Militar do 1º Batalhão/187º Regimento de Infantaria recolhe impressões digitais em um vilarejo afegão, 07 Mai 13, durante a Operação *Shamshir VI*, em Khoti Kheyl, Distrito de Zormat. (Cb Chenee' Brooks, Exército dos EUA)

Identificação
Capacitando Soldados e Apoiando a Missão

Matt McLaughlin

Um inimigo precisa ser classificado estrategicamente. Ele é convencional, terrorista, insurgente ou híbrido? Ademais, faz-se necessário identificá-lo taticamente. O indivíduo é combatente ou não combatente? Talvez isso possa parecer uma tarefa simples à primeira vista. No entanto, a guerra não convencional contra inimigos assimétricos faz com que, atualmente, tais distinções se tornem difíceis de se estabelecer na prática. Sem essa preocupação, nenhum estado-maior poderá elaborar uma operação militar coerente, e tropas em campanha talvez não consigam diferenciar entre ameaças verdadeiras e civis inofensivos.

Um agente da Polícia Local Afegã olha em um scanner óptico biométrico durante o processo seletivo de ingresso na força conduzido por integrantes do Ministério do Interior Afegão no Distrito de Gizab, Província de Uruzgan. A Polícia Local Afegã é uma força defensiva orientada para a proteção da comunidade em que serve, a fim de trazer segurança e estabilidade às áreas rurais do país. (Sgt David Brandenburg, Marinha dos EUA)

Forças não convencionais se ocultam e escondem suas afiliações para ampliar sua liberdade de ação, organizar a estrutura de comando e controle e produzir efeitos letais. Essas capacidades são ampliadas por tecnologias cada vez mais baratas e comuns, como comunicações sem fio criptografadas e pequenos veículos aéreos não tripulados. O que se busca é encobrir a identidade daqueles que agem contra os interesses dos EUA e comprometer nossa resposta.

As atividades de identificação, como delineadas no Aviso de Doutrina Conjunta 2-16, *Atividades de Identificação* (Joint Doctrine Note [JDN] 2-16, *Identity Activities*), visam a mitigar essa área nebulosa para as forças dos EUA[1]. Trata-se de um conjunto de ferramentas como exploração de área [*site exploitation* — coleta de dados, apreensaõ de material e captura de pessoas em um local específico, como por exemplo durante uma "entrada tática", para posterior análise por equipes de inteligência — N. do T.], investigações forenses e recursos de biometria com sistemas de informações, análises de dados, treinamento e, no futuro, inteligência artificial. As atividades de identificação ajudam as forças conjuntas a negarem o anonimato ao inimigo, permitindo-lhes distinguir entre combatentes e não combatentes e, com isso, levam a luta aos nossos verdadeiros oponentes.

O Problema do Anonimato

Hoje, os interesses dos EUA são desafiados por uma variedade de ameaças estatais e não estatais. A maioria delas compartilha uma característica comum: a dificuldade de identificá-las e atribuir-lhes a responsabilidade por seus atos. Terroristas escondem suas intenções e afiliações verdadeiras para, depois, atacarem centros urbanos sem advertência alguma. Insurgentes, após conduzirem operações violentas contra seus governos, descartam as armas, misturando-se novamente à população nativa. E, nas guerras híbridas, militares de um Estado hostil abandonam seus uniformes, a fim de fomentar a inquietação contra os governos de Estados rivais. Em cada caso, os perpetradores dependem do anonimato para obter êxito, violando as Convenções de Genebra.

Como descrito anteriormente, a identificação de um terrorista, insurgente ou combatente híbrido o tornaria operacionalmente ineficaz por diferentes razões. A Tabela 1 analisa essas variantes. Vale a pena considerar as diferenças na natureza de cada tipo de ameaça antes de discutir como as atividades de identificação podem ajudar a combatê-las.

Como definido na Circular de Instrução 7-100, *A Ameaça Híbrida* (Training Circular 7-100, *Hybrid Threat*), um terrorista é "um indivíduo que comete um ato ou atos de violência ou ameaça usar violência em busca de objetivos políticos, religiosos ou ideológicos"[2]. Insurgentes se engajam no "uso organizado da subversão e da violência [...] para derrubar um governo ou forçar mudanças de uma autoridade central"[3]. Em qualquer caso, eles provavelmente serão classificados como "combatentes inimigos ilegais", isto é, "pessoas sem os direitos de imunidade no combate, que se engajam em atos contra os Estados Unidos ou seus parceiros de coalizão em violação às leis e costumes da guerra durante um conflito armado"[4]. Uma ameaça híbrida pode fazer uso dessas estruturas não convencionais em conjunto com forças militares regulares ou paramilitares.

Matt McLaughlin é contratado na área de comunicações estratégicas da Defense Forensics and Biometrics Agency. Profissional certificado em dados biométricos, é bacharel pela Northwestern University, mestrado em Administração de Empresas pela Loyola University Chicago e mestrado pelo U.S. Naval War College. Durante seu tempo no Serviço Ativo e na Reserva, trabalhou em três navios e um estado-maior naval no exterior.

O termo "terrorista" é amplo. Ele pode ser um indivíduo que atua sozinho com motivos idiossincráticos ou um membro de um grupo mais organizado baseado em células, como a Al Qaeda. Em qualquer caso, o objetivo imediato do terrorista não é controlar território ou estabelecer qualquer autoridade específica, mas simplesmente executar um ataque eficaz, principalmente com efeitos psicológicos contra uma população alvo, independentemente da brutalidade empregada. Isso significa que *o terrorista requer anonimato para atacar sem aviso*. Ele precisa ser capaz de cruzar fronteiras sem ser identificado e necessita de tempo para planejar sua ação e reunir suprimentos para levá-la a cabo, livre da interferência das autoridades. Contudo, uma vez realizado o ataque (geralmente letal para o próprio agressor), o anonimato deixa de ser necessário. Na verdade, o oposto pode ser mais conveniente, considerando que os perpetradores, quase sempre, desejam que suas biografias, reivindicações e afiliações sejam transmitidas ao mundo, como um ato final de autojustificação.

Uma breve observação sobre terroristas domésticos: é bem provável que criminosos que planejem e executem ataques dentro do seu país de origem (e.g., o responsável pela bomba de Oklahoma City) sejam problemas eminentemente policiais, sem envolvimento militar. Como resultado, o terrorismo doméstico está além do alcance deste texto. Dessa forma, a Tabela 1 se refere apenas ao terrorista "internacional". No entanto, para os fins deste artigo, desde que realize viagens ao estrangeiro para receber treinamento, um terrorista doméstico pode ser considerado como "internacional". Considerando que, nesse caso, ele precisaria cruzar fronteiras internacionais, o pretenso perpetrador adquire o perfil dos terroristas internacionais ao visitar locais terroristas no exterior e estar diante da possibilidade de enfrentar forças militares, engajando-se em atividades que claramente o vinculam a grupos hostis.

Os insurgentes têm objetivos mais concretos do que a maioria dos terroristas — visam a minar a legitimidade da autoridade existente em um dado território e substituí-la por uma nova ordem. Assim, os insurgentes precisam planejar o futuro e manter seu sistema e organização. Consequentemente, *insurgentes requerem anonimato para preservar sua força*, bem como para conseguir surpresa tática. Uma ameaça terrorista pode findar-se com a realização de um ataque suicida, mas as insurgências perduram além de um único incidente. Seus líderes, que talvez não estejam diretamente envolvidos nas ações táticas, precisam permanecer vivos e livres, a fim de

Tabela 1. Tipologia dos Combatentes Anônimos

	Área de operações	Motivação	Densidade	Coordenação	Valor principal do anonimato
Terrorista internacional	Alvo no exterior, viagens através das fronteiras internacionais	Várias; individual ou coletiva	Um ou mais indivíduos	Nenhuma; informal	Promover ataques inesperados
Insurgente	Terra natal	Inspirar o movimento popular antigoverno	Células, pequenas e grandes	No nível das células; líderes insurgentes	Preservar a própria força
"Soldado híbrido"	País estrangeiro	Objetivos políticos do governo do seu país	Depende da missão; provavelmente um grande grupo	Responde ao governo do seu país	Negação do envolvimento do governo do seu país

(Tabela pelo autor)

fornecer tanto uma continuidade operacional quanto um fluxo de propaganda. Porém, a não ser que um terceiro país os patrocine, eles só podem fazer isso se estiverem escondidos. Da mesma forma, líderes sem subordinados não têm poder suficiente para influenciar eventos. Assim sendo, os combatentes comuns da insurgência também precisam permanecer anônimos, evitando a detenção preventiva pelas forças de segurança.

Os soldados híbridos se diferenciam dos grupos terroristas e das insurgências em um aspecto chave — respondem a um governo estrangeiro. Isso significa que *o propósito principal do anonimato é proporcionar a um governo estrangeiro a negação do seu envolvimento*. Nesse caso, enquanto o anonimato dos soldados é usado para capacitar as operações híbridas, da mesma forma como terroristas e insurgentes, o maior propósito é ajudar um Estado agressor a furtar-se da culpa por atividades beligerantes. A capacidade ou a incapacidade de atribuir ações a atores estatais tem imensas implicações diplomáticas e geoestratégicas.

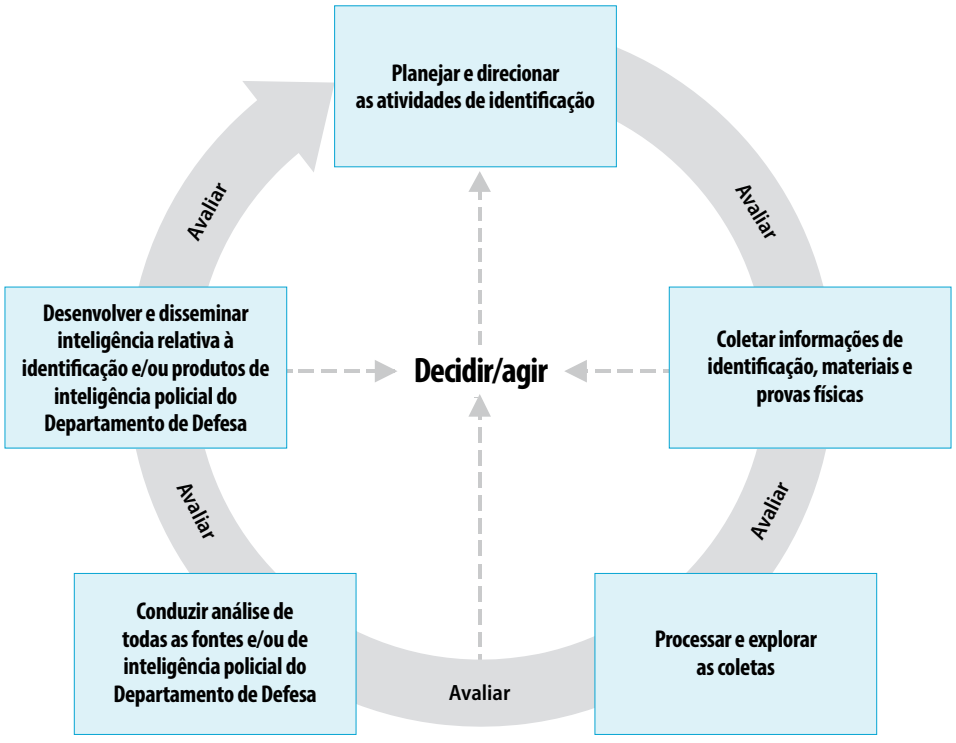
Fornecendo *Insight* por Meio das Atividades de Identificação

Quando as operações requererem a determinação ou a verificação de uma identidade por qualquer motivo, as atividades de identificação exercerão um papel crucial na solução. Contudo, esse conceito engloba uma ampla gama de ferramentas e doutrina.

Segundo o JDN 2-16, as atividades de identificação são "um conjunto de funções e ações que reconhecem e diferenciam apropriadamente uma entidade de outra, apoiando o processo decisório"[5]. Elas podem resolver conflitos; vincular ou definir identidades com precisão; descobrir características compartilhadas de um determinado grupo; caracterizar identidades para avaliar níveis de ameaça ou de confiança; e desenvolver ou gerenciar as informações relativas a identidade. O Ciclo Operacional de Atividades de Identidade (Figura 1) demonstra como vários aspectos das atividades de identificação apoiam o processo decisório[6].

A Publicação Conjunta 3-0, *Operações Conjuntas* (JP 3-0, *Joint Operations*), coloca decididamente a identificação dentro das funções operacionais de inteligência e proteção. Ao discorrer sobre a atividade de inteligência, a JP 3-0 observa:

> Ao identificar primeiro os atores relevantes e aprender tanto quanto possível sobre eles e suas inter-relações, o [comandante da força conjunta] pode desenvolver uma abordagem que facilitará o processo decisório e o comportamento (ativo ou passivo) desses atores que sejam coerentes com o estado final desejado da operação. A análise sociocultural e as atividades de inteligência de identificação (I2) permitem um melhor entendimento dos atores relevantes[7].



(Figura proveniente do JDN 2-16, *Identity Activities*, 03 Aug. 16; as atividades de identificação não são uma única ferramenta ou procedimento, mas um conjunto de várias tarefas e determinações referentes à identificação de indivíduos)

Figura 1. Ciclo Operacional das Atividades de Identificação

Além disso, as "atividades de coleta de identidade" são especificadas como uma das quinze tarefas de proteção[8].

Em ambos os casos, tem-se o entendimento da identificação como uma ferramenta que apoia o processo decisório. Considerando que decisões precisam ser tomadas em todas as fases do conflito e através de uma grande diversidade de operações militares, a identificação se aplica em qualquer situação. Nas missões de cooperação em segurança, por exemplo, as ferramentas de identificação podem ajudar a nação anfitriã a manter o Estado de Direito ao identificar criminosos. Essas mesmas ferramentas podem ajudar a identificar insurgentes ou tropas não uniformizadas durante as hostilidades. E, no decurso das operações de estabilização, as atividades de identificação podem ajudar a estabelecer boa governança ao enfrentar a fraude e as ameaças internas.

As atividades de identificação começaram a demonstrar seu valor operacional durante as missões de combate contra os dispositivos explosivos improvisados (IED, na sigla em inglês) no Iraque e no Afeganistão, em meados da década de 2000. A análise forense dos detritos de IED e da identificação biométrica de indivíduos ajudaram as forças da coalizão a "atacar a rede" dos seus fabricantes e usuários[9]. A infraestrutura montada para essa tarefa específica mostrou-se gradualmente útil a outros propósitos, como a triagem da população, a fim de evitar que terroristas conhecidos ou suspeitos se juntassem à polícia e às forças militares.

Graças ao compartilhamento entre bancos de dados biométricos do Departamento de Defesa e de seus parceiros interagências e internacionais, as informações relativas à identidade de pessoas nefastas reunidas desde 2004 permanecem disponíveis para as necessidades de segurança de fronteira e de imposição da lei, mesmo depois do fim das hostilidades. No mínimo, aqueles indivíduos cujos aspectos biométricos os vinculam a alguma atividade beligerante anterior podem ser requeridos para prestar esclarecimentos adicionais. Nos casos mais sérios, eles podem ter sua entrada negada em outro país ou até mesmo serem detidos. Seja qual for o uso, seus antecedentes históricos teriam passado despercebidos se não fossem os cadastros biométricos e o compartilhamento de dados.

Empregos Variados

A *National Military Strategy* ("Estratégia Militar Nacional"), de 2015, enumera 12 missões típicas de operações conjuntas, muitas das quais estão em curso, e todas podem ser apoiadas, de certa forma, por atividades de identificação[10]. Por exemplo, a biometria e outras ferramentas de certificação de identidade podem ajudar em uma dissuasão nuclear tão bem quanto apoiar uma campanha de contrainsurgência. No entanto, as ideias a seguir concentrar-se-ão em campanhas

e nos indivíduos que os militares norte-americanos poderão, de fato, enfrentar. Cenários reais serão considerados, junto com missões definidas na *Estratégia Militar Nacional*, como mostrado na Tabela 2.

Enfrentando o Estado Islâmico. A luta contra o autoproclamado Estado Islâmico (IE) é um esforço duplo: primeiro, um engajamento para reverter os seus ganhos territoriais no Iraque e na Síria por meio do emprego de uma coalizão internacional e, segundo, a contenção da ameaça terrorista a outros Estados distantes. O EI está resistindo à coalizão, de certo modo, como uma força híbrida; tem (ou tinha) que defender território, algo que geralmente não é feito por grupos terroristas, mas emprega táticas terroristas, como bombardeios suicidas e combatentes não uniformizados. As atividades de identificação ajudam a localizar militantes do EI que se escondem entre o povo, como se fossem insurgentes. Contudo, o aspecto mais pertinente a esta discussão é o esforço para impedir a fuga de seus membros. À medida que o EI é desmantelado na Síria e no Iraque, seus remanescentes se dispersam, voltando a seus países de origem ou buscando refúgio em outras nações. Esses indivíduos precisam ser identificados, rastreados e detidos durante suas viagens para evitar que cometam mais atrocidades. Alguns serão enquadrados como mero aventureiros ou simples soldados e serão permitidos sair. Outros revelar-se-ão líderes superiores ou vinculados diretamente por dados forenses a atos condenáveis que justificam a instauração de processos judiciários. As atividades de identificação são um recurso essencial para a "limpeza" pós Estado Islâmico.

Afeganistão. Embora, já há algum tempo, tenha se tornado um exemplo familiar para muitos leitores, vale observar a relevância das atividades de identificação para as operações de contrainsurgência em

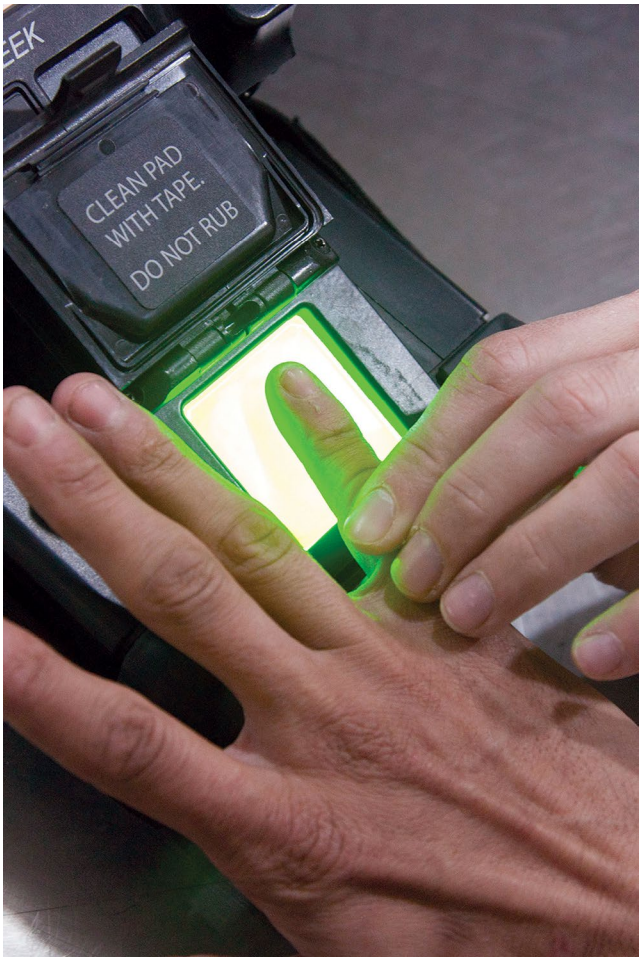
Tabela 2. Identificação na Prática

	Missões dos EUA (*Estratégia Militar Nacional*, 2015)	Tipo de ameaça	Objetivo inimigo imediato	Como a identificação pode impedir o inimigo
Estado Islâmico (terror real; quase híbrido)	• Combater o terrorismo • Responder às crises e conduzir operações de contingência limitadas	Ataques terrestres tradicionais combinados com infiltração urbana e terrorismo global descentralizado	Visa a governar um determinado território pelo qual pode se espalhar e inspirar o terror no exterior	Impedir viagens internacionais do terrorista; atacar a rede terrorista; identificar combatentes/terroristas entre o povo
Afeganistão (insurgente real)	• Conduzir operações de estabilização e de contrainsurgência • Conduzir engajamento militar e cooperação em segurança	Ameaça interna; campanha de terror localizada	Governar território limitado; enfraquecer o Estado	Atacar a rede terrorista; detectar ameaças internas; identificar combatentes/ insurgentes entre o povo
Ucrânia (híbrido real, papel teórico para identidade)	• Negar os objetivos do adversário • Conduzir engajamento militar e cooperação em segurança	Combatentes estrangeiros anônimos fomentam inquietação; guerra convencional misturada com subversão	Desestabilizar o governo rival, com custos mínimos	Atribuir atividades beligerantes a um governo estrangeiro; identificar intrusos estrangeiros
Mar da China Meridional (híbrido teórico)	• Proporcionar uma presença global de estabilização • Negar os objetivos do adversário	Milícia marítima não reconhecida que nega acesso livre ao Mar do Sul da China	Proteger reivindicações de território marítimo	Identificar trânsito marítimo legítimo; atribuir atividades beligerantes a um governo estrangeiro

(Tabela pelo autor)

andamento contra o Talibã e outros grupos armados no Afeganistão. Como uma insurgência, o Talibã se concentra em controlar território e minar a autoridade do governo. A identificação de combatentes anônimos dispersos entre o povo é essencial para desmantelar suas redes clandestinas. É valiosa, também, para impedir a proliferação de outras ameaças internas. Infelizmente, os ataques continuam, mas provavelmente seriam muito piores sem as capacidades de verificação e triagem que as atividades de identificação proporcionam.

Ucrânia. As operações híbridas russas na Ucrânia são bem conhecidas, se não bem entendidas, nos Estados Unidos. Isso se dá, sobretudo, porque a Rússia tem logrado manter um véu de negação do seu papel no conflito "interno" da Ucrânia. Sem dúvida, o anonimato individual



Militar das Forças de Segurança Iraquianas tem suas impressões digitais escaneadas durante uma triagem no Campo de Provas Besmaya, no Iraque. Besmaya é um dos quatro locais onde a Força-Tarefa Conjunta da Operação *Inherent Resolve* dedica-se ao desenvolvimento de capacidades de parceiros. Lá, militares espanhóis e portugueses aprimoram o treinamento das Forças de Segurança Iraquianas. (Sgt Joshua Wooten, Exército dos EUA)

desempenha um papel tático, como exemplificado em 2014 quando tropas não identificadas tomaram o controle de vários prédios governamentais e a incapacidade de atribuir responsabilidade contribuiu para que as forças ucranianas não expulsassem seus ocupantes — embora seja bem provável que fossem militares russos[11]. A Ucrânia reconheceu implicitamente o impacto potencial das ameaças híbridas anônimas — e a dificuldade de identificá-las — ao fechar sua fronteira para todos os cidadãos russos do sexo masculino com idade entre 16 e 60 anos, durante o recrudescimento das tensões em novembro de 2018[12].

Mas, além disso, o anonimato permite que a nação agressora evite a culpabilidade. Invasões ostensivas pede por respostas ostensivas, como ocorreu nas Operações *Desert Shield* e *Desert Storm*. A ação clandestina, contudo, permite que outros Estados aversos ao risco possam, de forma plausível, fazer "vista grossa". Não obstante, a atribuição de responsabilidade é possível. Por exemplo, apesar da natureza supostamente interna do conflito na Ucrânia, reportagens de fontes abertas têm continuamente identificado funerais para tropas russas mortas no país vizinho[13]. Se os jornalistas podem chegar a esse tipo de conclusão pelo simples monitoramento das mídias sociais, então uma capacidade mais elaborada de atividades de identificação, respaldada pelo Estado, oferece grande potencial para se contrapor à narrativa de um Estado agressor[14].

Mar da China Meridional. Por meio de vários esforços diplomáticos e militares, a República Popular da China está criando uma forte presença no Mar da China Meridional. Iniciativas, como a criação de ilhas artificiais e o estabelecimento de uma zona de identificação de defesa antiaérea, chamaram bastante a atenção da comunidade internacional ao longo dos últimos anos[15]. Menos perceptível, mas talvez não menos significativo, tem sido o emprego de forças de "milícia marítima" para impor reivindicações chinesas a bancos de pesca e ilhas dentro de zonas econômicas exclusivas de outros países (algumas dessas nações possuem disputas e reivindicações pendentes entre si, mas todas concordam que as áreas não são chinesas). Barcos de pesca ostensiva com cascos azuis, embora pesquem pouco, aparecem seguramente em lugares disputados[16]. Eles são o eixo central da estratégia híbrida chinesa de afirmar sua dominância nas águas do Sudeste da Ásia. Os proprietários, capitães e tripulantes podem ser rastreados — frequentemente usando registros públicos — e esse tipo de informação pode ajudar a determinar a verdadeira natureza e propósito das embarcações.

O Estado Atual das Atividades de Identificação

Hoje, a maioria do trabalho sobre as atividades de identificação é feita nos bastidores por organizações como a Defense Forensics and Biometrics Agency (Agência Forense e de Biometria de Defesa) e o National Ground Intelligence Center (Centro Nacional de Inteligência Terrestre). Em termos práticos, o trabalho depende de dados coletados por soldados em campanha e seus parceiros interagências, capacitando e aprimorando o processo decisório.

Individualmente, a maioria dos militares reconhecerá nos equipamentos biométricos portáteis (e, até certo grau, os equipamentos de investigação forense) a vanguarda das atividades de identificação. Por mais de uma década, os soldados têm feito uso de aparelhos biométricos portáteis para cadastrar rostos, impressões digitais e íris de milhões de pessoas e registrado informações contextuais para construir o depósito biométrico oficial do Departamento de Defesa. Pelo uso de listas de vigilância armazenadas nos próprios aparelhos, esses registros já permitiram que militares identificassem indivíduos procurados em apenas poucos minutos ou até mesmo segundos após a inscrição.

Hoje, a maior parte da instrução sobre o manuseio desse equipamento é fornecida durante os ciclos de treinamento pré-desdobramento ou após o ingresso no teatro de operações. Normalmente, não é repetida ao longo dos processos de reciclagem da instrução individual ou da unidade, mas é intrínseca às necessidades da missão. O treinamento inclui os sistemas atualmente empregados: o Biometrics Automated Toolset-Army (BAT-A), um laptop com equipamento periférico; e o Secure Electronic Enrollment Kit (SEEK II), um aparelho autônomo portátil.

Alguns soldados, em particular os integrantes da polícia do Exército e os engenheiros de combate do Centro de Excelência de Apoio à Manobra, recebem treinamento mais especializado sobre a investigação forense de locais sensíveis ou de análise pós-detonação. Atualmente, o Exército está desenvolvendo um conjunto padronizado de investigação forense. Outras Forças Singulares empregam, também, a investigação forense em campanha — notadamente, os destacamentos de aplicação da lei do Corpo de Fuzileiros Navais têm apresentado uma razoável capacidade orgânica de análise forense embarcado ou desembarcado desde 2014[17].

Nenhum sistema para a análise de inteligência baseado em recursos de identificação existe no nível operacional, a não ser que se inclua listas de vigilância armazenadas nos aparelhos SEEK II como uma ferramenta que fornece dados de identificação. Em termos práticos, o trabalho de apoio analítico e de decisão associado com as atividades de identificação limita-se ao fornecimento de respostas apenas àqueles "clientes" que as requererem. Se, por ventura, um indivíduo não constar da lista de vigilância entre vários milhares de identidades armazenadas na memória de um aparelho, uma solicitação pode ser enviada para verificação no banco de dados biométricos do Departamento de Defesa. A rapidez das respostas pode variar segundo as circunstâncias, como a prioridade atribuída ao pedido ou a infraestrutura de comunicações. As forças de operações especiais obtêm respostas confiáveis em apenas alguns minutos; outros podem levar mais tempo devido aos caminhos de dados indiretos ou ao tempo de espera atrás de pedidos de prioridade mais elevada.

No nível operacional, cada comando conjunto tem uma pequena equipe de identificação nas seções de inteligência (E2) ou operações (E3). Independente da configuração, o E2 e o E3 coordenam intimamente o planejamento das atividades de identificação, que funcionam como uma fusão "Intel/Op". As operações geram dados que alimentam a inteligência e a inteligência ajuda a conduzir mais operações, em um ciclo virtuoso.

Estado Atual: Cenários Comuns

Com a configuração atual descrita acima, as atividades de identificação já proporcionaram bons resultados ao Departamento de Defesa e seus parceiros interagências ao longo dos últimos anos. Os seguintes cenários comuns demonstram como as atividades de identificação podem ser empregadas com êxito.

Combate aos dispositivos explosivos improvisados. O material recuperado para análise pós-detonação e os locais de fabricação de bombas permitem a instauração de uma investigação forense. Especialistas são capazes de recuperar impressões digitais do material e compará-las com os registros disponíveis no banco de dados biométrico oficial do Departamento de Defesa. Se o dono das impressões digitais for conhecido, seu nome pode ser acrescentado à lista de vigilância e ele pode ser eventualmente detido para interrogatório quando for encontrado. Se as impressões digitais pertencerem a um desconhecido, esse

indivíduo poderia ser futuramente identificado, se seus dados biométricos forem devidamente cadastrados.

Contrainsurgência. Um computador recuperado de um posto de comando dos insurgentes pode ser submetido a uma avaliação forense. Seu hardware provavelmente conterá as impressões digitais dos usuários e a análise dos dados mostrará fotos de integrantes de uma célula clandestina. Isso permitiria a identificação biométrica desses indivíduos no futuro, caso eles tentassem adentrar em instalações de acesso restrito ou fossem mortos ou capturados por tropas da coalizão.

Prevenção de fraude. Um comandante de tropa da nação anfitriã pode identificar e evitar o pagamento indevido a soldados "fantasmas" inexistentes. Para isso, faz-se o cadastro biométrico de cada militar da unidade. As ferramentas de biometria ajudam os oficiais de pagamento a identificar a tentativa de fraude financeira, evitam pagamentos errôneos e permitem implicar judicialmente os comandantes desonestos.

Segurança orgânica. Um indivíduo que se candidata a um emprego como prestador de serviço em uma base de operações avançadas, por exemplo, deve ter sua identidade verificada por meio do seu cadastro biométrico. Esse procedimento básico de contrainteligência impede a infiltração de militantes radicais em áreas de acesso negado.

Proteção de fronteira. Impressões digitais descobertas em um dispositivo explosivo improvisado devem ser carregadas no banco de dados biométrico do Departamento de Defesa. Suponhamos que essas digitais nunca foram vinculadas à identidade de uma pessoa. Porém, anos mais tarde, um indivíduo desconhecido tenta entrar nos Estados Unidos pela fronteira sul. Ao se fazer a verificação de seus dados biométricos constata-se que são coincidentes com aquele velho registro do dispositivo explosivo improvisado. Isso permitirá que ele seja detido para prestar maiores esclarecimentos e sua entrada no país poderá ser negada.

Apoio à manutenção da ordem pública. Se um indivíduo for detido por tráfico de drogas pela guarda costeira de um país aliado, seu cadastro biométrico pode ser, por meio do compartilhamento internacional de dados biométricos, confrontado com os registros existentes nos EUA. Uma eventual afiliação a grupos terroristas ou criminosos permitirá às autoridades policiais competentes instaurar um processo legal contra ele.

Um Exemplo Concreto

O mais importante "golpe" proporcionado pela biometria, medido pela conexão de diversos incidentes, aconteceu no Iraque. Forças de operações especiais detiveram um indivíduo, em 21 de julho de 2011, cujas impressões digitais foram reconhecidas pelos examinadores no momento em que as imagens chegaram. Suas impressões já haviam sido registradas 121 vezes ao longo dos últimos 14 meses, totalizando 35 casos distintos de dispositivos explosivos improvisados. Um recorde! As forças dos EUA o retiraram da luta pelo uso de algoritmos de computador de atuação rápida, análises biométricas profissionais e conexões de dados globais[18].

Estado Futuro: Aspirações

As atividades de identificação já provaram seu valor inúmeras vezes. Com melhorias contínuas de novas tecnologias e processos, combatentes no futuro poderão obter resultados ainda mais expressivos. Mas, independente da forma que as atividades de identificação adquirirem, o Departamento de Defesa deve garantir que as seguintes condições sejam atingidas:

Treinamento. Os soldados precisarão ser treinados e equipados para conduzir atividades de identificação em uma ampla gama de cenários. Em vez de considerar esse tipo de atividade como um sistema particular, justificando a criação de qualificação militar específica, é melhor considerá-las como um "fuzil" — ou seja, uma ferramenta que a infantaria talvez utilize com maior ou menor frequência, mas com a qual todos devem estar familiarizados.

É por essa razão que a criação de uma qualificação militar específica para as atividades de identificação, investigação forense e dados biométricos talvez seja excessivamente restritiva. Essa atividade teria que se encaixar dentro de uma Arma ou especialização já existente como a Infantaria, a Inteligência, a Polícia do Exército, as Comunicações no Corpo de Exército ou algo do gênero — porém, se os responsáveis pelas atividades de identificação ficarem confinados dentro de uma única comunidade, a disponibilidade desse conjunto de competências para todos aqueles que realmente precisam estaria comprometida. Isso pode causar redundância, à medida que outras comunidades descobrirem que também precisam dessas mesmas capacidades entre seus próprios quadros ou pode provocar uma falta de interesse, conforme outras comunidades descartarem o potencial das atividades de identificação porque ela se tornou demasiadamente difícil acessar.

Richard A. Swearengin, um analista de impressões digitais da Divisão de Investigação Criminal do Exército dos EUA, utiliza um monitor para comparar uma impressão digital residual (à esquerda) com uma impressão digital arquivada na Base Aérea Kandahar, Afeganistão, 04 Mai 10. (Sgt Michele A. Desrochers, Força Aérea dos EUA)

Uma estrutura ideal para treinamento seria um único curso disponível para qualquer militar, a fim de disseminar as atividades de identificação por todo o Exército. Uma única escola teria que ser responsável (e.g., a Escola de Polícia do Exército dos EUA), porém isso não significaria que essa comunidade fosse o único gestor do conhecimento requerido. Os graduados podem ganhar um certificado de competência em seus assentamentos, mas não precisam trocar sua qualificação militar. Esse curso básico seria seguido por reciclagens periódicas, na internet ou de outra maneira, tirando proveito das últimas mudanças de currículo validadas pelas autoridades competentes do Comando de Instrução e Doutrina do Exército dos EUA (TRADOC), como o TRADOC Capability Manager for Terrestrial and Identity (TCM-TI) [Gerente de Capacidade para Fisiografia e Identidade — N. do T.]. Isso seria mais importante para as unidades que se preparam para o desdobramento.

Equipamentos e redes. Militares em campanha devem contar com os melhores equipamentos disponíveis, para facilitar cadastramento, cruzamento de dados e apoio ao processo decisório. Primeiro, uma ferramenta eletrônica portátil simples é necessária para a condução do cadastramento biométrico de impressões digitais, rostos e íris em campanha. Com um conjunto de investigação forense adicional que caiba dentro do bolso, esse mesmo aparelho deverá ser capaz, também, de registrar impressões digitais ocultas. Segundo, um aparelho que registra passivamente as informações de rosto ou íris — talvez uma câmera conectada à proteção ocular do soldado — deve ser capaz de identificar indivíduos dentro do seu campo de visão e advertir o militar sobre potenciais pessoas na lista de vigilância.

Esses aparelhos portáteis interagiriam com o banco de dados oficiais do Departamento de Defesa por meio de ferramentas e redes comuns de transmissão de dados, como o próximo rádio tático e a rede WIN-T do Exército. Isso possibilitaria a busca e o cruzamento de dados em tempo real com todos os bancos de dados interagências, indo além das listas de vigilância armazenadas no aparelho. Comunicações estáveis, usando quaisquer nós que estejam disponíveis, seriam essenciais. Os atuais pontos de estrangulamento nos fluxos de trabalho de identificação têm menos a ver com as capacidades dos bancos de dados do que com a eficácia dos meios de comunicações.

Durante o planejamento da aquisição de material, vale lembrar dois aspectos conflitantes: Primeiro, a rápida obsolescência dos aparelhos portáteis devido às céleres mudanças nas capacidades e padrões dessa indústria; e, segundo, a necessidade da comunidade global de defesa de

Um instrutor espanhol fotografa um militar das Forças de Segurança Iraquianas (ISF, na sigla em inglês) antes de dar início ao seu curso de treinamento no Campo de Provas Besmaya, 10 Jan 17. Por todo o país, o processo de triagem faz parte da fase inicial para todos os candidatos das ISF. (Sgt Joshua Wooten, Exército dos EUA)

comprar grandes quantidades de equipamentos resistentes e compatíveis entre si, que sejam capazes de interagir com as redes de dados globais por um prazo muito longo[19]. O governo dos EUA precisa aceitar a premissa de que não é o líder na tecnologia de informações, e quaisquer compras feitas serão obsoletas, segundo os padrões industriais, antes dos produtos serem distribuídos a seus usuários. Assim, o governo precisa estar preparado para manter um único sistema com o mínimo apoio industrial, talvez em parceria com outros aliados. De forma complementar, pode estabelecer uma arquitetura aberta em que uma ampla variedade de aparelhos, servidores e aplicativos adquiridos por processos de compra descentralizados possam ser úteis, contanto que estejam em conformidade com os padrões previamente estabelecidos.

Integração no planejamento de estado-maior. As atividades de identificação podem oferecer benefícios expressivos se forem integradas ao planejamento operacional, mas os estados-maiores precisam entender "como" e "porque". Isso pode começar com treinamento nos escalões mais altos sobre a importância da coleta de dados de identificação pessoal e as análises que elas podem proporcionar. Uma vez que as atividades de identificação podem constar da intenção do comandante, os escalões subordinados devem ter os meios para incorporá-las às suas operações, preferencialmente como parte das normas gerais de ação da unidade. Experiências recentes demonstram que não há somente um único responsável pelas atividades de identificação no nível estado-maior. Normalmente, trata-se de uma atribuição do E2 (Inteligência) ou E3 (Operações), dependendo do comandante ou da preferência do seu estado-maior. Em uma nova estrutura, seria razoável fazer com que o E3 se tornasse responsável pela coleta; a Seção de Comando e Controle (E6) recebesse o encargo de distribuição; e o E2 tivesse a atribuição da análise e confecção dos relatórios, com um único assistente de estado-maior (um oficial identificador, ou algo do tipo) que coordenasse essas ações.

Essa institucionalização das atividades de identificação requer, também, uma revisão gradual das várias publicações conjuntas e do Exército, como aquelas que regulam as ordens de operações. A especificação de um parágrafo ou um anexo no formato de uma ordem de operações padrão para as atividades de identificação (por meio do Manual de Campanha 6-0, *Organização e Operações do Comandante e Estado-Maior* [FM 6-0, *Commander and Staff Organization and Operations*], e outras referências) seria de grande valor para incentivar os militares a considerar o papel da identificação nas operações[20].

Estado Futuro: Inteligência Artificial

Como um processo essencialmente cognitivo, as atividades de identificação proporcionam vários pontos nos quais futuras iterações empregando Inteligência Artificial (IA) e aprendizado de máquina exercerão um papel importante. A coleta, o processamento e a análise de informações de identificação requerem a separação

dos dados relevantes daquilo que não interessa, além da busca por padrões e tendências no conjunto de informações filtrado. A IA e o aprendizado de máquina aumentarão a velocidade e precisão desses processos — e, em alguns casos, já estão fazendo isso. A IA oferece grande potencial para apoiar a obtenção dos cadastros biométricos em condições difíceis, identificando padrões com dados imperfeitos, colocando a identidade em contexto por meio de análises de dados e enfrentando as tentativas dos adversários de evitar ou confundir o sistema.

Em termos de coleta, a IA pode ajudar na criação de registros úteis, mesmo com dados deficientes. As operações militares ocorrem frequentemente em ambientes "sem restrições". Ou seja, a luminosidade é imperfeita, as câmeras estão se movendo, o barulho de fundo é ensurdecedor e as condições predominantes são, de um modo geral, inapropriadas para uma coleta de dados de qualidade, sejam imagens faciais, leitura da íris, gravações de voz ou impressões digitais residuais. Os humanos podem identificar pessoas conhecidas nessas circunstâncias, mas os sistemas biométricos antigos talvez não. A IA pode ajudar a mitigar esse problema, até o ponto de identificar rostos atrás de máscaras, óculos de sol e outras "oclusões"[21]. Testes laboratoriais já produziram algoritmos capazes de identificar corretamente rostos obscurecidos por lenços e chapéus em até 77% das vezes[22]. O conceito pode ser estendido visando ao aperfeiçoamento de imagens com baixa iluminação, ângulos deficientes e outros fatores.

Isso tem o potencial de transferir o ônus de criar um registro útil do hardware de cadastramento para o software inteligente. Por exemplo, uma maneira para obter imagens faciais de longo alcance seria empregar sistemas avançados de câmeras com óticas sensíveis. Um método alternativo é empregar câmeras baratas disponíveis no mercado, mas aprimorar as imagens produzidas por meio de IA para criar registros confiáveis. Em ambos os casos, o usuário obterá o mesmo resultado, mas a segunda solução pode ser a mais simples para instalar e usar em um ambiente operacional.

Uma vez feito o cadastramento, a IA pode aumentar a velocidade e precisão de cruzamento dos dados anteriores para definir a identidade de um indivíduo. Tanto os novos cadastramentos quanto os registros antigos podem conter apenas dados parciais ou outras características imprecisas (como rostos cobertos por lenços como mencionado acima). Atualmente, em tais circunstâncias, analistas humanos estudam as imagens do cadastro para verificar alinhamento ou a falta de alinhamento quando os algoritmos existentes não são capazes de fazê-lo. Embora isso ocorra apenas em uma pequena porcentagem dos casos, ainda assim, exige um grande empenho de tempo e mão de obra. A IA adequadamente "treinada", contudo, aprimorará a precisão, confiabilidade e eficiência dos algoritmos, reduzindo progressivamente a necessidade de humanos no ciclo de análise. Os algoritmos produzidos pelo aprendizado de máquina associado a um grande conjunto de dados complexos de diversas características de indivíduos serão ferramentas poderosas.

Além do cruzamento de registros e da construção de repositórios de dados, a IA será importante para conseguir entendimentos holísticos das identidades individuais. A informação da identidade é obtida por uma série de fluxos de dados, como os biométricos, biográficos e reputacionais, como definidos no JDN 2-16[23]. Em termos ideais, todos esses dados devem ser armazenados em um repositório de informações. A IA proporcionará os meios de encontrar a informação útil em diferentes acervos de dados, na forma de padrões, tendências e associações que analistas humanos e tecnologias antigas talvez jamais tenham feito. Informações disponíveis em registros financeiros poderão ser instantaneamente cruzadas com dados biométricos, a fim de confirmar uma identidade.

Em todas as fases das atividades de identificação, a IA lidará com uma ameaça sempre presente: outras IA. Imagens modificadas — mesmo em vídeo — são cada vez mais comuns e convincentes[24]. Em um exemplo bem conhecido, mas inofensivo, produtores de cinema removeram digitalmente o bigode de Henry Cavill durante refilmagens de *Liga da Justiça*, de 2017, com parcos resultados. Em resposta, um usuário da internet, com quase nenhum orçamento, usou um algoritmo "deepfake" [técnica de síntese de imagens — N. do T.] de um computador pessoal para melhorar o trabalho do estúdio[25]. Com a difusão da tecnologia para criar falsificações em diferentes domínios, incluindo o biométrico, talvez chegue o dia em que somente as IA poderão diferenciar entre dados verdadeiros e falsos — entre identidades reais e engodos. As atividades de identificação continuarão a ser uma capacidade vital, mas, também, farão parte de um ambiente operacional disputado.

Conclusão

Nascidas das necessidades do combate, amadurecendo tanto como uma capacidade operacional quanto um projeto empresarial do Departamento de Defesa, as atividades de identificação representam um facilitador contínuo para as operações militares e as funções internas de segurança. Reduzem a fraude e aumentam a contabilidade, tanto em assuntos civis quanto nos negócios diários. De maior importância para os militares em campanha, permitem que eles melhor façam a distinção entre amigo e inimigo em qualquer circunstância. A tecnologia e os procedimentos apenas melhorarão nos anos vindouros, e o Exército e o Departamento de Defesa precisam estar preparados para negar o anonimato ao inimigo. ■

Referências

1. Joint Doctrine Note (JDN) 2-16, *Identity Activities* (Washington, DC: U.S. Government Publishing Office [GPO], 3 Aug. 2016), p. vii.
2. Training Circular (TC) 7-100, *Hybrid Threat* (Washington, DC: U.S. Government Printing Office, November 2010), p. 2-4.
3. Ibid.
4. Ibid.
5. JDN 2-16, *Identity Activities*, p. vii.
6. Ibid., p. I-15.
7. Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 January 2017), p. III-24.
8. Ibid., p. III-36.
9. David F. Eisler, "Counter-IED Strategy in Modern War", *Military Review* 92, no. 1 (January–February 2012): p. 13, acesso em: 19 mar. 2018, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20120229_art006.pdf.
10. U.S. Joint Chiefs of Staff, *The National Military Strategy of the United States of America* (Washington, DC: U.S. Joint Chiefs of Staff, June 2015), p. 10-13, acesso em: 19 mar. 2018, https://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.
11. John Chambers, "Countering Gray-Zone Hybrid Threats: An Analysis of Russia's 'New Generation Warfare' and Implications for the U.S. Army" (report, West Point, NY: Modern War Institute, 18 Oct. 2016), p. 15, acesso em: 19 mar. 2018, https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf.
12. "Ukraine Closes Border to Russian Men", PBS News Hour, 30 Nov. 2018, acesso em: 6 dez. 2018, https://www.pbs.org/newshour/show/news-wrap-ukraine-closes-border-to-russian-men.
13. James Miller, Pierre Vaux, Catherine A. Fitzpatrick e Michael Weiss, "An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine", *The Interpreter* (report, New York: Institute of Modern Russia, 2015), p. 49, acesso em: 7 jul. 2017, http://www.interpretermag.com/wp-content/uploads/2015/11/IMR_Ukraine_final_links_updt_02_corr.pdf; Catherine A. Fitzpatrick, "Finding Putin's Dead Soldiers in Ukraine", *The Daily Beast*, 16 Sep. 2015, acesso em: 19 mar. 2018, https://www.thedailybeast.com/finding-putins-dead-soldiers-in-ukraine/.
14. Patrick Tucker, "The Science of Unmasking Russian Forces in Ukraine", Defense One, 16 Apr. 2014, acesso em: 19 mar. 2018, https://www.defenseone.com/technology/2014/04/science-unmasking-russian-forces-ukraine/82693/.
15. Colin Dwyer, "The Multiplex and the Plane: China's Moves in Surrounding Seas Raise Eyebrows", National Public Radio, 25 Jul. 2017, acesso em: 19 mar. 2018, https://www.npr.org/sections/thetwo-way/2017/07/25/539248350/the-multiplex-and-the-plane-chinas-moves-in-surrounding-seas-raise-eyebrows/.
16. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 2017, 15 May 2017, p. 56, acesso em: 19 mar. 2018, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF?ver=2017-06-06-141328-770.
17. Matthew Finnerty, "SPMAGTF MPs Exploit Vital Material", Defense Visual Information Distribution Service, 21 Dec. 2014, acesso em: 19 mar. 2018, https://www.dvidshub.net/news/151673/spmagtf-mps-exploit-vital-material/.
18. Biometrics Identity Management Agency [now Defense Forensic and Biometrics Agency], *Annual Report FY11*, "The Super Hit", p. 25.
19. Sean Lyngaas, "Can the Pentagon Keep Pace on Biometrics?", FCW (website), 11 Mar. 2015, acesso em: 2 Apr. 2018, https://fcw.com/articles/2015/03/11/can-the-pentagon-keep-pace-on-biometrics.aspx.
20. Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. GPO, May 2014).
21. Amarjot Singh et al., "Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network" (apresentação de estudo, IEEE International Conference on Computer Vision Workshop (ICCVW), Venice, Italy, 22–29 Oct. 2017), acesso em: 10 abr. 2018, https://arxiv.org/pdf/1708.09317.pdf.
22. Matt Reynolds, "Even a Mask Won't Hide You from the Latest Face Recognition Tech", *New Scientist* (website), 7 Sep. 2017, acesso em: 16 mar. 2018, https://www.newscientist.com/article/2146703-even-a-mask-wont-hide-you-from-the-latest-face-recognition-tech/.
23. JDN 2-16, *Identity Activities*, p. I-13.
24. David Pierson, "Fake Videos Are on the Rise. As They Become More Realistic, Seeing Shouldn't Always Be Believing", *Los Angeles Times* (website), 19 Feb. 2018, acesso em: 16 mar. 2018, https://www.latimes.com/business/technology/la-fi-tn-fake-videos-20180219-story.html.
25. James Vincent, "Cheap AI Is Better at Removing Henry Cavill's Superman Mustache Than Hollywood Special Effects", The Verge, 7 Feb. 2018, acesso em: 16 mar. 2018, https://www.theverge.com/tldr/2018/2/7/16985570/superman-mustache-ai-deepfakes-henry-cavill.