Cuando se Busca Liderar el Desarrollo Tecnológico del Sector Defensa, la Guerra en el Espectro Electromagnético es un Aspecto a Tener en Cuenta

RESUMEN EJECUTIVO
-Primer Ejercicio de Ciberdefensa en CODALTEC -CODALTEC busca liderar el desarrollo tecnológico del sector defensa, integrando sectores productivos de Colombia y por esto inicia su investigación sobre los elementos de la guerra electrónica y la Ciberdefensa por medio de un ejercicio de simulación que contempla acciones sobre el espectro electromagnético. -Villavicencio, Colombia 2014
OBJETIVOS: -Simular procedimientos militares frente a ataques cibernéticos. -Generar información relevante para aportar al proceso de Investigación y desarrollo de CODALTEC.
SOLUCIÓN: -Parametrización y Personalización del Simulador de Guerra VRFORCES de VTMAK para representar escenarios de operaciones sobre el espectro electromagnético colombiano. -Integración del simulador de guerra cibernética Network DefenseTrainer (NDT) de SCALABLE NETWORK TECHNOLOGIES, con el simulador de guerra VRFORCES de VTMAK y COMM Net Radio (CNR) de CALYTRIX para efectuar los ataques con el NDT y representar sus consecuencias en las operaciones militares en el VRFORCES. -Estructuración de un ejercicio de simulación en las instalaciones de CODALTEC, para realizar maniobras de ataque y defensa sobre el espectro electromagnético y sus respectivas consecuencias en operaciones militares
RESULTADOS: -Los participantes visualizan las graves consecuencias de la vulneración de los sistemas de Defensa y así mismo son consientes de lo importante que debe ser la estrategia de Ciberdefensa en su planeamiento operativo y de respuesta a eventos de guerra. -Ejercicio que logra representar procedimientos cibernéticos de ataque y defensa sobre radares, Aeronaves UAV y Sistema de Comunicaciones. -CODALTEC inicia su proceso de investigación y desarrollo sobre la Ciberguerra.

OBJETIVOS:

CODALTEC con el soporte de ITM Consulting de Colombia, inició un proceso de investigación con miras a incluir en un futuro dentro de sus capacidades la simulación de guerra en el espectro electromagnético, mediante la generación de un espacio didáctico y participativo, en donde ingenieros de su equipo tecnológico se reunieron a evaluar consecuencias de ataques delictivos sobre el ciberespacio y los posibles procedimientos militares para responder a dichos eventos.

Dentro de los objetivos también se encontraba la evaluación de herramientas de simulación de Ciberdefensa y guerra electrónica como el Network Defense Trainer (NDT) que representa las interacciones de ataque y defensa sobre el espectro electromagnético y el VRFORCES que en conjunto logra representar los ataques y sus respectivos efectos sobre la operación militar colombiana.

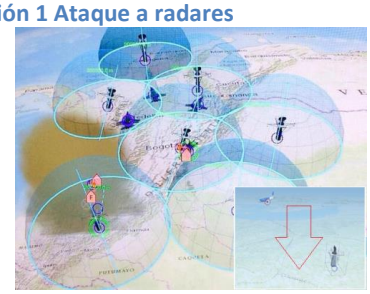
El ejercicio fue programado para representar varias situaciones de riesgo cibernético como lo son ataques a los sistemas de detección (radares), Aeronaves de inteligencia UAV y Sistemas de Comunicaciones. El Objetivo de los simuladores fue la representación de entidades simuladas con alto grado de similitud frente a las reales y sus capacidades, como Radares Militares, aviones no tripulados de inteligencia y vigilancia y estaciones de comunicación que faciliten observar lo que ocurre al perder elementos de detección de unidades enemigas y sus efectos sobre la protección de la soberanía nacional. Una vez efectuaran ataques cibernéticos sobre el sistema de información, se debería efectuar ataques cinéticos a la estructura de defensa del país, complicando con esto las maniobras defensivas y aumentando el riesgo de los efectos de la guerra.

SOLUCION:

Para alcanzar los objetivos trazados se planteó una integración del simulador NDT con el VRFORCES buscando con el NDT efectuar los ataques sobre el espectro electromagnético y con el VRFORCES representar las consecuencias de los ataques en las operaciones militares de defensa. El equipo de CODALTEC inició el ejercicio con un conjunto de entidades colombianas situadas en el VRFORCES con un escenario con cartografía colombiana y un conjunto de personalizaciones implementadas sobre la interfaz gráfica del mismo, para iniciar ataques cibernéticos que lleguen al simulador NDT que se encarga de efectuarlos y posteriormente regresar la información al VRFORCES quien ejecuta las consecuencias y afecta la operación normal de las diferentes entidades de las Fuerzas Militares Colombianas del el juego de guerra cibernético.

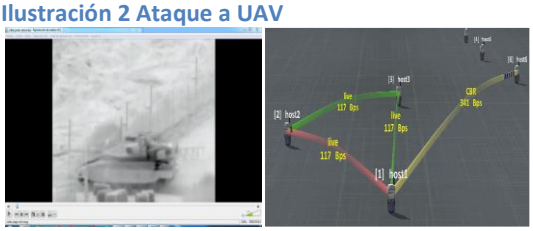
Para el ataque de radares se implementa una tarea para las entidades del equipo atacante, responsable de desplegar una interfaz en el VRFORCES que le hace posible seleccionar el radar y la frecuencia deseada para realizar el ataque, con el fin de inhibir los sensores del radar. Una vez seleccionado el objetivo, en el NDT 1.0 se realiza un ataque DOS por medio de línea de comandos causando inicialmente un engaño en la posición de los elementos reportados y luego una pérdida funcional de los sensores del radar (Ver Ilustración 1).

Ilustración 1 Ataque a radares



Teniendo en cuenta que actualmente se emplean aeronaves no tripuladas para monitorear zonas geográficas de interés y riesgo, se desarrollo un módulo que permite distorsionar la información de los receptores y alterar los procesos de toma de decisiones. Desde el VRFORCES un UAV de inteligencia transmite video de una zona en posible riesgo de ataque y el NDT realiza un ataque a la entidad causando distorsión y pérdida de la transmisión. (Ver Ilustración 2)

Ilustración 2 Ataque a UAV



La importancia de las comunicaciones en una operación militar hace que sean un blanco para fuerzas enemigas. Para simular este tipo de ataque se realiza un procedimiento similar al empleado, para deteriorar la información de video del UAV, solo que esta se emplea afectando los equipos de transmisión de comunicaciones radiales y los respectivos receptores mediante un ataque sobre el NDT. El sistema de comunicación empleado es simulado por COMM Net Radio (CNR) de CALYTRIX que se encarga de representar las comunicaciones por radio y las respectivas interferencias.

Finalmente una vez representadas las vulnerabilidades, se desarrollo para el ejercicio un sistema de alertas que permita notificar al Centro de Comando y Control los diferentes ataques y se puedan iniciar las respectivas acciones.

RESULTADOS:

Los ejercicios de simulación desarrollados logran sensibilizar acerca de la importancia de la seguridad y defensa del ciberespacio, adicionalmente permiten iniciar con un proceso de Investigación y Desarrollo en CODALTEC.

Se evidencia que Colombia requiere mayor desarrollo tecnológico en su trabajo sobre el espectro electromagnético para lograr simular la infraestructura crítica del país, sobre plataformas como las utilizadas en este ejercicio, con el fin de identificar estrategias de acción y reacción en caso de crisis o amenazas cibernéticas.

Se logra la integración de 3 simuladores permitiendo la representación de los ataques cibernéticos objetivo.