em Hong Kong, a Apple retirou o aplicativo "HKmap.live" em 10 de outubro de 2019, porque estava permitindo que os manifestantes em Hong Kong acompanhassem o movimento das forças policiais. (Ilustração fotográfica: Philip Fong, Agence France-Presse)

Ao retomarmos o exemplo do pelotão de infantaria operando perto de uma aldeia, é, então, plausível que um adversário pudesse ampliar, artificialmente, ou falsificar completamente uma tendência ou "evento" que indicasse, para um analista desprevenido, a existência de uma ameaça emergente nas proximidades. Se o analista apoiando esse pelotão de infantaria utilizasse o recurso de *geofencing* para delimitar seus parâmetros de busca de modo que coincidissem, aproximadamente, com os limites da aldeia, então talvez algumas dezenas de tuítes e retuítes apenas já pudessem apresentar um cenário fundamentalmente diferente da opinião ou suposta ameaça presente no local. Se o analista não pudesse confirmar a ameaça emergente com uma outra disciplina de inteligência, ele deveria apoiar-se, então, na agregação de OSIF das mídias sociais e gerar um relatório de OSINT para o comandante das forças terrestres. O comandante se veria, então, diante de três opções: solicitar apoio de IRVA ao comando superior, redirecionar seus próprios sensores ou simplesmente confiar na inteligência que ele recebeu e reagir de acordo com ela.

Embora o nível de gravidade dessa situação possa parecer relativamente inofensivo (ou apenas mais um exemplo do "ruído branco" que os analistas conhecem tão bem), quando se estende essa problemática para uma próxima etapa de sua evolução natural, surgem algumas sérias preocupações. Suponha que o analista do exemplo identifique três eventos novos: a concentração de combatentes na aldeia a leste, o estabelecimento de uma guarnição de morteiros a quatro quilômetros a oeste e a destruição da ponte necessária para retirar-se ao sul. Bem, agora há três eventos que o analista, o comando superior

e o comandante das forças terrestres precisam confirmar. Três novas áreas de interesse e necessidades de inteligência acabam de se desenvolver; três novos eventos precisam ser corroborados por meios separados de IRVA; e o comandante das forças terrestres precisa tomar uma decisão sobre sua próxima ação. Agora, aumente o número de eventos de três para dez. Esse método de inundar uma força terrestre com tendências de OSIF nas mídias sociais pode ser chamado de barragem de eventos. Supondo que os meios de IRVA disponíveis sejam redirecionados para atender a essas novas necessidades de inteligência, é preciso lembrar que eles serão desviados de uma outra missão para a qual tenham sido originalmente designados, na qual, provavelmente, teriam efetuado a coleta com base em necessidades de inteligência prioritárias com verdadeiro mérito. A barragem de eventos pode, então, ser utilizada como um meio de exercer enorme pressão sobre os meios de IRVA disponíveis, desorganizar os planos de busca de inteligência e ocultar feeds de informações verdadeiras. Nesse sentido, a barragem de eventos pode ser vista como um meio de fogos não letais, dificultando, deliberadamente, o ciclo de decisão dos comandantes, com o objetivo de desorganizar as operações táticas, na pior das hipóteses, e neutralizar operações, na melhor delas.

Um analista ou comandante frustrado, que descartasse completamente as informações durante uma barragem do eventos, poderia gerar problemas ainda maiores. Conforme abordado na primeira parte deste artigo, as OSIF e as mídias sociais oferecem aos analistas e comandantes uma incrível vantagem no terreno. Forças Armadas em todo o mundo estão, cada vez mais, ficando incapazes de manobrar através do campo de batalha sem que cidadãos comuns as observem e informem sobre elas. Além disso, se considerarmos que ainda há pessoas *reais* informando, *verdadeiramente*, sobre a movimentação de pessoal — mesmo em meio a uma barragem de eventos — então um ou mais fatos emergentes poderiam ser legítimos. Presumindo que a barragem de eventos seja totalmente composta de fatos iminentes ou de alta prioridade, a força terrestre e os analistas que a apoiam serão obrigados, então, a confirmar tudo o que virem para determinar exatamente quais deles são verdadeiros.

Um adversário poderia produzir barragens de eventos para outros propósitos além de desorganizar as operações dos EUA em curso. Podem ser usadas para encobrir o movimento adversário, impedir que forças estadunidenses entrem em uma área, dificultar a validação de alvos, interromper as linhas de comunicação terrestres, atrair as forças estadunidenses para uma área ou servir de reforço no desenvolvimento da área de engajamento adversária. Isso será especialmente verdade caso os adversários tomem até mesmo medidas mínimas para complementar a barragem de eventos em curso fora das mídias sociais, utilizando vídeos gerados por computador, produzindo *deepfakes*, falsificando literatura cinzenta ou reportagens da imprensa ou plantando pequenas evidências físicas ou eletrônicas que possam levar a uma falsa confirmação. Por exemplo, se um adversário quisesse interromper linhas de comunicação terrestres, ele poderia conduzir uma barragem de eventos na área desejada e fazer com que um único ator revolvesse a terra no local (para reproduzir a instalação de um dispositivo explosivo improvisado), enganando a análise de imagens. Barragens de eventos sobre distúrbios civis poderiam ser falsamente corroboradas com vídeos adaptados (ou gerados por computador) e algumas pilhas de pneus em chamas. A concentração de combatentes poderia ser falsamente corroborada com a transmissão de informações incorretas na rede por uma pessoa com um sistema de rádio para ludibriar a análise de comunicações. Embora esses exemplos sejam muito simplificados, o fato é que a barragem de eventos tem o potencial de transformar esforços iniciais de dissimulação, fazendo-os passar de relatórios isolados de uma única fonte para relatórios que pareçam ser legítimos e de múltiplas fontes.

Como exemplo de falsa corroboração de distúrbios civis, considere a confusão em torno da Zona Autônoma de Capitol Hill, em Seattle, em junho de 2020. Além das narrativas contrárias criadas no submundo das mídias sociais, relatando "acontecimentos no terreno", os próprios veículos da grande mídia se tornaram vítimas do caos (ou contribuíram deliberadamente para ele). Por exemplo, a rede Fox News exibiu uma imagem de guardas armados que ocupavam a área, mas a retirou logo após o jornal *Seattle Times* ter observado que ela era de um incidente completamente diferente, ocorrido em Minnesota. Embora a Fox News tenha alegado que a fotografia fazia parte de uma "colagem" que "não demarcava claramente" imagens de Seattle e de outros acontecimentos em todo o país, o fato é que as linhas entre a realidade digital e a realidade física foram obscurecidas.[15]

A maioria desses exemplos está relacionada com a contrainsurgência, mas a aplicação da barragem de eventos durante operações de combate em larga escala poderia ser tão, se não mais, eficaz. Considere a pressão que uma

barragem de eventos poderia adicionar a operações já extremamente complexas, como no caso de uma divisão ou brigada que conduz a recepção, concentração, movimento para as linhas de frente e integração; uma transposição de curso de água; ou uma ultrapassagem. Nesses casos, um Estado-nação poderia produzir várias barragens de eventos, apresentando, simultaneamente, múltiplos dilemas para um comandante em meio ao comando e controle de uma operação já multifacetada. Um grupo ou Estado-nação com visão de futuro poderiam até criar, de antemão, múltiplas barragens de eventos (e medidas complementares) e deixá-las prontas para serem liberadas em momentos e locais cruciais. Barragens de eventos poderiam ser criadas com dias, semanas ou meses de antecedência. Crises humanitárias, rompimentos de represas, distúrbios civis, pontes destruídas e brigadas blindadas falsas poderiam praticamente preencher o campo de batalha, sobrecarregando os meios de IRVA disponíveis e desviando os esforços de reconhecimento estadunidenses para longe dos verdadeiros alvos. Sucessivas barragens de eventos poderiam afastar, cada vez mais, a atenção estadunidense dos verdadeiros objetivos, e o inimigo só teria de concretizar uma eventual barragem de eventos para direcionar o foco dos EUA.

Algo imprescindível para conduzir uma barragem de eventos eficaz é obter a participação do maior número possível de atores cibernéticos diferentes. Embora um exército de *bots* controlado por um pequeno grupo de pessoas possa falsificar e/ou ampliar um determinado evento, as técnicas e tecnologias empregadas atualmente podem, de modo geral, identificar e assim eliminar ou desconsiderar um evento ou tendência que pareça particularmente falso. A análise léxica avançada, a análise de palavras-chave e a análise do perfil de frequência podem ser usadas para atribuir a responsabilidade por um texto escrito a um grupo demográfico, a um grupo de pessoas específico ou até mesmo a um único autor.[16] Por exemplo, se uma série inicial de tuítes ou artigos comentando o surgimento de uma crise humanitária contiver as características inconfundíveis de escrita de um conhecido grupo nocivo, tal evento poderá ser desconsiderado como uma mera tentativa de desinformação. No entanto, se o evento ganhar força junto ao público global e milhares de pessoas comentarem, publicarem ou contribuírem com seus próprios textos ou imagens para a discussão, será necessário investir mais energia e tempo para identificar o que é real e o que é falso. Considere a hashtag #DCblackout no Twitter em 2020. Iniciada por apenas três seguidores, a hashtag explodiu em uma questão de horas, apesar das tentativas do Twitter de interromper a campanha de desinformação. Meio milhão de pessoas retuitaram o dado, e uma grande parte do país acreditou que o governo havia fechado a internet local para suprimir um distúrbio civil.[17] A ilegitimidade da hashtag #DCblackout acabou sendo exposta, mas a confusão inicial serve como um exemplo convincente dos efeitos potencialmente desorganizadores que uma barragem de eventos pode ter sobre operações táticas agilizadas e rápidas.

O potencial de que a barragem de eventos passe a integrar a doutrina adversária não deve ser subestimado. Apesar de não ter sido designada como uma barragem de eventos, talvez a primeira forma dessa tática tenha se manifestado em 2014 na Ucrânia. Embora a análise

Elementos gráficos de myriammira e starline via Freepik, www.freepik.com. Composição visual: Arin Burgess, Army University Press

dos acontecimentos na Ucrânia tenha sido coberta em detalhes por pensadores políticos e estratégicos em todo o mundo, vale destacar alguns pontos principais. A Rússia demonstrou a capacidade de 'bombardear' as manifestações ucranianas em 2014 com "uma rede de dezenas de grupos das mídias sociais [...] utilizados para difundir boatos falsos com o objetivo de prejudicar as tropas ucranianas ou desacreditar a liderança do exército".[18] Os próprios soldados ucranianos foram diretamente visados com "mensagens de SMS, que chegaram aos seus celulares vindo, mais provavelmente, de sistemas de guerra eletrônica russos".[19] Por último, atores russos utilizaram métodos simples como *bikini trolls* com fotos de perfil de mulheres atraentes para atrair seguidores digitais e neutralizar "algumas das ferramentas de análise de *trolls* e *bots*".[20] Essas características de disseminação digital de eventos informacionais, focalização em locais e pessoas específicas como alvos e neutralização de ferramentas analíticas de detecção de dissimulação são indicadoras de uma doutrina em evolução, que poderia ser executada no nível tático.

Outra consideração que devemos levar em conta é a análise custo-benefício de executar uma barragem de eventos. Sua eficácia vale o custo da alocação de recursos, organização e execução? Essa questão talvez seja mais bem contextualizada com uma comparação da análise custo-benefício com as de outros tipos de obstáculo, fogos não letais e letais e esforços de dissimulação militar. Para começar, conforme delineado por Penninger, a Agência de Pesquisa da Internet de Mikhail Burchik, uma empresa russa diretamente responsável por campanhas de desinformação em curso nos EUA, operava com um orçamento no nível de um "dígito de milhões de dólares por alguns anos de assédio e inquietação".[21] Além disso, a empresa RAND observa que, na "fábrica" de trolls russa em São Petersburgo, "os funcionários recebem pelo menos USD 500 por mês para administrar contas falsas, difundindo propaganda e desinformação".[22] Combinando esses números, parece lógico que uma equipe de cerca de 50 atores cibernéticos russos dedicados possa executar uma campanha de desinformação contínua e abrangente por aproximadamente USD 40 mil por mês. Cabe lembrar, também, que essa despesa inclui o custo de comprar anúncios e operar uma infinidade de servidores e *botnets* (redes de *bots*) relacionados. Portanto, o custo de um mês de operações desse grupo relativamente pequeno equivaleria a pouco menos da metade de um único míssil Hellfire, cerca de 40 munições não guiadas de obuseiro ou 400 cartuchos de munição 30 mm para um helicóptero Apache AH-64. Ou ainda: o custo de um mês inteiro de barragem de eventos poderia corresponder a apenas dez horas de voo de um único veículo aéreo não tripulado MQ-1B Predator.[23]

Conduzir uma barragem de eventos é uma maneira econômica, precisa e rápida de desorganizar o processo decisório tático dos EUA, sobrecarregar os recursos de IRVA, gerar efeitos vantajosos no campo de batalha e degradar o valor das OSIF disponíveis. Gerar e executar uma barragem de eventos está, seguramente, entre as capacidades da maioria de Estados-nação modernos, muitos grupos adversários e talvez até mesmo atores cibernéticos individuais, munidos de enormes exércitos de *bots*.

A morte da OSINT no nível tático

As consequências de barragens de eventos, campanhas de desinformação, apropriação de tendências e dissimulação militar reduzirão, fundamentalmente, a utilidade da OSINT no nível tático. A informação na internet não é uma entidade abstrata independente, que seja relativamente maleável, mas ainda sim capaz de manter sua verdadeira forma apesar dos repetidos esforços de usuários interconectados para provocar e manipular continuamente. Ao contrário, a informação na internet *são* os usuários interconectados presentes em tal domínio, e seu conteúdo se manifesta com base na vontade e no poder desses usuários. À medida que a internet crescer e se expandir, o mesmo ocorrerá com a capacidade dos Estados-nação e atores para alterá-la. Como no exemplo do pelotão de infantaria perto da aldeia, a informação obtida a partir da internet será questionada até o ponto de se tornar praticamente inútil. Em vez de responder a necessidades de informação, as OSIF servirão simplesmente para gerar *mais* dessas necessidades. Há, realmente, um distúrbio acontecendo em Cabul? O inimigo, de fato, acabou de reposicionar uma de suas baterias de mísseis Pantsir? A ponte em minha rota de saída foi realmente destruída?

Talvez nem seja demais supor que os Estados-nação considerarão que os cidadãos têm o *dever* de inundar a internet com informações falsas. Ao contrário do slogan de tempo de guerra no século XX "loose lips sink ships" (algo como "a língua solta afunda navios"), poderíamos, potencialmente, assistir a um mundo onde os governos incentivem os cidadãos a inundar o domínio digital com informações falsas. Isso não só serviria para proteger a vida dos soldados na área de operações e/ou desorganizar

os planos inimigos, como também poderia ser realizado por todo cidadão que tivesse um smartphone e acesso à internet, independentemente de sua distância geográfica da zona de combate. De fato, os governos poderiam até mesmo oferecer estímulos monetários ou civis para induzir os cidadãos a conduzir campanhas de desinformação, talvez sob a forma de incentivos fiscais ou medalhas de cidadania. Quanto maior o número de pessoas que contribuam para a barragem de eventos e a desinformação, maior será a probabilidade de êxito. Um milhão de pessoas diferentes publicando postagens, tuitando, retuitando e escrevendo sobrepujarão os mecanismos destinados a identificar campanhas de desinformação on-line, como a análise léxica, de rede ou geoespacial. Na verdade, a abordagem da "nação como um todo" em relação à guerra poderia, certamente, incentivar a organização e transformação da informação de fontes abertas em arma em um grau nunca visto antes.

Recomendações

Existem algumas opções disponíveis quando se considera como superar os impactos prejudiciais da barragem de eventos, apropriação de tendências e campanhas de desinformação direcionadas, embora nenhuma seja ideal isoladamente: (1) como nação, continuar a dedicar recursos e energia ao desenvolvimento de melhores ferramentas e processos analíticos para lidar com o aumento da desinformação na internet; (2) conter nossa dependência em relação às mídias sociais como meio de rastrear as atividades adversárias durante o combate; e (3) visar, agressivamente, *botnets* adversárias, "fábricas" de trolls e atores nocivos conhecidos durante atividades globais e de preparação do teatro de operações. Com a combinação dessas três iniciativas, poderíamos assistir a uma redução de risco para a nossa força e missão e, potencialmente, salvaguardar a utilidade das OSIF.

O desenvolvimento de ferramentas cada vez mais sofisticadas para lidar com novas ameaças cibernéticas tem sido uma política de defesa estadunidense desde o início da era do computador.[24] No entanto, poderíamos nos beneficiar, potencialmente, de reconsiderar alguns processos e procedimentos simples. Por exemplo, registrar todas as *botnets* significativas, adversários cibernéticos e suas respectivas assinaturas digitais; reunir essas informações em um local centralizado e com o recurso de filtros; e disseminar essas informações aos analistas no nível tático para o rápido cruzamento de referências poderiam ajudar a reduzir as implicações de OSIF utilizadas como arma.[25] Em 2017, a RAND observou que as brigadas de combate precisavam reforçar suas capacidades cibernéticas defensivas e ofensivas, em parte devido à necessidade de que seus comandantes pudessem "responder com velocidade suficiente a tais eventos, no que provavelmente será um ambiente dinâmico e rico em informações".[26] Enfrentar um ataque cibernético não letal como uma barragem de eventos decerto conta como um desses casos, o que seria mitigado, pelo menos parcialmente, pela sincronização ou integração de profissionais de cibernética e de inteligência no nível tático. Além disso, padronizar e exigir o treinamento em OSINT para analistas do nível tático possibilitaria a disseminação de melhores práticas e lições aprendidas e informaria todas as partes envolvidas sobre ameaças e tendências emergentes. Embora procedimentos militares convencionais proíbam a prática de OSINT por analistas não treinados, seria ingênuo supor que eles ignorem totalmente as OSIF, especialmente quando uma parcela maior da população mundial comunica, deliberadamente, as atividades do adversário. Ademais, mesmo que os analistas de todas as fontes se abstenham de incorporar OSIF abertamente em suas avaliações, sua exposição às informações nas mídias sociais provavelmente contribuirá para vieses ou análises inerentemente falhas.

Além de mais treinamento, melhor compartilhamento de informações e integração de especialistas em cibernética no nível tático, também devemos abordar as OSIF com uma cautela ainda maior que a praticada anteriormente. Com o crescente uso de *botnets* e apropriação de tendências por parte do adversário, agregar OSIF com base em pequenas amostras poderia gerar preocupações legítimas quanto à distorção de resultados e, consequentemente, permitir que o adversário manipulasse ou previsse futuras ações militares estadunidenses. As informações obtidas a partir de uma pequena amostra demarcada por *geofencing* ou características demográficas devem ser sempre tratadas com um alto grau de ceticismo, e a necessidade de confirmação por meio de disciplinas de inteligência além da OSINT deve ser priorizada. Infelizmente, muitos adversários dos EUA reconhecem esse fato, o que, atualmente, está induzindo países como a China e a Rússia a desenvolverem e instituírem sua própria intranet nacional ou censurar fortemente as informações que chegam a seu país a partir da internet global.[27]

Por último, visar entidades adversárias responsáveis pela execução de barragens de eventos e campanhas de

desinformação deve ser uma das prioridades máximas dos EUA durante as fases de "moldar" e "dissuadir" de qualquer operação militar em que esteja previsto o emprego de tropas terrestres. Embora visar atores cibernéticos nocivos esteja longe de ser um conceito inovador, é importante observar como seria difícil fazê-lo com eficácia, especialmente quando se considera a facilidade com que algo como uma barragem de eventos pode ser rapidamente projetado por todo o mundo. Por exemplo, os controladores de *botnets* na Rússia podem e provavelmente vão conduzir campanhas de desinformação direcionadas em apoio a operações terrestres em guerras por procuração (*proxy*) nas quais não estejam envolvidos abertamente. Além disso, as dificuldades para superar as fronteiras políticas e legais internacionais entre Estados-nação poderiam representar um grave problema para visar atores residentes em outras nações soberanas. Como vimos ao longo das últimas décadas, já é difícil atribuir um único ataque cibernético a um ator ou atores, quanto mais reagir com um ação retaliatória ou preemptiva. Contudo, devemos aos comandantes responsáveis pelo bem-estar de seus soldados e pela segurança da nação o desenvolvimento e implementação de mecanismos para superar esses obstáculos.

Referências

1. Libor Benes, "OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm", *Journal of Strategic Security* 6, no. S3 (2013): S24, http://dx.doi.org/10.5038/1944-0472.6.3S.3.

2. Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), p. 3, acesso em 22 out. 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

3. Ben Sullivan, "Twitter's the Only Tool You Need for Tracking the Military", Vice News, 24 April 2017, acesso em 22 out. 2020, https://www.vice.com/en/article/wn3g99/twitters-the-only-tool-you-need-for-tracking-the-military.

4. Ron Penninger, "Operationalizing OSINT Full-Spectrum Military Operations", Small Wars Journal, 14 January 2019, acesso em 22 out. 2020, https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations.

5. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, p. 34.

6. "About", Live Universal Awareness Map, acesso em 22 out. 2020, https://usa.liveuamap.com/about#history.

7. "Libya", Live Universal Awareness Map, acesso em 22 out. 2020, https://libya.liveuamap.com/en/2020/26-june-6-antiaircraft-russianmade-pantsyr-vehicles-arrived.

8. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, p. 37.

9. Ibid., p.10.

10. Penninger, "Operationalizing OSINT".

11. Jarred Prier, "Commanding the Trend: Social Media as Information Warfare", *Strategic Studies Quarterly* 11, no. 4 (2017): p. 54, acesso em 22 out. 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

12. Ibid.

13. "White Racially Motivated Violent Extremists Developing Program to Create Bulk Social Media Accounts", Open Source Intelligence Bulletin 20-06-59 (Orlando, FL: Central Florida Intelligence Exchange, 25 June 2020).

14. Janus Rose, "Spoofing Tool Lets You Catch Pokémon from Julian Assange's Embassy Prison", Vice News, 19 July 2016, acesso em 22 out. 2020, https://www.vice.com/en/article/53d5pk/skylift.

15. Jesse Drucker, "Fox News Removes a Digitally Altered Image of Seattle Protests", *New York Times* (site), 23 June 2020, acesso em 22 out. 2020, https://www.nytimes.com/2020/06/13/business/media/fox-news-george-floyd-protests-seattle.html.

16. Williams and Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, p. 24-25.

17. Kate O'Flaherty, "Twitter Suspends Accounts Posting about DC Blackout for Spreading 'Misinformation'", *Forbes* (site), 2 June 2020, acesso em 22 out. 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/06/02/twitter-suspends-accounts-posting-about-dc-blackout-for-spreading-misinformation/#4375b9f8530d.

18. Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corporation, 2018), p. 16.

19. Ibid.

20. Ibid., p. 23.

21. Penninger, "Operationalizing OSINT".

22. Helmus et al., *Russian Social Media Influence*, p. 22.

23. Mark Thompson, "Costly Flight Hours", *Time* (site), 2 April 2013, acesso em 22 out. 2020, https://nation.time.com/2013/04/02/costly-flight-hours/.

24. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), p. 12-13.

25. "Spamhaus Botnet Controller List", Spamhaus, acesso em 3 nov. 2020, https://www.spamhaus.org/bcl/. Veja a *Botnet Controller List* ("Lista de Controladores de *Botnets*") como um exemplo de uma abordagem para reunir e rapidamente disseminar grandes quantidades de *botnets* conhecidas.

26. Isaac R. Porche III et al., "Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below" (Santa Monica, CA: RAND Corporation, 2017), p. 2.

27. Jane Wakefield, "Russia 'Successfully Tests' Its Unplugged Internet", BBC News, 24 December 2019, acesso em 22 out. 2020, https://www.bbc.com/news/technology-50902496.