El Campo de Batalla ha Cambiado y Ahora el Ciberespacio ha Mostrado Ser de Gran Relevancia en la Toma de Decisiones Estratégicas de Seguridad

RESUMEN EJECUTIVO

-Taller de Simulación Primer Foro de Seguridad y Defensa Cibernética del Pais.
-El Gobierno Nacional representado por el Ministerio de las Tecnologías de la Información, La Escuela Superior de Guerra de Colombia, La Universidad de los Andes y la Empresa privada, acordaron unir esfuerzos para generar un espacio de debate en torno a las tendencias, retos y oportunidades, consecuencia de eventos, ataque o defensa en el ciberespacio
-Bogotá, Colombia Mayo de 2014

OBJETIVOS:
-Establecer un Marco de trabajo conjunto que le permita al país por medio de la simulación de ataques cibernéticos crear una visión a largo plazo teniendo en cuenta los principales actores que intervienen en la protección de la infraestructura crítica del país.
-Simular Procedimientos Cibernéticos de Ataque y Defensa sobre Infraestructura crítica.
-Generar información relevante para representar el proceso de toma de decisiones estratégicas.

SOLUCIÓN:
-Parametrización y Personalización del Simulador de Guerra VRFORCES de VT MAK para representar 3 escenarios de operaciones sobre el espectro electromagnético colombiano.
-Estructuración de un taller asistido y orientado por la Escuela Superior de Guerra para dos equipos que por medio de libretos predefinidos representan operaciones de ataque y defensa cibernética sobre el marco de la doctrina colombiana.
-Representación grafica de los eventos cibernéticos con apoyo de la infraestructura tecnológica especializada del sector académico .

RESULTADOS:
-Visión de las posibles consecuencias de ataques cibernéticos como insumo para la búsqueda de un marco de cooperación entre El Gobierno, la Academia, la sociedad y la Empresa Privada, para aportar a la defensa del país y mitigar o contrarrestar sus efectos sobre la infraestructura critica.
-Necesidad de simular y validar permanentemente los procedimientos de resilencia en caso de ataques cibernéticos de sobre infraestructura critica del país, como en este caso fueron los radares, Aeronaves UAV, sistemas de control de hidroeléctricas y sensores de presión en oleoductos.

OBJETIVOS:

La Escuela Superior de Guerra con apoyo de la empresa ITM Consulting de Colombia, quisieron mediante la generación de un espacio didáctico y participativo, generar un debate en torno a las consecuencias de ataques sobre el ciberespacio y sobre el Espectro Electromagnético a la infraestructura critica colombiana y los posibles procedimientos para responder a dichos eventos. Para esto los proponentes unieron esfuerzos y capacidades en busca de la representación por medio de una herramienta tecnológica de operaciones y procedimientos de Guerra Electrónica , Guerra Cibernética y eligió al simulador VR-FORCES de VTMAK por su efectividad en la parametrización y personalización de entidades, por sus más de 8 años de implementación exitosa en la Escuela Superior de Guerra de Colombia y por el dominio de la herramienta por parte de ITM una empresa Colombiana con más de 10 años de experiencia en el manejo este tipo de software.

El Ejercicio fue programado para representar varias situaciones de riesgo Cibernético en la infraestructura critica del país como lo es el sistema

de detección primario (radares), y sensores. Para trabajar estos escenarios se crearon y Modelaron entidades de Radares Militares y Civiles de Comunicación vulnerables frente a ataques Cibernéticos, para que se pueda observar lo que ocurre al perder elementos de detección de unidades enemigas y sus efectos sobre la protección de la soberanía nacional, se planteó la Modelación y representación gráfica de la Infraestructura Critica Petrolera mediante un Oleoducto buscando la sensibilización de posibles consecuencias de una alteración de los mecanismos de vigilancia de esta infraestructura y como puede ser la capacidad de respuesta frente a los mismos, y finalmente se representaron los componentes de una Hidroeléctrica donde es posible controlar las compuertas que permiten alterar el flujo de agua a las turbinas y así poder generar consecuencias negativas sobre el fluido eléctrico de una población.

SOLUCION:

Para lograr cumplir con el objetivo, se realizó una completa personalización a la interfaz gráfica del simulador y se incluyeron funcionalidades de escáner de frecuencias, ataque Jamming a radares, controlador de flujo de petróleo en las válvulas de una petrolera, monitoreo de válvulas, ataque a aeronaves de vigilancia no tripuladas, controlador de compuertas de hidroeléctrica, monitoreo de turbinas, indicadores de fluido eléctrico, controlador de flujo de agua en hidroeléctrica y finalmente daño físico a infraestructura de operación. Para simular las situaciones planteadas se plantea un ejercicio entre 2 bandos Azul y Rojo y la participación de un Director del ejercicio.

El primer escenario se desarrolló sobre todo el territorio colombiano e iniciaba con la aparición de un avión comercial del equipo rojo que cuenta con el sistema de escaneo y Jamming y que tiene como misión alterar la frecuencia de uno de los radares del equipo azul, con el fin de alterar su proceso de detección para posteriormente ingresar aeronaves de combate que terminen de vulnerar el sistema de defensa (Ver Ilustración 1).

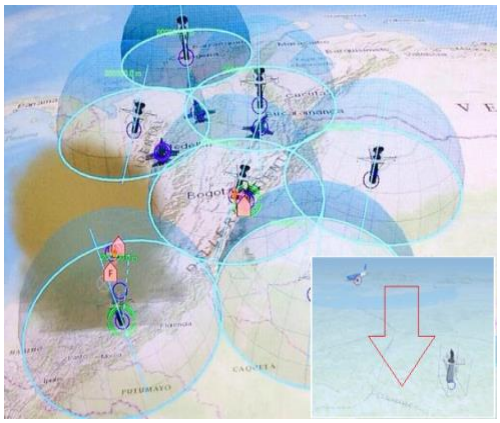
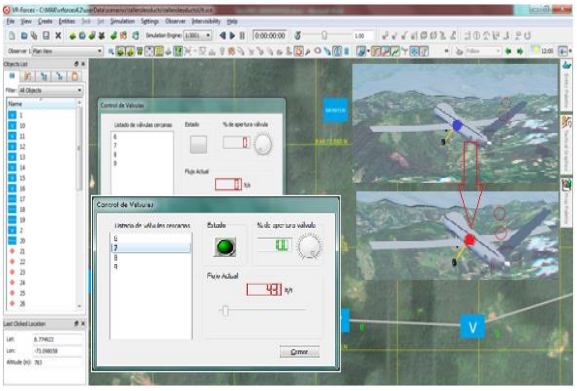


Ilustración 1 Ataque a radares

El Segundo Escenario se desarrollo sobre una región del territorio colombiano en donde la infraestructura petrolera es de suma importancia y es víctima de frecuentes ataques terroristas. En el ejercicio, el equipo Rojo se encarga de alterar las lecturas de las válvulas por medio de ataques electrónicos que hacen prender aletas y desplegar dispositivos de seguridad y vigilancia como las aeronaves no tripuladas y unidades de respuesta del equipo azul. Con estas movilizaciones varios puntos del oleoducto quedan con vulnerabilidades provocadas y los recursos de vigilancia quedan expuestos al ataque que el equipo rojo puede realizar sobre los estos, como el control o destrucción de aeronaves no tripuladas (Ver Ilustración 2)

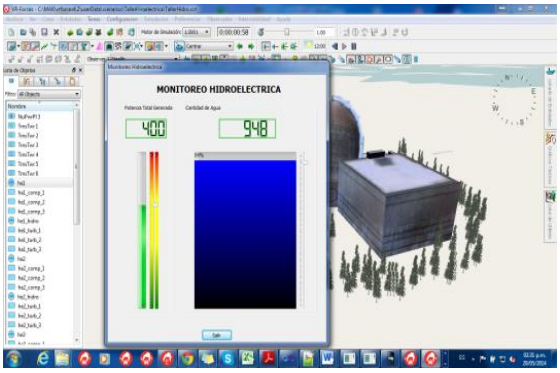
Ilustración 2 Ataque cibernético a Infraestructura Petrolera



El Escenario Final fue planteado para que el equipo azul se defendiera frente a intentos de controlar las

turbinas de una hidroeléctrica y con esto representar algunas de las consecuencias sobre la población civil. El equipo Rojo por medio de ataques cibernéticos se encarga de causar incoherencias en los sistemas de la hidroeléctrica, causando variaciones en los niveles de agua que implican a su vez cambios en la potencia y en la energía generada. Las variaciones causan que el servicio de electricidad en la población cercana presente variantes (Ver Ilustración)

Ilustración 3 Ataque cibernético a infraestructura crítica



RESULTADOS:

La teoríaa se pone en práctica y se grafican en el simulador los Modelos de Radares, Redes de Comunicaciones, Redes Scada y demás recursos que están disponibles en VR-FORCES. Los ejercicios son un gran aporte a la investigación y Desarrollo liderados por el Departamento de Telemática de la ESDEGUE y en especial su línea de investigación en Ciberseguridad y Ciberdefensa.

El desarrollo realizado sobre el motor de simulación VRForces me permitió liderar el proceso de investigación para la Modelación y Simulación del sistema para el Componente de Guerra Electrónica y Cibernetica, describiendo su comportamiento y estructura para determinar escenarios, tendencias y cursos de acción operacionales de la Escuela Superior de Guerra con excelentes resultados.

El Ejercicio cumplió con su principal objetivo de presentar a los participantes del Foro la importancia de tener en cuenta el ciberespacio en su procesos de toma de decisiones, y que tan graves pueden ser las consecuencias y la importancia de un marco de cooperación interinstitucional incluyendo en primer orden a organismos estatales, para mitigar o contrarrestar los efectos de los ataques cibernéticos.

Coronel Martha Liliana Sanchez Lozano
Oficial Fuerza Aérea Colombiana
Jefe de Telemática y Coordinadora del programa de Ciberseguridad y Ciberdefensa de la ESCUELA SUPERIOR DE GUERRA