La prestigiosa web de inteligencia militar, Veterans Today, ha advertido que el fraude o hackeo electoral está siendo el tema central de la política y geopolítica y se refiere a los extraños sucesos acaecidos en las últimas elecciones españolas. Bajo el título “Israel hackea elecciones en todo el mundo”, el periodista Whitney Webb aclara en la entradilla que software de Microsoft Election Guard es un troyano para que el complejo militar-industrial modifique el sentido de las elecciones.

Acto seguido apunta que la compañía anteriormente liderada por Bill Gates (y de la que sabemos que creó su sistema operativo Windows 8 en colaboración con el Pentágono para tener acceso a nuestros ordenadores) está muy preocupada por la seguridad en el proceso de votación y escrutinio y para ello ha desarrollado un software de encriptación del voto y de seguridad del recuento llamado Election Guard que, a diferencia de los demás, ofrece gratuitamente y en abierto.

Por supuesto que tanta generosidad en una compañía que ha demostrado una falta absoluta de ética y respeto a la privacidad, ha puesto en alarma a la comunidad del software libre, y en este artículo se detalla minuciosamente los estrechos vínculos de Microsoft, no sólo con la NSA, sino con su equivalente israelita, la Unidad 8200.

En los últimos años, Microsoft ha comprado pequeñas compañías de seguridad informática israelíes, como Adallon, Team 8 y Hollolens, comandadas por militares de esta unidad, como Assaf Rappaport o Nadaf Zafrir, que han pasado a ser altos ejecutivos de la compañía.

Sobre el interés de Israel en manipular las elecciones, ya ha aparecido en la prensa oficial, **(ht**

tps://www.haaretz.com/israel-news/facebook-busts-israel-based-campaign-to-disrupt-elections-in-african-asian-nations-1.7249342)
reconociendo que han contratado trolls en Facebook para adulterar las elecciones en África, Latinoamérica y Asia.

Interesado en la naciente tecnología informática de los procesos electorales (amenazada por el hackeo de ellos mismos: otra bandera falsa), Microsoft se ha aliado con otras compañías creadas por la élite en el sector del voto electrónico como Democracy Live, Election Systems Software, Hart Inter Civic, BPro, Micro Vote, and Voting Works. Dicen poder asegurar el voto por una encriptación, pero la realidad, según el articulista, es que el voto así asegurado es maleable; es decir, que aunque no se pueda desencriptar, sí se puede modificar.

Como prueba de que el complejo militar industrial está detrás de estos movimientos, la compañía socia de Microsoft en este sector, Galois, recibió una subvención del Pentágono por valor de 10 millones de dólares; su consejo de administración está compuesto de miembros del DARPA y la inteligencia naval. Los directivos de otras compañías que pugnan en el sector son ex directivos de Amazon y políticos que trabajaron con Obama. Free Fair Technologies tiene vínculos con el Departamento de Seguridad Nacional, que ya intentó hackear las elecciones del 2016 en Georgia, Indiana, Idaho, Kentucky y West Virginia.

En definitiva: que la presunta amenaza rusa no ha sido más que el pretexto para que se consumara la (real) amenaza de hackeo por parte de Israel.

Este documentadísimo artículo, del que apenas he hecho un pequeño resumen, demuestra que las elecciones son ya un arma de guerra y de control de los gobiernos nacionales. Como siempre, Israel está detrás de todas estas conspiraciones. De hecho, Netanyahu ganó las últimas elecciones en su propio país por unos pocos votos…

La empresa que escrutó el 26-M está financiada por el ideólogo del espionaje telefónico de EEUU

La empresa a la que el Ministerio del Interior español adjudicó el contrato del escrutinio de las elecciones del 26-M, **‘Scytl Secure Electronic Voting SA’** , se encuentra financiada por un fondo de inversión donde es directivo el desarrollador de los

programas informáticos de escuchas telefónicas
que utilizan los servicios secretos de Estados Unidos.

Según el Registro Mercantil, 'Scytl Secure Electronic Voting SA' está participada por tres grandes fondos de inversión: **Balderton Capital**, radicado en Reino Unido; **Nauta Capital,** con filiales en Hong Kong y Malasia; y
Spinnaker SCR
, con sede en Barcelona.

El director de operaciones de Nauta Capital es **Dominic Endicott**. Se trata de un experto en telecomunicaciones, que también forma parte de la empresa Booz Allen. Esta compañía fue la encargada de diseñar los programas
'Projects TrailBlazer'
y
'Pioneer Groundbreaker'
, que han sido utilizados en los últimos años por la Agencia de Seguridad Nacional (ANS) de EEUU.

Otra de las empresas en las que figura Dominic Endicott es Carlye Group. Esta compañía diseñó un software denominado **'CarrierIQ'** que fue utilizado por numerosos dispositivos móviles hasta que fue sancionado por violar la Ley de Privacidad de las Comunicaciones Electrónicas de EEUU. Este software registraba **sin el conocimiento del usuario**
la ubicación del mismo, el tiempo de duración de las llamadas, los mensajes de texto, las búsquedas en Internet y hasta las pulsaciones de las teclas.

Facebook denuncia campaña israelí para perturbar elecciones en naciones africanas, asiáticas y latinoamericanas

Facebook hizo público que prohibió a una compañía israelí que realizó una campaña de influencia dirigida a interferir las elecciones en varios países y que canceló docenas de cuentas involucradas en difundir la desinformación.

Nathaniel Gleicher, jefe de la política de seguridad cibernética de Facebook, dijo a los

periodistas que el gigante de la tecnología había eliminado 65 cuentas israelíes, 161 páginas, docenas de grupos y cuatro cuentas de Instagram. Muchos estaban vinculados al Grupo Arquímedes, una firma de cabildeo y consultoría política con sede en Tel Aviv que se jacta de sus habilidades en las redes sociales y de "cambiar la realidad".

Gleicher dijo que Facebook no podía especular sobre los motivos de Arquímedes, que "pueden ser comerciales o políticos".

Pero dijo que Facebook descubrió un "comportamiento coordinado inauténtico", con cuentas que se hacen pasar por ciertos candidatos políticos, difamar a los opositores y presentarse como organizaciones locales de noticias que venden información supuestamente filtrada.

La actividad parecía centrada en los países del África subsahariana, pero también estaba dispersa en partes del sudeste asiático y América Latina. Las páginas han acumulado 2,8 millones de seguidores y cientos de miles de visitas.

Gleicher dijo que Arquímedes había gastado unos $ 800,000 en anuncios falsos y que su actividad engañosa se remonta a 2012. Dijo que Facebook ha prohibido Arquímedes.

En su sitio web, Arquímedes se presenta como una firma consultora involucrada en campañas para las elecciones presidenciales.

Hay poca información disponible más allá de su eslogan, que es "campañas ganadoras en todo el mundo", y una vaga propaganda sobre el software de "administración masiva de redes sociales" del grupo, que dijo que permitía el funcionamiento de un número "ilimitado" de cuentas en línea.

El sitio, con un montaje de fotos de archivo de África, América Latina y el Caribe, se jacta de su "posición única dentro del ámbito de las redes sociales" y de sus esfuerzos para "aprovechar todas las ventajas disponibles para cambiar la realidad de acuerdo con los deseos de nuestros clientes"

El director ejecutivo de Arquímedes es Elinadav Heymann, según la consultora de negociaciones suiza Negotiations.CH, donde figura como uno de los consultores del grupo.

Una biografía publicada en el sitio web de la compañía lo describe como el ex director del grupo de presión europeo ***Amigos de Israel*** con sede en Bruselas, un ex asesor político en el parlamento israelí y un ex agente de inteligencia de la Fuerza Aérea israelí.

El informe polémico: Israel hackea elecciones en todo el mundo

Whitney Webb *es una periodista de MintPress News con base en Chile. Ha contribuido a varios medios de comunicación independientes, entre ellos Global Research, EcoWatch, el Instituto Ron Paul y 21st Century Wire, entre otros. Ella ha hecho varias apariciones en radio y televisión y es la ganadora en 2019 del Premio Serena Shim por su integridad en el periodismo.*
(Más de Whitney Webb)

A principios de este mes, el gigante tecnológico Microsoft anunció su solución para "proteger" las elecciones estadounidenses de toda interferencia, a la que denominó "Election Guard". La tecnología electoral ya está lista para ser adoptada por la mitad de los fabricantes de máquinas de votación y algunos gobiernos estatales para las elecciones generales de 2020. A pesar de que ha sido fuertemente promovido por los principales medios de comunicación en las últimas semanas, ninguno de esos informes ha revelado que **Election Guard** tiene varios conflictos de interés flagrantes que socavan en gran medida su afirmación de proteger la democracia estadounidense.

En esta investigación, *MintPress* revela cómo Election Guard fue desarrollado por compañías con profundos vínculos con las comunidades de defensa e inteligencia de los EE. UU. y la inteligencia militar israelí, así como el hecho de que está lejos de ser claro que la tecnología evite la interferencia extranjera o nacional en, o la manipulación de, totales de votos u otros aspectos de los sistemas electorales estadounidenses.

El analista forense y autor Jonathan Simon, así como la periodista de investigación Yasha

Levine, quien ha escrito extensamente sobre cómo los militares han tratado de armar tecnologías públicas, incluida Internet, fueron consultados por sus opiniones sobre Election Guard, sus conexiones con el complejo militar-industrial. y la implicación de esas conexiones para la democracia estadounidense como parte de esta investigación.

En enero, *MintPress* publicó una exposición que luego se volvió viral en una empresa de clasificación de noticias conocida como Newsguard. Dirigido oficialmente a la lucha contra las "falsas noticias", las numerosas conexiones de la compañía con la inteligencia de los EE. UU., un grupo de expertos neoconservador y los autor-admitidos propagandistas del gobierno revelaron que su verdadera intención era promover los medios corporativos en lugar de alternativas independientes.

Newsguard fue una de las primeras iniciativas que comprende el programa " **Defending Democracy** " de Microsoft , un programa que el gigante tecnológico creó bajo los auspicios de proteger los "procesos democráticos estadounidenses de la interferencia cibernética [que] se han convertido en una preocupación fundamental". A través de su asociación con Microsoft, Newsguard se ha instalado en bibliotecas y universidades públicas de todo el país, incluso mientras las empresas del sector privado han seguido evitando adoptar el complemento problemático del navegador.

Ahora, Microsoft está promoviendo una nueva iniciativa de "Defensa de la democracia", una que está igualmente llena de conflictos de intereses, que amenaza a la democracia estadounidense de una manera que Newsguard nunca pudo. Election Guard es promocionado por Microsoft como un sistema que **apunta a** "hacer que la votación sea segura, más accesible y más eficiente en cualquier lugar que se use en los Estados Unidos o en naciones democráticas de todo el mundo". Desde entonces, ha sido **fuertemente promovida por los gobiernos y el gobierno de los Estados Unidos. Así como medios de comunicación financiados** en preparación para su uso en **las elecciones generales de 2020** .

Sin embargo, según Jonathan Simon, analista forense de elecciones y autor de ***CODE RED: Elecciones informatizadas y la guerra en la democracia estadounidense***

, esta campaña de relaciones públicas es probable que promueva más control interno sobre las elecciones en los Estados Unidos. "Es alentador que después de casi dos décadas de ignorar los problemas de seguridad con la votación computarizada, de repente haya una lucha por proteger nuestra próxima elección que sugiere que esos problemas finalmente se están tomando en serio", dijo Simon a
MintPress
. "Desafortunadamente, la solución propuesta es solo una mayor informatización y complejidad, lo que se traduce en un mayor control por parte de expertos, aunque, por supuesto, eso no forma parte de la campaña de relaciones públicas".

En cuanto a la posible identidad de esos expertos, el hecho de que Election Guard de Microsoft se desarrolló en conjunto con un contratista de inteligencia y militar privado cuyo único inversor es el Departamento de Defensa de EE. UU. ofrece una pista preocupante. Como consecuencia, la promesa de Election Guard de "asegurar" las elecciones es dudosa, especialmente dado que Microsoft es un contratista militar estadounidense. Además, en medio del **escándalo** de **la intromisión israelí en las elecciones extranjeras** , los crecientes vínculos de Microsoft con la inteligencia militar israelí y las empresas privadas de ciberseguridad israelíes plantean aún más preocupaciones sobre si el verdadero propósito de Election Guard es "asegurar" las elecciones estadounidenses
para los candidatos afectos al establishment
, especialmente el complejo militar-industrial.

Explicando Election Guard

Según un anuncio hecho a principios de mayo por Tom Burt, Vicepresidente de Seguridad y Confianza del Cliente de Microsoft, Election Guard es "un kit de desarrollo de software de fuente abierta (SDK) gratuito" que "hará que la votación sea segura, más accesible y más eficiente en cualquier lugar que se use". La declaración de Burt afirma que el sistema Election Guard" permitirá la verificación de las elecciones de principio a fin, abrirá los resultados a las organizaciones de terceros para una validación segura y permitirá que los votantes individuales confirmen que sus votos fueron contabilizados correctamente ". Aunque parezca que solo se trata de boletas electrónicas, el anuncio indica que el sistema "está diseñado para funcionar con sistemas que usan boletas de papel" mediante el uso de **un escáner óptico.**

En particular, Microsoft eligió anunciar Election Guard solo después de que *ya* se *había* asocia do "con los principales proveedores de tecnología electoral que están explorando la integración de Election Guard en sus sistemas de votación". Burt señaló que Microsoft ahora tiene "asociaciones con proveedores de tecnología electoral responsables de más de la mitad" de las

máquinas de votación vendidas en los EE. UU. ”Las empresas asociadas de Election Guard incluyen Democracy Live, Election Systems & Software, Hart Inter Civic, BPro, Micro Vote y Voting Works.

Otra admisión interesante y profundamente preocupante en el anuncio de Microsoft es que el socio de desarrollo de Election Guard, la firma de ciberseguridad con sede en Portland Galois, “recibió recientemente $ 10 millones en fondos de la Agencia de Proyectos de Investigación Avanzada de Defensa del Pentágono (DARPA) para construir un sistema para ayudar a evaluar el hardware seguro que los investigadores de DARPA están desarrollando como parte de un programa separado".

El anuncio de Microsoft señala luego que "la agencia considera que garantizar la integridad y la seguridad del proceso electoral es un problema crítico de seguridad nacional y los planes para implementar el SDK de Election Guard como parte de su esfuerzo para habilitar un componente verificable de extremo a extremo en futuras versiones de su sistema de votación".

Por más preocupante que pueda parecer la inversión indirecta de 10 millones de dólares de DARPA en Election Guard, simplemente se está rascando la superficie, ya que el propio Galois es esencialmente una extensión de DARPA en la industria de la ciberseguridad privada.

La empresa "privada" cuyo único inversor es el Pentágono

Fundada en 1999 por John Launchbury, Galois se convirtió rápidamente en cliente de numerosas agencias gubernamentales que ahora, según el sitio web de Galois, forman la gran mayoría de su clientela. De hecho, Galois actualmente enumera a **las siguientes agencias gubernamentales de los EE. UU.** en su sección de "clientes": DARPA, el Departamento de Defensa, el Departamento de Energía, el Departamento de Seguridad Nacional, "Comunidad de Inteligencia" (es decir, CIA, NSA, etc.)) y la NASA. Sin embargo, otros clientes de Galois **incluyen al** principal fabricante estadounidense de armas, General Dynamics. El enfoque declarado de Galois como empresa es la investigación y el desarrollo en informática avanzada, con énfasis en la protección de sistemas críticos y ciberseguridad. También incursiona en inteligencia artificial, interacción hombre-computadora y aprendizaje automático.

Aunque se describe a sí mismo como "una empresa privada que opera en los Estados Unidos", los registros públicos indican que los únicos inversores de Galois son DARPA y la Oficina de Investigación Naval (ONR), ambas divisiones del Departamento de Defensa. **En otras palabras, mientras que "oficialmente" es una empresa privada, su único inversor es el gobierno de los Estados Unidos, más específicamente el Pentágono.**

Sin embargo, las conexiones de la compañía a DARPA van aún más lejos. El fundador y científico principal de la compañía, John Launchbury, dejó Galois en 2014 para convertirse en gerente de programas y, posteriormente, **director** de la Oficina de Innovación para la Información de DARPA, que se ocupa de "inversiones a escala nacional en ciberseguridad e inteligencia artificial". En 2017, dejó DARPA y se fue Volver a trabajar en Galois como **científico jefe de** la compañía. El propósito oficial de la Oficina de Innovación de la Información de DARPA es desarrollar tecnología avanzada para temas de seguridad nacional, pero también se enfoca en **mejorar la** "asociación entre personas y máquinas".

Una compañía spin-off de Galois llamada Free & Fair, que desarrolla tecnología electoral, se asoció con Microsoft para producir Election Guard. **El sitio web de Free & Fair** enumera a sus socios como DARPA, Microsoft, el fabricante de máquinas de votación Voting Works, el desarrollador de software de conteo de votos Verificatum, el gobierno del estado de Colorado y el Instituto OSET (Open Source Election Technology) Voting Works es un fabricante de máquinas de votación "sin fines de lucro" fundado por un ex director de ingeniería de Mozilla y **estrechamente afiliado** al Centro para la Democracia y la Tecnología (CDT). Además de Colorado, otros estados **como Minnesota** se han asociado con el programa "Defendiendo la democracia" de Microsoft, pero no está claro si han adoptado o planean adoptar Election Guard como consecuencia de esa asociación.

Según el anuncio de la CDT sobre el lanzamiento de Voting Works:

CDT servirá como sede para Votingworks hasta que se convierta en su propia entidad sin fines de lucro. Esta asociación significa que Votingworks está trabajando estrechamente con el experimentado equipo de CDT para acelerar rápidamente las operaciones y comenzar a desarrollar en serio el desarrollo de máquinas de votación de código abierto, asequibles y seguras para su uso en las elecciones públicas de los Estados Unidos".

El presidente y director ejecutivo de CDT es **Nuala O'Connor** , quien fue vicepresidente de cumplimiento y confianza del cliente de Amazon antes de convertirse en presidente de CDT. O'Connor también fue anteriormente director de privacidad del Departamento de Seguridad Nacional de los Estados Unidos y también trabajó en General Electric y en el Departamento de Comercio de los Estados Unidos.

La **junta** de CDT incluye al ex Coordinador Adjunto de Cumplimiento de la Propiedad Intelectual de la Casa Blanca bajo la presidencia de Obama y al actual Consejero Principal de Apple **Philippa Scarlett** ; la vicepresidenta corporativa de Microsoft, Julie Brill; y el vicepresidente de política global de Mozilla, Alan Davidson. Más preocupante, sin embargo, es **su consejo asesor** , que incluye representantes de RAND Corporation, Walmart, Verizon, el Instituto Charles Koch, Facebook y el American Enterprise Institute (AEI).
Y
AEI, uno de los think tanks neoconservadores más notorios del país, conocido por emplear a John Bolton y Paul Wolfowitz, entre otros. Uno de los co-fundadores de Newsguard, Louis Gordon Crovitz, es **también miembro de** la AEI.

Otro socio de Galois 'Free & Fair es el Open Source Election Technology Institute (OSET Institute, u OSETI), cuya iniciativa principal se llama “Trust The Vote”. Uno de los cofundadores de OSETI y su actual CTO es **E. John Sebes** , quien trabajó anteriormente para DARPA y DHS. La **junta de asesores estratégicos** de OSETI incluye a Chris Barr, de la Fundación John S. y James L. Knight, que es **un importante inversor** en Newsguard; el ex Secretario de Estado de Oregon Phil Keisling; el ex subdirector de la NSA William Cromwell; el ex jefe de la Dirección de Ciberseguridad del DHS y el ex gerente de proyectos de DARPA Doug Maughan; y Norm Ornstein del neoconservador American Enterprise Institute y co-director del Proyecto de Reforma Electoral AEI-Brookings.

Aparte de los numerosos enlaces a grandes corporaciones, agencias gubernamentales y grupos de expertos neoconservadores, de especial interés para la misión de Free & Fair de desarrollar una tecnología electoral "segura", son sus conexiones con DHS. Esto se debe a que, antes, durante y después de las elecciones de 2016, el DHS fue pillado tratando de introducirse en los sistemas electorales estatales en al menos tres estados - Georgia, **Indiana e Idaho** -
acusaciones similares
también se están realizando en Kentucky y Virginia Occidental. En

el caso de Indiana
, los intentos de piratería del DHS se produjeron casi 15,000 veces en un período de 46 días. En una respuesta oficial a la acusación de Georgia, el DHS había intentado penetrar en el cortafuegos de su sistema electoral, el DHS que inicialmente negó estar detrás del intento de pirateo,
luego respondió
que el intento de violación fue una "acción legítima" destinada a "verificar la licencia profesional administrada por el estado". Algunos de los estados seleccionados por el DHS rechazaron la oferta del departamento de "apuntalar" los sistemas electorales antes de la elección de 2016.

Compare esto con la supuesta piratería rusa en los sistemas electorales estatales, que hasta la fecha **solo** incluye **una reclamación** del FBI, los piratas informáticos presuntamente afiliados a la inteligencia militar rusa penetraron los datos de registro de votantes en dos condados de Florida. Ese presunto hackeo, cuyos detalles permanecen clasificados y para los cuales no se ha puesto a disposición pública ninguna evidencia de que haya ocurrido, no produjo alteraciones en los datos ni ninguna otra manipulación de esos sistemas, según funcionarios del FBI. El DHS, por el contrario, intentó piratear los sistemas, no de condados individuales, sino de estados enteros, y reconoció que lo hizo, a pesar de que optaron por no utilizar el "pirateo" y defendieron su actividad. Al centrarse en la interferencia extranjera, y especialmente en la rusa, pueden convertirse en una historia más patriótica los peligros planteados por *los* medios *nacionales* de actores que con una participación tan grande en los resultados de las elecciones en los Estados Unidos parecen haber sido subestimados y prácticamente ignorados por los medios de comunicación.

Las asociaciones de Free & Fair con grupos vinculados al DHS parecen socavar aún más su misión declarada de proporcionar tecnología electoral segura y confiable, además de los profundos vínculos de su empresa matriz con el Departamento de Defensa, especialmente DARPA.

Yasha Levine , periodista de investigación ruso-estadounidense y autora de ***Surveillance Valley: The Secret Military History of Internet***
, explicó a
MintPress
por qué DARPA está probablemente interesada en el software del sistema electoral estadounidense como Election Guard y por qué el interés de la agencia es peligroso para la democracia estadounidense:

Los sistemas electorales ahora se ven cada vez más como un teatro para la guerra entre

estados nacionales competidores. Luego, si eres DARPA y tu razón de ser es crear armas de alta tecnología para el futuro, entonces estarás viendo los sistemas de votación electrónica como un teatro de guerra donde el país podría ser atacado por un adversario extranjero. Eso explica por qué DARPA está involucrado.

Pero DARPA y algunas de estas compañías involucradas también pueden verse como enemigos de la voluntad popular de los estadounidenses... Podemos plantearnos hipótesis sobre lo que realmente está sucediendo y cuáles son sus intenciones, pero claramente el laboratorio de investigación y desarrollo del Pentágono para la guerra no debería estar cerca del sistema electoral de Estados Unidos, porque representa una fuerza enorme, poderosa e irresponsable en el sistema político estadounidense cuyos intereses a menudo van en contra de la democracia.

El hecho de que estamos entregando las llaves de la democracia estadounidense al complejo militar-industrial, es como darle las llaves del gallinero a un zorro y decir: 'ven aquí y toma lo que quieras'. Obviamente es peligroso".

¿De control mental a control electoral?

Vale la pena describir brevemente por qué el papel de DARPA en Galois es preocupante. Esto se debe principalmente al hecho de que DARPA actualmente está desarrollando tecnologías orwellianas y de pesadilla "Terminator", que incluyen esfuerzos para **implantar chips en el cerebro de los soldados**
,
reemplazar a la mayoría de los soldados humanos con robots soldados
y crear
robots asesinos tipo "Terminator"
- e inteligencia artificial autónoma, sistemas de focalización que
utilizarán los medios sociales
para identificar objetivos potenciales.

En 2015, Michael Goldblatt, entonces director de la subdivisión DARPA Defence Sciences Office (DSO), que supervisa el programa de "súper soldado", le dijo a la periodista Annie Jacobsen que no veía ninguna diferencia entre "tener un chip en su cerebro que podría ayudar a controlar" sus pensamientos" y "un implante coclear como el que ayuda a los sordos a oír". Cuando se les presiona sobre las consecuencias no deseadas de dicha tecnología, Goldblatt

declaró que" hay consecuencias no deseadas para todo".

No hace falta decir que el hecho de que una institución que actualmente desarrolla lo que significa tecnología de control mental, y que tampoco ve nada de *malo* en esa tecnología, de repente se haya interesado tanto en crear y financiar con millones de dólares de forma gratuita, un sistema electoral "seguro" para proteger a la democracia estadounidense de la interferencia, es más que extraño y sugiere un motivo ulterior.

Del mismo modo, la **afirmación** de Microsoft de que "no cobrará por usar Election Guard y no se beneficiará de asociarse con proveedores de tecnología electoral que lo incorporen en sus productos" también debería hacer surgir preguntas. Teniendo en cuenta que Microsoft tiene **una larga historia** de prácticas depredadoras, incluida **la manipulación de precios para su software de seguridad OneCare**, su oferta de ofrecer el software Election Guard sin costo es reveladora y sugiere un motivo oculto detrás del reciente interés filantrópico de Microsoft en "defender democracia."

Además, la doble función de Microsoft como una importante empresa de tecnología y un contratista, tanto para el **ejército de Estados Unidos** y **la comunidad de inteligencia de Estados Unidos** también debe levantar banderas rojas. De hecho, Microsoft ha dejado en claro que planea forjar vínculos cada vez más estrechos con el gobierno de los EE. UU., especialmente después de que el presidente de Microsoft, Brad Smith, **anunció en diciembre pasado** que Microsoft "proporcionará al ejército de los EE. UU. el acceso a la mejor tecnología ... toda la tecnología que nosotros creamos. Colaboración completa". Un mes antes de esa declaración, Microsoft **aseguró un contrato de $ 480 millones** con el Pentágono para proporcionar al ejército de los EE. UU. su tecnología HoloLens.

Esta estrecha relación que Microsoft está construyendo con el Pentágono puede explicar el motivo oculto de la compañía para crear y promocionar Election Guard, ya que la promoción de la tecnología electoral financiada en gran medida por DARPA podría ayudar a mejorar las posibilidades de Microsoft en su **actual oferta por un contrato de servicios en la nube de $ 10 mil millones** con el Pentágono.

Además, dadas las numerosas conexiones corporativas, así como las conexiones con la AEI, se podría argumentar que la participación íntima de Microsoft y Galois en este sistema podría ayudar a "proteger" las elecciones de los candidatos que amenazan con regular o controlar sus industrias, particularmente el complejo militar-industrial. Por supuesto, la afirmación de que Election Guard es de "código abierto" está destinada a mitigar dicha especulación, ya que la naturaleza de código abierto de la tecnología significa ostensiblemente que no se oculta ningún código discreto que pueda usarse para manipular los resultados. Sin embargo, como se mostrará en breve, el hecho de que una tecnología sea de código abierto *no significa necesariamente que los datos que pasan a través de esa tecnología no* estén *abiertos a la manipulación de un tercero.*

Election Guard no es inmune a la manipulación

El **comunicado** de prensa de Microsoft que anuncia Election Guard destaca su afirmación de que su sistema haría las elecciones más verificables, seguras y auditables al estar basada en código abierto y mejorar la experiencia de votación. Si bien todas estas cosas suenan bastante bien, hay razones para creer, según la descripción dada por Microsoft, que algunas de estas afirmaciones son dudosas y engañosas. Desafortunadamente, por ahora, el análisis de Election Guard está restringido a la descripción de Microsoft del software, ya que aún no está disponible para examen público. Se espera que el kit de software Election Guard se lance a finales de este año en la plataforma GitHub.

El primer aspecto de la reclamación "verificable" se relaciona con un sistema de seguimiento de votantes, donde cada votante recibe una identificación de seguimiento única que les permite "seguir una versión cifrada de la votación de todo el proceso electoral a través de un portal web proporcionado por las autoridades electorales. "Los votantes pueden elegir la opción de confirmar" que sus rastreadores y votos encriptados reflejen con precisión sus selecciones".

Sin embargo, Microsoft señala que "una vez que se emite un voto, ni el rastreador ni los datos proporcionados a través del portal web se pueden usar para revelar el contenido de la votación", lo que significa que si bien una persona puede realizar un seguimiento de si se contó su voto, no puede verificar si el contenido de la votación (es decir, a quién votaron) se cuenta correctamente o no. Microsoft continúa señalando que solo “después de que se complete la elección” la página de seguimiento permitirá ver el contenido de la votación.

El segundo componente de "verificabilidad" de Election Guard "es una especificación abierta, o una hoja de ruta, que permite a cualquiera escribir un verificador de elecciones". Microsoft luego señala que esta especificación abierta significaría que "los votantes, candidatos, medios de comunicación y cualquier observador pueden verificar los datos propios o descargados de las fuentes de su elección para confirmar las tabulaciones".

Microsoft describe estas dos características como constitutivas de "verificabilidad de extremo a extremo" (E2E-V), que Free & Fair describe como "tecnología criptográfica que permite a los votantes votar de manera normal en un lugar de votación y tener evidencia de que la elección es digna de confianza."

Otro enfoque de Election Guard es la seguridad, para la cual el sistema emplea "encriptación homomórfica, que permite que los procedimientos matemáticos, como el conteo, se realicen con datos totalmente encriptados" y esto permite que los votos encriptados individualmente se "combinen para formar una tabulación encriptada de todos los votos que luego puede ser descifrada para producir un recuento de elecciones que proteja la privacidad de los votantes". En particular, el cifrado homomórfico es la única medida de seguridad de Election Guard nombrada en el comunicado de prensa.

El analista forense de elecciones Jonathan Simon, autor de ***CODE RED: Elecciones informatizadas y guerra en la democracia estadounidense***, no fue completamente persuadido por la afirmación E2E-V. "Perdone mi escepticismo", dijo Simon a *MintPress*, "pero he leído el folleto de Election Guard de " buenas noticias " de Microsoft y me recuerda mucho a los volantes y al material de relaciones públicas que los proveedores y programadores del equipo de votación *actual han* prestado "computadoras en las que descubrieron los expertos en TI que podrían ser hackeadas por personas externas y programadas para agregar, eliminar y cambiar los votos ".

Simón continuó:

En este momento, por ejemplo, están vendiendo dispositivos de marcado de boletas (bmd) costosos y completamente innecesarios que convierten sus votos en un código de barras, un código que ningún votante puede leer o verificar. Muy hábil pero otro nivel

de no transparencia, otro paso más para el público, el conteo de votos observable y otro vector para el fraude.

He pasado los últimos 17 años examinando los patrones de conteo de votos y prestando atención a un desfile de notables banderas rojas que indican la manipulación computarizada del conteo de votos. Ha sido un sistema diseñado para el ocultamiento y tan poco transparente como puede serlo un proceso. Sería genial si una tecnología más avanzada trajera por fin la transparencia, como Microsoft parece prometer.

Pero lo que veo hasta ahora es aún más complejo: el cifrado que, ya sea de código abierto o no, requiere que los expertos penetren o comprendan. Y solo hay un paso corto para la votación en línea, incluso más conveniente y tan segura como, por ejemplo, es Facebook.

Pendiente de una demostración que muestre con perfecta claridad accesible cómo una entidad de terceros puede verificar los recuentos de votos agregados sin tener que creernos por fe algún paso en el proceso (la verificación individual de que 'su' voto fue 'contado' es una campaña inútil), todavía se siente como el mismo viejo juego de "confía en nosotros". Estoy dispuesto a ser persuadido, pero el contexto histórico aquí es muy cauto".

Las preocupaciones de Simon reflejan algunos aspectos controvertidos del enfoque de Election Guard. Si bien el cifrado protegería aparentemente los votos de manipulación y, por lo tanto, los resultados de las elecciones, es importante señalar que el cifrado homomórfico es una forma de cifrado *maleable*.

Según ***Brilliant.org*** :

Un sistema criptográfico maleable es uno en el que cualquier persona puede interceptar un texto cifrado, transformarlo en otro texto cifrado y luego traducirlo en un texto simple que tenga sentido. La maleabilidad generalmente se considera indeseable en un sistema criptográfico. Imagina que intentas enviar el mensaje "te quiero" a tu amiga mediante el cifrado. Lo cifras y lo envías. Pero, es interceptado por un hacker en el camino. Todo lo que ven es un texto cifrado, pero pueden cambiar ese texto cifrado a algo que se

descifre a "te odio" cuando tu amiga intente descifrarlo. Es por eso que la maleabilidad no suele ser deseada".

Si ese es el caso, entonces, ¿qué detiene a un "pirata informático" u otro tercero? Digamos que una agencia del gobierno de los EE. UU. como la NSA o un agente político con acceso al ciber-ducto electoral - cambien el voto de una persona de demócrata a republicano o viceversa ¿O alterando la tabulación encriptada de todos los votos?

Si bien el cifrado homomórfico parece ser una opción razonable en un sentido para permitir que los votos sean contabilizados sin descifrar, existe un nivel adicional de preocupación dado el pasado de Microsoft, particularmente el historial de Microsoft de trabajar realmente con las agencias del gobierno de EE. UU. para evitar el cifrado.

De hecho, los documentos filtrados por Edward Snowden revelaron que Microsoft **ayudó a** la Agencia de Seguridad Nacional a evitar su propio cifrado para que la agencia pudiera descifrar los mensajes enviados a través de ciertas plataformas de Microsoft, incluido el chat web de Outlook.com, el servicio de correo electrónico de Hotmail y Skype. Además, en 2009, un alto funcionario de la NSA
testificó
ante el Congreso, Microsoft y la NSA trabajaron juntos para crear su sistema operativo Windows 7, lo que lleva a algunos a preocuparse de que Microsoft haya incorporado una "puerta trasera" en el sistema operativo para ayudar a las actividades de vigilancia del gobierno. Ahora que los vínculos de Microsoft con la comunidad militar y de inteligencia de los EE. UU. son más profundos que nunca, surge la pregunta de si la cooperación encubierta de Microsoft con las agencias gubernamentales en detrimento de los consumidores también es un factor que guía su papel en la creación y promoción de Election Guard.

Además, como el presidente de Microsoft se **comprometió** a entregar todas sus tecnologías al ejército de los EE. UU., uno se pregunta si este tipo de encriptación y metodología no se eligió a propósito, especialmente dado el hecho de que la NSA es
bastante eficaz
para romper tipos de seguridad mucho más seguras, incluso sin la ayuda de Microsoft.

Otro de los puntos del discurso de Microsoft utilizados para promover Election Guard es el hecho de que será de código abierto, lo que significa que el código del programa estará disponible públicamente, un movimiento aparentemente dirigido a resolver las preocupaciones

de que el código de Election Guard podría contener manipulaciones ocultas o vulnerabilidades.

Sin embargo, el periodista de investigación Yasha Levine comparó la promoción de Microsoft del código de fuente abierto aún no publicado de Election Guard como una "cuestión de relaciones públicas". Levine le dijo a *MintPress* :

El código abierto inevitablemente tiene errores y vulnerabilidades que existen accidentalmente porque todo el código tiene vulnerabilidades. Esto es cierto para los sistemas de código abierto y de código cerrado. El código abierto solo significa que la gente puede verlo, pero luego ese código debe ejecutarse a través de un compilador que realmente ejecuta un programa. Entonces, ya tienes un grado de abstracción y separación del código fuente abierto. Pero incluso si el código ejecutable y el código fuente son los mismos, hay errores que pueden ser explotados.

Entonces, lo que hace el código abierto es dar una apariencia de claridad que nos lleva a pensar que miles de personas probablemente han examinado el código y han marcado cualquier error en él. Pero, en realidad, muy pocas personas tienen el tiempo y la capacidad de mirar este código. Entonces, esta idea de que el código de fuente abierto es más transparente no es realmente cierta porque pocas personas lo están comprobando".

Levine continuó señalando que hay muchos ejemplos de sistemas de código abierto, incluidos los sistemas de código abierto ampliamente utilizados, que tienen vulnerabilidades importantes que no se detectan durante años. Uno de los mejores ejemplos, en opinión de Levine, es **el error "Heartbleed"** , que era una vulnerabilidad de seguridad en el software de código abierto OpenSSL, un sistema que permite el cifrado básico del tráfico web al cifrar las conexiones "http". Heartbleed permitió a los piratas informáticos acceder a la memoria de los servidores de datos de aproximadamente medio millón de sitios web y no se detectó durante años, a pesar de que OpenSSL es un sistema de código abierto.

Levine también subrayó el hecho de que tanto las agencias de inteligencia estadounidenses como las extranjeras "más que cualquier otra persona o grupo" están involucradas en la búsqueda de tales vulnerabilidades, que ocultan al público para otorgarse una ventaja en la guerra cibernética. Algunas de las listas de vulnerabilidades o vulnerabilidades de la CIA se revelaron en el **lanzamiento de WikiLeaks Vault 7** .

Los vínculos de Microsoft con la inteligencia militar israelí

Election Guard se está promoviendo actualmente como un paso clave para prevenir la "interferencia" de un gobierno extranjero o actor estatal en las elecciones de EE. UU. en el futuro. Sin embargo, no hay garantía de que Election Guard esté libre de influencias extranjeras, dado que Microsoft tiene vínculos profundos con la comunidad de inteligencia militar de una nación extranjera: Israel.

Los enlaces de Microsoft a la unidad de inteligencia militar israelí conocida como Unidad 8200, que se discutirán momentáneamente, son preocupantes por varias razones. El primero es el hecho de que el principal desarrollador de un nuevo sistema de software electoral destinado a proteger las elecciones estadounidenses de la "interferencia extranjera" tiene vínculos estrechos con una agencia de inteligencia militar extranjera. No hace falta decir que si el principal desarrollador de Election Guard tuviera tales vínculos con otra agencia de inteligencia militar extranjera, como la inteligencia militar rusa, el software no tendría una posibilidad de adopción en los EE. UU. y probablemente sería un escándalo nacional.

Podría decirse que aún una preocupación más grave en términos de la relación Microsoft-Unit 8200 y Electionguard, es la reciente serie de escándalos que rodean la interferencia israelí en las elecciones extranjeras en todo el mundo. El más reciente de esos escándalos involucró a la compañía israelí Grupo Arquímedes y sus redes sociales, que influyen en las campañas de desinformación **para atacar las elecciones** en varias naciones africanas y asiáticas. Según **el ** ***Times of Israel*** , el CEO del Grupo Arquímedes, Elinadav Heymann, es un antiguo agente de inteligencia para el ejército israelí. El grupo gastó una cantidad estimada de $ 800,000 en anuncios engañosos de Facebook como parte de su campaña de desinformación, una suma **mucho mayor** de los $ 100,000 presuntamente gastados por una compañía rusa en una campaña de desinformación similar en las elecciones de 2016.

Antes de este último escándalo, varias empresas privadas israelíes **fueron acusadas** de intentar conspirar en la campaña de Trump en 2016 , a saber, el ahora cerrado **Grupo PSY**

, que estaba dirigido por ex agentes de inteligencia israelíes, y Wikistrat, que también tiene **estrechos vínculos** con la inteligencia israelí. El hecho de que las firmas israelíes privadas con vínculos con la inteligencia israelí y la inteligencia militar hayan sido atrapadas en recientes escándalos de injerencia en las elecciones, incluso en los Estados Unidos, debería ser una gran señal de alerta al examinar los numerosos conflictos de intereses que envuelven a los desarrolladores de Election Guard y cómo esos conflictos puede informar sobre la auténtica funcionalidad del programa.

Microsoft tiene presencia en Israel desde hace mucho tiempo que se remonta a 1989. Sin embargo, en los últimos años, han invertido y adquirido varias empresas con profundos vínculos con la Unidad 8200 de las FDI.

En 2015, Microsoft **adquirió** la compañía israelí de seguridad en la nube Adallom por $ 320 millones, que luego serviría como una nueva base para el Centro de Investigación y Desarrollo (I&D) de Microsoft en Israel, que ha estado activo desde 1989. El producto de Adallom fue posteriormente renombrado como Microsoft Seguridad de aplicaciones en la nube. El CEO y cofundador de Adallom es Assaf Rappaport, quien **ahora dirige** el Centro de Investigación y Desarrollo de Microsoft en Tel Aviv. Rappaport, entre otras cosas, se graduó en el programa IDF "Talpiot" de las FDI y también prestó servicios en la unidad de inteligencia militar israelí conocida como Unidad 8200.

La Unidad 8200 es una unidad de élite del cuerpo de inteligencia israelí que forma parte de la Dirección de Inteligencia Militar de las FDI y está involucrada principalmente en inteligencia de señales (es decir, vigilancia), ciberguerra y descifrado de códigos. A menudo se lo describe como el equivalente israelí de la NSA y Peter Roberts, investigador principal en el Royal United Services Institute de Gran Bretaña, caracterizó a la unidad en **una entrevista** con el *Financial Times* como "probablemente la agencia de inteligencia técnica más importante del mundo" a la par con la NSA en todo excepto en la escala ".

En particular, la NSA y la Unidad 8200 han colaborado en proyectos como el infame **virus Stuxnet** y el malware Duqu, una **sofisticada variedad** de los cuales se utilizó para espiar a los países que participan en la negociación del acuerdo nuclear con Irán. Además, se sabe que la NSA trabaja con veteranos de la Unidad 8200 en el sector privado, como cuando la NSA

contrató a
dos compañías israelíes, cuyos ejecutivos están vinculados a la Unidad 8200, para crear puertas traseras a todas las principales compañías de telecomunicaciones y tecnología de los EE. UU. Incluyendo Facebook, Microsoft y Google. La unidad también es
conocida por espiar
a civiles en los territorios palestinos ocupados con “propósitos de coerción”, es decir, recopilar información para chantaje, y también para
espiar a los palestinos-estadounidenses a
través de un acuerdo de intercambio de inteligencia con la NSA.

Sin embargo, las conexiones de Microsoft con la Unidad 8200 van mucho más allá de Adallom. Otro ejemplo es la **considerable inversión de** Microsoft en Illusive Networks, una firma de seguridad cibernética israelí creada por Team8, en la que Microsoft
también ha realizado grandes inversiones
. El CEO y cofundador de Team8 es Nadav Zafrir, quien solía liderar la Unidad 8200, y dos de los otros tres fundadores de la compañía también son veteranos de la Unidad 8200. El ex CEO de Google (ahora Alphabet), Eric Schmidt, es un importante patrocinador de Team8.

Team8 se ha reunido con ex directores de la NSA, con Zafrir haciendo presentaciones junto con el ex director de la NSA Keith Alexander, por ejemplo. Esos esfuerzos finalmente culminaron en la **contratación de Team8 del almirante retirado Mike Rogers** , ex director de la NSA y del Ciber Comando de los EE. UU., como un "asesor principal". "He trabajado con los recursos altamente talentosos de la Unidad 8200 en el pasado y cuando tuve "La oportunidad de unirme a Team8, sabía que esta era una oportunidad valiosa", dijo Rogers sobre su contratación. Team8 describió la decisión de contratar a Rogers como "un instrumento para ayudar a desarrollar estrategias" en la expansión de Team8 en los Estados Unidos.

La contratación de Rogers por parte de una firma encabezada por el ex jefe de una agencia de inteligencia militar extranjera provocó **fuertes críticas** de los veteranos de la NSA. Uno de esos ex empleados de la NSA, Jake Williams, un veterano de la unidad de piratería Tailored Access Operations de la NSA, **le dijo a **
CyberScoop
que "Rogers no está siendo llevado a este cargo debido a su experiencia técnica... Es simplemente debido a su conocimiento de las operaciones clasificadas y su capacidad de influenciar a muchos en el gobierno de EE. UU. y contratistas del sector privado".

Además de los vínculos de Microsoft con la Unidad 8200 a través de sus conexiones con

Adallom, Illusive Networks y Team8, Microsoft también está **desarrollando vínculos directos** con los militares de Israel, y las FDI han adoptado la tecnología HoloLens de la compañía. El Departamento de Sistemas C2 de la FID
ha estado utilizando
un par de dispositivos HoloLens para adaptar la tecnología para su uso en la guerra durante los últimos tres años, un precursor de lo que seguramente será un lucrativo contrato militar para Microsoft, considerando que sus contratos HoloLens con las Fuerzas Armadas de los EE. UU. fue de
casi medio billón de dólares
.

Election Guard, un golpe incruento del complejo militar-industrial

Después de las elecciones de 2016 y las preocupaciones sobre los "hackers rusos" que se infiltraron en los sistemas electorales, las agencias federales como la NSA han utilizado esa amenaza para presionar por un mayor control sobre la democracia estadounidense. Por ejemplo, **durante una audiencia de 2017, el** entonces director de la NSA, el almirante Mike Rogers, declaró:

Si definimos la infraestructura electoral como fundamental para la nación y nos lo ordena el presidente o el secretario, puedo aplicar nuestras capacidades en asociación con otros, porque no seremos los únicos, el Departamento de Seguridad Nacional, el FBI. Puedo aplicar esas capacidades de manera proactiva con algunos de los propietarios de esos sistemas".

Rogers, que ahora está empleado por la compañía conectada a la inteligencia militar israelí y financiada por Microsoft, Team8, ha presionado para involucrar directamente a las agencias del gobierno de los EE. UU. Esas agencias deben supervisar las elecciones estadounidenses con particular facilidad, especialmente dado el pasado de Microsoft de la colaboración entre bambalinas con la NSA.

Dado que el sistema de Election Guard como se describe actualmente no es tan "seguro" ni "verificable" como afirma Microsoft, parece claro que los conflictos de intereses de sus desarrolladores, en particular sus conexiones con los militares de EE. UU. e Israel, son una receta para el desastre y equivalen a una toma del sistema electoral estadounidense por parte del complejo militar-industrial.

“La gran ironía y tragedia, aquí”, según el analista Jonathan Simon, “es que para que pudiéramos ir fácilmente en la dirección opuesta y rápidamente resolver todos los problemas de seguridad de las elecciones con ordenadores *en el* proceso de votación debemos estar dispuestos a invertir colectivamente el esfuerzo mínimo necesario para que los ciudadanos puedan contar los votos de manera visible en público como lo hacían antes. Si la democracia no vale ese esfuerzo, tal vez no la merecemos".