El especialista Jordon Purgat, asignado al 1er Batallón, 187° Regimiento de Infantería, toma las huellas digitales de un afgano el 7 de mayo de 2013 durante la operación Shamshir VI en Khoti Kheyl, distrito de Zormat, Afganistán. (Foto: Especialista Chenee' Brooks, Ejército de Estados Unidos)

La identidad
Habilitando a los soldados, apoyando la misión

Matt McLaughlin

Un enemigo debe ser clasificado según su valor estratégico (¿es convencional, terrorista, insurgente o híbrido?) y su función táctica (¿es el sujeto combatiente o no combatiente?). Esto puede parecer simple a primera vista, sin embargo, en una guerra no convencional con enemigos asimétricos, tomar este tipo de decisiones no es una tarea fácil para una fuerza conjunta. Sin estas consideraciones, ningún estado mayor podría planificar una operación militar coherente y es posible que las tropas en el terreno no puedan diferenciar entre amenazas y civiles inofensivos.

Las fuerzas no convencionales se ocultan, y también ocultan sus filiaciones, para mejorar la libertad de maniobra, organizar el comando y control, y crear efectos letales. Estas capacidades son amplificadas por tecnologías que son cada vez más económicas y comunes como las comunicaciones inalámbricas encriptadas y las aeronaves no tripuladas pequeñas. El objetivo es oscurecer las identidades de aquellos que actúan contra los intereses de EUA y confundir nuestra respuesta.

Las actividades de identidad, como se articula en la Joint Doctrine Note (JDN) 2-16, *Identity Activities*,

buscan mitigar esta área gris para la fuerzas estadounidenses[1]. Al combinar herramientas como la explotación de sitios web, las investigaciones forenses y la biometría con los sistemas de información, el análisis de inteligencia y el entrenamiento —y la inteligencia artificial en el futuro—, las actividades de identidad permitirán a la fuerza conjunta negar el anonimato al enemigo, distinguir combatientes de no combatientes y llevar la lucha donde el oponente.

El anonimato, un problema

En la actualidad, Estados Unidos enfrenta una miríada de amenazas estatales y no estatales que, por lo general, tienen una característica en común, lo difícil que son de identificar y atribuir. Los terroristas esconden sus verdaderas intenciones y filiaciones para atacar los centros de las ciudades por sorpresa. Los insurgentes se alzan en armas, conducen operaciones violentas contra sus Gobiernos y después descartan sus armas y se desvanecen entre la población. En las guerras híbridas, los soldados de un Estado hostil fomentan revueltas contra los Gobiernos de Estados rivales de forma clandestina. En cada uno de estos casos, los perpetradores dependen del anonimato —en contravención de los Convenios de Ginebra— para conseguir sus objetivos.

Al ser identificado, el terrorista, el insurgente o el soldado híbrido pierde su capacidad operativa, pero las razones por lo que esto sucede varían (tabla 1). Vale la pena considerar las diferencias en la naturaleza de estas amenazas antes de discutir cómo las actividades de identidad ayudan a combatirlas mejor.

Según la Training Circular 7-100, *Hybrid Threat*, un terrorista es «un individuo que comete un acto o actos de violencia o amenaza con violencia en busca de objetivos ideológicos, religiosos o políticos»[2]. Los insurgentes «usan la subversión y la violencia de manera organizada […] para derrocar o forzar el cambio de una autoridad gobernante»[3]. Ambos probablemente pueden ser clasificados como combatientes enemigos ilegales, «personas sin derecho a la inmunidad de combate que participan en actos contra Estados Unidos o sus socios de coalición en violación de las leyes y las costumbres de la guerra durante un conflicto armado»[4]. Una amenaza híbrida puede hacer uso de estos constructos no convencionales junto con fuerzas paramilitares y regulares.

«Terrorista» es un término amplio; él o ella puede ser un individuo solitario con motivos idiosincrásicos o miembro de un grupo organizado con células como al-Qaeda. En cualquiera de los casos, el objetivo inmediato del terrorista no es controlar territorio o establecer autoridad específica, sino solo llevar a cabo un ataque eficaz con efectos principalmente psicológicos contra la población (aparte de la carnicería inmediata). Esto significa que *un terrorista requiere el anonimato para poder atacar sin levantar sospechas*. Él o ella debe ser capaz de cruzar fronteras sin ser detectado y necesita tiempo para planificar y reunir abastecimientos sin la interferencia de las autoridades. Pero una vez que se lleva a cabo el ataque (usualmente letal para el atacante), el anonimato deja de ser una prioridad. También es posible que ocurra lo opuesto, dado que los atacantes a menudo quieren que sus biografías, reivindicaciones y filiaciones sean divulgadas al mundo en un acto final de justificación.

Una breve mención sobre el terrorismo doméstico, los ataques terroristas ejecutados por aquellos que los planifican y los llevan a cabo en su país de origen (p. ej. el terrorista de Oklahoma City) probablemente serán

Un miembro del Ministerio del Interior afgano utiliza un dispositivo biométrico para escanear los ojos de un candidato a la Policía Local Afgana el 18 de diciembre de 2011 en el distrito de Gizab, provincia de Uruzgan, Afganistán. La Policía Local Afgana es una fuerza de protección comunitaria que busca traer estabilidad a las áreas rurales de Afganistán. (Foto: Sargento segundo David Brandenburg, Armada de Estados Unidos)

un asunto de la policía y no de las fuerzas militares. Como resultado, el terrorismo doméstico va más allá del alcance de este artículo y por eso se incluye el adjetivo «internacional» en la tabla 1. Sin embargo, viajar al extranjero para entrenarse como terrorista es suficiente para incluir al terrorista doméstico en la lista «internacional» de este análisis. Una vez en el exterior, estos individuos pueden visitar sitios terroristas, reunirse con fuerzas militares y participar en actividades que claramente los vinculan a grupos hostiles, lo cual es suficiente para clasificarlos como terroristas internacionales.

Los insurgentes tienen objetivos más concretos que la mayoría de los terroristas porque buscan socavar la legitimidad de la autoridad existente de un territorio específico para remplazarla con la suya. Ellos deben planificar para el futuro y mantener su aparato y organización. Por ello, *el anonimato se vuelve esencial para preservar la fuerza* como también para lograr la sorpresa táctica. Una amenaza terrorista particular puede culminar con un ataque suicida, las insurgencias, sin embargo, son más que un solo acto. Los líderes insurgentes, quienes tal vez no participen directamente en acciones tácticas, deben permanecer vivos y libres para proporcionar continuidad operativa y propaganda; pero, a menos que un tercer país los esté patrocinando, ellos solo pueden hacer esto si están escondidos. Asimismo, los líderes sin seguidores no tienen mucho poder para influenciar los sucesos; por lo tanto, los insurgentes en el terreno también deben permanecer anónimos si quieren evitar ser capturados por las fuerzas de seguridad antes de lograr sus objetivos.

Matt McLaughlin es un contratista encargado de las comunicaciones estratégicas en la Agencia de Defensa para la Investigación Forense y Biométrica (DFBA). Además de poseer un certificado de biometría profesional, McLaughlin también cuenta con una licenciatura de la Universidad de Northwestern, un MBA de la Universidad de Loyola en Chicago y una maestría de la Escuela Superior de Guerra Naval. Entre sus cometidos en la reserva y en el servicio activo figuran misiones en tres buques y la participación en un estado mayor naval avanzado.

Los soldados híbridos se diferencian de los grupos terroristas y las insurgencias en un aspecto clave, ellos responden a un Gobierno extranjero. Esto significa *que el propósito principal del anonimato es proporcionar al Gobierno extranjero la capacidad de negar cualquier vínculo con las acciones llevadas a cabo*. En este caso, si bien el anonimato permite a los soldados híbridos conducir las operaciones, como también a los terroristas y a los insurgentes, el objetivo principal es evitar responsabilizar al Estado agresor por actividades beligerantes. La capacidad o incapacidad para atribuir acciones a un Estado tiene consecuencias geoestratégicas y diplomáticas significativas.

Las actividades de identidad facilitan la información

Cuando las operaciones requieren determinar o verificar la identidad por cualquier razón, las actividades de identidad juegan un papel importante en la realización de esta tarea. Sin embargo, el término «actividades de información» abarca una amplia gama de herramientas y doctrina.

Conforme a la JDN 2-16, las actividades de identidad son «una serie de funciones y acciones que reconocen y diferencian apropiadamente las identidades para apoyar la toma de decisiones»[5]. Ellas pueden consolidar, vincular o armonizar las identidades de manera precisa, detectar las características comunes de un grupo, caracterizar las identidades para evaluar los niveles de amenaza o de confianza, o desarrollar o gestionar la información de identidad. El Ciclo Operacional de Actividades de Identidad demuestra cómo varios aspectos de las actividades de identidad apoyan la toma de decisiones[6].

La Joint Publication (JP) 3-0, *Joint Operations* considera la identidad parte de las funciones operacionales de inteligencia y protección. En la discusión sobre la inteligencia, la JP 3-0 declara:

> Al identificar primero los actores relevantes y aprender tanto como sea posible sobre ellos y sus interrelaciones, el comandante de la fuerza conjunta puede desarrollar un enfoque que facilitará la toma de decisiones e influirá en la conducta (activa o pasiva) de los actores relevantes para llegar al estado final deseado de la operación. El análisis sociocultural y las actividades de inteligencia de identidad (I2) permitirán una mejor comprensión de los actores relevantes[7].

Además, las «actividades de recopilación de identidad» son una de las quince tareas de protección[8].

Básicamente, la identidad puede ser utilizada como una herramienta para apoyar la toma de decisiones. Dado que la toma de decisiones ocurre en todas las fases de

Tabla 1. Tipos de combatientes anónimos

	Área de operaciones	Motivos	Densidad	Coordinación	Importancia del anonimato
Terrorista internacional	Blanco extranjero, con viajes transfronterizos	Varios, tanto personales como generales	Puede ser hasta solo uno	Ninguna, poca	Atacar sin aviso
Insurgente	País de origen	Inspirar un movimiento antigubernamental popular	Células, tanto pequeñas como grandes	Célula a célula, tienen un líder	Preservar su fuerza
Soldado híbrido	País extranjero	Políticas del Gobierno de su país de origen	Depende de la misión, probablemente un grupo grande	Responden al Gobierno de su país de origen	Evitar atribuir responsabilidad a su Gobierno

(Tabla del autor)

conflicto y en todo el espectro de las operaciones militares, la identidad es útil en un sinnúmero de escenarios. Por ejemplo, en las misiones de cooperación de seguridad, las herramientas de identidad pueden ayudar a la nación anfitriona a mantener el Estado de derecho mediante la identificación de criminales. Esas mismas herramientas pueden ayudar a identificar insurgentes o tropas sin distintivos durante hostilidades. Y, durante operaciones de estabilidad, las actividades de identidad pueden ayudar a mitigar eficazmente el fraude y las amenazas internas.

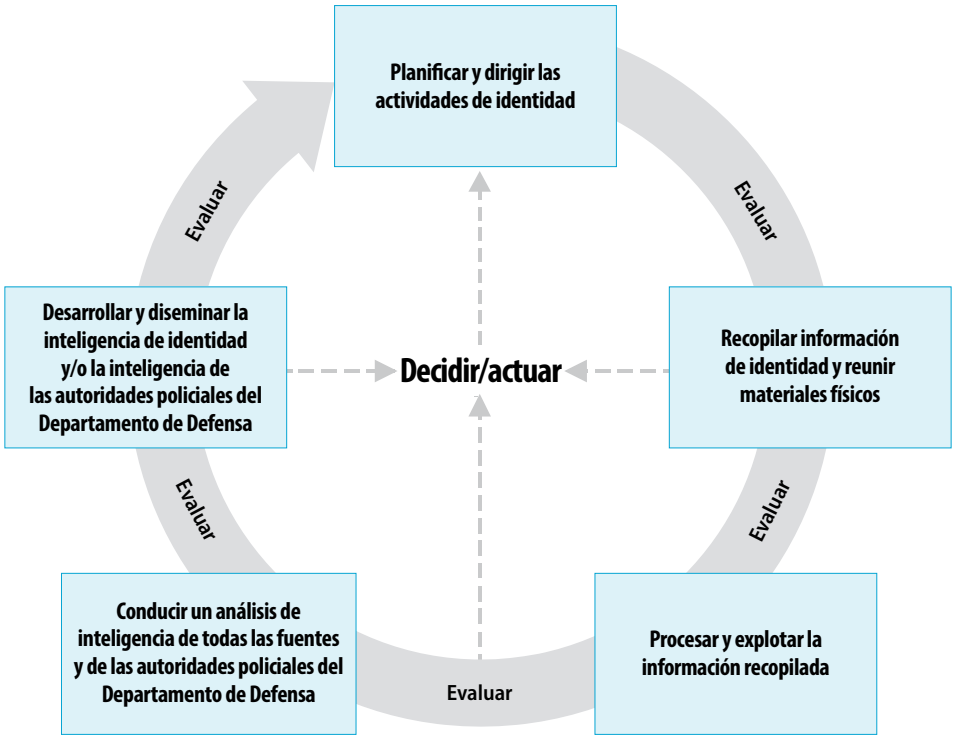
Las actividades de identidad empezaron a demostrar su valor operacional en las misiones contra artefactos explosivos improvisados (IED) en Iraq y en Afganistán a mediados de la década de 2000. La explotación forense de restos de IED y la identificación biométrica de individuos permitieron a las fuerzas de coalición «atacar la red» de fabricantes e instaladores de IED[9]. Estas actividades abarcaron gradualmente otras áreas, como por ejemplo, la identificación de sospechosos de terrorismo y terroristas conocidos entre la población para impedir su ingreso a la Policía o a las Fuerzas Armadas.

Gracias al intercambio de información entre las bases de datos biométricos del Departamento de Defensa (DoD), sus agencias y sus socios internacionales, los datos de identidad de criminales registrados desde 2004 están disponibles para las autoridades policiales y de seguridad fronteriza, incluso después de que las hostilidades cesan. Como mínimo, aquellos cuyos datos biométricos los vinculen a actividades beligerantes pueden ser sujetos a un interrogatorio extenso; en los casos más serios, la entrada a un país puede ser negada o hasta pueden ser arrestados. En cualquiera de los casos, sus historias habrían pasado desapercibidas sin los registros biométricos y el intercambio de información.

Varias aplicaciones

En la *National Military Strategy* de 2015 se enumeran las doce misiones de la fuerza conjunta, muchas de las cuales ya se llevan a cabo, y todas ellas pueden beneficiarse de cierta manera de las actividades de identidad[10]. Por ejemplo, la biometría y otras herramientas de identidad pueden ser tan útiles en la disuasión nuclear como en una campaña de contrainsurgencia. Sin embargo, la siguiente discusión se centrará en las operaciones de campo y en los individuos que los soldados pueden encontrarse. También se incluyen escenarios realistas junto con misiones definidas por la *National Military Strategy* (tabla 2).

Contrarrestar al Estado Islámico. La lucha contra el llamado Estado Islámico (EI) es un esfuerzo de dos enfoques para, primero, capturar el terreno controlado por el EI en Iraq y Siria y, segundo, contener la amenaza terrorista que representan para otros Estados distantes. La defensa del EI ante la coalición es un tipo de fuerza híbrida puesto que tiene (o tenía) que defender territorio, algo que los grupos terroristas no hacen típicamente, usando tácticas como terroristas suicidas y combatientes no uniformados. Las actividades de identidad asisten en la identificación de combatientes del EI que se esconden entre la población, como si fueran insurgentes. Pero lo más pertinente para esta discusión es el esfuerzo para



(Figura del JDN 2-16, *Identity Activities,* 3 de agosto de 2016; las actividades de identidad no son una herramienta o procedimiento individual, sino un conjunto de varias tareas y decisiones relacionadas con la identidad de los individuos)

Figura. Ciclo operacional de las actividades de identidad

contener a los miembros que huyen. A medida que el EI colapsa en Siria y en Iraq, los miembros sobrevivientes intentan regresar a sus países de origen o refugiarse en otros países. Estos individuos deben ser identificados, seguidos y capturados cuando se desplazan para impedir que cometan más atrocidades. Algunos serán clasificados como simples buscadores de experiencia extremas o soldados de a pie y no serán detenidos mientras que otros serán líderes importantes o tendrán vínculos directos a actos monstruosos, determinado a través de una investigación forense, que requerirán la detención. Las actividades de identidad son *la* capacidad crucial que permitirá lidiar con lo que quede del EI.

Afganistán. Aunque es un ejemplo antiguo con el que muchos lectores están familiarizados, las actividades de identidad en las operaciones de contrainsurgencia en curso contra el Talibán y otros grupos en Afganistán son relevantes. Como insurgencia, el Talibán está centrado en controlar territorio y socavar la autoridad gubernamental. Para desmantelar sus redes, identificar combatientes anónimos que se encuentran dispersos entre la población es clave. La identificación también es importante para prevenir las amenazas internas. Lamentablemente, estas continúan, pero probablemente serían mucho peores si no contáramos con las capacidades de identificación y evaluación proporcionadas por las actividades de identidad.

Ucrania. El público estadounidense está bastante familiarizado, y hasta podría decirse que entienden, las operaciones híbridas que Rusia ha estado llevando a cabo en Ucrania. Esto se debe en gran parte porque Rusia ha podido negar su participación en los conflictos «internos» de Ucrania. El anonimato individual sin duda juega un papel táctico, como quedó evidenciado en 2014, cuando tropas no identificadas capturaron varios edificios gubernamentales y la falta de atribución impidió que las fuerzas ucranianas expulsaran por la fuerza a los ocupantes, que probablemente eran rusos[11]. Ucrania implícitamente reconoció el impacto potencial de las amenazas híbridas anónimas —y la dificultad de identificarlas— cerrando sus fronteras a todos los varones rusos de entre dieciséis y sesenta años en medio de las altas tensiones en noviembre de 2018[12].

Pero más que eso, el anonimato permite a la nación agresora negar su culpabilidad. Invasiones abiertas invitan respuestas abiertas, las operaciones Desert Shield y Desert Storm son ejemplo de ello. Acciones encubiertas, por otro lado, permiten a los Estados conservadores atacados evitar el conflicto sin dañar su imagen. Sin embargo, la atribución *es* posible. Por ejemplo, a pesar del supuesto carácter interno del conflicto ucraniano, reportes de fuentes abiertas continuamente han identificado funerales para soldados rusos que murieron en Ucrania[13]. Si los periodistas pueden obtener esta

información con tan solo monitorear los medios sociales, entonces una capacidad de actividades de identidad respaldada por el Estado agredido tiene un gran potencial para contrarrestar la narrativa del Estado agresor[14].

Mar de China Meridional. La República Popular China está dejando su huella en el mar de China Meridional a través de varios medios militares y diplomáticos. En los últimos años, China ha emplazado armas en islas artificiales y ha declarado una zona de identificación para la defensa aérea, lo cual ha llamado mucho la atención[15]. Otra aspecto que recibe menos atención, pero no por ello deja de ser menos significativo, es el empleo de una «milicia marítima» para reclamar caladeros e islas en las zonas económicas exclusivas de otros países (algunos de estos países se disputan entre ellos mismos estas zonas, pero todos están de acuerdo en que ellas no pertenecen a China). Barcos pesqueros en apariencia, estas embarcaciones de casco azul realizan pocas actividades pesqueras, pero siempre aparecen en lugares disputados[16]. Ellos son clave en la estrategia híbrida china para dominar las aguas del sudeste asiático. Los dueños, los capitanes y las tripulaciones pueden ser identificados —a menudo usando registros públicos— y esta información puede ayudar a determinar la verdadera naturaleza de la embarcación.

Estado actual de las actividades de identidad

En la actualidad, la mayoría de las actividades de identidad se realizan en el trasfondo por organizaciones como la Agencia de Biometría y Actividades Forenses de Defensa (Defense Forensics and Biometrics Agency) y el Centro Nacional de Inteligencia Terrestre (National Ground Intelligence Center). El trabajo de estos dos organismos depende de la información recopilada por los soldados en el terreno y por las agencias y las ramas homólogas, que a su vez posibilita y mejora la toma de decisiones de ellos.

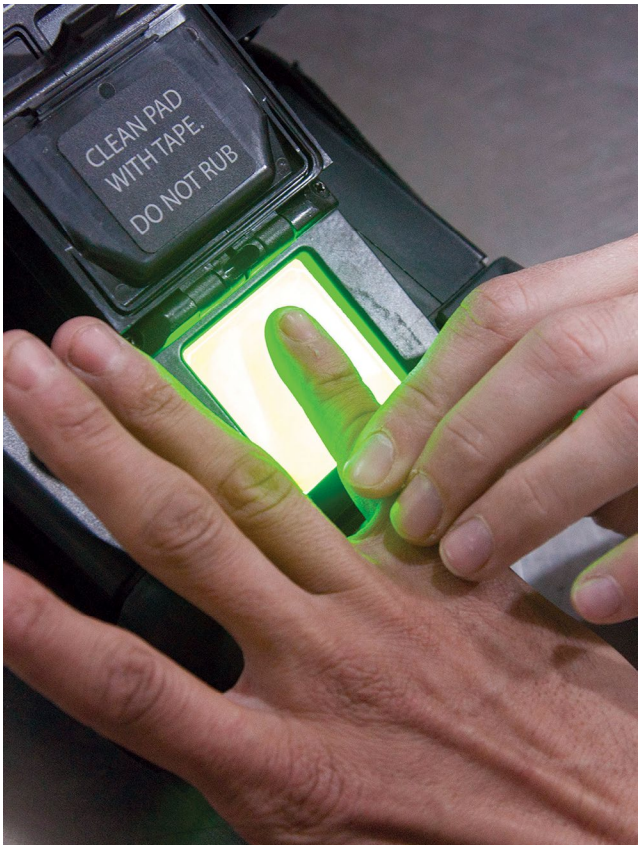
Tabla 2. La identidad en la práctica

	Misiones de Estados Unidos (*National Military Strategy*, 2015)	**Tipos de amenaza**	**Objetivo enemigo inmediato**	**Cómo la identidad frustra al enemigo**
Estado Islámico (terrorismo comprobado, casi híbrido)	• Combatir el terrorismo • Responder a las crisis y conducir operaciones de contingencia limitadas	Ataques terrestres convencionales junto con infiltraciones urbanas, terrorismo global descentralizado	Busca gobernar un territorio definido para expandirse y fomentar el terrorismo en el extranjero	Permite limitar los viajes internacionales del terrorista, atacar sus redes e identificar combatientes conocidos entre la población
Afganistán (insurgencia comprobada)	• Conducir operaciones de contrainsurgencia y de estabilidad • Cooperar en materias militares y de seguridad	Amenaza interna, campaña terrorista localizada	Gobernar un territorio limitado, debilitar al Estado	Permite atacar las redes terroristas, detectar las amenazas internas e identificar combatientes conocidos entre la población
Ucrania (caso híbrido comprobado)	• Negar los objetivos del adversario • Cooperar en materias militares y de seguridad	Combatientes extranjeros fomentan revueltas, combate convencional junto con subversión	Desestabilizar al Gobierno rival con un costo mínimo	Permite atribuir actividades beligerantes a un Gobierno extranjero e identificar extranjeros en territorio nacional
Mar de China Meridional (posible caso híbrido)	• Proporcionar una presencia estabilizadora global • Negar los objetivos del adversario	Una milicia marítima no reconocida niega el acceso libre al mar	Reivindicación territorial marítima	Permite identificar el tráfico marítimo legítimo y atribuir actividades beligerantes al Gobierno extranjero involucrado

(Tabla del autor)

A nivel de soldado, la mayoría de ellos estarán de acuerdo en que el equipo de mano biométrico (y, hasta cierto punto, el equipo de explotación forense) es la línea de vanguardia de las actividades de identidad. Por más de una década, estos dispositivos portables han permitido a los soldados capturar los datos biométricos de las caras, las huellas digitales y los iris de millones de individuos e información contextual para construir el repositorio biométrico autoritativo del DoD. Y mediante unas listas de vigilancia que se suben a los dispositivos, estos registros permiten a los soldados identificar individuos buscados en cuestión de minutos o segundos.

El entrenamiento con estos dispositivos ocurre antes del despliegue y cuando los soldados se encuentran en el teatro de operaciones. Este entrenamiento no se repite a menos que sea necesario para una misión específica. Algunos de los sistemas que son parte del entrenamiento y que se emplean actualmente en el terreno son el Biometrics Automated Toolset-Army (BAT-A), una computadora portátil con periféricos, y el Secure Electronic Enrollment Kit (SEEK II), un dispositivo de mano autónomo.



Las huellas digitales de un soldado de las fuerzas de seguridad de Iraq son escaneadas el 10 de enero de 2017 durante un proceso de selección en la base de Besmaya, Iraq. La base de Besmaya es uno de cuatro centros de la Fuerza de Tarea Conjunta Combinada-Operación Inherent Resolve en los que soldados españoles y portugueses entrenan a fuerzas de seguridad iraquíes para mejorar su alistamiento. (Foto: Sargento Joshua Wooten, Ejército de Estados Unidos)

Algunos soldados, en particular la policía militar y los ingenieros de combate del Centro de Excelencia de Apoyo a la Maniobra, reciben un entrenamiento más especializado sobre la explotación forense de sitios sensibles y el análisis de explosiones. El Ejército en la actualidad está desarrollando un equipo forense estándar. Otras ramas también aplican las investigaciones forenses en el terreno, en particular, los destacamentos de policía del Cuerpo de Infantería de Marina, los cuales han estado proporcionando una capacidad de explotación orgánica tanto por mar como por tierra desde 2014[17].

Actualmente no contamos con sistemas de campo para la inteligencia de identidad, a menos que las listas de vigilancia del SEEK II se consideren una herramienta de inteligencia de identidad. En su lugar, las tareas de apoyo a la decisión y al análisis asociadas con las actividades de identidad se realizan en el trasfondo, proporcionando repuestas al «cliente» que las solicite. Si un individuo no está en la lista de vigilancia del dispositivo, que contiene decenas de miles de identidades, se puede enviar una solicitud para buscar en toda la base de datos biométricos del DoD. El tiempo de respuesta varía dependiendo de circunstancias como la prioridad y la infraestructura de comunicaciones. Las fuerzas de operaciones especiales generalmente reciben una respuesta en minutos mientras que responder a otros puede tomar más tiempo si las vías de transmisión de datos son indirectas o si la prioridad no es urgente.

En el nivel operacional, cada uno de los comandos combatientes cuenta con un pequeño grupo dedicado a la identidad en la secciones J3 (operaciones) o J2 (inteligencia). Independientemente de la configuración que tengan, las secciones J2 y J3 coordinan estrechamente la planificación de las actividades de identidad, funcionando como una fusión de inteligencia y operaciones. Es un círculo virtuoso en el que las operaciones generan los datos que alimentan la inteligencia y la inteligencia, por su parte, ayuda a avanzar las operaciones.

Estado actual: escenarios comunes

En la configuración que se acaba de describir, las actividades de identidad han permitido al DoD y a sus socios interagenciales tener éxito por varios años. Los siguientes

escenarios comunes demuestran cómo las actividades de inteligencia pueden ser empleadas con éxito.

Contrarrestar artefactos explosivos no improvisados. El material recuperado después de una explosión o de un sitio de fabricación de bombas es trasladado a un centro de explotación forense. Los técnicos recuperan las huellas digitales del material y las comparan con los registros de la base de datos biométricos del DoD. Si el dueño de las huellas digitales es conocido, ese individuo puede ser agregado a la lista de vigilancia y detenido para interrogación si nos cruzamos con él. Si las huellas pertenecen a un individuo desconocido, entonces ese individuo será identificado si sus datos biométricos son registrados en el futuro.

Contrainsurgencia. Una computadora recuperada de un puesto de mando ilícito es sometida a un análisis forense. Sus componentes físicos contienen las huellas digitales de sus dueños y la explotación de los datos revela fotos de los miembros de la célula. Este descubrimiento permitirá la identificación biométrica de estos individuos si intentan obtener acceso a instalaciones de la coalición o si tropas de la coalición se cruzan con ellos.

Prevención del fraude. Un comandante de la nación anfitriona intenta recolectar el pago de varios soldados «fantasmas» que presuntamente pertenecen a su unidad. Sin embargo, un registro biométrico es necesario antes de efectuar un pago a cualquier individuo. La falta de datos biométricos únicos de soldados inexistentes permite al personal a cargo de los pagos darse cuenta del intento de fraude, prevenir pagos equivocados e implicar al comandante deshonesto.

Mitigar amenazas internas. Un individuo solicita empleo como peón en una base de operaciones avanzada. Sin embargo, sus datos biométricos coinciden con registros de la base de datos que lo vinculan a un grupo radical. Este vínculo lo convierte en una amenaza de contrainteligencia y el acceso a la base es negado.

Protección de fronteras. Las huellas digitales descubiertas en un IED son subidas a la base de datos biométricos del DoD, pero no coinciden con una identidad. Años después, un individuo desconocido intenta entrar a Estados Unidos por la frontera sur. Cuando sus datos biométricos son procesados y coinciden con el antiguo registro del IED, el individuo es detenido e interrogado, en vez de permitirle entrar al país.

Apoyo a las autoridades policiales. Un guardacostas aliado registra los datos biométricos de un individuo arrestado por traficar drogas. Gracias al intercambio de datos biométricos a nivel internacional, sus datos coinciden con registros estadounidenses que indican un vínculo con grupos terroristas y criminales, lo cual ayudará a las autoridades policiales de la nación anfitriona a construir un caso contra él.

Viñeta

La «coincidencia» biométrica más grande, medida por número de incidentes relacionados entre sí, es un caso de 2011 en Iraq. Fuerzas de operaciones especiales se cruzaron con un individuo el 21 de julio de 2011 y sus huellas digitales llamaron la atención de los examinadores inmediatamente cuando recibieron las imágenes. Las huellas coincidían con 121 huellas latentes de incidentes separados que habían sido identificadas en los 14 meses anteriores para un récord de 35 casos de IED. Las fuerzas estadounidenses detuvieron al individuo y pudieron neutralizar su influencia en el combate gracias a algoritmos, examinadores biométricos profesionales y enlaces de datos globales rápidos[18].

Estado futuro: aspiraciones

Las actividades de identidad han demostrado su importancia en repetidas ocasiones. Mejoras continuas en la tecnología y en los procesos harán que los soldados del futuro las aprovechen incluso mucho más. Sin embargo, cualquiera que sea la forma en la que las actividades de identidad se lleven a cabo en el futuro, el DoD debe garantizar que las siguientes condiciones se cumplan:

Entrenamiento. Los soldados del futuro necesitarán ser entrenados y equipados adecuadamente para poder conducir actividades de identidad en una amplia variedad de escenarios. En vez de pensar que esto requiere un campo de carrera específico, es mejor considerar las actividades de identidad como un fusil, una herramienta que la infantería es quien más la utiliza, pero una con la que todos deben estar familiarizados.

Esta es la razón por la que crear una especialidad ocupacional militar (MOS) para actividades de identidad, investigaciones forenses y biometría podría convertirse, si bien esa no la intención, en un esfuerzo contraproducente. Una MOS tendría que caer en un campo de carrera como la infantería, la inteligencia militar, la policía militar, el cuerpo de señales o algo totalmente diferente y si los practicantes se estancan en una sola comunidad, exponer a otros a estas habilidades podría ser una tarea difícil. Esto

podría generar esfuerzos duplicados, si las comunidades consideran que necesitan desarrollar las mismas capacidades entre sus propios soldados, o falta de interés, si las mismas comunidades ignoran el potencial de las actividades de identidad porque es muy difícil acceder a él.

Una mejor alternativa para el entrenamiento sería crear un curso abierto para todos los soldados con el objetivo de difundir las actividades de identidad en todo el Ejército. Una sola escuela sería responsable del curso (p. ej. la Escuela de Policía Militar del Ejército), pero esto no significa que esa comunidad sería la única responsable de aprender estas habilidades necesarias. Los graduados podrían obtener un certificado una vez que concluyan el curso sin necesidad de cambiarse a una nueva MOS. Este curso básico podría ser complementado con cursos de actualización, en línea o en otro formato, para aprovechar los últimos cambios curriculares validados por autoridades relevantes del Comando de Entrenamiento y Doctrina (TRADOC), como el Gestor de Capacidades Terrestres y de Identidad del TRADOC (TCM-TI). Este curso tiene que ser una prioridad para las unidades que están a punto de cumplir una misión.

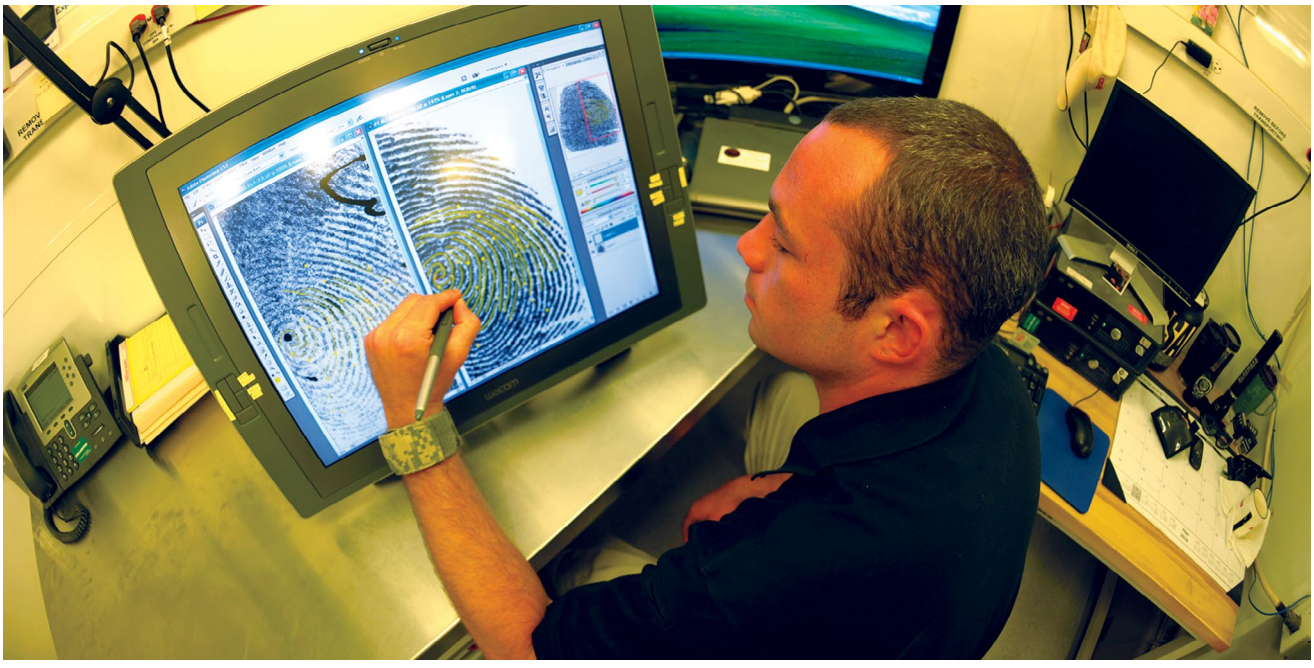
Equipo y redes. Los soldados en el terreno deberían contar con el mejor equipo disponible para facilitar la obtención de datos biométricos, la búsqueda de coincidencias y la toma de decisiones. Pero antes que nada, es necesario contar con una simple herramienta electrónica de mano para poder registrar los datos biométricos de huellas digitales, caras e iris en el terreno. Con un equipo de explotación forense adicional, que quepa en el bolsillo de un pantalón, también se podrían procesar las huellas digitales latentes. Segundo, un dispositivo que capture de forma pasiva la información de las caras o los iris, tal vez una cámara incorporada a las gafas de protección del soldado, debería ser capaz de identificar los individuos dentro de su campo de visión y alertar a los soldados sobre potenciales personas de interés.

Estos dispositivos móviles se comunicarían con la base de datos autoritativa del DoD mediante herramientas y redes de transmisión de datos comunes como los radios tácticos y la red WIN-T del Ejército. Esto permitiría una búsqueda de coincidencias en tiempo real en bases de datos interagenciales, en vez de simplemente limitar la búsqueda a las listas que vienen en los dispositivos. Comunicaciones estables usando todos los nodos disponibles también es clave. Los cuellos de botella en los flujos de trabajo de identificación se deben menos a la capacidad de la base de datos que a la capacidad de las vías de comunicación.

Con respecto a la estrategia de adquisición de este equipo, es importante resaltar dos tendencias contradictorias: primero, los dispositivos móviles se están tornando obsoletos a un ritmo cada vez más rápido debido a los avances constantes de las capacidades y los estándares de la industria, y, segundo, la comunidad de defensa a nivel mundial compra grandes cantidades de equipos interoperables y duraderos para poder comunicarse con las redes de datos globales a largo plazo[19]. El Gobierno estadounidense debe dar por hecho que ya *no* es líder en la tecnología de la información y cualquier compra que haga será obsoleta, conforme los estándares industriales, antes de que se emplee en el terreno. Por lo tanto, el Gobierno debe prepararse para sostener un sistema único con apoyo industrial mínimo, tal vez en asociación con otros aliados. Por otro lado, también se puede establecer una arquitectura abierta en la cual varios dispositivos, servidores y aplicaciones adquiridas mediante procesos descentralizados son utilizables siempre que sean compatibles con los estándares de cualquier plataforma.

Integración de la planificación de estado mayor. Las actividades de identidad pueden ofrecer beneficios considerables si se integran en la planificación operacional, pero los estados mayores primero deben entender cómo y por qué. Esto puede empezar con entrenamientos en los escalones superiores sobre cómo la recopilación puede ayudar en el análisis. Cuando las actividades de identidad son incorporadas en la intención del comandante, los escalones inferiores deberían contar con los medios para incorporarlas en sus operaciones, y lo ideal sería que formaran parte de un procedimiento operativo estandarizado. No hay personal dedicado específicamente a las actividades de identidad a nivel de estado mayor y esto queda evidenciado por las secciones J2 y J3, las cuales asumen la responsabilidad de estas actividades dependiendo de lo que prefiera el comandante o el estado mayor. En un esquema nuevo, sería razonable responsabilizar a la J3 de la recopilación, a la J6 (comando, control, comunicaciones, computadoras, ciber) de la transmisión de datos y a la J2 del análisis y los reportes y contar con un solo asistente de estado mayor (un oficial de operaciones de identidad, o alguien con un título similar) para coordinar todas estas acciones.

Tal institucionalización también requeriría la revisión gradual de numerosas publicaciones conjuntas y del



Richard A. Swearengin, un examinador de huellas digitales latentes asignado a la División de Investigaciones Criminales del Ejército, compara una huella digital latente (izquierda) con una de una base de datos (derecha) el 4 de mayo de 2010 en la base aérea de Kandahar, Afganistán. (Foto: Sargento técnico Michele A. Desrochers, Fuerza Aérea de Estados Unidos)

Ejército como aquellas que rigen las órdenes de operación. Especificar un párrafo o un anexo en un formato de orden de operaciones estándar para las actividades de identidad (mediante el Field Manual 6-0, *Commander and Staff Organization and Operations* y otras referencias) sería de gran ayuda para incentivar a los soldados a considerar el papel de la identidad en las operaciones en curso[20].

Estado futuro: inteligencia artificial

Puesto que las actividades de identidad son esencialmente un proceso cognitivo, la inteligencia artificial (IA) y el aprendizaje automático desempeñarán un papel importante en cómo estas se llevan a cabo en el futuro. Durante las fases de recopilación, procesamiento y análisis de la información de identidad será necesario separar los datos relevantes de los que no lo son y buscar patrones y tendencias de los que sean útiles. La IA y el aprendizaje automático aumentarán la velocidad y la precisión de estos procesos, y en algunos casos ya lo están haciendo. La IA tiene un gran potencial para ayudar a obtener datos biométricos en condiciones difíciles, identificar coincidencias con datos incompletos, contextualizar identidades mediante el análisis de datos y neutralizar los intentos de los adversarios para evadir o confundir el sistema.

En el momento de recopilar, la IA puede ayudar a crear archivos utilizables incluso con datos subóptimos. Las operaciones militares a menudo tienen lugar en ambientes «incontrolables», lo que significa que la iluminación es errática, las cámaras se tambalean, el ruido de fondo es ensordecedor y las condiciones prevalentes no permiten capturar datos de calidad, ya sean imágenes faciales, escaneos de iris, grabaciones de voz o huellas digitales latentes. Los humanos pueden identificar individuos conocidos en estas circunstancias, pero los sistemas biométricos antiguos tal vez no. La IA puede aliviar esto, incluso al punto de identificar caras con máscaras, gafas y otras «oclusiones»[21]. Ya se han realizado pruebas de laboratorio en el que los algoritmos son capaces de identificar correctamente caras cubiertas con bufandas y sombreros hasta un 77 % de las veces[22]. Esta tecnología podría aplicarse a imágenes con, por ejemplo, iluminación o ángulos malos.

Esto significa que programas inteligentes, en vez de dispositivos de registro, serían los encargados de crear los archivos utilizables. En la actualidad, por ejemplo, las imágenes faciales a larga distancia se obtienen mediante sistemas de cámaras avanzados con ópticas sensibles. Sin embargo, con la IA, bastaría con simplemente emplear cámaras baratas y mejorar la calidad de las imágenes usando la IA para crear archivos utilizables. En cualquiera de los casos, el usuario obtendría el mismo resultado, pero

Un entrenador español fotografía un soldado de las fuerzas de seguridad de Iraq el 10 de enero de 2017 antes de que este comience el entrenamiento en la base de Besmaya, Iraq. El proceso de selección es parte de la fase inicial para todo el personal de las fuerzas de seguridad de Iraq que se inscribe en cursos de entrenamiento. (Foto: Sargento Joshua Wooten, Ejército de Estados Unidos)

la segunda solución puede ser mucho más simple de implementar en un ambiente operacional.

Cuando se registran los datos biométricos, la IA puede aumentar la velocidad y la precisión de la búsqueda de coincidencias con registros anteriores para establecer una identidad. Tanto los registros nuevos como los antiguos pueden contener datos parciales u otras características subóptimas (como caras cubiertas con bufandas). En tales circunstancias, los examinadores humanos analizan las imágenes para determinar si hay una coincidencia cuando los algoritmos no son capaces de llegar a una conclusión, que generalmente es un porcentaje muy bajo de los casos, pero esto, sin embargo, consume bastante tiempo y esfuerzos adicionales. Una IA «entrenada» de manera apropiada mejorará la precisión, la fiabilidad y la eficiencia de los algoritmos y reducirá la intervención de los humanos. Los algoritmos entrenados mediante el aprendizaje automático y datos complejos, diversos y extensos serán herramientas poderosas.

Además de identificar coincidencias y construir galerías de perfiles, la IA desempeñará un papel relevante para entender de forma integral las identidades individuales. Según la JDN 2-16, la información de identidad es como una corriente de datos, como por ejemplo, biométricos, biográficos y de reputación[23]. Idealmente, la corriente va a parar a un «lago» de datos. La IA proporcionará los medios para identificar información útil en este lago, en la forma de patrones, tendencias y asociaciones que los analistas humanos y las tecnologías antiguas tal vez nunca hubieran sido capaces de identificar por sí solos. Más allá de los registros financieros o los identificadores biométricos, aquí es donde verdaderamente la «identidad» será encontrada.

En todas las etapas de las actividades de identidad, la IA tendrá que lidiar con otra amenaza omnipresente: otra IA. Imágenes alteradas, incluso videos, son cada vez más prevalentes y convincentes[24]. Un ejemplo notorio, si bien inofensivo, es el bigote de Henry Cavill en la película *Liga de la Justicia*, el cual los productores decidieron eliminar de manera digital, pero con resultados decepcionantes. En respuesta a este incidente, un usuario de Internet con un presupuesto cero usó un algoritmo «deepfake» e hizo un mejor trabajo que el estudio[25]. Como la difusión de la tecnología está permitiendo crear falsificaciones en el dominio biométrico y en otros, es posible que dentro de poco, la IA sea la única herramienta capaz de diferenciar entre lo original y lo falso, y en nuestro caso, las identidades verdaderas de las falsas. Las actividades de identidad continuarán siendo una capacidad vital, pero también encontrarán desafíos en el ambiente operacional.

Conclusión

Nacidas en el combate y madurando como capacidad operacional y como parte de la iniciativa empresarial del DoD, las actividades de identidad son un habilitador robusto para las operaciones militares y las funciones internas. Ellas reducen el fraude y aumentan la responsabilidad, tanto en los asuntos civiles como en las tareas diarias. Pero más importante aún para los soldados en el terreno, las actividades de identidad permiten distinguir mejor a amigos de enemigos en cualquier circunstancia. La tecnología y los procedimientos solo mejorarán en los próximos años y tanto el Ejército como el DoD deben estar preparados para aprovecharlos y negar al enemigo el anonimato. ■

Notas

1. Joint Doctrine Note (JDN) 2-16, *Identity Activities* (Washington, DC: U.S. Government Publishing Office [GPO], 3 de agosto de 2016), vii.

2. Training Circular (TC) 7-100, *Hybrid Threat* (Washington, DC: U.S. Government Printing Office, noviembre 2010), 2-4.

3. Ibíd.

4. Ibíd.

5. JDN 2-16, *Identity Activities*, vii.

6. Ibíd., I-15.

7. Joint Publication 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 de enero de 2017), III-24.

8. Ibíd., III-36.

9. David F. Eisler, «Counter-IED Strategy in Modern War», *Military Review* 92, nro. 1 (enero-febrero 2012): 13, accedido 19 de marzo de 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, junio 2015), 10-13, accedido 19 de marzo de 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», (informe, West Point, Nueva York: Modern War Institute, 18 de octubre de 2016), 15, accedido 19 de marzo de 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 de noviembre de 2018, accedido 6 de diciembre de 2018, https://www.pbs.org/newshour/show/news-wrap-ukraine-closes-border-to-russian-men.

13. James Miller, Pierre Vaux, Catherine A. Fitzpatrick y Michael Weiss, «An Invasion by Any Other Name: The Kremlin's Dirty War in Ukraine», *The Interpreter* (informe, Nueva York: Institute of Modern Russia, 2015), 49, accedido 7 de julio de 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 de septiembre de 2015, accedido 19 de marzo de 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 de abril de 2014, accedido 19 de marzo de 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 de julio de 2017, accedido 19 de marzo de 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 de mayo de 2017, 56, accedido 19 de marzo de 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 de diciembre de 2014, accedido 19 marzo de 2018, https://www.dvidshub.net/news/151673/spmagtf-mps-exploit-vital-material/.

18. Biometrics Identity Management Agency [ahora conocida como Defense Forensic and Biometrics Agency], *Annual Report FY11*, «The Super Hit», 25.

19. Sean Lyngaas, «Can the Pentagon Keep Pace on Biometrics?», *FCW* (sitio web), 11 de marzo de 2015, accedido 2 de abril de 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, mayo 2014).

21. Amarjot Singh y otros, «Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network», (presentación, IEEE International Conference on Computer Vision Workshop (ICCVW), Venecia, Italia, 22–29 de octubre de 2017), accedido 10 de abril de 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* (sitio web), 7 de septiembre de 2017, accedido 16 de marzo de 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*, 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* (sitio web), 19 de febrero de 2018, accedido 16 de marzo de 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 de febrero de 2018, accedido 16 de marzo de 2018, https://www.theverge.com/tldr/2018/2/7/16985570/superman-mustache-ai-deepfakes-henry-cavill.