INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

USO DE LA TECNOLOGÍA 5G EN GUERRA ELECTRONICA Y CIBERDEFENSA

Integrantes del Equipo Nro 1:

ARMANDO OSVALDO DI CHIARA

JOSE ALBERTO COPETTI

VICTOR EDUARDO ALLAR

MAURO HUGO REALI MORRONE

Títulos Profesionales / de Grado

Ingeniero Electrónico

Ingeniero Electrónico

Técnico Superior en Electrónica Digital

Analista de Sistemas de Computación

19 de noviembre de 2024

Resumen

Los Conflictos modernos se caracterizan por ser operaciones del tipo Multidominio (o tipo capas), donde el denominador común que encontramos para este caso especial es que el dominio donde la tecnología 5G, la Guerra Electrónica y la Ciberdefensa se desarrollan, es un dominio INTANGIBLE.

En ese contexto, las Operaciones Multidominio (capas) son una eficiente e innovadora solución táctica para enfrentar las nuevas amenazas que se presentan en el escenario geopolítico actual. Este nuevo paradigma táctico-operacional es una integración sinérgica entre tecnología, entrenamiento y liderazgo. Su propósito principal es mantener la iniciativa, la libertad de acción y de maniobra en todas las dimensiones del campo de batalla, mediante acciones bélicas directas y no directas, con capacidad de apoyar a fuerzas conjuntas y combinadas en todo tipo de escenario y de respuesta casi inmediata.

Los tres elementos mencionados apuntan al funcionamiento y protección de los elementos de comando y las infraestructuras críticas. Indudablemente estamos en presencia de elementos de interés nacional, que requiere ser abordado de manera integral a nivel nacional para velar por los intereses de los argentinos, aunando los diferentes esfuerzos contra el accionar de actores indeseados que buscan afectar los sistemas e Infraestructuras Críticas (IICC) usando especialmente este dominio para el desarrollo de sus acciones.

El presente trabajo de investigación de diplomatura, que a su vez integra las diferentes materias y clases brindadas por los profesores, busca aportar ideas que contribuyan a la determinación de la interacción de las redes 5G y las actividades de Guerra Electrónica y Ciberdefensa dentro de las operaciones multidominio.

Para abordar esta temática, en la introducción y marco teórico se describen sucintamente como se caracterizan las operaciones multidominio, describir las acciones de Guerra Electrónica y Ciberdefensa, para finalizar con algunas de las acciones desarrolladas por países donde las redes 5G ya se encuentran en total integración y funcionamiento y que por situaciones generadas por los conflictos de Ucrania y Rusia, deben tomar aspectos bélicos.

En el primer capítulo se analizan las Operaciones Multidominio (capas), las capacidades de las redes 5G, sus potencialidades y sus debilidades, y sus estructuras internas

En el segundo capítulo, como se pueden integrar las actividades de Guerra Electrónica y las de Ciberdefensa, a las mencionadas redes 5G.

Palabras Claves: operaciones multidominio (capas), 5G, Guerra Electrónica, Ciberdefensa

Índice General

Justificación / Fundamentación / Aportes

La evolución de las amenazas en el ciberespacio permite que tanto individuos como grupos de terroristas o Estados Nación lo utilicen para realizar ciberataques. Por lo visto en el reciente conflicto entre Ucrania y Rusia, donde se cumplieron los pasos de los modernos Conflictos Multidominio.

En Estados Unidos, la «Estrategia 5G», aprobada el 2 de mayo de 2020, estipula que «*el Departamento de Defensa de los Estados Unidos debe desarrollar y utilizar nuevos conceptos operacionales que utilizan la omnipresente conectividad que ofrece la 5G para incrementar la eficiencia, la resiliencia, la velocidad y la letalidad de nuestras fuerzas armadas*».

Es por ello que ya está experimentando con aplicaciones militares de esa tecnología (5G) en 5 bases de las fuerzas aéreas, navales y terrestres.

Los expertos estiman que la 5G tendrá un papel determinante en el desarrollo de las armas hipersónicas, incluyendo las de tipo nuclear. Para guiar esas armas en trayectorias variables, haciéndolas escapar a los misiles interceptores, es necesario recoger, elaborar y transmitir enormes cantidades de datos en lapsos de tiempo muy reducidos. Lo mismo se hace necesario a la hora de activar las defensas, en caso de ataque, confiando dicha defensa a sistemas automáticos.

La tecnología 5G tendrá también un papel clave en la llamada «red de batalla» (battle network) ya que es capaz de vincular entre sí millones de dispositivos de transmisión y recepción en áreas determinadas.

La 5G será extremadamente importante para los elementos de inteligencia y las fuerzas de despliegue rápido ya que hará posible el uso de sistemas de obtención de información mucho más eficaces, e incrementará la letalidad de los sistemas de drones y municiones inteligentes.

Las redes de 5G trabajando en conjunción con lo aportado por los sistemas de Guerra Electrónica permitirán un flujo de información más ágil y veloz.

Planteamiento del Problema

Relacionado con el planteo del problema, y como se expresó precedentemente en el resumen, el presente trabajo integrador final analizará la posibilidad de integrar la información producida por los Sistemas de Guerra Electrónica, y las acciones de la Ciberseguridad con las futuras redes de 5G que se instalen el país, en un ambiente de Operaciones Multidominio.

Formulación del Problema

Integrar la tecnología de las futuras redes 5G al Sistema de Defensa del Estado Argentino dentro de las estructuras de Guerra Electrónica y Ciberdefensa, en apoyo de las Operaciones Multidominio.

Solución Propuesta

Para dar respuesta al problema planteado, y dado el carácter específico de las operaciones Multidominio y de las tecnologías involucradas en las mismas, el equipo considera que es menester contar con una integración entre las redes tácticas actuales con la nueva red 5G.

Asimismo, para alcanzar dicha solución a la problemática planteada, el equipo pretende alcanzar los objetivos de acuerdo a cómo se detallan a continuación.

Objetivos

Principal o General

Analizar las ventajas de crear una estructura de apoyo basándose en las redes 5G a las actividades que desarrollan las FFAA en las Operaciones Multidominio.

Particulares o Intermedios

Objetivo Particular Nro 1.

Analizar las características de las Operaciones Multidominio, desde el punto de vista de la Guerra Electrónica y la Ciberdefensa.

Objetivo Particular Nro 2.

Determinar la integración de las redes 5G en las estructuras de Ciberdefensa y Guerra Electrónica con que ya cuentan las FFAA en el quinto dominio. Analizando sus capacidades y sus vulnerabilidades.

Marco Teórico

Al investigar el estado del arte y el marco teórico del tema propuesto, se puede destacar que la doctrina sobre las Operaciones Multidominio no se encuentra al día de hoy publicada en nuestras FFAA, no obstante el tema en sí, es ya de conocimiento y hay numerosos artículos escritos respecto del mismo, apreciándose que a la brevedad se publicara doctrina propia al respecto, modificando el término Multidominio por Multicapas.

No obstante, la nomenclatura, la concepción de Operaciones Multidominio (capas) es ya al día de hoy aceptada en el marco de la OTAN, y tomando el reciente conflicto entre Ucrania y Rusia, en donde la OTAN interviene solapadamente, mediante el suministro de equipos específicos y doctrina. Ambos contendientes han realizado operaciones basándose en estos conceptos.

Metodología

El método a emplear para desarrollar el trabajo de investigación será del tipo deductivo, con ciertas inferencias inductivas, para ello se realizarán distintos análisis y descripciones durante el desarrollo de cada capítulo a fin de obtener conclusiones parciales surgidas de cada uno de ellos y que permitan dar respuesta al objetivo general planteado por la investigación.

Capítulo 1

Operaciones y tecnologías

Como se expresara en la introducción, en el presente capítulo se analizarán las características de la Operaciones Multidominio de Guerra Electrónica y de Ciberdefensa con el objetivo de extraer conclusiones e identificar sus características distintivas para su integración con las redes 5G.

Sección 1

Características de las Operaciones Multidominio (capas)

En los actuales contextos internacionales y sumados a ello, los radicales cambios tecnológicos que aparecen día a día, hacen que cada guerra posea sus características propias y que, si bien podrán existir similitudes entre algunas, no serán iguales en su totalidad.

Se diferenciarán unas de otras por la tecnología empleada, el tipo de gobierno, la organización militar, la cultura de los combatientes implicados, etc, es decir, por los aspectos diferenciadores que proporcionan la dinámica particular de una guerra determinada. Aunque mayormente en occidente se ha conservado una filosofía Clausewitziana, existen también actores internacionales que han optado por un enfoque similar al del estratega militar Sun Tzu, quien estableció que: “Someter al enemigo sin luchar es el colmo de la destreza”.

En la actualidad, también se manejan conceptos novedosos como el de “Guerra Irrestricta”, cuyo origen se sitúa en oriente, e incorpora el concepto de que "*usando todos los métodos, incluyendo fuerzas armadas o fuerzas no armadas, militares y no militares, letales y no letales, para imponer al enemigo aceptar nuestros propios intereses*” se amplía el concepto guerra a partir de las nuevas posibilidades de ejercer la violencia, las que no se limitan sólo a las operaciones militares.

Es por consiguiente que el concepto de que las Operaciones Multidominio mantienen la definición tradicional de guerra, pero entendiendo que las acciones por debajo del umbral del conflicto actualmente forman parte de ella. Operar en este entorno cada vez más interconectado entre diferentes dominios puede ser el reto más importante entre el éxito y el fracaso. El desafío consistirá en superar la predilección de lo ya conocido, ser capaces de entender el cambio y utilizar la creatividad y el pensamiento crítico al planificar operaciones eficientes para la guerra venidera.

Esta tarea no es fácil, sin embargo, un hecho algo reconfortante es que la misma no es nueva.

Como se mencionó anteriormente, en el escenario internacional actual, muchos actores que optan por explotar las condiciones del ambiente operacional para lograr sus objetivos sin recurrir al conflicto armado, fracturando las alianzas, las asociaciones y la determinación de sus oponentes. Intentan crear una situación de distanciamiento mediante la integración de acciones diplomáticas y económicas, guerra no convencional, de información (medios de comunicación, falsas narrativas, ciberataques, etc.), y el empleo disuasivo o real de sus fuerzas convencionales. Al crear inestabilidad dentro de los países y alianzas *de sus adversarios*, buscan generar una separación política que da

lugar a una ambigüedad estratégica que reduce la velocidad de reconocimiento, decisión y reacción de los actores que cooperan entre sí.

A través de estas acciones, la meta es alcanzar objetivos por debajo del umbral del conflicto armado.

En este sentido, las OPERACIONES MULTIDOMINIO son operaciones planificadas y ejecutadas por una Fuerza Conjunta para contrarrestar y derrotar a un adversario con capacidad de disputar en todos los dominios (aire, tierra, mar, información, espacio, ciberespacio, etc.) **tanto sea antes del conflicto armado, como durante el mismo**.

Resumiendo:

En primera medida, las Operaciones Multidominio son aquellas que se desarrollan en un espacio tanto **físico** (dominio terrestre, marítimo, aéreo y espacio exterior) como **intangible** (dominio ciber: incluye el espectro electromagnético y el conocimiento), se entiende a este último como la información y la opinión que fluye en “la nube” (cloud computing) vertida por los medios de comunicación en los distintos portales de noticias y en las redes sociales.

La segunda variable y más importante es que las Operaciones Multidominio comienzan a ***desarrollarse mucho antes del conflicto armado mismo***, incluso anterior a su gestación durante la etapa de crisis, estando dirigidas hacia aquellos Estados o grupo de Estados considerados enemigos.

La tercera condición para desarrollar estas operaciones está dada en convertir debilidades del oponente en vulnerabilidades, sobre distintas áreas, zonas o espacios en forma simultánea, con la finalidad de generar caos y confusión en la toma de las decisiones.

La cuarta condición está signada por la descentralización y disminución, hacia niveles subalternos, de la autorización para empeñar los fuegos de largo alcance sobre objetivos identificados como blancos de prioridad. A su vez existen dos condiciones como consecuencia de la implementación de las anteriores; que es, por un lado, el desarrollo de la inteligencia artificial con el fin de reunir, procesar y analizar el gran volumen de información que se recibe, para disminuir exponencialmente el tiempo empleado en el ciclo OODA (observar, orientar, decidir y actuar) para la toma de la decisión.

En resumen, básicamente este tipo de operaciones sienta sus bases sobre el control del dominio espacial y ciber, el desarrollo tecnológico y la inteligencia artificial.

De esta forma, los distintos medios de obtención distribuidos tanto en tierra, mar, aire y espacio identificarán distintas amenazas aportando dicha información a “la nube”. A partir de allí, los sensores

de superficie tripulados y no tripulados procesarán la información determinando qué plataforma o sistema de armas será el más conveniente para neutralizar la amenaza.

Sección 2
Tecnología de las redes 5G

Las redes 5G ofrecen una amplia gama de características y avances técnicos que las distinguen y las sitúan por encima de las generaciones anteriores de redes móviles. A pesar de sus ventajas, diversas organizaciones y entidades europeas, incluyendo la Comisión Europea, la Agencia Europea de Ciberseguridad (ENISA) y el Grupo de Cooperación NIS, han expresado **preocupaciones acerca de un aumento significativo en los riesgos de seguridad asociados con las redes 5G en comparación con las generaciones previas de redes móviles.** Estos riesgos están estrechamente vinculados a la **disponibilidad, integridad, privacidad, confidencialidad y accesibilidad de las redes.**

Adicionalmente, se han identificado **aspectos críticos relacionados con la proliferación de proveedores y operadores en las cadenas de suministro, así como con la inseguridad del suministro debido a la dependencia de un único proveedor**. Estas preocupaciones subrayan la necesidad de abordar los riesgos de seguridad en las redes 5G de manera proactiva y de desarrollar estrategias que garanticen la protección adecuada de la infraestructura.

La tecnología 5G está creando una red aún más interconectada, donde los dispositivos con diferentes capacidades y restricciones de calidad de servicio deben interoperar de manera efectiva.

En comparación con las generaciones anteriores, se espera que 5G resuelva seis desafíos: mayor capacidad, mayor velocidad de datos, menor latencia de extremo a extremo, conectividad masiva de dispositivos, reducción de costos y calidad de servicio constante.

Sin embargo, también se presenta un nuevo desafío: las capacidades de los atacantes han aumentado en comparación con las generaciones anteriores. De hecho, el poder computacional de los dispositivos móviles actuales permite lanzar ataques complicados desde el interior de la red móvil. Además, los tipos de ataques y malwares generados son más eficientes y efectivos que los enfrentados por generaciones anteriores. Por lo tanto, es fundamental implementar medidas de seguridad más rigurosas para proteger la red y los dispositivos conectados.

Debido a la mayor cantidad de servicios y dispositivos conectados, y a pesar de la medida de seguridad introducida, 5G aún puede ser vulnerable a diferentes tipos de ataques. En las siguientes secciones discutiremos las vulnerabilidades identificadas, organizando las tecnologías y los vectores de amenazas asociados según el modelo OSI

5G se refiere a la quinta generación de la capacidad de red inalámbrica para teléfonos móviles. Ha captado atención y entusiasmo debido a su capacidad para conectar a personas, objetos y dispositivos de manera más frecuente y fluida que nunca, junto con sus mayores velocidades de red, latencia extremadamente baja y un rendimiento de red más confiable. Se encuentra relativamente temprano en su evolución, pero las previsiones predicen que habrá más de 3.5 mil millones de conexiones 5G en todo el mundo para 2025. Gobiernos y empresas anticipan muchos cambios en nuestra forma de vivir y hacer negocios. Con esta nueva iteración de la tecnología móvil, se espera que el 5G esté en uso durante al menos un par de décadas más, hasta que se desarrolle la tecnología 6G. Como resultado, es importante considerar el impacto y los nuevos desafíos que 5G traerá y tendrá sobre la ciberseguridad. Adoptar nueva tecnología sin consideraciones de ciberseguridad puede impactar significativamente la seguridad y protección de los gobiernos, el público y las empresas en todos los niveles. Cada uno debe compartir la responsabilidad de la concienciación sobre la ciberseguridad del 5G, tomando medidas para remediar vulnerabilidades y mitigar los problemas asociados con la tecnología 5G.

La red 5G frente a las generaciones anteriores

Para explorar completamente lo que 5G significa para la ciberseguridad, es útil examinar más de cerca la tecnología móvil del pasado y por qué el salto de 4G a 5G es diferente al cambio entre otras generaciones de redes de telefonía móvil.

- **Primera generación (1G):** Desde la década de 1980, la red retrospectivamente denominada 1G ofreció a los usuarios tecnología de voz analógica, funcionando sobre un área geográfica con transmisores de radio de baja potencia.

- **Segunda generación (2G)** - A principios de la década de 1990, la segunda generación introdujo capacidades digitales y servicios de SMS y MMS. Las conversaciones telefónicas se cifraban entre el teléfono y la estación base celular, si no en toda la red. La tecnología digital permitió que los teléfonos móviles utilizaran las frecuencias de radio de manera más eficiente, ya que más usuarios podían utilizar cada banda de frecuencia. El Servicio de Paquetes de Radio General (GPRS) ofrecía velocidades de hasta 5 kB/s, mientras que la adición de las Mejores Tasas de Datos para la Evolución GSM (EDGE) mejoró las velocidades hasta un máximo teórico de 48 kB/s

- **Tercera generación (3G)** : A mediados de 2001 se introdujo la transmisión de datos móviles, permitiendo llamadas de video, televisión móvil y acceso a Internet inalámbrico fijo. La velocidad de conexión promedio era de 3 Mbps, 30 veces más rápida que la velocidad promedio de 2G, mientras que las velocidades máximas estaban en el rango de 7 Mbps. La tecnología iPhone y Android también fue fundamental para aumentar la popularidad de la comunicación móvil, con la

introducción de los smartphones y el uso del término banda ancha móvil para esta tecnología inalámbrica. La 3G vio mejoras en la seguridad en comparación con generaciones anteriores porque el equipo del usuario podía autenticar una red antes de conectarse. Esta generación de redes utilizó un cifrado de bloque KASUMI actualizado para mejorar la seguridad de la infraestructura de red}.

- **Cuarta generación (4G)**: En la década de 2010, los consumidores comenzaron a acceder a la red celular de banda ancha 4G. Cumpliendo con las especificaciones de la Unión Internacional de Telecomunicaciones (UIT), 4G permitió a los usuarios acceder a servicios de telefonía IP, videoconferencias y juegos. Las velocidades máximas eran de 150 Mbit/s para descargas y 5 Mbit/s para cargas, mejorando enormemente la experiencia del usuario. La UIT incluyó la Evolución a Largo Plazo (LTE) en su definición de 4G desde 2010, mejorando las velocidades típicas a través de mejoras en la red central y utilizando una interfaz de radio diferente

- **Quinta generación (5G)**

5G representa una banda ancha móvil mejorada, que permite una mayor conectividad, incluyendo el Internet de las Cosas (IoT) y otros servicios y despliegues potenciales. Estos servicios pueden incluir logística digitalizada, cirugía remota (con latencia de tan solo un milisegundo) y procesos agrícolas más precisos utilizando drones.

La quinta generación de tecnología de redes móviles también pretende ser más confiable para los usuarios, con una latencia despreciable (hasta diez veces menor que la de 4G, típicamente alrededor de cuatro milisegundos), ofreciendo una mejor experiencia para consumidores individuales y empresas, con velocidades de descarga de hasta 10 gigabits por segundo, lo que equivale a alrededor de 100 veces más rápido que 4G.

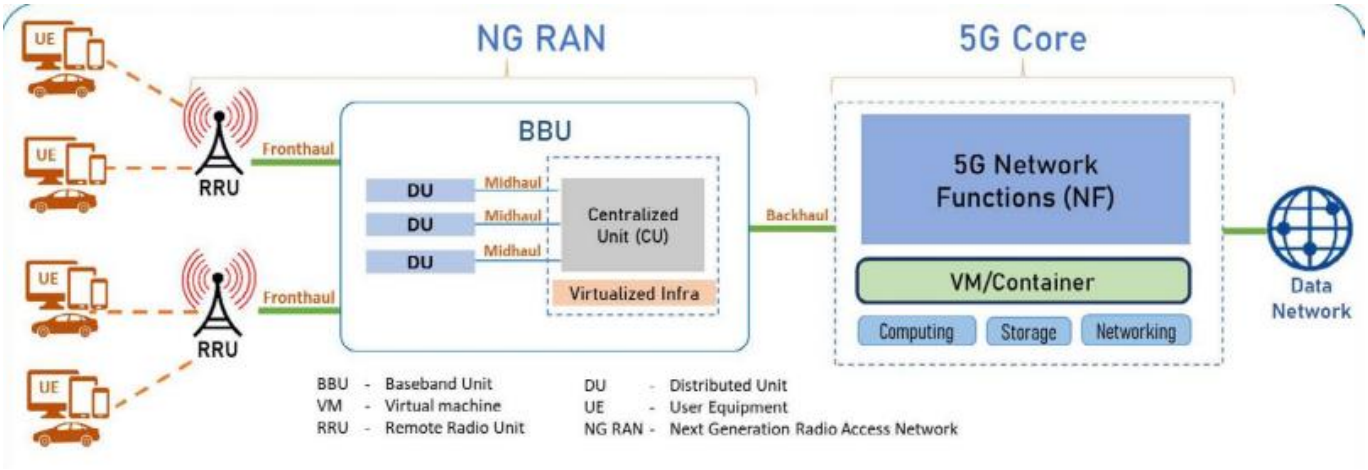
La transición de 4G a 5G continúa siendo apoyada por el Proyecto de Asociación de Tercera Generación (3GPP). Formado en 1998, el 3GPP es una iniciativa global que une a siete organizaciones de desarrollo de estándares de telecomunicaciones. Juntos, buscan maximizar la compatibilidad entre 5G y la infraestructura y equipos heredados para facilitar la transición hacia 5G y futuras redes, asegurando un ecosistema continuo, robusto y ampliamente disponible de extremo a extremo que sea compatible hacia atrás y hacia adelante.

Como una revisión de la arquitectura tradicional, 5G puede soportar servicios y tecnologías emergentes que hubieran sido imposibles con generaciones anteriores. Esto significa que 5G tendrá un gran impacto en la infraestructura crítica. En comparación con generaciones anteriores de infraestructura celular, 5G no solo es una red más rápida. Se diferencia enormemente en términos de funcionalidad, capacidad, accesibilidad, alcance y potencial.

Arquitectura General de la Red 5G

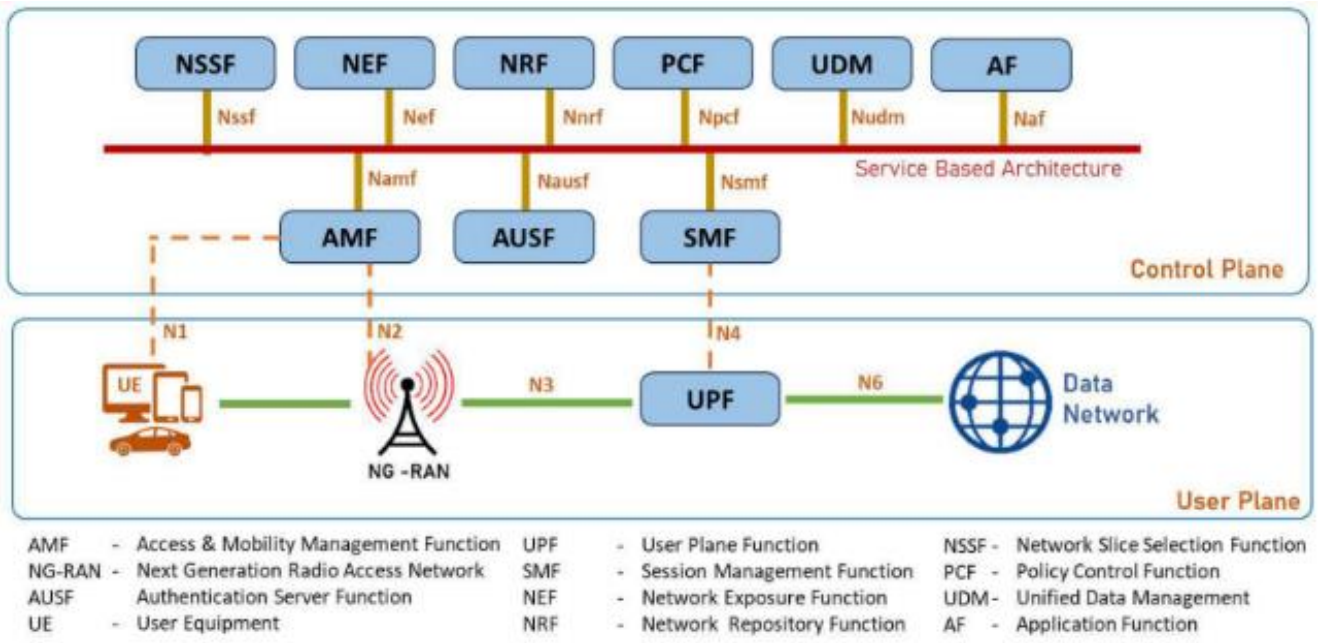
Fuente: 5G Network Management System With Machine Learning Based Analytics - M. Ramachandran et al IEE Access – Creative Commons Attiburion-NonCommercial-NoDerivatives 4.0 Licence.

Referencias externas: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity



Arquitectura de los servicios de Core de la Red 5G

Fuente: 5G Network Management System With Machine Learning Based Analytics - M. Ramachandran et al IEE Access – Creative Commons Attiburion-NonCommercial-NoDerivatives 4.0 Licence.



Las principales diferencias entre 4G y 5G son:

Velocidad

La 5G ofrece velocidades de descarga hasta 100 veces más rápidas que la 4G, alcanzando varios Gbps.

Latencia

La 5G tiene una latencia mucho más baja, de entre 1 ms y 10 ms, mientras que la 4G tiene una latencia mínima de 30-40 ms.

Número de dispositivos conectados

La 5G puede soportar hasta 1 millón de dispositivos por kilómetro cuadrado, mientras que el 4G tiene una capacidad menor.

Tecnología

La 5G utiliza ondas de radio de alta frecuencia, mientras que la 4G LTE utiliza una tecnología diferente.

Eficiencia energética

La 5G es más eficiente en términos de energía gracias a mejoras tecnológicas y a una gestión más inteligente de la red.

Desafíos de la ciberseguridad 5G

Con la tecnología 5G, surgen nuevos desafíos de Ciberseguridad y riesgos de seguridad que deben ser abordados antes de su adopción generalizada. Dado que la implementación de 5G implica esencialmente una revisión completa de redes y tecnologías más antiguas, los factores que la convierten en una tecnología emocionante y empoderadora también la hacen una preocupación para todos, no solo para los profesionales de Ciberseguridad.

Además, dado que 5G será la primera red completamente basada en software, los desarrolladores no tendrán más opción que utilizar la red y crear aplicaciones en 5G. Las implicaciones de un posible hackeo de la red son enormes, ya que el enrutamiento digital y la gestión de redes basados en software crean nuevas vulnerabilidades que deben ser aseguradas.

A continuación, se presentan algunos ejemplos de las áreas que están cada vez más conectadas y, por lo tanto, en mayor riesgo debido al ancho de banda y la conectividad de 5G:

- Aviación
- Drones
- IoT

- Máquinas de votación

Los principales desafíos de la Ciberseguridad en 5G podrían categorizarse de la siguiente manera:

- Nueva tecnología
- Vulnerabilidad del software
- IoT y conectividad
- Falta de seguridad integrada
- Problemas de protección de datos
- Potencial de DDoS
- Ancho de banda
- Disponibilidad generalizada

Nueva tecnología

Dado que la tecnología 5G se encuentra en una etapa temprana de su desarrollo, aún queda mucho por saber sobre su implementación. Si bien organizaciones como el 3GPP y profesionales de la Ciberseguridad de todo el mundo están ayudando a que la tecnología 5G sea segura, confiable y accesible, aún forma parte de un panorama tecnológico que cambia rápidamente y que presenta muchos riesgos desconocidos.

Se requiere más concientización, inversión y políticas gubernamentales para identificar y abordar los problemas potenciales de la infraestructura 5G, cuya responsabilidad debe ser compartida entre los gobiernos y las empresas 5G.

Sin embargo, con técnicas de Ciberseguridad de vanguardia, incluido el uso de inteligencia artificial (IA), aprendizaje automático, gestión en tiempo real, detección y servicios de respuesta, las soluciones integrales de Ciberseguridad pueden ayudar a orientar la implementación de 5G y mantener a las organizaciones lo más seguras posible frente a amenazas conocidas y desconocidas.

Vulnerabilidad del software

La seguridad que se necesita para ver una película en streaming es diferente a la que se necesita para controlar un sistema doméstico o de tráfico. Una forma de resolver el problema de la necesidad de tener más control sobre la velocidad y la seguridad de la red es la segmentación de la red.

En este tipo de arquitectura de red, las redes virtuales e independientes se mantienen sobre la misma infraestructura de red física, lo que permite que cada una satisfaga las diversas necesidades de una aplicación a pedido.

La segmentación de la red 5G es una de las principales razones por las que la 5G está tan alejada de la 4G y por la que la Ciberseguridad de la 5G es tan diferente de las iteraciones anteriores.

La 5G utiliza redes definidas por software (SDN) y virtualización de funciones de red (NFV). Ofrece varios servicios que permiten implementar y escalar segmentaciones de red de forma dinámica sobre una infraestructura de red existente.

El impacto de la tecnología 5G en la ciberseguridad es significativo porque la tecnología 5G se basa en gran medida en software. Las funciones SDN reemplazan al hardware y las actualizaciones de la red serán, en su mayor parte, actualizaciones de software. Lamentablemente, esto significa que la tecnología 5G enfrentará nuevas vulnerabilidades que muchas otras soluciones de software enfrentan.

Además, mientras que las redes de hardware 4G presentaban un diseño de concentrador y radios, las redes 5G admiten una transición a la computación de borde, donde los recursos van a donde esté la infraestructura y no a una ubicación central.

Un sistema de concentrador y radios tiene puntos de estrangulamiento donde los arquitectos de red pueden implementar la seguridad. Sin embargo, la tecnología 5G existe en una red de conexiones de enrutadores digitales. Su red distribuida elimina deliberadamente los cuellos de botella, lo que significa muchos más puntos de enrutamiento de tráfico y un requisito adicional de seguridad de extremo a extremo.

Internet de las Cosas (IoT) y conectividad

Mientras que la tecnología 4G brinda acceso a Internet, la tecnología 5G potencia infraestructuras cada vez más complejas. Estamos ante un futuro de ciudades inteligentes, por ejemplo, que conectarán dispositivos IoT , hogares inteligentes, automóviles inteligentes e incluso sistemas de tráfico.

Existen miles de millones de dispositivos IoT en todo el mundo y, si bien las posibilidades son apasionantes, cada dispositivo conectado también aumenta la superficie de ataque. Actualmente, el ecosistema IoT necesita más organización y regulación. Si bien los proveedores de servicios de Internet y los fabricantes tienen el deber de cuidar a los consumidores, no está claro quién es responsable de la seguridad de IoT.

Falta de seguridad incorporada

Muchos dispositivos IoT carecen de cualquier tipo de seguridad integrada. Si bien a veces se requiere autenticación, a menudo las contraseñas predeterminadas de estos dispositivos no se cambian para que el dispositivo funcione. Además, es posible que los fabricantes envíen dispositivos IoT que contienen malware sin saberlo.

Si bien los dispositivos IoT suelen tener cortafuegos (firewall), tienden a carecer de la potencia computacional necesaria para una seguridad eficiente. Esto, combinado con un control de acceso deficiente y limitaciones técnicas y financieras, genera un área de preocupación importante.

Sin una seguridad integrada y eficaz, los piratas informáticos pueden tomar el control de los dispositivos IoT con mayor facilidad, lo que significa que podrían poner en peligro las cámaras conectadas, modificar el comportamiento de los robots de fabricación o tomar como rehenes hogares inteligentes mediante ciberataques. Además, los piratas informáticos podrían obtener acceso no autorizado a las redes 5G a través de vulnerabilidades no corregidas en los dispositivos IoT.

Algunos casos de vulnerabilidades en dispositivos IOT

- **Conficker:** Este gusano afectó a millones de dispositivos en 2008, incluyendo dispositivos IoT en el sector de la salud.
- **Kaiji:** Una botnet que apareció en mayo de 2023, dirigida principalmente a dispositivos IoT y servidores Linux.
- **Cryptojacking:** Casos de dispositivos IoT utilizados para minar criptomonedas sin el conocimiento del propietario.
- **DDoS (Denegación de Servicio):** Ataques masivos que utilizan dispositivos IoT comprometidos para sobrecargar y cerrar servicios en línea

Cuestiones de protección de datos

El 98 % del tráfico de IoT no está cifrado, lo que revela información personal y datos confidenciales. Los problemas técnicos no solo permiten a los cibercriminales acceder fácilmente a las redes 5G, sino que también es esencial tener en cuenta la creciente amenaza que representan los estados-nación. Los actores maliciosos pueden usar el acceso a una red 5G para comprometer la red en sí y sus dispositivos conectados, lo que representa un riesgo para la seguridad nacional.

Potencial de denegación de servicio distribuido (DDoS)

El aumento de dispositivos IoT también aumenta la frecuencia y el impacto potenciales de los ataques de denegación de servicio distribuido (DDoS) . En 2016, por ejemplo, los cibercriminales lanzaron tres ataques DDoS contra el proveedor de sistemas de nombres de dominio (DNS) Dyn, lo que provocó graves interrupciones durante horas en el funcionamiento de muchas de las principales plataformas y servicios de Internet, entre ellos Amazon, CNN, The New York Times, The Wall Street Journal y Twitter.

El ataque se llevó a cabo mediante solicitudes de búsqueda de DNS desde decenas de millones de direcciones IP desde dispositivos conectados a Internet infectados con malware, incluidas impresoras, cámaras y monitores para bebés.

Por lo tanto, los operadores de redes también deben tomar medidas de seguridad consistentes para proteger la infraestructura 5G, incluida la infraestructura crítica como la energía, la atención médica y el transporte, que están cada vez más conectadas.

Ancho de banda

Un mayor ancho de banda permite velocidades de transferencia de datos más altas y tiempos de descarga más cortos. Desde una perspectiva de ciberseguridad, un mayor ancho de banda en las redes 5G también significa potencialmente más vías de ataque y ataques más rápidos. Debido a que las redes 5G tienen un ancho de banda mucho mayor en comparación con las generaciones anteriores, permite a los delincuentes emplear herramientas más baratas y de menor potencia que pueden llegar a muchas más personas a una velocidad mucho más rápida.

Amplia disponibilidad

Se espera que una cantidad récord de usuarios se unan a las redes 5G en comparación con las de 4G y que cada vez dependan más de las conexiones de red, lo que también aumentará significativamente la superficie de ataque, lo que crea más puntos de entrada para posibles atacantes. Muchos de los problemas de ciberseguridad asociados con 5G serán consecuencia de procesos de desarrollo deficientes en las primeras etapas.

Variación en la seguridad

Al considerar la seguridad de la infraestructura 5G, una red solo puede ser tan fuerte como su eslabón más débil. Con tantos usuarios previstos y dispositivos conectados, realizar evaluaciones de riesgo periódicas de terceros y un monitoreo continuo de la cadena de suministro digital será más importante que nunca.

Amenazas y vulnerabilidades desconocidas

Es imposible predecir cada vulnerabilidad o problema antes de que una persona, organización o pirata informático los encuentre. El ecosistema digital 5G será vulnerable porque el riesgo cibernético no es estático, sino que forma parte de un panorama de amenazas cibernéticas en evolución.

Cómo la tecnología 5G beneficia a la Ciberseguridad

A pesar de las serias preocupaciones sobre 5G y la ciberseguridad, también son evidentes varios beneficios. La ciberseguridad 5G ofrece mejoras en velocidad, confiabilidad y seguridad debido al mayor ancho de banda y al aumento de puntos de conexión.

Cifrado mejorado

Las ofertas de ciberseguridad 5G incluirán el cifrado de identidad de suscriptor móvil internacional (IMSI) , conocido en redes 5G como Identificador Permanente de Suscripción (SUPI).

Si bien existen problemas sobre cómo se puede utilizar esto para rastrear a los usuarios y la posibilidad de que se capture información confidencial con un receptor IMSI, estos problemas se

mitigan con el uso de un identificador oculto de suscripción (SUCI), que protege a los usuarios y la red 5G. Sin embargo, para implementar un cifrado mejorado también se requieren sólidos conocimientos de la práctica y una configuración y gestión adecuadas para que sea eficaz.

Detección de amenazas mejorada

Las enormes mejoras de velocidad de 5G con respecto a 4G lo convertirán en un poderoso aliado para los directores de seguridad de la información (CISO). Permitirá a las organizaciones y a los profesionales de la ciberseguridad identificar amenazas con mayor rapidez y mejorará la velocidad con la que se analizan, descargan y transmiten los datos esenciales para la ciberseguridad.

Auditorías cibernéticas mejoradas

Con más dispositivos conectados y los medios para acceder a ellos, los profesionales de la ciberseguridad podrán realizar auditorías más exhaustivas y amplias, lo que les permitirá mitigar las vulnerabilidades con mayor rapidez y en más dispositivos y ubicaciones. Además, la tecnología 5G permitirá el uso de inteligencia artificial y soluciones de cadena de bloques, que son fundamentales para las técnicas innovadoras de ciberseguridad.

Soluciones para mejorar la seguridad de la red 5G

Para que las redes 5G sean más seguras y confiables para los consumidores, aquí hay algunas formas en que las empresas pueden intentar mejorar la seguridad de su red:

- **Evaluaciones de riesgos periódicas**

Las evaluaciones periódicas de riesgos siempre han sido importantes, pero quizás nunca han sido tan críticas como cuando se enfrenta a una nueva tecnología asociada con 5G. Las evaluaciones de riesgos y el análisis repetidos de los casos de uso de 5G ayudarán a las partes interesadas a reducir o eliminar los riesgos de ciberseguridad de los dispositivos no confiables que un cibercriminal podría explotar.

Estas evaluaciones de riesgos deben considerar no sólo la tecnología de próxima generación, sino también las redes tradicionales cuyos componentes conectados podrían aumentar las amenazas cibernéticas.

- **Seguridad integrada para dispositivos IoT**

Las conexiones simultáneas de dispositivos IoT aumentan drásticamente las superficies de ataque. Una solución para manejar el aumento del riesgo es garantizar una mayor seguridad en la etapa de diseño de los dispositivos IoT.

Para lograr una mayor y mejor seguridad integrada, un organismo regulador específico para los dispositivos IoT podría ayudar a estandarizar la industria y proteger a los consumidores y la infraestructura, incluida la infraestructura crítica.

Las nuevas regulaciones pueden ser más efectivas cuando se centran en generar conciencia y ofrecer asesoramiento, apoyo y cooperación a las empresas, especialmente las marcas de IoT de gama baja, en lugar de depender excesivamente de la imposición de sanciones por incumplimiento.

Un incentivo para cumplir con los nuevos estándares de ciberseguridad de la IoT podría ser el reconocimiento ventajoso de que una empresa cumple con un estándar de ciberseguridad, similar al sistema de codificación por colores de los alimentos que ayuda a los consumidores a tomar decisiones saludables sobre lo que comen. Otro posible incentivo podría incluirse en un plan de apoyo logístico para las empresas que cumplan los requisitos.

- **La red celular 5G autónoma**

En última instancia, la infraestructura 5G se mantendrá de la misma manera que se mantienen otros sistemas digitales, con actualizaciones, parches y mejoras digitales. Sin embargo, actualmente, la 5G existe en conjunción con la infraestructura de red física 4G.

Uno de los problemas de los dispositivos IoT es que actualmente se conectan a 5G utilizando la infraestructura de red 4G existente. Las transmisiones de seguridad entre dispositivos y nodos se envían en texto sin formato, lo que las hace vulnerables a ser explotadas por piratas informáticos. Este problema se mitigará con el tiempo, si no se solucionará por completo, cuando se implemente el uso generalizado de una red de acceso por radio (RAN) independiente y dedicada a 5G.

- **Seguridad de red y transferencia de datos mejoradas**

Si bien muchas soluciones de seguridad se centran en solucionar las debilidades y vulnerabilidades identificadas, las pruebas de fuzzing están orientadas a localizar problemas desconocidos en las capas de la red. Esto es crucial en la gestión de vulnerabilidades y será fundamental para mejorar la seguridad de las redes 5G y los dispositivos conectados.

Las soluciones de seguridad de endpoints dedicadas pueden detectar, identificar y monitorear amenazas de seguridad 5G. Las organizaciones pueden usar tecnologías que permitan respuestas remotas a problemas detectados por el sistema.

Un marco de confianza cero hace que la verificación y la autorización sean obligatorias, lo que beneficia la seguridad de la red en redes vastas y ultrarrápidas. Elimina la confianza implícita en favor de la verificación y validación de cada etapa de cada interacción digital, lo que reduce la superficie de amenaza.

Una de las ventajas de un marco de confianza cero es que funciona en todos los dispositivos, lo que es esencial cuando se considera la tecnología de IoT. Este marco también requiere un monitoreo continuo de las configuraciones de seguridad para cada usuario que solicita o accede a datos, ya sea interno o externo a una organización.

- **Fomentando la colaboración**

La tecnología 5G ofrece posibilidades únicas, pero también plantea desafíos únicos. Independientemente de las técnicas que se apliquen, se requiere la cooperación entre fabricantes, gobiernos, minoristas, proveedores de servicios de Internet y usuarios.

En lugar de las relaciones algo adversas entre empresas y reguladores, una transición a un sistema más proactivo y colaborativo, en el que se incentive a las empresas a alcanzar estándares mínimos de ciberseguridad 5G en lugar de penalizarlas.

- **Intercambio de información**

El intercambio de información será fundamental para proteger las redes 5G, ya que la tecnología, y por lo tanto sus vulnerabilidades, son nuevas. Basta con un eslabón débil para que otros usuarios de la red sean vulnerables. Para que todos estén al día, es necesario centrarse en informar rápidamente y de forma completa sobre los problemas de seguridad.

Esto puede significar un aumento de la notificación de problemas incluso cuando no hay una pérdida significativa del servicio ni un riesgo grave para los clientes. Cuanta más información tengan los profesionales de la ciberseguridad sobre las amenazas emergentes, más eficazmente podrán responder.

- **Detección de amenazas en tiempo real**

El uso de la IA para detectar amenazas cibernéticas mejora la velocidad de detección y mitigación de amenazas. Si bien la tecnología 5G implica un aumento de la superficie de ataque , también ofrece el potencial de mitigar las amenazas con una detección más rápida y una mejor gestión con la ayuda de tecnologías de IA y aprendizaje automático.

- **Inteligencia artificial y aprendizaje automático para la gestión de redes**

Dado que la infraestructura 5G es dinámica y capaz de alcanzar velocidades enormes, requiere sistemas de gestión de red igualmente eficaces. Las soluciones basadas en software pueden proporcionar contramedidas eficaces para la próxima generación de amenazas cibernéticas en las redes 5G.

Además de respuestas rápidas y automatizadas, la tecnología de IA y ML es útil porque puede aprender y actualizarse en respuesta a amenazas emergentes, lo que las convierte en poderosos aliados para mantener la ciberseguridad 5G.

Implementar las mejores prácticas de ciberseguridad

Si bien la tecnología 5G transforma las redes de celulares del mundo, requiriendo nuevas regulaciones y nuevas técnicas de ciberseguridad, muchas de las mejores prácticas actuales en materia de ciberseguridad siguen siendo tan relevantes como siempre.

Las empresas y las personas deben mantener las mejores prácticas de ciberseguridad establecidas para reducir su riesgo cibernético, incluidas las siguientes.

- Usar una VPN al conectarse a cualquier dispositivo conectado a Internet
- Uso de autenticación multifactor (MFA)
- Usar contraseñas seguras siempre que se requiera una contraseña para la autenticación y mantener una excelente higiene de contraseñas

- Implementar el control de acceso para restringir el acceso a información confidencial y datos de misión crítica
- Actualizar dispositivos y aplicaciones periódicamente para garantizar que se solucionen las vulnerabilidades.
- Instalar software anti-malware, preferiblemente con un sistema de detección de amenazas

Referencias externas: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity

Sección 3
Guerra Electrónica

El empleo de los medios de comunicaciones permite al Comandante, el comando y control durante el desarrollo de las operaciones militares desde el Nivel Operacional hasta llegar a la mínima fracción de combate en el Teatro de Operaciones (TO), transmitiendo las órdenes en tiempo real y permitiendo contar con los datos proporcionados por sus elementos para la evaluación de la situación existente y su posterior resolución.

Esto implica el empleo en forma permanente de las facilidades radioeléctricas y consecuentemente del espectro electromagnético (EM) por lo que da inicio al accionar de la Guerra Electrónica (GE), ya sea para asegurar el uso del espectro por propia tropa, o para dificultar o impedir el uso del mismo por parte del enemigo.

A su vez, la GE se caracteriza por la lucha permanente para lograr el control del EM y la debida explotación tecnológica de los Sistemas de Armas buscando la destrucción de los sistemas del oponente y a la protección de los propios, cuya supervivencia dependerá de un adecuado empleo de los sistemas electrónicos en el momento y lugar, a fin de contrarrestar las acciones del enemigo.

La doctrina conjunta en Argentina define a la GE como “**Cualquier acción que implica el uso de la Energía Electromagnética dirigida para controlar el Espectro Electromagnético o atacar al enemigo”**. En este sentido, se interpreta que es una acción ofensiva que busca impedir el Comando y Control y consecuentemente la conducción de la campaña por parte del comandante enemigo.

La GE tiene como propósito negar al oponente el empleo del Espectro Electromagnético y asegurar el empleo efectivo de éste por la propia fuerza, pero se hace necesario entender que para negar el uso del espectro primero se deberá contar con una inteligencia referida a las capacidades de comunicaciones y no comunicaciones con que cuenta el oponente y en segundo lugar poseer un sistema que planifique y dirija las operaciones conjuntas en el espectro electromagnético, aunando los

esfuerzos de los componentes del TO y coordinando los efectos sobre el Sistema de Comando y Control del oponente.

La GE se divide por su finalidad en **tres grandes grupos** que se caracterizan por la naturaleza de la acción, la diferencia está dada por su carácter de actividades defensivas u ofensivas determinadas por la irradiación o no de energía electromagnética y su afectación a las comunicaciones del enemigo y la protección de las propias.

“Apoyo de Guerra Electrónica AGE (Electronic Warfare Support - EWS): Es la división de la Guerra Electrónica que incluye acciones conducidas por o bajo el Control directo de un Comandante Estratégico, para obtener información de la energía presente en el medio ambiente, mediante la **búsqueda, interceptación, escucha, localización, análisis, identificación, evaluación y registro** de las características de las emisiones detectadas, intencionales o no. Con el fin de contribuir al inmediato reconocimiento y seguimiento de amenazas presentes en el Espectro Electromagnético y proporcionar bases para la planificación y conducción de futuras operaciones”

La característica de esta actividad está dada por su naturaliza pasiva, ya que sus medios de ejecución no necesitan de irradiación al espectro

El segundo grupo en que se clasifica la GE es el

“Ataque electrónico: AE (Electronic Attack - EA): consiste en el uso de la energía electromagnética, energía dirigida o armas anti-radiación para atacar al personal, instalaciones y equipamientos con la intención de degradar, neutralizar o destruir la capacidad de combate del enemigo”.

Estas acciones son ejecutadas para impedir o dificultar el uso del espectro electromagnético por parte del enemigo a fin de afectar su comando, control y comunicaciones como sus sistemas de armas que empleen la energía irradiada para su funcionamiento.

Se caracteriza por ser una actividad ofensiva, ya que emplea en forma eficiente la irradiación, reirradiacción y/o refracción de la energía electromagnética con la finalidad de afectar los sistemas de comunicaciones del enemigo.

Para finalizar, el tercer grupo en que se divide la GE es el denominado **Protección Electrónica** que “consiste en todas aquellas acciones realizadas para proteger al personal, instalaciones y equipamientos de cualquier efecto producido por el uso del espectro EM por parte de la propia fuerza o enemigo que degrade, neutralice, o destruya la capacidad de combate propio”.

La congestión del espectro, las vulnerabilidades de la ciberseguridad y el desarrollo de contramedidas por parte de los adversarios plantean obstáculos continuos.

De cara al futuro, el campo de la guerra electrónica encierra un inmenso potencial. Los avances en el dominio del espectro, la integración con la inteligencia artificial y el aprendizaje automático, las actividades cibernéticas ofensivas, las armas de energía dirigida, las tecnologías cuánticas y fotónicas, y las capacidades espaciales darán forma a la evolución de la guerra electrónica.

De cara al futuro, la integración entre guerra electrónica y acciones cibernéticas será aún mayor a la hora de detectar y responder a amenazas exteriores

Conclusiones Parciales

Con lo visto hasta este momento, vemos que las operaciones en el Multidominio, se abastecen de la información necesaria, a través de las redes orgánicas convencionales, pero La convergencia de acciones en múltiples dominios se convierte en una necesidad, más que una herramienta, para el Comandante Operacional, en el logro de una ventana de oportunidad para dominar en tiempo y espacio para alcanzar sus objetivos.

El dominio del ciberespacio, cobra relevancia en el actual conflicto entre Rusia y Ucrania. Rusia generó una serie de acciones cibernéticas con una diversidad de efectos, ciberoperaciones con los bautizados "cibermilicias (dark werb)", en el contexto de integrar milicias y actores no militares, en una campaña. Se ejecuta un "ciberataque, el 20 diciembre del 2016 en sector de Ucraniano… dejando sin electricidad a 250.000 personas en un país azotado por la guerra y en pleno invierno", antes de iniciar con las operaciones convencionales.

Las redes 5G en sus múltiples configuraciones son una tecnología compleja con múltiples posibilidades de funcionamiento que se deben conocer para entender las soluciones que se pueden utilizar en el mundo militar.

Es de vital importancia entender la evolución que ha supuesto el sistema 5G frente a los sistemas tradicionales en cuanto al modelo de creación de redes y los múltiples sistemas radio que es capaz de manejar.

Capítulo 2
Integración de la información

La evolución de las redes de telecomunicaciones móviles ha sido significativa en las últimas décadas, comenzando con la 1G, que introdujo las comunicaciones móviles analógicas, y avanzando a la 2G, que trajo consigo la digitalización y los servicios de mensajes. La 3G mejoró la capacidad y velocidad, enfocándose en la transmisión de datos y soporte para internet, mientras que la 4G se centró en la alta velocidad y la computación en la nube. La 5G, siendo una evolución natural, hereda

y mejora tecnologías de generaciones anteriores, ofreciendo mayor velocidad, capacidad, y plantea nuevos desafíos y consideraciones en cuanto a seguridad.

Las redes 5G aprovechan tecnologías ya existentes como la MIMO: **Multiple-Input Multiple-Output (MIMO),** basándose el principio de que utilizando múltiples antenas, se pueden enviar y recibir múltiples flujos de datos simultáneamente, lo que aumenta significativamente la capacidad y la calidad de la conexión.

También aplican tecnologías nuevas como el slicing, mediante el cual se introduce la virtualización de redes y la computación lógica para facilitar aplicaciones emergentes que pueden tener diversos requisitos de servicio. Por medio del slicing se divide una red física en múltiples redes lógicas virtualizadas únicas sobre una infraestructura común de múltiples dominios. A través de este concepto, se pueden asegurar tanto QoS como recursos de red.

Con estas mejoras técnicas las 5G presenta como principales beneficios frente a tecnologías anteriores una ostensible mejora en la tasa de transferencia de datos, en la latencia, en la eficiencia energética, en el volumen de tráfico soportado y en la densidad de conexiones

Sección 1
Estructuras

A la hora de desplegar las redes 5G existen dos modelos: el **modelo Stand Alone (SA)** y el **modelo Non Stand Alone (NSA)**. El 5G SA es el modelo de implementación donde el 5G proporciona una red 5G de extremo a extremo; en esta arquitectura, tenemos una red independiente como 5G New Radio.

SA presenta una arquitectura 5G pura, esta implementación se basará en el uso de 5G para el Plano de Control y el Plano de Usuario.

La opción **Non Stand Alone** por el contrario responde a una red 5G respaldada por la infraestructura 4G y las radios 5G acopladas a la LTE EPC. Es decir las redes NSA ofrecen conectividad vía tanto a través de 4G AN (E-UTRA) como de 5G (NR) Esta doble característica también se denomina EN-DC, o doble conectividad E-UTRAN-NR .

Un país (Letonia) , durante un ejercicio militar, ya ha hecho demostraciones en el manejo remoto de drones a través de conexiones 5G, habiendo materializado la posibilidad de controlar vuelos transfronterizos, haciendo volar una nave desde Letonia hasta Estonia sin perder el control al cambiar de redes de comunicación.

Para estas maniobras se desplegaron dos redes 5G. Una en la banda de 3,4 a 3,7 GHz, licenciada por una prestadora civil, para la que utilizó una estación base de comunicaciones en modo NSA (non-standalone) como red principal.

NSA es el tipo de tecnología utilizada para las redes que se abren al público, las que habitualmente se pueden conectar desde un Smartphone en la calle; mientras que el modo SA

('independiente') es el que se utiliza para conexiones punto a punto y en redes privadas, como las que pueda desplegar una compañía dentro de sus instalaciones.

La segunda red adicional, utilizada en estas maniobras militares, fue una red táctica en modo standalone de la compañía finlandesa Bittium, participante en el consorcio.

Este tipo de redes 'independientes' tienen todavía muy limitada visibilidad y, de hecho, expertos señalan que esta demostración práctica sobre el terreno podría ser la primera que se ha hecho. Al menos, en Europa.

La letona LMT, que fue la principal organizadora de la jornada, asumió la integración coordinada de ambas redes de comunicaciones a través de su **Battle Information Management System (sistema de gestión de información de batalla)**. Entre las pruebas desarrolladas, también se utilizó tecnología de comunicación 4G, compatible con las redes desplegadas.

Para la puesta en práctica de la acción, LMT contó con el apoyo de las Fuerzas Armadas Nacionales de Letonia, que, obviamente, aportaron también las tropas.

Conclusiones Finales

Las redes 5G son la apuesta de futuro en las comunicaciones tácticas.

A lo largo del trabajo se ha estado analizando en profundidad las características de esta nueva generación de comunicación 5G como es el caso de la latencia, la eficiencia energética, la velocidad y el ancho de banda en diferentes escenarios tácticos militares.

En los diferentes casos de uso del 5G en entornos militares, se ha comprobado como gracias al 5G es posible compartir en tiempo real grandes cantidades de información en cortas y largas distancias, y ante cualquier tipo de adversidad, bien sea mediante el uso de UAVs, sensores IoT, etc.

Además, algunas tecnologías asociadas al 5G como, IoT o realidad aumentada ayudan a que la gran mayoría de misiones tácticas transcurran bien, anticipándose a posibles ataques enemigos, reduciendo tiempos de respuesta ante una emergencia o simplemente proporcionando mucha más seguridad a la red y las comunicaciones mediante el uso de encriptación y autenticación de usuarios

Toma así también, especial relevancia el factor de la seguridad. La seguridad en las redes de comunicaciones es un factor sumamente importante y lo es aún más para las redes militares.

Las redes 5G no son ajenas a ello y ha evolucionado notablemente en comparación con sus predecesoras y en gran medida las 5G implementan nuevas formas de mejoras en la seguridad de las redes o mejoran las ya existentes.

Por lo tanto las redes 5G en el uso militar deben de hacerse cargo e implementar todas estas medidas o en su defecto sustituirlas por otras que al menos las igualen en capacidades. A estos efectos durante esta monografía se han explorado los mecanismos y las vulnerabilidades de seguridad.

De todas las amenazas conocidas a las redes 5G la solución de trabajar con redes Stand Alone (SA) implementada es la menos vulnerable. Se trata de una solución SA con todo el equipamiento de

red propietario y aislado. Este esquema plantea una red SA integrada con CN (COMBAT NETWORK), y demás sistemas. A su vez tampoco permite la conexión a otras redes como 4G.

Tras analizar las vulnerabilidades que pueden afectarla se puede considerar una red segura más aun teniendo en cuenta que se trata de una red cifrada.

A partir de esta configuración las posibilidades que puede aportar a un entorno táctico son muy elevadas gracias a la velocidad, baja latencia y disponibilidad que otorga.

A medida que la efectividad de las redes 5G militares mejore, aumentarán los casos de uso.

Referencias

Baqués, J. (2015). El papel de Rusia en el conflicto de Ucrania: ¿La guerra híbrida de las grandes potencias? en Revista de estudios en seguridad internacional, 1(1), 41-60.

Bauman, Z. (2013). Liquid modernity. John Wiley & Sons.

Jordán, J. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo, en Revista Española de Ciencia Política, (48), 129-151.

Pulido, G. (2022). Guerra multidominio y mosaico: el nuevo pensamiento militar estadounidense. Los libros

NIST SPECIAL PUBLICATION 1800-33A 1 - 5G Cybersecurity - https://www.nccoe.nist.gov/projects/building-blocks/5g-cybersecurity

Ing. Bolivar Rolando Quizphe Vasquez (2023) Análisis de la seguridad en redes 5G y propuesta de mejoras, en la Maestría de Telecomunicaciones de la Universidad Nacional de Loja (Ecuador)

Referencias externas: https://www.upguard.com/blog/how-5g-technology-affects-cybersecurity