INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GESTIÓN DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

GUERRA HÍBRIDA Y CIBERGUERRA: EL ROL DE LAS TOPOLOGÍAS DE RED INTELIGENTES EN EL CONFLICTO ISRAEL-HEZBOLLÁH.

Integrantes del Grupo Nro 3:

LILIANA BEATRÍZ LOPEZ MEZANZA

EDUARDO ANDRÉS GALVEZ

ROBERTO ARMANDO GROSSO

Títulos Profesionales / de grado

Licenciada en Informática

Licenciado en Conducción y Gestión Operativa

Licenciado en Estrategia y Organización

08 de noviembre de 2024

Resumen

El presente trabajo de investigación, combina los conocimientos obtenidos de las diferentes materias dadas por los profesores y académicos y una investigación exploratoria y descriptiva realizada. A través de un estudio de caso se busca aportar nuevas ideas sobre la integración de los conceptos de Guerra Hibrida, Ciberguerra y Topologías de las Redes Inteligentes que se pueden llegar a vislumbrar en el ataque ocurrido en la "Operación Pagers", dirigido a Hezbollah.

En el mencionado evento identificamos los diferentes factores que poseen la capacidad de influir dentro del espectro de las operaciones, incidiendo dentro del ambiente del espacio en la Guerra Multidominio actual.

Para abordar esta temática, en la introducción y en el marco teórico se enuncian algunas de las definiciones de los términos más importantes que se analizan posteriormente para comprender las acciones ejecutadas por agentes del grupo Unidad 8200 y como las mismas pueden representar un cambio de paradigma en el concepto de Guerra Híbrida y sus implicancias.

En el primer capítulo se analiza como los medios cibernéticos y físicos empleados en el ataque a través de la cadena logística alterada, se transformaron en un elemento que tuvo gran impacto psicológico en las operaciones de las fuerzas de Hezbollah, haciendo que las mismas tengan un gran impacto en la continuidad de sus operaciones ofensivas contra Israel.

En el segundo capítulo, por un lado, se desarrolla el Análisis de ciberinteligencia de la Unidad 8200 para planificar ataques a pagers, explotando sus vulnerabilidades y finalmente cómo este nuevo modo de ciberataques puede lograr cambiar el paradigma para entender a una nueva forma de ciberguerra.

PALABRAS CLAVES: Guerra Hibrida, Ciberguerra, Topologías Inteligentes, Operación Pagers, Cadena Logística.

Índice General

Justificación / Fundamentación

El conflicto Israel-Hezbollah es un ejemplo paradigmático de la complejidad de la guerra híbrida y el ciberconflicto en el contexto del Medio Oriente. A través de un análisis histórico que abarca desde sus orígenes hasta la actualidad, se comprenden las múltiples capas de participación, la influencia del marco internacional y el papel decisivo de las unidades de inteligencia como la Unidad 8200 de Israel. A medida que el conflicto sigue evolucionando, las topologías inteligentes y las tecnologías emergentes seguirán transformando la naturaleza del enfrentamiento, obligando a los actores involucrados a adaptarse a un escenario en constante cambio.

El ataque del 17 de septiembre de 2024 contra Hezbollah, en el que explotaron dispositivos de comunicación personal se lo etiquetó “Operación Pagers”. Dicho ataque ejemplifica la guerra híbrida y la ciberguerra al combinar la capacidad de manipulación remota de tecnología con efectos físicos destructivos.

A fin de tratar de identificar al/los autores del mencionado ataque, se realizará un análisis de diferentes fuentes para determinarlos. Si bien la mayor parte de las fuentes sugieren a Israel desde el primer momento, su Gobierno al momento de realizar este trabajo, no confirma ni desmiente la autoría de estas operaciones. Sin embargo, fuentes oficiales que cita The New York Times y otros medios confirman que detrás de la misma está el Mossad, poderoso servicio de inteligencia israelí, junto con la Unidad 8200.

Planteamiento del problema

Ante este panorama, nos replanteamos la forma o técnicas en que los conceptos y definiciones de ciberguerra y guerra electrónica fueron empleados en la planificación y ejecución de esta innovadora forma de ataques cinéticos y el método empleado.

Este ataque representa una de las mayores brechas de seguridad para Hezbollah en años recientes. La operación no solo demostró el alcance de las capacidades cibernéticas de ataque de Israel, sino también su habilidad para penetrar los sistemas de comunicación de un grupo fundamentalista armado en un nivel extremadamente profundo, nunca antes visto.

Se observa cómo en la guerra híbrida, un ciberataque puede cruzar la frontera del ámbito digital para producir efectos cinéticos, es decir, daños físicos en el mundo real.

Esto conlleva un cambio de paradigma en los métodos empleados, llevando a replantear los conceptos de Redes Inteligentes, Ciberguerra y Guerra Hibrida, dando lugar a la formulación del problema de este trabajo.

Formulación del Problema

¿Se produjo un cambio de paradigma en la interpretación del empleo de los conceptos de la guerra hibrida y ciberguerra después de la "Operación Pagers" contra Hezbollah?

Solución Propuesta

Para dar respuesta a la hipótesis planteada, se debe realizar un estudio del caso, profundizando en un análisis de los hechos y contexto del conflicto, contemplando los eventos que se desataron con anterioridad y durante el ataque propiamente dicho.

De dicho análisis se determinarán los nuevos enfoques o nuevos paradigmas en los conceptos de Guerra Hibrida, Ciberguerra y la evolución de las redes inteligentes que la abarcan.

Objetivos

Principal o General

Analizar las técnicas empleadas en la "Operación Pagers" para determinar el cambio de paradigma en el concepto de guerra híbrida y ciberguerra.

Particulares o Intermedios

Objetivo Particular Nro 1

Describir los medios cibernéticos y físicos empleados en el ataque, analizando la alteración de la información en la web, la manipulación de la cadena logística, los dispositivos de comunicación y el posterior impacto psicológico producido en las filas de Hezbollah.

Objetivo Particular Nro 2

Explotar las técnicas de ciberinteligencia de la Unidad 8200 para planificar un ataque explotando vulnerabilidades en la tecnología y las vulnerabilidades de los Pagers.

Marco teórico

Definiciones

Guerra Híbrida.

Podemos citar que entendemos por Guerra híbrida a "*Una estrategia militar que combina elementos de la guerra convencional (fuerza militar directa) con tácticas irregulares como la insurgencia, el terrorismo, la ciberguerra, la propaganda y la influencia política"*.

Son acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. (Revista-CEERI-Global-N2-1-59-75)

Ciberguerra

Es la agresión promovida hacia un estado con la finalidad de dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para

sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos pero con la característica principal que el medio empleado no será la violencia física sino un ataque informático que va desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento (SANCHEZ MEDERO, 2010).

Topologías Inteligentes

No hay un concepto de este establecido desde el punto de vista que buscamos en este trabajo. Normalmente se lo toma como la integración de IA a las redes tradicionales. Nuestro enfoque está centrado a la unión de las redes Militares a las Redes Civiles y su utilización, no hacia la forma que tiene dicha topología (BUS, ESTRELLA, etc.).

Nuestra investigación sobre el rol de las topologías de red inteligentes en el conflicto Israel-Hezbollah resalta cómo la interconexión y la tecnología de la información han transformado las estrategias militares y la comunicación en escenarios de conflicto. Las redes inteligentes permiten una coordinación más efectiva de las operaciones y facilitan la recopilación y el análisis de datos en tiempo real, mejorando la toma de decisiones (Hassan, A. 2022).

Además, se explora la influencia de estas redes en la propaganda y la movilización social, así como su impacto en la seguridad cibernética. Este enfoque revela la dinámica evolutiva del conflicto contemporáneo y la necesidad de adaptarse a nuevas tecnologías. (Smith, J. 2023).

Para poder proponer una definición de cómo se utilizan las redes militares y civiles para la creación de una topología de red inteligente daremos a la misma como: *una arquitectura de red que, a través de mecanismos humanos/automatizados y protocolos avanzados, permite la interconexión concreta y segura de redes militares y civiles en Operaciones Militares*.

La misma facilita la transferencia de información, la colaboración en servicios y una respuesta unificada y coordinada en operaciones militares, circunstancia en la que también protege la información clasificada y la infraestructura crítica.

Algunas características fundamentales que deben tener son: la interoperabilidad, la escalabilidad, la seguridad, la resiliencia y la Adaptabilidad.

Técnicas de ciberinteligencia

La Ciberinteligencia es el conjunto de actividades de generación y difusión de conocimiento oportuno y veraz, basado en necesidades y requerimientos a fin de obtener el conocimiento de los escenarios de riesgos y capacidades, vulnerabilidades y formas de acción de los actores en el ciberespacio, para la toma de decisiones y la protección de Activos Críticos Nacionales (ACN).

Comprende la orientación del esfuerzo de búsqueda en la nube, la búsqueda y análisis de información en el ciberespacio, principalmente de fuente cerrada, cuyo producto final es la inteligencia que es diseminada para su utilización.

Entre las fases del Procesamiento de Información y la Orientación del Esfuerzo de Búsqueda se puede dar una reorientación, siempre que la información obtenida lleve a replantear la hipótesis inicial sobre un escenario de riesgo y consecuentemente se generen nuevas necesidades de información. (PINEDO LIMA, Jorge E., 2018)

Beepers o Buscapersonas

Los beepers, también conocidos como buscapersonas o pagers son unos pequeños dispositivos inalámbricos que se usaban comúnmente para enviar y recibir mensajes de texto cortos antes de que los teléfonos celulares se difundieran masivamente.

Los primeros, fueron patentados en 1949 por el ingeniero Alfred J. Gross, considerado como el inventor de los walkie-takie (comunicadores portátiles).

Los aparatos, los cuales funcionan enviando señales de radio a través de redes inalámbricas, fueron muy populares entre el personal médico, los empresarios y miembros de las fuerzas de seguridad y agencias gubernamentales en muchos países entre la década de 1980 y hasta principios del siglo XXI. Se utilizaban para una comunicación rápida en casos de emergencias o situaciones en las que las personas no podían responder a las llamadas directamente.

Estos dispositivos operan en frecuencias altas (FM) y en redes distintas a las telefónicas, pueden enviar mensajes a mayor distancia, sobre todo en zonas remotas y ofrece una mayor autonomía ya que emplea baterías de larga duración, de acuerdo a lo expresado por el ingeniero de sistemas Aditya Rayaprolu, en un artículo publicado en la revista Techjury. Asimismo, no pueden ser rastreados por GPS u otros medios.

Cuando una persona recibe un mensaje, los dispositivos emiten un tono o vibran para dejarle saber a sus propietarios sobre la recepción de un mensaje. (BBC, 2024)

Enfoque histórico del conflicto Israel-Hezbollah

Origen del conflicto

El conflicto entre Israel y Hezbollah tiene raíces profundas que se remontan a diversas tensiones regionales, políticas y religiosas en el Medio Oriente. La creación del Estado de Israel en 1948 marcó un punto de inflexión en la región, generando una serie de guerras árabes-israelíes y desarraigando a cientos de miles de palestinos, lo que cultivó un fuerte resentimiento hacia Israel. Hezbollah, que fue fundado en 1982 durante la invasión israelí del Líbano, surgió inicialmente como un grupo de resistencia para combatir la ocupación israelí de su territorio (Mansour, 2016).

La ideología de Hezbollah está profundamente influenciada por el islamismo chiita y la Revolución Islámica de 1979 en Irán, que promovió la idea de un "eje de resistencia" contra Israel y los Estados Unidos. En este contexto, Hezbollah se establece no solo como un actor militar sino también como un partido político y un proveedor de servicios sociales, lo que le ha permitido mantener una sólida base de apoyo en Líbano (Gordon, 2017).

Participantes del conflicto

El conflicto Israel-Hezbollah no es solo una confrontación bilateral, sino que involucra múltiples actores regionales e internacionales. Al lado de Hezbollah, se encuentran países como Irán, que proporciona apoyo militar y financiero al grupo, y Siria, que ha servido como un canal para el armamento y la logística (Wald, 2020). Por otro lado, Israel, con su Ejército de Defensa (IDF), busca mantener su seguridad nacional y proteger a sus ciudadanos de los ataques de Hezbollah y otros grupos militantes en la frontera norte.

Es crucial considerar el papel de las potencias mundiales en este conflicto, ya que Estados Unidos ha sido uno de los principales aliados de Israel, proveyendo asistencia militar y apoyo diplomático. Por otro lado, ciertos países árabes, aunque mayoritariamente han mantenido una postura conciliadora, a menudo son manipulados como parte del entramado regional que influencia la dinámica del conflicto (Khalil, 2019).

Marco internacional

El marco internacional que rodea el conflicto Israel-Hezbollah es intrincado. Las Resoluciones de la ONU, particularmente la Resolución 1701, adoptada en 2006 tras la Guerra del Líbano, establecieron un cese al fuego entre Israel y Hezbollah, pero no resolvieron las causas subyacentes del conflicto. Estas resoluciones están dirigidas a garantizar la soberanía del Líbano y la estabilidad regional, aun cuando en muchas ocasiones se cuestiona su

efectividad, especialmente en la hegemonía de Hezbollah en el sur del Líbano y su despliegue de armas (Sullivan, 2021).

Adicionalmente, la intervención de potencias extranjeras en conflictos del Medio Oriente, como Rusia y Turquía, han añadido una capa más de complejidad a las relaciones internacionales en esta problemática. La dinámica global actual, caracterizada por la rivalidad estadounidense-rusa y la influencia de potencias emergentes en la región, continúa moldeando el enfoque hacia el conflicto Israel-Hezbollah (Quigley, 2022).

Situación actual

La situación actual del conflicto Israel-Hezbollah está marcada por una tensa calma y un constante estado de alerta. Tras la última guerra en 2006, Hezbollah ha acumulado un significativo arsenal militar, estimado en decenas de miles de misiles y cohetes, muchos de los cuales pueden alcanzar el corazón de Israel (Lindsay, 2020). Israel, por su parte, ha intensificado sus operaciones ofensivas en Siria contra las instalaciones militares de Hezbollah, mientras que también ha implementado un enfoque defensivo a través del sistema de defensa antimisiles Iron Dome.

La reciente escalada de tensiones en la región, incluida la guerra civil en Siria, la crisis en Gaza y el debilitamiento de la autoridad central en Líbano, ha llevado a muchos analistas a prever un posible nuevo conflicto. Sin embargo, tanto Hezbollah como Israel parecen estar conscientes de las devastadoras consecuencias de una nueva confrontación y muestran una preocupación cautelosa por evitar una guerra abierta (Friedman, 2023).

Unidad 8200

La Unidad 8200 de las Fuerzas de Defensa de Israel (IDF) es uno de los elementos más críticos en el manejo del conflicto Israel-Hezbollah, siendo responsable de la inteligencia

militar y las operaciones cibernéticas. Este organismo ha desarrollado capacidades avanzadas para la recopilación de inteligencia, supervisión de actividades de Hezbollah y, en general, para estar un paso adelante en la guerra cibernética que acompaña a los conflictos convencionales (Brown, 2021).

La relevancia de la Unidad 8200 se extiende más allá de las fronteras de Israel, teniendo un impacto en las dinámicas de la guerra híbrida. La intersección de las operaciones de inteligencia y la capacidad de llevar a cabo ciberataques está redefiniendo las tácticas militares contemporáneas. Entre sus logros se destaca la interceptación de comunicaciones de Hezbollah y la neutralización de operaciones en tiempo real, influyendo en la toma de decisiones de la cúpula militar israelí (Zohar, 2022).

Metodología

Capítulo 1. Guerra Híbrida

En este trabajo final se analiza el ataque del 17 de septiembre a Hezbollah, del cual se desprende que en él se emplearon diferentes medios cibernéticos y físicos.

A su vez, se estudian las estrategias de encubrimiento utilizados como la creación de diferentes sitios web para tal fin, así como la manipulación y modificación de los dispositivos de comunicaciones empleados por miembros de Hezbollah.

Sección 1. Alteración de la información en la web.

De acuerdo a diferentes fuentes periodísticas se determinó que el Mossad llevó a cabo una manipulación de la información y creación de sitios falsos creando un velo de engaño en la operación, siendo un papel clave en el ataque.

En primera instancia, el Mossad explotó las redes sociales para difundir rumores sobre la inseguridad de los dispositivos de comunicación, incluyendo reportes de que incluso otros

dispositivos, como iPhone, podrían estallar. Esto contribuyó a un ambiente de miedo no solo dentro de Hezbollah sino también en la población civil.

Este tipo de manipulación buscaba amplificar el caos y la paranoia en torno a los dispositivos de comunicación que Hezbollah utilizaba, específicamente a través de mensajes y videos que se compartieron en redes sociales, provocando que los miembros de Hezbollah y la población en Líbano perdieran la confianza en sus propios dispositivos electrónicos.

De este modo, el Mossad empleó la desinformación y el pánico en el espacio digital para debilitar la cohesión de Hezbollah y alterar sus operaciones.

Posteriormente, una vez implantada la duda y desconfianza en los medios tecnológicos actuales, la operación incluyó tácticas como el registro de sitios web y perfiles en línea para dar autenticidad los dispositivos beepers, particularmente, los modelos Apollo AR924 y AP900, de la marca Gold Apollo y encubrir así la modificación de los dispositivos en la cadena de suministro. Se crearon tiendas en línea, páginas y publicaciones falsas que podrían engañar a Hezbollah, de acuerdo a una revisión de los archivos web realizada por Reuters.

El buscapersonas Apollo AR924 era algo voluminoso pero ideal para las condiciones de combate. Era impermeable y estaba equipado con una batería de larga duración que podía durar meses sin recarga. Sin embargo, su principal ventaja era su supuesta protección contra manipulaciones. Los líderes de Hezbollah quedaron tan impresionados que compraron 5.000 unidades y comenzaron a distribuirlas a los combatientes de nivel medio y al personal de apoyo en febrero.

Este enfoque innovador de guerra psicológica y cibernética se considera una escalada en el uso de desinformación y ataques de influencia digital, diseñados para debilitar e influir a un adversario incluso antes de un enfrentamiento directo.

Sección 2. Manipulación de la cadena logística

En la preparación de esta operación, se habrían usado diversas tácticas de infiltración y manipulación de la cadena logística, como la creación de una "historia de fondo" para la autenticidad del producto y el desarrollo de una red de suministro falsa que daba la impresión de fiabilidad.

La evidencia sobre la posible alteración de la cadena logística para los dispositivos utilizados en el ataque a Hezbollah proviene de varias fuentes de investigación en inteligencia.

Un reporte de *Reuters* detalla cómo los dispositivos, en particular los pagers, parecían pertenecer a una conocida marca taiwanesa, Gold Apollo, pero en realidad habían sido manipulados para incluir componentes personalizados que los hacían vulnerables a explosiones a distancia.

Sección 3: Alteración de los equipos beepers y radios.

Si bien no hay ninguna fuente que lo asegure, de acuerdo a diferentes artículos periodísticas consultados, se puede establecer que los agentes que alteraron los beepers modelos Apollo AR924 y AP900 diseñaron una batería que ocultaba una pequeña pero potente carga de explosivo plástico.

La mencionada batería, LI-BT783, estaba formada por una lámina delgada y cuadrada con seis gramos de explosivo plástico blanco tetra nitrato de pentaeritritol (PETN), colocada entre dos celdas de batería rectangulares. El espacio restante entre las celdas estaba ocupado por una tira de material altamente inflamable, e indetectable por rayos X, que actuó como detonador, según una fuente libanesa.

El componente de la bomba estaba tan cuidadosamente escondido que era casi imposible detectarlo, incluso si se desmontaba el dispositivo.

El 17 de septiembre, a las 15.30 horas en Líbano, los buscapersonas recibieron un mensaje supuestamente de la cúpula de Hezbollah, que activó los explosivos. Los aparatos estaban programados para sonar durante varios segundos antes de la explosión.

La activación de las explosiones ocurrió mediante una señal remota, aprovechando un mecanismo de doble botón que alentaba a los usuarios a manipular los dispositivos antes de que estos detonaran.

Un día después, se produjeron explosiones de los equipos de radios. Han surgido menos detalles sobre las explosiones de los walkie-talkies, pero una fuente de seguridad dijo a Reuters que Hezbollah los había comprado hace cinco meses, aproximadamente al mismo tiempo que se compraron los buscapersonas.

De las evidencias que se encontraron, se puede determinar que las explosiones de estos equipos, fueron más violentas que la de los beepers e iban dirigidas a los integrantes de Hezbollah con un rango medio dentro de la cúpula.

Sección 4. Impacto psicológico posterior al ataque

Del análisis realizado se puede observar que los estallidos de los aparatos, los cuales son utilizados por miembros de Hezbollah, dejaron doce muertos, entre ellos dos niños, y más de 2.800 heridos, muchos de gravedad, según autoridades del Ministerio de Salud libanés. Pero no solo Líbano fue afectado, sino también la vecina Siria, donde 14 personas resultaron heridas luego de que estallaran sus beepers, aseguró el Observatorio Sirio de Derechos Humanos.

Las explosiones de buscapersonas y walkie-talkies "representan un nuevo avance en la guerra donde las herramientas de comunicación se convierten en armas", dijo el alto comisionado de las Naciones Unidas para los Derechos Humanos Volker Türk. Añade que las explosiones han "desatado miedo, pánico y horror generalizados" en el Líbano y subraya que "esto no puede ser la nueva normalidad".

El Líbano aún está tratando de lidiar con la ola de ataques sin precedentes que no fueron realizados con misiles o drones, sino con buscapersonas y walkie-talkies que explotaron cuando quienes los portaban estaban haciendo compras o en casa con sus familias.

Incluso para una población que ha pasado por tanto en los últimos años (una grave crisis económica, la explosión del puerto de Beirut, protestas callejeras), el golpe psicológico ha sido inmenso, y se suma a la ansiedad de casi un año de ataques transfronterizos casi diarios entre Hezbollah e Israel.

Este tipo de ataque afecta la moral y la percepción de seguridad de los enemigos, dado que los dispositivos que eran considerados seguros y confiables se transformaron en amenazas.

Este aspecto de guerra psicológica refuerza el elemento de disuasión en conflictos asimétricos, donde la tecnología puede manipularse de forma oculta para generar temor e inseguridad.

Conclusiones Parciales

Este ataque ha sido calificado como una de las mayores brechas de seguridad en la historia de Hezbollah, subrayando la capacidad de Israel para realizar ciberataques con consecuencias físicas devastadoras.

La operación no solo demostró el alcance de las capacidades cibernéticas de Israel, sino también su habilidad para penetrar los sistemas de comunicación de un grupo armado en un nivel extremadamente profundo.

Esto ha llevado a Hezbollah a revisar sus procedimientos de seguridad y posiblemente a abandonar dispositivos vulnerables como los beepers, los cuales han sido ampliamente usados para evitar la interceptación directa de mensajes en teléfonos móviles

La combinación de guerra cibernética y manipulación física en esta operación refleja una estrategia de "guerra híbrida" que podría tener efectos duraderos en las tácticas de comunicación y organización de Hezbollah y otros grupos similares en la región.

Capítulo 2. Ciberguerra

Capítulo 2. Ciberguerra

Sección 1. Técnicas de Ciberinteligencia empleadas en la planificación del ataque.

Algunas fuentes indican que la primera parte del plan fue iniciada en Líbano en el año 2015. El concepto de la operación de buscapersonas surgió en 2022 y comenzó a implementarse más de un año antes del ataque de Hamas del 7 de octubre, informa The Washington Post. Desde ese momento, Israel se dedicó a emplear diferentes técnicas de ciberinteligencia como la manipulación de información en las redes sociales para condicionar el accionar de Hezbollah en la adquisición de los dispositivos de comunicación, así como la alteración de los mismos.

A su vez, la intervención de la Unidad 8200 en esta operación subraya la sofisticación en el uso de malware, manipulación de señales y control remoto de dispositivos para provocar sobrecargas que causen explosiones, lo que ilustra cómo la guerra cibernética se despliega sin una presencia física y con alto impacto sobre la infraestructura y el personal enemigo

Sección 2. Explotación de vulnerabilidades de la tecnología de los Pagers.

Analizando cómo se gestó y ejecutó el ataque a Hezbollah en el cual explotaron un gran número de dispositivos de comunicaciones que no poseían alto grado de tecnificación en sus sistemas, se observa que Israel explotó una vulnerabilidad que presentaba su topología de red en la forma de comunicarse, la cual consistía en emplear tecnología, que se consideraba obsoleta y segura de rastreos e interferencias en el envío de información ya que los mismos solo recibían, no transmitían.

Hezbollah se concentró en proteger el mensaje, dejando sin protección el medio que se empleaba, como lo eran los dispositivos en sí.

Este descuido y exceso de confianza llevo a Israel a planificar una operación brillante en la cual convirtió el canal en un arma, atacando y destruyendo su topología de comunicación que empleaba la cadena de comando del grupo terrorista.

Conclusiones Parciales

Los pagers fueron entregados a toda la cadena de comando de Hezbollah y sembraron una trampa explosiva en toda la red de mando. El golpe incapacitó a toda la estructura de un grupo que, por su verticalismo, es vulnerable a la pérdida de jefes.

Sin una cadena de comunicación activa y las filas de Hezbollah sumidas en la paranoia, resulta más complicado coordinar a una organización de 130.000 integrantes repartida en cientos de miles de km2, en dos países y con una compleja trama de instalaciones y sistemas de mando

Israel y las fuerzas especiales especialmente preparadas para la defensa de sus intereses, lograron producir una acción lo suficientemente eficiente que logro decapitar a casi todo el comando de Hezbollah en una sola acción que demostró la vulnerabilidad más importante de todo el sistema, sus dispositivos de comunicaciones.

Este tipo de operación destaca cómo los ataques cibernéticos permiten desactivar o debilitar al enemigo sin exponerse a represalias inmediatas, complicando las defensas tradicionales que no pueden interceptar o neutralizar ataques digitales en tiempo real.

Conclusiones finales

El ataque del 17 de septiembre de 2024 contra Hezbollah marca un nuevo paradigma en la guerra híbrida y los ciberataques al fusionar métodos de ciberinteligencia con efectos cinéticos en el campo de batalla. Este ataque va más allá de los ataques cibernéticos tradicionales, donde se afectan redes y sistemas digitales, al lograr manipular dispositivos de comunicación personales para que se convirtieran en armas de manera remota y sincronizada. Esta combinación de tecnología cibernética y efectos físicos introduce una innovadora modalidad en la que la infraestructura digital de un enemigo puede ser transformada en un vector de ataque directo, un enfoque que rompe con los límites convencionales de los ataques digitales y físicos.

Al emplear técnicas avanzadas de modificación en la cadena de suministro, como se hizo en este caso, el ataque representa una evolución en la guerra híbrida, donde la logística y la infraestructura civil pueden ser manipuladas antes de llegar al usuario final, permitiendo que dispositivos, aparentemente benignos, se conviertan en armas con consecuencias en el nivel estratégico nacional de los oponentes.

Este tipo de operación plantea desafíos de seguridad complejos para cualquier organización que dependa de tecnología comercial y crea un nivel de vulnerabilidad nuevo y difícil de contrarrestar.

Este caso establece nuevos precedentes donde los ciberataques puedan tener consecuencias directas y devastadoras en el mundo físico, y apunta a la necesidad de que los estados adapten sus políticas y acciones de defensa a esta nueva forma de guerra híbrida, donde tanto el hardware como el software de uso común pueden convertirse en amenazas.

Este incidente marca un importante punto de inflexión en las tácticas donde se combinan las acciones de la guerra híbrida con el concepto de ciberguerra actual.

Referencias

Brown, A. (2021). Israeli Military Intelligence: Organizational Evolution and Adaptation. Journal of Military History, 85(2), 145-162.

Friedman, T. L. (2023). New Alignments in the Middle East: Analyzing Israel and Hezbollah's Future. Foreign Affairs.

Gordon, P. R. (2017). Hezbollah: A Force to Be Reckoned With. Middle East Review of International Affairs, 21(1), 23-37.

Khalil, S. (2019). Regional Dynamics: The Lebanese Hezbollah in Context. Peace and Security in the Middle East, 17(1), 75-92.

Lindsay, J. (2020). The Changing Nature of Warfare: The Case of Hezbollah. Armed Forces & Society, 46(4), 605-639.

Mansour, R. (2016). Understanding Hezbollah’s Strategy and Tactics. Journal of Conflict Studies, 28(1), 111-127.

Quigley, F. (2022). International Relations and the Israel-Hezbollah Conflict: Implications for Regional Stability. International Journal of Middle East Studies, 54(3), 423-444.

Sullivan, K. (2021). The United Nations and the Israeli-Lebanese Conflict: A Critical Review. Global Security Studies, 12(1), 58-73.

Wald, R. (2020). Iran’s Role in Supporting Hezbollah: A Geopolitical Perspective. Journal of Strategic Studies, 43(5), 745-763.

Zohar, Y. (2022). Cyber Warfare and Intelligence in Israel: A New Era of Military Operations. Cyber Conflict, 4(2), 90-105.

Hassan, A. (2022). The impact of smart networks on conflict dynamics: A case study of Israel-Hezbollah. Journal of Conflict Resolution, 66(5), 1083-1107.

Smith, J. (2023). Digital warfare and smart networks: Transforming military strategy in the Middle East. Military Technology Review, 45(3), 45-58.

Pinedo Lima, Jorge Enrique Leon (2018). Aplicación de la ciberinteligencia en el proceso de inteligencia en la dirección de inteligencia del ejército del Perú

Sanchez Medero, (2010) p. 64). ReDiU_1847_art5-La ciberguerra y derecho internacional humanitario

Ignacio Montes de Oca, Operación Pagers, que se sabe de la acción de Israel y cuáles son sus consecuencias. 18set24

https://www.patreon.com/posts/operacion-pagers-112300083

Operación Pagers: qué se sabe de la acción de Israel y cuáles son sus consecuencias. 18set24

https://www.pucara.org/post/operaci%C3%B3n-pagers-qu%C3%A9-se-sabe-de-la-acci%C3%B3n-de-israel-y-cu%C3%A1les-son-sus-consecuencias

Explosión de los 'busca' (beepers) de Hezbollah: ¿Cómo ha podido ocurrir esto? 18set2024

https://hipertextual.com/2024/09/explosion-beepers-hezbola-que-ha-sucedido-y-como

Revelaron más detalles sobre las explosiones de los buscapersonas de Hezbollah: el talón de Aquiles de los aparatos - 16oct24

https://www.infobae.com/america/mundo/2024/10/16/revelaron-mas-detalles-sobre-las-explosiones-de-los-buscapersonas-de-hezbollah-el-talon-de-aquiles-de-los-aparatos/

Informes en vivo BBC. 19Sep24

https://www.bbc.com/news/live/cwyl9048gx8t

Israel colocó explosivos en buscapersonas dirigidos a Hezbollah (actualizado). 19Set24

https://blog.segu-info.com.ar/2024/09/israel-coloco-explosivos-en.html

Explosiones de dispositivos de Hezbollah: ¿cómo explotaron los buscapersonas y los walkie-talkies y qué sabemos sobre los ataques? 19Set24

https://www.theguardian.com/world/2024/sep/18/hezbollah-pagers-what-do-we-know-about-how-the-attack-happened

AP-900: Esto es lo que sabemos sobre uno de los buscapersonas que explotaron en el Líbano https://www.trtworld.com/middle-east/ap-900-this-what-we-know-about-one-of-the-pagers-that-exploded-in-lebanon-18209359

BBC (2024). Qué son los *beepers* y por qué esta tecnología de hace décadas sigue siendo utilizada por Hezbollah. 18Set24 https://www.bbc.com/mundo/articles/cjwd0xv4997o

Cómo el voluminoso buscapersonas engañó a Hezbollah. 16Oct24 https://www.jpost.com/israel-news/article-824901

La operación de buscapersonas del Mossad: el Washington Post descubre cómo Israel se infiltró en Hezbollah. 06Oct24 https://newsukraine.rbc.ua/news/mossad-s-pager-operation-washington-post-1728189332.html

¿Quién está detrás de las explosiones de buscapersonas en el Líbano? ¿Responderá Hezbollah? https://newsukraine.rbc.ua/news/who-is-behind-pager-explosions-in-lebanon-1726655980.html

Lo que se sabe del estallido de buscas de Hezbollah: la manipulación con explosivos y las consecuencias https://www.libertaddigital.com/internacional/oriente-medio/2024-09-18/las-claves-de-la-explosion-de-buscas-de-hezbola-explosivos-ejecucion-del-plan-y-consecuencias-7164583/?utm_campaign=url_rewrite&utm_medium=Social&utm_source=Twitter

Cómo la inteligencia de Israel engañó a Hezbollah con los beepers explosivos https://www.lanacion.com.ar/el-mundo/como-la-inteligencia-de-israel-engano-a-hezbollah-con-los-beepers-explosivos-nid16102024/

XXVII Curso internacional de defensa “Amenaza Híbrida, La Guerra imprevisible” año 2019.

Revista-CEERI-Global-N2-1-59-75. Amenazas híbridas: nuevas herramientas para viejas aspiraciones. 12dic18

https://www.realinstitutoelcano.org/documento-de-trabajo/amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones/

Ciberseguridad y guerra híbrida: La ampliación del espectro. 26set23

https://www.unav.edu/web/global-affairs/ciberseguridad-y-guerra-hibrida-la-ampliacion-del-espectro

Revista de Estudios en Seguridad Internacional: Conflicto en Ucrania. Cuando la estrategia híbrida no funciona

https://seguridadinternacional.es/resi/html/conflicto-en-ucrania-cuando-la-estrategia-hibrida-no-funciona/