













COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación

 Félix Gómez Mármol¹,  José A. Ruipérez-Valiente¹,  Pantaleone Nespoli¹,  Gregorio Martínez Pérez¹,  Diego Rivera Pinto²,  Xavier Larriva Novo²,  Manuel Álvarez-Campana²,  Víctor Villagrà González²,  Jorge Maestre Vidal³,  Francisco A. Rodríguez López³,  Miguel Páramo Castrillo³,  Javier I. Rojo Lacal³, Ramón García-Abril Alonso⁴

¹Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, 30100, Murcia, España
{felixgm, jruiperez, pantaleone.nespoli, gregorio}@um.es

²ETSI Telecomunicación, Universidad Politécnica de Madrid, España
{diego.rivera, xavier.larriva.novo, manuel.alvarez-campana, victor.villagra}@upm.es

³Indra, Avenida de Bruselas, 35, Alcobendas, 28108 Madrid, España
{jmaestre, farodriguez, mparamo, jirojo}@indra.es

⁴Mando Conjunto del Ciber Espacio, Base de Retamares, 28223 Pozuelo de Alarcón, España
rgaralo@et.mde.es

Resumen—Una formación en ciberdefensa de alta calidad que permita adquirir competencias que luego sean aplicables en escenarios reales es altamente compleja. A pesar de que la mayoría de las organizaciones y cuerpos involucrados en este área están de acuerdo en afirmar que generar mecanismos para el desarrollo de estas capacidades es prioritario, aún existen importantes carencias a nivel de metodologías y competencias, así como de sistemas y entornos de entrenamiento. En este sentido, el proyecto COBRA de “Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación” es ambicioso en combinar diversas tecnologías para alcanzar este objetivo, teniendo intrínsecamente un carácter multidisciplinar pero con unas metas claras.

Index Terms—Cyber Range, Ciberseguridad, Simulación APTs, Gamificación

Tipo de contribución: *Investigación en desarrollo*

I. INTRODUCCIÓN

Tal y como han anunciado una y otra vez las distintas organizaciones para la ciberdefensa, el éxito de cualquier iniciativa para su salvaguarda depende de la combinación adecuada de doctrina, organización, formación, procedimientos y comportamientos, así como de la disponibilidad de productos adecuados (infraestructuras y software).

Pero, a pesar de los esfuerzos de la Unión Europea (UE) y sus estados miembro hacia la disposición de habilitadores de formación y educación para operaciones en el ciberespacio, la revisión del estado del arte [1], [2] y la evaluación de las diferentes soluciones comerciales actuales sugiere la existencia de una lista emergente de desafíos y brechas tecnológicas a cubrir de cara a mejorar la capacidad de toma de decisiones en el ciberespacio [3], [4], destacando entre ellas:

- Las soluciones existentes a menudo tienen dificultades a la hora de proporcionar acceso a la formación bajo

demanda, a través de infraestructuras de formación reutilizables, escalables y adaptables, permitiendo así la reducción de los costes de los equipos específicos de formación.

- Las soluciones existentes no suelen proveer la capacidad de realizar ejercicios de formación especializada adaptada a las Especificidades del Dominio de Usuario (UDS) en el ámbito de las operaciones en el ciberespacio, como sus capacidades Tecnológicas Operativas (OTS) o los dispositivos conectados al Internet de las Cosas (IoT) portados por los diferentes efectivos.
- El estado del arte presenta marcadas carencias a la hora de adaptar los procesos de operación a amenazas específicas con impacto en diferentes niveles del entorno operacional [5]. Esto incluye la dificultad de adiestrar la capacidad de toma de decisiones de los ciber comandos ante dichas amenazas.
- La tendencia a la virtualización y la construcción de gemelos digitales sugieren una incipiente demanda de escenarios para cibermaniobras con la capacidad de representar entornos operacionales mucho más complejos, permitiendo a los ciber comandos ejercitarse con un mayor realismo.

Desde un punto de vista educacional, uno de los grandes problemas de los actuales sistemas es la pérdida de motivación y sensación de aburrimiento por parte de los estudiantes. Esto puede suceder por diversas razones, como bajo interés por la materia que se está recibiendo, sensación de apatía ante los contenidos porque no interesen o sean muy fáciles o, por el contrario, la sensación de incapacidad de entender contenidos o completar ejercicios debido a su alta dificultad, con la consiguiente frustración.

Numerosos estudios han demostrado que cuando los alum-

nos se encuentran más motivados por su proceso de aprendizaje, los resultados finales mejoran de forma significativa. Todos estos problemas son tratados por el proyecto COBRA en el contexto específico de práctica, aprendizaje y entrenamiento en materias de ciberdefensa en un Cyber Range, a través de la implementación de cibermaniobras dinámicas y adaptativas al estudiante, en oposición a las estáticas actuales. Por lo tanto, nos alejamos de la idea de “one-size-fits-all” y nos adentramos en la dirección de una educación personalizada a las necesidades y estado del estudiante.

Por otra parte, la introducción de elementos de gamificación en el sistema también puede tener un efecto positivo en la motivación de los estudiantes [6], [7]. De este modo, mediante una educación más personalizada y haciendo uso de los distintos componentes de diseño que pueden mejorar la motivación de los estudiantes, esperamos que se puedan mejorar de forma significativa resultados previos de aprendizaje con el Cyber Range.

Así mismo, mediante el uso de las trazas de datos telemétricas y las señales biométricas generadas por los estudiantes mientras resuelven los escenarios planteados seremos capaces de evaluar las competencias clave en un entorno militar, no solo relacionadas con contenidos en ciberseguridad, sino también las habilidades transversales como capacidad de trabajo bajo presión.

Por último, y en lo que respecta a las capacidades de defensa (a saber, Defensa, Explotación y Respuesta) en el ámbito del Ministerio de Defensa español (derivadas de la OTAN), el proyecto COBRA permitirá desarrollar fundamentalmente la capacidad de Respuesta.

II. OBJETIVOS

El objetivo principal del proyecto COBRA (Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación) se resume en:

Desarrollo de un conjunto de herramientas para la simulación hiperrealista de Amenazas Persistentes Avanzadas (APTs), orientada a la ejecución de cibermaniobras adaptativas y personalizables mejoradas con técnicas de gamificación.

Dicho objetivo se divide, a su vez, en cinco subobjetivos, que serán descritos con más detalle a continuación.

II-A. Simulación de topologías de red y tráfico real

Uno de los elementos necesarios para el desarrollo del proyecto es, a partir de una infraestructura virtualizada de red, permitir la generación de una serie de topologías de red simuladas que puedan servir de base para los escenarios de entrenamiento. En este sentido, se desarrollarán una serie de herramientas que permitan la definición flexible y parametrizada de topologías de red, y se integrarán estas herramientas en el Cyber Range utilizado como infraestructura base del proyecto. Esto implica por una parte ofrecer un sistema para la definición de estas topologías, y por otra, desarrollar un sistema capaz de, a partir de estas definiciones, desplegar y configurar de manera efectiva los nodos que componen

la topología, comunicándose para ello con el sistema de virtualización del Cyber Range.

Por otro lado, una vez establecidas las topologías de red, y para ofrecer un escenario simulado completamente realista, es necesario generar tráfico de red que se asemeje al tráfico que pudiera darse en una red real. Este tráfico deberá modelarse adecuadamente para asegurar el realismo de la simulación, y posteriormente deberá inyectarse en la red simulada, utilizando para ello herramientas de generación e inyección de tráfico.

II-B. Simulación de amenazas avanzadas persistentes

Los ataques informáticos son una amenaza generalizada para cualquier sistema informático. Los ataques evolucionan al mismo tiempo que los sistemas. Es por ello que los entornos de formación y entrenamiento en ciberseguridad deben contar con sistemas que permitan conocer y practicar sobre las distintas tipologías de amenazas que existen actualmente y que están continuamente avanzando. Las amenazas más sofisticadas se integran en lo que se denominan “Amenazas Avanzadas Persistentes”, del inglés Advanced Persistent Threats (APT), en las que los atacantes diseñan una estrategia de ataque, con múltiples etapas. Este objetivo propone la definición y diseño de Simulaciones de Amenazas Avanzadas Persistentes. Para ello, se partirá de un modelado formal de un ataque avanzado persistente APT genérico apoyándonos en modelos basados en estados (como, por ejemplo, en cadenas de Markov, STIX), de una forma realista y parametrizable siguiendo los pasos definidos en el modelo Unified Kill Chain (evolución de la Cyber Kill Chain en base al marco ATT&CK del MITRE). Estos modelos serán diseños propios que permitan acoplarse en su aplicación a los escenarios aleatorios y parametrizables. Para la simulación de APT se tomará en cuenta los patrones y herramientas de ataque de las propias amenazas con el objetivo de brindar un escenario lo más realista posible. Posteriormente se definirá una plataforma de simulación de los distintos estados y la evolución de eventos discretos temporales, para su aplicación en herramientas de simulación de APT en un Cyber Range.

II-C. Escenarios aleatorios y parametrizables

Otro objetivo de este proyecto tiene que ver con añadir funcionalidades a los sistemas Cyber Range en cuanto a la posibilidad de generar escenarios simulados aleatorios y parametrizables. Esto permitirá una mayor facilidad y flexibilidad a la hora de definir e instanciar ciberejercicios. Esta funcionalidad supondrá una mejora con respecto a la utilización del sistema por parte de sus usuarios, tanto instructores como estudiantes. Desde el punto de vista de los instructores, la generación de plantillas de escenarios y la definición de ciberejercicios será mucho más libre y automatizada. Desde el punto de vista de los estudiantes, la aleatorización y la posibilidad de contar con escenarios dinámicos permite una experiencia de aprendizaje mucho más rica, al proporcionarse una gran cantidad de posibles desafíos y una adecuación a las capacidades de cada uno.

Para la consecución de este objetivo se desarrollarán herramientas que permitan comunicarse con los sistemas subyacentes de definición de topologías de red, de generación de tráfico y de simulación de amenazas avanzadas persistentes,

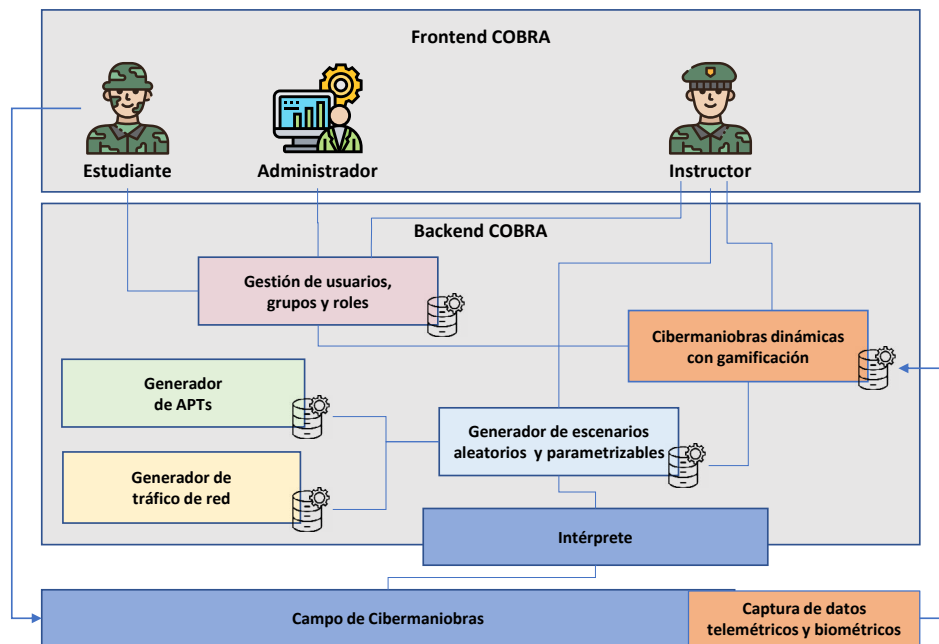


Figura 1. Arquitectura preliminar del proyecto COBRA

para transformar la definición de escenarios y plantillas en una infraestructura real sobre la que realizar los ciberejercicios. Contarán además con interfaces gráficas de usuario que permitan a los instructores realizar dichas definiciones con facilidad.

II-D. Cibermaniobras adaptativas con gamificación

A partir de los sistemas desarrollados en el proyecto para la flexibilización y la definición aleatoria y parametrizada de diversos escenarios de red sobre los que simular amenazas, en este proyecto se tiene como objetivo la incorporación de técnicas de Inteligencia Artificial con aprendizaje adaptativo para que los escenarios puedan adaptarse de forma específica a cada estudiante.

Para ello se proporcionarán sistemas de telemetría que permitan recoger información acerca del desempeño de los usuarios en los ejercicios planteados, así como diversos datos biométricos sobre el uso del sistema. Esto, junto con la aplicación de técnicas de gamificación, permitirá la adaptación de los escenarios de acuerdo a las capacidades, el desempeño y el estrés de los estudiantes.

II-E. Validación en el Cyber Range del MCCE

El quinto subobjetivo del proyecto tiene que ver con la instalación e integración de los sistemas desarrollados en la infraestructura de Cyber Range desplegada por el Mando Conjunto del Ciber Espacio (MCCE). Mediante la integración de los desarrollos se pretende evaluar la viabilidad de las soluciones definidas en el proyecto, así como determinar las competencias de los estudiantes mediante la realización de diversas pruebas diseñadas específicamente para la validación de la propuesta del proyecto.

El objetivo final del proyecto por tanto sería la generación de un demostrador operativo, instalado e integrado en el Cyber Range del MCCE, que permita la definición de entornos relevantes y cibermaniobras realistas.

III. ESTADO ACTUAL DE COBRA

El proyecto COBRA, en el que participan la Universidad de Murcia, la Universidad Politécnica de Madrid y la empresa tecnológica Indra, comenzó el 1 de diciembre de 2020 y tiene una duración total de 24 meses. En el momento actual se han desarrollado ya una serie de trabajos iniciales entre los que destacan los que se describen a continuación.

Se ha elaborado un Plan de Gestión del Proyecto (PGP) donde se especifica toda la metodología de gestión del proyecto COBRA, la división del mismo en paquetes de trabajo y tareas, con la consiguiente planificación temporal de los mismos. También se ha incluido un Plan de Gestión de Riesgos (PGR), así como un Plan de Gestión de la Calidad (PGA) y un Plan de Gestión de la Configuración (PGC). Se han identificado además todos los entregables, tanto de tipo documentación como software, que se irán desarrollando a lo largo de la vida del proyecto, agrupados por hitos o Plazos Parciales (PP).

Por otra parte se ha diseñado un Plan de Validación y Verificación (PVV) incluyendo la metodología a seguir para la evaluación sistemática de la consecución de los objetivos planteados. También se han identificado y descrito un total de 41 requisitos funcionales y no funcionales asociados a los 5 principales objetivos del proyecto, junto con su método de verificación y su prioridad. Además, se ha trabajado para obtener una arquitectura de alto nivel del proyecto, identificando cada uno de sus principales componentes, así como las principales interconexiones e interfaces entre los mismos (véase la Figura 1). Para cada uno de dichos componentes se ha proporcionado una descripción o principios de diseño, unas premisas operacionales y unas limitaciones.

Por último, cabe también destacar el comienzo de los trabajos técnicos asociados a los objetivos II-A, II-B y II-C, respectivamente. En este sentido, y en lo que respecta al objetivo II-A, se ha llevado a cabo un profundo análisis del estado del arte en cuanto a herramientas de simulación de

tráfico de red, clasificadas en función del tipo de generación de tráfico aplicada: i) Generación basada en la replicación de tráfico, ii) Generación de tráfico sintético mediante creación de paquetes, iii) Generación de tráfico basada en modelos, iv) Generación de tráfico de alto nivel y auto configurables, y v) Generación de tráfico para escenarios específicos. En esta revisión exhaustiva de la literatura se han analizado un total de 46 herramientas distintas.

En cuanto al objetivo II-B de simulación de APTs, también se ha realizado una revisión detallada del estado del arte sobre modelado y simulación de amenazas avanzadas persistentes. En este sentido, se han analizado diversas propuestas de modelado de APTs (como por ejemplo STIX), se han estudiado en detalle varios métodos de modelado de ataques multi-paso (basados en correlación, en similitud, en estructura, etc.) y se han descrito los principales pasos que componen la Cyber Kill Chain.

Y en lo que respecta al objetivo II-C de COBRA, se ha realizado otro análisis exhaustivo del estado del arte en cuanto a plataformas Cyber Range se refiere. En concreto se han estudiado los distintos tipos de Cyber Ranges, así como los posibles dominios de aplicación. También se han analizado los diferentes equipos que pueden participar en un Cyber Range (equipo rojo, equipo azul, etc.), además de las principales tipologías de ataques (explotación de vulnerabilidades, ataque a protocolos, ataques de ingeniería social, etc.) y de defensas (prevención, detección, reacción o análisis forense digital) que se pueden encontrar más comúnmente en un Cyber Range.

Con respecto al objetivo II-D, ya se han empezado a analizar las distintas arquitecturas que permitan recolectar telemetría por parte del Cyber Range y señales biométricas por parte de los usuarios que se encuentren haciendo las cibermaniobras. Se ha analizado la viabilidad de distintos dispositivos para poder recolectar dichas señales biométricas. Como próximos pasos, nos encontramos analizando los posibles indicadores de desempeño que se pueden computar, así como aquellas competencias que pueden ser valiosas de evaluar con dichos datos dentro del contexto de ciberseguridad de que deben de afrontar dichos usuarios. Por último, nos encontramos en proceso de análisis de los algoritmos de inferencia de conocimiento y aprendizaje adaptativo a aplicar en este contexto.

IV. CONCLUSIONES Y TRABAJO FUTURO

A pesar de los grandes esfuerzos hacia consolidar un marco europeo para la adecuada educación y entrenamiento en materia de ciberseguridad, a día de hoy existen importantes carencias marcadas entre otras por: 1) fallos a la hora de equipar a los profesionales de los conocimientos, competencias y aptitudes necesarios para prevenir y responder a ciberamenazas reales; 2) el acceso limitado a capacidades de análisis coste-impacto basados en pruebas; 3) dificultades a la hora de comprender la naturaleza interdisciplinar de la ciberseguridad; y 4) la necesidad de entornos de formación colaborativos y coherentes con el espacio de operaciones real.

Esta problemática se extiende al sector defensa, donde además de las restricciones inherentes a sus líneas de desarrollo (doctrina, organización, liderazgo, etc.), es necesario formar en la intersección entre las aptitudes necesarias para

operar en escenarios militares, y las características de técnicas y sociocognitivas presentes en el ciberespacio. Alcanzar estas capacidades implica avanzar hacia entornos de formación colaborativos centrados en el usuario, los cuales han de ser capaces de generar dinámicamente patrones de tráfico de red y comportamientos artificiales (neutros, aliados, hostiles) suficientemente creíbles.

En este contexto, el proyecto “COBRA: Cibermaniobras adaptativas y personalizables de simulación hiperrealista de APTs y entrenamiento en ciberdefensa usando gamificación” pretende desarrollar una solución innovadora que dé respuesta a estas deficiencias desde cinco objetivos principales, a saber: i) la simulación de topologías de red y tráfico real, ii) la simulación hiperrealista de amenazas avanzadas persistentes (APT), iii) el desarrollo de escenarios aleatorios y parametrizables, iv) el desarrollo de cibermaniobras adaptativas utilizando gamificación, y v) la validación de toda la propuesta en el Cyber Range del Mando Conjunto del Ciber Espacio (MCCE) del Ministerio de Defensa de España.

Este ambicioso proyecto, que aún se encuentra en su primer año de vida, aún tiene bastante recorrido por delante hasta alcanzar todas las metas propuestas. Y cuando esto ocurra, se convertirá en un referente en su campo, dados los novedosos avances que proporcionará, y que hasta donde los autores conocen, no existen en ninguna otra solución actual similar.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente financiado por el proyecto COBRA (10032/20/0035/00), concedido por el Ministerio de Defensa, así como por las ayudas FJCI-2017-34926 y RYC-2015-18210, concedidas por el Gobierno de España y cofinanciadas por el Fondo Social Europeo.

REFERENCIAS

- [1] I. Priyadarshini, “Features and architecture of the modern cyber range: A qualitative analysis and survey,” Ph.D. dissertation, University of Delaware, 09 2018.
- [2] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, “A review of cyber-ranges and test-beds: Current and future trends,” *Sensors*, vol. 20, no. 24, 2020.
- [3] E. C. S. O. (ECSO), “Gaps in european cyber education and professional training,” 2017, position paper of WG5 for Education, training, awareness, cyber ranges. [Online]. Available: <https://ecs-org.eu/documents/publications/5fdb282a4dcdbd.pdf>
- [4] —, “Understanding cyber ranges: From hype to reality,” 2020, position paper of SWG 5.1 for Cyber Range Environments and Technical Exercises. [Online]. Available: <https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf>
- [5] R. Daton Medenou, V. Calzado Mayo, M. Garcia Balufo, M. Páramo Castriello, F. González Garrido, A. Luis Martínez, D. Nevado Catalán, D. Hu, A. Sandoval Rodríguez-Bermejo, J. Maestre Vidal, G. Ramis Pasqual De Riquelme, A. Berardi, P. De Santis, F. Torelli, and S. Llopis Sanchez, “CYSAS-S3: a novel dataset for validating cyber situational awareness related tools for supporting military operations,” in *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES)*, Dublin, Ireland, August 2020, pp. 1–9.
- [6] F. F.-H. Nah, Q. Zeng, V. R. Telaprolu, A. P. Ayyappa, and B. Eschenbrenner, “Gamification of education: A review of literature,” in *HCI in Business*. Cham: Springer International Publishing, 2014, pp. 401–409.
- [7] P. Blikstein and M. Worsley, “Multimodal learning analytics and education data mining: using computational technologies to measure complex learning tasks,” *Journal of Learning Analytics*, vol. 3, no. 2, pp. 220–238, 2016.