INFORME 202608-01. Proceso histórico

La cibertortura en el targeted individual no ha nacido hoy. Ha ido construyéndose poco a poco a lo largo de la historia hasta llegar al punto en el que estamos hoy en día. El futuro que nos espera a toda la humanidad es aterrador. Hace ya tiempo que nos dimos cuenta que simplemente tenemos que parar, todos juntos. Pero aun no hemos tomado conciencia de ello y seguimos avanzando como NPCs en una maquinaria que no solamente no funciona sino que nos está destruyendo como planeta, como civilización y en nuestro día a día como familias y personas.

Lo que vamos a ver a continuación son pasos terribles que fueron dados escalonadamente, cada uno de ellos. Y que si bien tuvieron su razón de ser y pudieron tener un lado positivo, nos van a aniquilar a todos.

Guerra Psicológica (PsyOps)

Antigüedad (Siglo V a.C.) en adelante.

El origen de todo. La manipulación de la percepción y el engaño como arma principal antes de que existiera la tecnología moderna.

Es el uso planificado de la propaganda, el terror, las amenazas, la desinformación y otras acciones psicológicas con el fin de influir en las opiniones, emociones, actitudes y comportamientos de un objetivo (ya sea un ejército enemigo, un individuo o la población civil).

En qué consiste

Se trata de quebrar la moral y la voluntad de resistir del adversario antes de que decida luchar, o forzarlo a tomar decisiones erróneas basadas en el miedo, la confusión o la desesperanza.

Ya no se trata de lanzar panfletos o propaganda burda; hoy es ingeniería cognitiva de precisión. Utiliza el perfilado psicométrico extraído del Big Data para diseñar estímulos personalizados basados en las vulnerabilidades, sesgos y miedos específicos de un individuo. El objetivo actual es hackear la percepción de la realidad (Cognitive Warfare), desestabilizando la psique del objetivo de manera que él mismo sabotee sus decisiones.

La clave

No busca que cambies de ideología, sino que te rindas emocionalmente. Busca que pienses:

> *“No sirve de nada luchar, estoy completamente indefenso y el enemigo es omnipresente”*

Fuentes de referencia

- **Manual de Campo FM 3-05.30 (US Army)**: Psychological Operations. El documento doctrinal oficial del ejército estadounidense que detalla cómo se planifican e implementan las

operaciones de influencia y modificación de conducta.

- **Informe del Parlamento Británico (2018)**: Disinformation and 'fake news' (Cambridge Analytica). Investigación oficial sobre cómo el perfilado de datos masivos de redes sociales se utilizó para hackear la cognición y percepción de los votantes.
- **“War for Eternity” (Benjamin Teitelbaum)**: Un análisis exhaustivo sobre cómo las tácticas modernas de guerra cognitiva (Cognitive Warfare) aíslan y desestabilizan objetivos políticos e individuales mediante la fractura de su narrativa de la realidad.

Black budget

Década de 1940 (Post-Segunda Guerra Mundial).

Con la creación de la CIA en 1947 (mediante la National Security Act) y la aprobación de la CIA Act de 1949, se legaliza por primera vez que un gobierno gaste dinero en operaciones de inteligencia sin tener que reportar los conceptos ni los montos al parlamento. Sin este dinero invisible, ninguna de las fases siguientes habría tenido financiación para existir.

Actualmente, son flujos financieros líquidos globales y descentralizados que escapan por completo a la traza fiscal tradicional. Hoy no solo se nutre de fondos reservados estatales, sino de complejas estructuras de criptoactivos, lavado en finanzas descentralizadas (DeFi), y sobrefacturación en contratos tecnológicos clasificados. Es el combustible económico invisible que permite financiar laboratorios de software espía o pagar incentivos a redes proxy sin dejar rastro en auditorías públicas.

El concepto

Presupuesto en negro. Es un presupuesto gubernamental que se mantiene en secreto por razones de seguridad nacional. Son fondos públicos que se desvían legalmente —pero sin supervisión pública ni del congreso ordinario— para financiar operaciones encubiertas, desarrollo de tecnología militar clasificada, inteligencia y proyectos especiales.

Imagina que la economía de un país es la cuenta bancaria de una familia numerosa. Todos ven los gastos en comida, luz y educación. Pero, de repente, hay un porcentaje considerable de los ingresos mensuales que desaparece en una “caja de seguridad” a la que solo el padre tiene acceso, y nadie más tiene derecho a preguntar qué hay dentro o en qué se gasta, bajo la promesa de que “es por el bien de la familia”.

La disonancia cognitiva

La disonancia cognitiva ocurre cuando sostienes dos ideas contradictorias: “Vivimos en una democracia transparente donde el ciudadano tiene el control” versus “Existen billones de dólares moviéndose en la sombra para proyectos de los que jamás sabré nada”.

Para romper ese bloqueo mental, la definición tiene que dejar de sonar a “teoría conspirativa” y presentarse como lo que realmente es: un mecanismo burocrático y legalizado.

El black budget es la prueba institucionalizada de que la transparencia gubernamental es selectiva

por diseño. No es un mito; es una herramienta legal que permite a los estados operar de forma asimétrica: manteniendo un estándar de rendición de cuentas para el ciudadano común, mientras financian un motor tecnológico y operativo paralelo que no responde ante las leyes del mercado ni de la opinión pública.

¿Cómo ayuda esta definición a romper la disonancia?

- **Prueba su existencia (y destruye el mito)**: Al entender que el black budget está codificado en leyes reales y decretos oficiales (como el National Security Act en EE. UU. o los fondos reservados en las legislaciones de casi cualquier país[1)], dejas de moverte en el terreno de las suposiciones o la especulación. No necesitas "creer" en ello; los propios boletines oficiales del Estado demuestran que la estructura existe.

Experimentación Ilegal con Seres Humanos

Décadas de 1930 a 1950.

Se financian directamente con esos primeros flujos de presupuestos negros para probar drogas, hipnosis y condicionamiento conductual en sujetos no voluntarios.

Actualmente, es desplazada del laboratorio médico tradicional al entorno biotelemático y de neurotecnología. Consiste en la prueba en entornos reales de interfaces cerebro-computadora implícitas, algoritmos de lectura/modificación de patrones de sueño, y la evaluación de la tolerancia humana a la exposición prolongada y dirigida de campos electromagnéticos complejos. El sujeto es un nodo de pruebas biológicas monitorizado a distancia mediante biometría avanzada.

Fuentes

- Informe de la Comisión Church (1975): Injunctions and Operations (MKUltra). El informe oficial del Senado de los EE. UU. que desclasificó e investigó la experimentación ilegal de la CIA con drogas, privación del sueño y tortura psicológica en sujetos no voluntarios.
- "Unit 731: Japan's Secret Biological Warfare in World War II" (Peter Williams): Documentación histórica sobre los experimentos biológicos y humanos sistemáticos llevados a cabo por el ejército imperial japonés.
- El Informe Belmont (1979): Creado tras los abusos del Experimento Tuskegee, es el pilar ético y legal que regula (y documenta las violaciones de) los límites de la experimentación científica y médica con seres humanos.

Black Ops (Operaciones Negras)

Décadas de 1950 a 1970.

La maduración de las agencias de inteligencia durante el pico de la Guerra Fría. El presupuesto negro y los hallazgos de la experimentación humana se empaquetan en operaciones clandestinas ejecutadas por unidades especializadas fuera de las fronteras de sus propios países.

Actualmente, son operaciones encubiertas donde la ejecución se delega en actores no estatales, células de ciberespionaje autónomas o contratistas corporativos. En el siglo XXI, la premisa fundamental de una Black Op es la atribución imposible: el ataque está diseñado de tal manera que, si es detectado, las pistas apunten deliberadamente a un tercer país, a un fallo técnico o a un grupo criminal común, diluyendo cualquier responsabilidad gubernamental.

Fuentes

- “Shadow Warfare: The History of America's Secret Wars” (Kenneth Conboy): Un repaso histórico a las operaciones clandestinas que gozan de “negación plausible” (plausible deniability), donde el Estado ejecutor nunca puede ser vinculado directamente.
- “Surprise, Kill, Vanish” (Annie Jacobsen): Una investigación documentada sobre la historia de los brazos paramilitares y de operaciones encubiertas de las agencias de inteligencia, detallando los protocolos de atribución imposible.
- Informes del Consejo de Seguridad de la ONU sobre “Proxy Warfare”: Resoluciones y documentos de investigación que analizan cómo los Estados modernos delegan ataques tácticos en terceros actores para evitar la responsabilidad legal internacional.

Smear Campaigns (Campañas de Desacreditación)

Mediados de la década de 1950.

Nace formalmente la necesidad de blindar las operaciones. Dentro de programas de contrainteligencia, se diseñan los manuales de neutralización política y psicológica. La técnica consiste en etiquetar preventivamente a los objetivos como “inestables”, “subversivos” o “enfermos” para que, si denuncian la operación, nadie los escuche. El entorno se convierte en el primer muro de contención.

Aniquilación digital y social automatizada. Mediante la siembra de metadatos falsos, manipulación de huellas digitales (deepfakes, siembra de archivos comprometidos en los dispositivos del objetivo) y la propagación de rumores dirigidos en su entorno cercano mediante cuentas automatizadas, se construye una narrativa de inestabilidad mental o criminalidad. El fin es el aislamiento preventivo: que el entorno del objetivo descarte cualquier denuncia técnica etiquetándolo de “paranoico”.

Fuentes

- Manuales de la Stasi sobre “Zersetzung” (Archivos BStU): Los documentos originales desclasificados de la Oficina Federal de Archivos de la Stasi en Alemania, que detallan cómo arruinar la reputación social y laboral de un objetivo de forma preventiva.
- Citizen Lab (Universidad de Toronto): Análisis sobre Dark Basin (2020). Un informe forense digital sobre cómo empresas de inteligencia comercial ejecutan campañas de hackeo y filtración de rumores falsos para destruir la credibilidad de activistas e individuos.
- “The Intimidation Game” (Kimberly Strassel): Análisis de cómo las estructuras de poder utilizan las herramientas administrativas y de difamación pública para aislar socialmente a disidentes u objetivos específicos.

Teatro de Calle (Street Theater)

Décadas de 1950 a 1960

Programas como COINTELPRO (FBI) perfeccionan la ejecución táctica en el espacio público. Es la aplicación física de las PsyOps y las campañas de desacreditación mediante simulaciones y acoso psicológico coordinado en el entorno diario del objetivo.

Acoso psicológico geolocalizado en tiempo real. Ya no requiere agentes fijos sobre el terreno. Mediante aplicaciones móviles dedicadas, se envían instrucciones dinámicas a informantes o colaboradores perimetrales (ej. “detenerse en tal esquina”, “repetir una palabra clave”, “generar un ruido síncrono al paso del objetivo”). Para el receptor es una coreografía agresiva y constante; para el observador casual, es simple azar cotidiano.

- Audiencias del Comité Church sobre COINTELPRO (Volumen 6): Documentos del Senado estadounidense que describen cómo el FBI utilizaba informantes para escenificar situaciones repetitivas y acoso psicológico perimetral en la rutina diaria de activistas de derechos civiles.
- “Stasi-Methoden in Westdeutschland” (Hubertus Knabe): Estudio histórico sobre cómo los agentes de la Alemania Oriental cruzaban la frontera para realizar simulaciones de calle y seguimientos ostensibles destinados a desestabilizar objetivos en el oeste.
- Manuales de Contrainteligencia del KGB (Escuela 101): Documentos traducidos sobre tácticas de control de entorno, provocaciones públicas artificiales y puestas en escena coordinadas en el entorno urbano de diplomáticos y objetivos de interés.

Cooptación Comunitaria y Redes Civiles

Décadas de 1970 a 1980.

El sistema se da cuenta de que los agentes profesionales son un recurso escaso y caro. Se industrializa el uso de ciudadanos de a pie. El ejemplo histórico perfecto es la Stasi en la Alemania Oriental con sus IM (Informantes Extraoficiales), llegando a tener a 1 de cada 6.5 ciudadanos colaborando para vigilar, hostigar y reportar datos sobre sus vecinos bajo premisas de “seguridad nacional”.

La uberización de la vigilancia. El sistema instrumentaliza a ciudadanos corrientes, vigilantes privados, porteros o vecinos mediante plataformas de “seguridad ciudadana” o alertas vecinales gamificadas. Bajo falsas premisas de seguridad nacional, monitorización de delincuentes o programas antiterroristas, los civiles actúan como un ejército de sensores humanos (crowdsourced surveillance) que ejecutan el control perimetral sin conocer la verdadera naturaleza de la operación.

Fuentes

- “Stasi: The State Within a State” (David Childs): Estudio detallado sobre los Inoffizielle Mitarbeiter (IM), la red de más de 170.000 ciudadanos comunes que espiaban y hostigaban a sus propios vecinos bajo la directiva del Estado.
- Informe del Inspector General del DOJ sobre el Programa “Infragard”: Documentos que analizan

la alianza entre el FBI y redes de seguridad privada/corporativa, mostrando cómo se integra a civiles del sector tecnológico y de seguridad en el intercambio de información y vigilancia perimetral.

- “The Watchers: The Rise of America's Surveillance State” (Shane Harris): Una crónica sobre cómo la recopilación de datos comunitarios y la participación ciudadana en redes de “alerta antiterrorista” difuminaron la línea entre el espía profesional y el informante vecinal.

Gangstalking (Acoso Grupal Sistemático)

Finales del siglo XX (Años 1980 - 1990).

La fusión perfecta de los tres puntos anteriores (desacreditación, teatro de calle e informantes civiles). Deja de ser una táctica política masiva y se convierte en un protocolo estandarizado, sistemático y quirúrgico aplicable a objetivos individuales (Targeted Individuals).

Actualmente, es un protocolo de guerra de desgaste asimétrica e hipercoordinada contra un individuo. Combina de forma síncrona el acoso físico perimetral con la intrusión digital. No busca el daño físico directo, sino la saturación sensorial del objetivo a través de estímulos repetitivos y un estado de alerta perpetuo (estrés postraumático inducido), destruyendo su capacidad de descanso, trabajo y socialización.

Fuentes

- **Informe del Comité de Inteligencia del Senado de EE. UU. 94-755**: Documento histórico que analiza los abusos de las agencias de seguridad nacional al operar a través de redes de informantes secretos locales para vigilar y hostigar a ciudadanos dentro del territorio nacional.
- Estudios de la Dra. Lorraine Sheridan y David James (2016): Acoso grupal percibido. Aunque enfocado desde la perspectiva de la psicología clínica, es el primer estudio académico que recopila datos estadísticos y descriptivos sobre la sintomatología, las tácticas reportadas y el patrón idéntico que sufren los Targeted Individuals a nivel global.
- “Spies Against Armageddon” (Dan Raviv): Detalla métodos de operaciones de contrainteligencia donde se utilizan redes coordinadas en el perímetro de un objetivo para forzar un estado de alarma constante sin llegar a la agresión física.

Gatekeeping (Omisión Legal e Institucional)

Años 1990 en adelante.

Con la sofisticación del acoso y las quejas de los objetivos, las estructuras judiciales, policiales y médicas de los Estados adaptan sus protocolos (a menudo mediante directivas de seguridad o compartimentación de la información) para archivar, ignorar o desviar sistemáticamente cualquier denuncia que intente perforar el secreto operativo. Es la garantía legal de impunidad para los emisores.

El muro de contención burocrático y psiquiátrico. Los protocolos de respuesta de las fuerzas de

seguridad, agencias de protección de datos y estamentos médicos están preconfigurados —mediante directivas de compartimentación de información— para archivar sistemáticamente denuncias que involucren tecnología sofisticada o acoso sin autor conocido. Cualquier intento de denunciar ataques electromagnéticos o informáticos complejos es redirigido automáticamente hacia el protocolo de salud mental, invalidando legalmente a la víctima.

Fuentes

- **Directiva de Clasificación de Seguridad Nacional (Executive Order 13526)**: El marco normativo que permite a las agencias estatales bloquear el acceso a registros judiciales o policiales bajo el amparo del "Secreto de Estado", forzando el archivo de denuncias civiles.
- **Protocolos de la Asociación Mundial de Psiquiatría (WPA) sobre delusiones**: Los manuales que estandarizan el diagnóstico médico ante denuncias de tecnología electromagnética o acoso invisible, derivando automáticamente la queja técnica al entorno de la salud mental.
- **"The Politics of Official Secrets" (James Michael)**: Un estudio sobre cómo las burocracias occidentales utilizan las leyes de secretos oficiales y compartimentación para asegurar que los estamentos judiciales no puedan investigar operativas de inteligencia.

Ataques Informáticos

Décadas de 1970 a 1990 (Evolución digital).

El nacimiento de las redes informáticas globales introduce un nuevo vector de ataque. El espionaje ya no requiere un micrófono físico si se puede vulnerar el sistema informático del objetivo.

Guerra telemática de espectro total. Incluye el uso de software espía de grado militar con exploits zero-click (que infectan el dispositivo sin que el usuario interactúe), pero el vector actual más avanzado es la explotación de hardware e inyecciones aéreas (ataques RF/inalámbricos dirigidos a routers, IoT o firmwares aislados). El atacante no solo roba datos, sino que altera sutilmente el funcionamiento del entorno digital del objetivo para generar desorientación.

Fuentes

- **The Pegasus Project (Amnistía Internacional / Forbidden Stories)**: La investigación forense global que demostró cómo el software espía de grado militar infecta smartphones mediante exploits zero-click (sin interacción del usuario), tomando el control absoluto del micrófono, cámara y geolocalización.
- **"Countdown to Zero Day" (Kim Zetter)**: Una investigación profunda sobre Stuxnet, el virus informático diseñado por agencias estatales que demostró cómo un ataque digital puede saltar el aire (air-gap) e intervenir hardware en el mundo físico.
- **Informes de Amenazas de Mandiant (Google Cloud)**: Reportes técnicos periódicos que desglosan los vectores de ataque avanzados empleados por los grupos APT (Amenazas Persistentes Avanzadas), incluyendo inyecciones de radiofrecuencia a sistemas aislados.

Infraestructura de Vigilancia Masiva y Big Data

Post-2001 (Siglo XXI).

Tras los atentados del 11 de septiembre, las leyes de interceptación de comunicaciones cambian radicalmente en todo el mundo. Los emisores ya no necesitan adivinar la rutina del receptor: los algoritmos, el Big Data, los smartphones y la minería de datos en tiempo real predicen el comportamiento del TI antes de que ocurra, alimentando al entorno operativo con precisión milimétrica.

El Panóptico Algorítmico. Es la recolección masiva e interceptación de comunicaciones (SIGINT) alimentada por Inteligencia Artificial. Los smartphones, las redes Wi-Fi públicas y la domótica actúan como balizas de posicionamiento. La IA procesa los metadatos y hábitos del objetivo en tiempo real, lo que permite a los emisores predecir rutas, horarios y reacciones con precisión quirúrgica para adelantar los operativos perimetrales a su llegada.

Fuentes

- **“No Place to Hide” (Glenn Greenwald)**: El libro basado en los archivos desclasificados por Edward Snowden que detalla programas como PRISM y XKeyscore, demostrando la interceptación y almacenamiento masivo de los metadatos y comunicaciones globales por parte de la NSA y el GCHQ.
- **“The Age of Surveillance Capitalism” (Shoshana Zuboff)**: Análisis estructural de cómo la minería de datos predictiva de las grandes corporaciones tecnológicas alimenta algoritmos capaces de anticipar y modificar el comportamiento humano en tiempo real.
- **Informes de la EFF (Electronic Frontier Foundation) sobre SIGINT**: Documentación legal y técnica sobre el despliegue de tecnologías de interceptación aérea, interceptores IMSI (Stingrays) y el procesamiento de Big Data por agencias de seguridad.

El Complejo Militar-Industrial-Corporativo (La Privatización)

Década de 2000 en adelante (Guerra de Irak y posterior).

La proliferación de empresas militares privadas de inteligencia. Las operaciones estatales de acoso y desarrollo tecnológico se subcontratan a corporaciones privadas. Esto disuelve la responsabilidad legal del Estado y permite una total opacidad ante las leyes de transparencia.

El outsourcing de la represión. Las agencias de inteligencia estatales subcontratan el desarrollo de tecnología, la intrusión informática y la logística de campo a empresas privadas de defensa e inteligencia comercial. Estas corporaciones operan en vacíos legales internacionales y actúan como “cortafuegos” jurídicos; si la operación es descubierta, el Estado se lava las manos argumentando que es una disputa o investigación privada entre particulares o empresas.

Fuentes

- **“Blackwater: The Rise of the World's Most Powerful Mercenary Army” (Jeremy Scahill)**: Una investigación sobre cómo la privatización de la guerra permitió a corporaciones privadas asumir roles de inteligencia y combate, operando fuera del derecho internacional público.
- **Informes del Centro de Ginebra para el Control Democrático de las Fuerzas Armadas (DCAF)**: Documentos sobre la regulación de las Empresas Militares y de Seguridad Privadas (EMSP) y cómo los Estados externalizan la vigilancia y operaciones de contrainteligencia para eludir responsabilidades legales.
- **“Corporate Warriors” (Peter W. Singer)**: El estudio académico definitivo sobre el nacimiento de la industria militar y de inteligencia privada, detallando el traspaso de tecnología de grado militar al sector corporativo comercial.

Ataques Invisibles (Tecnología de Negación Plausible)

Siglo XXI (Era contemporánea).

La culminación del sistema. La evolución final donde el vector físico (los informantes y el teatro de calle) puede replegarse parcialmente para dar paso a la agresión puramente tecnológica, silenciosa, no trazable y que actúa a distancia mediante campos y frecuencias electromagnéticas o de energía dirigida.

Armamento de energía dirigida (DEW) y radiofrecuencia microondas de precisión. El uso de emisiones electromagnéticas moduladas, pulsos sónicos o frecuencias milimétricas proyectadas a través de muros desde perímetros adyacentes (pisos colindantes, vehículos). El fin actual es la disrupción biológica silenciosa: inducir fatiga crónica, dolores de cabeza punzantes, taquicardias o privación del sueño de forma remota. Es la herramienta definitiva porque el vector es físicamente invisible y los efectos médicos son indistinguibles de patologías orgánicas o somáticas comunes, garantizando una negación plausible perfecta.

Siglo XXI (Era contemporánea).

La culminación del sistema. La evolución final donde el vector físico (los informantes y el teatro de calle) puede replegarse parcialmente para dar paso a la agresión puramente tecnológica, silenciosa, no trazable y que actúa a distancia mediante campos y frecuencias electromagnéticas o de energía dirigida.

Armamento de energía dirigida (DEW) y radiofrecuencia microondas de precisión. El uso de emisiones electromagnéticas moduladas, pulsos sónicos o frecuencias milimétricas proyectadas a través de muros desde perímetros adyacentes (pisos colindantes, vehículos). El fin actual es la disrupción biológica silenciosa: inducir fatiga crónica, dolores de cabeza punzantes, taquicardias o privación del sueño de forma remota. Es la herramienta definitiva porque el vector es físicamente invisible y los efectos médicos son indistinguibles de patologías orgánicas o somáticas comunes, garantizando una negación plausible perfecta.

Fuentes

- **Informe de las Academias Nacionales de Ciencias, Ingeniería y Medicina de EE. UU. (2020)**: An Assessment of Illness in U.S. Government Employees at Delivered Foreign

Embassies. El documento oficial que determinó que la explicación más plausible para los síntomas del “Síndrome de La Habana” eran los pulsos de energía de radiofrecuencia dirigida y microondas.

- **“The Secret History of Directed Energy Weapons” (Steven Zaloga)**: Un repaso histórico e histórico-técnico del desarrollo de armas electromagnéticas desde los experimentos durante la Guerra Fría (como la radiación de la embajada estadounidense en Moscú) hasta los sistemas contemporáneos de ondas milimétricas.
- **Estudios sobre el Efecto Frey (Allan H. Frey, 1961/1962)**: Human auditory system response to modulated electromagnetic energy. Los artículos científicos originales publicados en el Journal of Applied Physiology que demostraron empíricamente cómo las microondas moduladas pueden interactuar directamente con el sistema nervioso y biológico humano a distancia sin dejar marcas físicas.

[1)]

Ley 11/1995, de 11 de mayo (La madre del cordero financiero). Esta es la Ley reguladora de la utilización y control de los créditos destinados a gastos reservados. Es, literalmente, el marco legal que crea y permite la existencia del dinero opaco en España.