

UNIVERSIDAD POLITÉCNICA DE MADRID

**ESCUELA TÉCNICA SUPERIOR
DE INGENIEROS DE TELECOMUNICACIÓN**



**GRADO EN INGENIERÍA DE
TELECOMUNICACIONES Y SERVICIOS DE
TELECOMUNICACIÓN**

TRABAJO FIN DE GRADO

**DISEÑO Y PROTOTIPADO DE UN MODELO
DE DETECCIÓN DE CORRELACIÓN
ENTRE EVENTOS EN EL CIBERESPACIO
Y OTROS DOMINIOS**

JUAN RODRÍGUEZ DELGADO

2022

GRADO EN INGENIERÍA DE TELECOMUNICACIONES Y SERVICIOS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

Título: DISEÑO Y PROTOTIPADO DE UN MODELO DE DETECCIÓN DE CORRELACIÓN ENTRE EVENTOS EN EL CIBERESPACIO Y OTROS DOMINIOS

Autor: D. Juan Rodríguez Delgado

Tutor: D. Víctor Abraham Villagra González

Ponente: D. Juan Rodríguez Delgado

Departamento: Departamento de Ingeniería de Sistemas Telemáticos

MIEMBROS DEL TRIBUNAL

Presidente: D.

Vocal: D.

Secretario: D.

Suplente: D.

Los miembros del tribunal arriba nombrados acuerdan otorgar la calificación de:
.....

Madrid, a de de 20...

UNIVERSIDAD POLITÉCNICA DE MADRID

**ESCUELA TÉCNICA SUPERIOR
DE INGENIEROS DE TELECOMUNICACIÓN**



**GRADO EN INGENIERÍA DE
TELECOMUNICACIONES Y SERVICIOS DE
TELECOMUNICACIÓN**

TRABAJO FIN DE GRADO

**DISEÑO Y PROTOTIPADO DE UN MODELO
DE DETECCIÓN DE CORRELACIÓN ENTRE
EVENTOS EN EL CIBERESPACIO Y OTROS
DOMINIOS**

JUAN RODRÍGUEZ DELGADO

2022

RESUMEN

Durante las últimas décadas, hemos visto como el ciberespacio se ha establecido como el quinto dominio de la seguridad, junto a la tierra, mar, aire y el espacio.

Sin ir más lejos, en el contexto del conflicto reciente entre Rusia y Ucrania han sucedido varios ataques cibernéticos con el objetivo de desestabilizar el país ucraniano. También Rusia tiene una larga historia de ciberataques con Estados Unidos, tanto con organismos nacionales como con empresas privadas. Algunos de estos ataques serán expuestos en este documento.

El objetivo principal de este trabajo es el diseño de un modelo capaz de detectar correlaciones entre eventos que suceden en el ciberespacio y los otros cuatro dominios de la seguridad con el fin de poder tener mayor conciencia sobre lo que sucede en ese momento. De esta manera el modelo será capaz de identificar riesgos de ciberseguridad e integrar estos en un entorno de gestión dinámico de riesgos de ciberseguridad.

En este documento se comenzará con una introducción y un estudio del estado del arte en cuanto a ciberseguridad se refiere. Se proseguirá con una explicación sobre las guerras híbridas y como ellas se pueden enlazar con conflictos más actuales, como la reciente guerra entre Rusia y Ucrania y la influencia que tuvo el país ruso en las elecciones de 2016 de la presidencia de Estados Unidos.

Además, se van a analizar ciertos conceptos más relacionados con la ciberdefensa, entre los que se encuentran la *Cybersituational Awareness* (CSA) y el *Key Cyber Terrain* (KCT). También se expondrán algunas de las soluciones existentes para la monitorización y correlación de eventos como los *Security Information and Event Management* (SIEMs), sistemas cuyo fin es detectar la correlación de varios eventos que suceden en sistemas diferentes de una red.

Por último, se analizará la efectividad del modelo creado y se indicarán algunos de los posibles avances que podrían realizarse en proyectos futuros.

SUMMARY

During the last decades, we have seen how the cyberspace has been established as the fifth domain of security, along with earth, sea, air, and space.

Without having to go any further, in the Russian-Ukrainian conflict there have been several cyberattacks with the objective of destabilizing Ukraine. In addition to that, Russia has a long history of performing cyberattacks to other countries, such as the United States of America, targeting both national institutions and private companies. Some of these attacks will be explained in this document.

The main objective of this project is the design of a model capable of detecting correlations between events that occur on the cyberspace and events that occur on the other four security domains with the purpose of having a greater understanding of what is happening at that moment. This way, the model will be capable of identifying cybersecurity risks and integrate them in a dynamic risk management environment.

This document starts with an introduction and an overview of the state-of-the-art in cybersecurity. Following that there is an explanation of the concept of hybrid wars and how they are related to recent conflicts such as the recent war between Russia and Ukraine and the Russian influence in the 2016 United States Presidential Election.

In addition to that, other concepts related to cyber defense are also analyzed, such as *Cybersituational Awareness* (CSA) and the *Key Cyber Terrain* (KCT). Also, some of the existing solutions for monitoring and correlation of events such as the *Security Information and Event Management* (SIEMs), systems which purpose is to detect the correlation between several events that occur in different systems of the same network.

Finally, the document ends with an analysis of the model and some suggestions for future works of possible lines of research.

PALABRAS CLAVE

Ciberseguridad, ciberdefensa, correlación, análisis de riesgos, ciberespacio, modelo

KEYWORDS

Cybersecurity, cyber defense, correlation, risk analysis, cyberspace, model

ÍNDICE DEL CONTENIDO

1. INTRODUCCIÓN Y OBJETIVOS	1
1.1. Introducción	1
1.2. Objetivos	1
1.3. Estructura del trabajo	1
2. ESTADO DEL ARTE	2
2.1. Reconocimiento Complejo de Eventos (<i>Complex Event Recognition</i>)	2
2.2. Ciberdefensa	2
2.2.1. Cibersituational Awareness (CSA)	2
2.2.2. <i>Key Cyber Terrain</i> (KCT).....	3
2.2.3. Tactical Clouds	4
2.2.4. Economic Denial of Sustainability (EDoS)	4
2.2.5. Tactical Denial of Sustainability (TDoS).....	5
2.3. Correlación.....	7
2.3.1. Modelos de correlación.....	9
2.4. Guerra Híbrida	10
2.5. Ataques cibernéticos de Rusia a EE. UU.....	11
2.6. Conflicto ruso-ucraniano.....	11
3. DISEÑO DEL PROTOTIPO.....	13
3.1. Entorno CIS	13
3.1.1. Modelo de información.....	13
3.1.2. Análisis de Riesgos	17
3.1.3. Proof of Concept	24
3.2. Entorno Misión	28
3.2.1. Modelo de Información.....	28
3.2.2. Análisis de Riesgos	30
3.2.3. Proof of Concept	35
3.3. Esquema de definición de correlaciones	36
4. ELABORACIÓN DEL PROTOTIPO	41
5. CONCLUSIONES Y LÍNEAS FUTURAS	45
5.1. Conclusiones.....	45
5.2. Líneas futuras.....	45
5.3. Valoración personal	45
6. BIBLIOGRAFÍA.....	46
ANEXO A: ASPECTOS ÉTICOS, ECONÓMICOS, SOCIALES Y AMBIENTALES	52

A.1 Introducción	52
A.2 Descripción de impactos relevantes relacionados con el proyecto	52
A.3 Análisis detallado de alguno de los principales impactos	52
A.4 Conclusiones	52
ANEXO B: PRESUPUESTO ECONÓMICO	53

ÍNDICE DE FIGURAS

FIGURA 1.- ARQUITECTURA DE LA HERRAMIENTA DE PROTECCIÓN PROPUESTA	5
FIGURA 2.- EJEMPLO DE PROPAGACIÓN VERTICAL DE UNA AMENAZA TDoS.....	6
FIGURA 3.- MODELO DE ESTADOS PARA LA DEFENSA DE ATAQUES TDoS	7
FIGURA 4.- ESQUEMA GENÉRICO DE UN CORRELADOR DE EVENTOS	8
FIGURA 5.- ESQUEMA DEL SISTEMA DE CORRELACIÓN DE EVENTOS	9
FIGURA 6.- ARQUITECTURA DEL RUN-TIME CORRELATION ENGINE.....	10
FIGURA 7.- INCREMENTO EN EL TRÁFICO MALICIOSO DIRIGIDO A USUARIOS UCRANIANOS ALREDEDOR DEL 8 DE MARZO.....	12
FIGURA 8.- TABLA DE CLASIFICACIÓN DE ACTIVOS CIS	16
FIGURA 9.- ACTIVOS AFECTADOS POR CADA AMENAZA CIS	18
FIGURA 10.- CRITERIO PARA EL ANÁLISIS CUANTITATIVO DE PROBABILIDAD	19
FIGURA 11.- PROBABILIDAD DE PARES ACTIVO-AMENAZA CIS	20
FIGURA 12.- CRITERIO PARA EL ANÁLISIS CUANTITATIVO DE IMPACTO	21
FIGURA 13.- IMPACTO DE PARES ACTIVO-AMENAZA CIS.....	21
FIGURA 14.- RIESGO DE PARES ACTIVO-AMENAZA CIS	23
FIGURA 15.- PROBABILIDADES CORREGIDAS ACTIVO-AMENAZA CIS	25
FIGURA 16.- IMPACTO CORREGIDO ACTIVO-AMENAZA CIS	26
FIGURA 17.- RIESGO CORREGIDO DE PARES IMPACTO-AMENAZA CIS	27
FIGURA 18.- TABLA DE CLASIFICACIÓN DE ACTIVOS MISIÓN	29
FIGURA 19.- ACTIVOS AFECTADOS POR CADA AMENAZA MISIÓN.....	31
FIGURA 20.- PROBABILIDAD DE PARES ACTIVO-AMENAZA MISIÓN.....	32
FIGURA 21.- IMPACTO DE PARES ACTIVO-AMENAZA MISIÓN	33
FIGURA 22.- RIESGO DE PARES ACTIVO-AMENAZA MISIÓN	34
FIGURA 23.- RIESGO CORREGIDO DE PARES ACTIVO-AMENAZA MISIÓN	35
FIGURA 24.- $P(\text{Riesgo CIS} \cap \text{Riesgo Misión})$	36
FIGURA 25.- $P(\text{Riesgo CIS} \mid \text{Riesgo Misión})$	37
FIGURA 26.- PROBABILIDADES AMENAZAS MISIÓN - ACTIVOS CIS.....	38
FIGURA 27.- $P(\text{Riesgo Misión} \mid \text{Riesgo CIS})$	39
FIGURA 28.- PROBABILIDADES AMENAZAS CIS - ACTIVOS MISIÓN.....	40
FIGURA 29.- FUNCIONAMIENTO DEL PROTOTIPO	41
FIGURA 30.- INTERFAZ GRÁFICA DEL PROTOTIPO	42
FIGURA 31.- ESTADO DEL PROTOTIPO TRAS SIMULAR UNA AMENAZA	43

1. INTRODUCCIÓN Y OBJETIVOS

1.1.INTRODUCCIÓN

El ciberespacio se ha convertido en una parte más de nuestras vidas, llegando al punto de que es necesario tenerlo en consideración a la hora de hablar sobre conflictos políticos.

Debido a la dificultad existente a la hora de probar que los autores de ciberataques han sido apoyados por un gobierno, varios países, entre ellos Rusia, realizan ciberataques para poder desestabilizar a sus oponentes políticos, como se explicará en este documento.

Además, los ciberataques se usan como arma en conflictos a gran escala, ya que actualmente todos los ejércitos utilizan las tecnologías de la información a la hora de llevar a cabo sus operaciones militares, por lo que realizar ataques a activos militares presentes en el ciberespacio puede llegar a causar daños en los ejércitos.

Sin embargo, las relaciones que pueden llegar a haber entre dichos ciberataques y sus consecuencias en el resto de los dominios de la seguridad no están claras, al igual que las relaciones entre ataques realizados en tierra, mar, aire y espacio y sus consecuencias en el ciberespacio.

Este trabajo servirá como un punto de partida para poder definir de manera concreta las relaciones existentes entre estos dominios, de manera que nos ayudará a entender mejor la importancia que puede llegar a tener el ciberespacio en conflictos a gran escala.

1.2.OBJETIVOS

Los principales objetivos que se pretenden cumplir en la elaboración de este trabajo son:

- Creación de dos modelos de información, uno para simbolizar los activos y amenazas presentes en el ciberespacio, conocido como Modelo CIS y otro para los activos y amenazas relacionados con el campo de batalla, llamado Modelo Misión.
- Realización de un análisis de riesgos en cada uno de estos dos modelos, para poder comprender como las amenazas de cada modelo afectan a los activos.
- Elaboración de un prototipo de modelo de correlación que nos ayude a entender las relaciones entre amenazas en uno de los modelos (CIS o Misión) y como estas pueden llegar a afectar a los activos del otro modelo.

1.3. ESTRUCTURA DEL TRABAJO

El presente trabajo se desarrolla a lo largo de cinco capítulos. El primer capítulo realiza una introducción a la materia y a los objetivos del presente trabajo. El segundo capítulo explica la situación actual en cuanto a ciberdefensa y a guerras híbridas se refiere. El tercer capítulo define ambos modelos de información y el esquema de correlación. El cuarto capítulo expone el prototipo realizado y, por último, el quinto capítulo describe las conclusiones extraídas del trabajo y se describen posibles líneas de trabajo futuras.

2. ESTADO DEL ARTE

2.1. RECONOCIMIENTO COMPLEJO DE EVENTOS (*COMPLEX EVENT RECOGNITION*)

El Reconocimiento Complejo de Eventos [1] o en inglés *Complex Event Recognition (CER)*, es una tecnología que permite analizar y correlacionar grandes cantidades de datos con el objetivo de detectar eventos importantes. Con esta información, los usuarios finales podrán tomar decisiones más fácilmente.

Para detectar estos eventos se utilizan patrones que especifican qué condiciones se han de cumplir para que los eventos sucedan. Estos patrones son diferentes en función del contexto en el que apliquemos esta tecnología.

2.2. CIBERDEFENSA

2.2.1. CIBERSITUATIONAL AWARENESS (CSA)

La conciencia situacional, también conocida como *Situational Awareness (SA)*, se basa en la obtención de información y entendimiento del entorno para una mejor toma de decisiones. [2]

El bucle ODDA es uno de los modelos de toma de decisiones más relacionados con la SA, inicialmente propuesto por John Boyd [3]. Este bucle consiste en cuatro fases (*Observe* → *Orient* → *Decide* → *Act*) que se iteran continuamente. En [4], se realizó un modelo basado en ODDA más adaptado al contexto del ciberespacio, de manera que se puedan delegar ciertas tareas a los sistemas informáticos, al contrario que el bucle ODDA, que necesita de la intervención de agentes humanos para su aplicación.

En el contexto del ciberespacio, hablamos de *Cybersituational Awareness* o (CSA). Según [5], se puede resumir este concepto en cuatro componentes:

1. Saber lo que debería estar sucediendo.
2. Averiguar lo que está sucediendo.
3. Inferir cuando lo que está sucediendo no es lo que debería estar sucediendo.
4. Resolver el conflicto si es necesario.

Para saber lo que debería estar sucediendo, tenemos que conocer: los usuarios, los dispositivos y su propósito y las aplicaciones y procesos y cuando se deben usar.

Si queremos averiguar lo que está sucediendo lo mejor es monitorizar los dispositivos, aplicaciones y usuarios, conocer las vulnerabilidades a las que están expuestas los dispositivos, y aplicaciones y los patrones de uso cotidianos de los dispositivos y cuentas de usuario.

De esta manera, si comparamos lo que sucede con lo que debería suceder podemos averiguar si está pasando algo inusual.

Para detectar intrusiones en nuestra red se utilizan sistemas de detección de intrusiones (o IDS de sus siglas en inglés *Intrusion Detection System*). Estos sistemas permiten descubrir, determinar e identificar acciones como el uso no autorizado, la duplicación, alteración y destrucción de información o de los sistemas informáticos. [6] Estas detecciones se pueden realizar para ataques que tienen su origen en la misma organización tanto como para ataques que se realicen desde el exterior.

Para encontrar posibles amenazas, los IDS pueden realizar ciber análisis basándose en anomalías, en firmas u optar por un análisis híbrido que combine los dos anteriores. [7]

Las firmas son conjuntos de acciones, condiciones o actividades, que cuando se cumplen indican una intrusión. Los IDS que realizan análisis basado en firmas suelen detectar un mayor número de intrusiones y un menor número de falsos positivos, pero solo pueden detectar ataques ya registrados en la base de datos, por lo que no pueden detectar ataques de día 0.

El análisis basado en anomalías puede detectar ataques de día 0, pero también genera un mayor número de falsos positivos, por lo que también es popular realizar un tipo de análisis híbrido que combine características de los dos métodos de análisis ya expuestos.

Herramientas como los IDS pueden hacer uso de los llamados *datasets*, conjuntos de datos que contienen el tráfico de datos realizado en ataques, sean estos simulados o no. Existen *datasets* con un carácter más centrado a la industria como LBNL [8] y otros más cercanos al mundo militar como DARPA'99 [9]. En este trabajo expondré el *dataset* CYSAS-S3 [10], debido a que es un *dataset* más reciente y porque fue diseñado para que su uso fuese posible en entornos militares.

Para la generación de los datos de CYSAS-S3, se realizaron varios ataques simulados de filtración de datos, denegación de servicios (DDoS) y robo de credenciales. Aparte de ello, también se han misiones militares para así poder generar datos más relevantes para la ciberdefensa. De esta manera, CYSAS-S3 es capaz de no solo descubrir potenciales ataques y amenazas, sino de también proponer posibles respuestas para ellas.

CRUSOE [11], es un conjunto de herramientas que facilita el CSA, la toma de decisiones y la respuesta contra incidentes.

Aplicando esto al entorno de la ciberseguridad, en la primera fase observa la red y los sistemas que están presentes en ella, mediante el descubrimiento de vulnerabilidades, identificación de los hosts y la observación de eventos medibles, como la detección de intrusos. Ya que en [11] se recalca que CRUSOE únicamente sirve para apoyar al operador mediante la recolección de datos y la posibilidad de realizar cambios en la red, es el operador el que se orienta por los datos recibidos, decide las acciones a realizar para incrementar la capacidad defensiva del entorno y, finalmente, ejecuta mediante CRUSOE dichas acciones.

2.2.2. KEY CYBER TERRAIN (KCT)

Key Cyber Terrain (KCT) es un término usado como una analogía al concepto de *Key Terrain* utilizado en la doctrina militar para describir posiciones geográficas que otorgan una ventaja estratégica. [12]

En [13] se divide el entorno del ciberespacio en cinco niveles en los cuales podemos identificar KCT:

- **Supervisor:** Es el nivel en el que se vigilan nuestros activos y desde en el que se controlan ataques cibernéticos y se defiende de ellos.
- **Ciber persona:** En este nivel se identifican las identidades (como cuentas de usuario, licencias de software...) y las relaciones entre sí.
- **Lógico:** Incluye el sistema operativo y software instalados en una máquina. Se puede subdividir en los seis niveles superiores del modelo OSI (aplicación, presentación, sesión, transporte, red y enlace).
- **Físico:** Se puede equiparar con el nivel restante del modelo OSI.
- **Geográfico:** Posición geográfica de nuestros activos.

Se pueden usar las metodologías expuestas en [14] para la identificación de KCTs:

- **Análisis de centralidad:** Se basa en representar áreas y los caminos entre sí como un grafo y declarar como KCT las áreas correspondientes a los nodos que están más cerca del centro del grafo. El problema de este análisis es el hecho de que no puede aplicar conciencia situacional, por lo que no considera cuales con las áreas controladas por el enemigo.
- **Sistema dinámico:** A través de un modelo basado en cadenas de Markov, se describen los movimientos que se realizan entre áreas, para así poder declarar como KCT las áreas más visitadas. A pesar de que este modelo puede tomar en cuenta las localizaciones del adversario, no puede representar los múltiples caminos que puede haber entre dos áreas.
- **Modelado basado en agentes:** Es muy flexible y el más realista, pero mucho menos eficiente que las otras dos metodologías.

Además de estas tres metodologías, en [15] se utiliza la metodología *Multi-Attribute Decision Making* (MADM), la cual elige el KCT entre un número finito de candidatos mediante la comparación de los atributos de los candidatos. [16]

Sin embargo, es complicado trasladar directamente el concepto de *Key Terrain* al ciberespacio, ya que, como se explica en [17], al contrario que en un terreno físico, es difícil identificar las áreas importantes de nuestra red con simplemente un vistazo y que, pese a que se podría dividir nuestra infraestructura de red en varios servicios más simples, el hecho de que todos ellos están conectados entre sí dificulta aislarlos y seleccionar uno como “servicio clave”.

2.2.3. TACTICAL CLOUDS

Como las comunicaciones militares en entornos *Beyond Line of Sight* (BLOS) se realizan con redes *ad hoc*, es decir, sin estación base, [18], sus redes se pueden desplegar más rápidamente y son más resilientes. Sin embargo, este tipo de redes también tienen una serie de debilidades, entre las que destacan son un ancho de banda y una energía limitadas. [19]

Para solucionar este problema, se han realizado técnicas similares a las que se aplican en entornos de computación en la nube con el fin de maximizar los escasos recursos de los que disponen. A esto se le conoce como *Tactical Clouds*. [20]

Algunos de las técnicas heredadas de la computación en la nube son *Cloudlets*, *Self-Organizing Networking* (SON) y *Group Centric Networking* (GCC).

Los *Cloudlets* son pequeños *datacenters* que se colocan al borde de Internet, de manera que estén posicionados más cerca de los usuarios y estos puedan disponer de sus recursos más rápidamente. [21]

SON es una tecnología que automatiza la configuración, automatización, optimización y administración de redes móviles. Ha sido estandarizada por el 3GPP para su uso en LTE. [22]

Por último, GCC se basa en crear una estructura de red formada por varios grupos, cuyos miembros colaboran entre sí para conseguir objetivos (pelotones, barcos...). Estos grupos pueden ser formados con anterioridad a la misión o sobre la marcha. De esta manera, la mayor parte del tráfico se envía únicamente entre los usuarios de un grupo. [23]

A pesar de todas las ventajas que las *Tactical Clouds* pueden aportar al entorno militar, estas también sufren de algunas de las vulnerabilidades propias de la computación en la nube, como es el caso de los ataques de *Economic Denial of Sustainability* (EDoS) [24] o el ampliamente conocido *Distributed Denial-of-Service attack* (DDoS attack).

2.2.4. ECONOMIC DENIAL OF SUSTAINABILITY (EDOS)

Ya en 2008 [25], Chris Hoff teorizó sobre las posibles consecuencias que tendría el hecho de que un atacante se aprovechara del hecho de que servicios como AWS pagan por el uso que se les da para realizar múltiples peticiones a los servidores de manera que pareciesen legítimas y de esa manera aumentar el coste de esos servicios.

En un artículo posterior a principios de 2009 [26], Hoff explicó un ejemplo que consiste en una página web cuyos ingresos provienen de compras de *ecommerce*. En este ejemplo se realizan varias peticiones legítimas, pero no se compra nada, por lo que el vendedor ha de pagar el coste que ha supuesto atender a esas peticiones sin haber conseguido ganancias por compras de *ecommerce*.

Sonami [27] estudió las consecuencias de esta subida de costes, ya que, aparte de afectar al cliente, la calidad del servicio ofrecida por el proveedor de infraestructura en la nube también se verá afectada. Esto, sumado al incremento de costes por parte del cliente como se ha mencionado anteriormente, provocará que el cliente busque un proveedor más barato y daños a la reputación del proveedor, lo que también afectará a los ingresos del proveedor a largo plazo.

En [28] se realiza una distinción entre dos tipos de EDoS: *Workload-based EDoS* (W-EDoS) e *Instantiation-based EDoS* (I-EDoS).

W-EDoS consiste en forzar al servidor a responder a peticiones que consumen una gran cantidad de recursos computacionales, de manera que su carga de trabajo aumenta y el gestor del servicio es forzado a contratar más recursos.

En cuanto a I-EDoS, este ocurre cuando el *software* de *cloud management*, para atender a una petición aparentemente legítima, pero que es en realidad maliciosa, utiliza un mayor número de recursos de los necesarios, aumentando de esta manera el número de recursos contratados.

Se han elaborado medidas de protección contra ataques EDoS como el expuesto en [29]. Ya que sus creadores opinan que todos los ataques a servidores de *cloud computing* se pueden clasificar en tres tipos (ataques de consumo de ancho de banda, ataques a la capa de transporte y ataques a aplicaciones específicas), decidieron crear una herramienta capaz de detectar y defenderse ante 3 tipos de ataques diferentes, de manera que cada uno de ellos se correspondiera con un tipo de ataque a servicios *cloud computing*.

Estos ataques son: ataques de inundación HTTP (correspondiente a los ataques de consumo de ancho de banda), ataques contra bases de datos (correspondiente a los ataques contra servicios específicos) y, por último, ataques de inundación SYN (correspondiente a los ataques a la capa de transporte).

Ya que cada uno de los servicios en *cloud computing* suele tener su propia máquina virtual, la herramienta de protección se conecta al enlace entre las máquinas virtuales y el hipervisor, de manera que pueda observar todo el tráfico entre MV e hipervisor y de esa manera detectar irregularidades.

Otra ventaja de este posicionamiento es que, cuando las MVs piden más recursos al hipervisor, la herramienta es capaz de decidir si se deben otorgar esos recursos o, por el contrario, se trata de un ataque y se limitan los recursos de la MV.

Por último, se evita la propagación del ataque a otros hipervisores, ya que normalmente, cuando un hipervisor está escaso de recursos, traslada la MV a otro hipervisor.

Se puede ver un diagrama más detallado de la herramienta en (Figura 1):

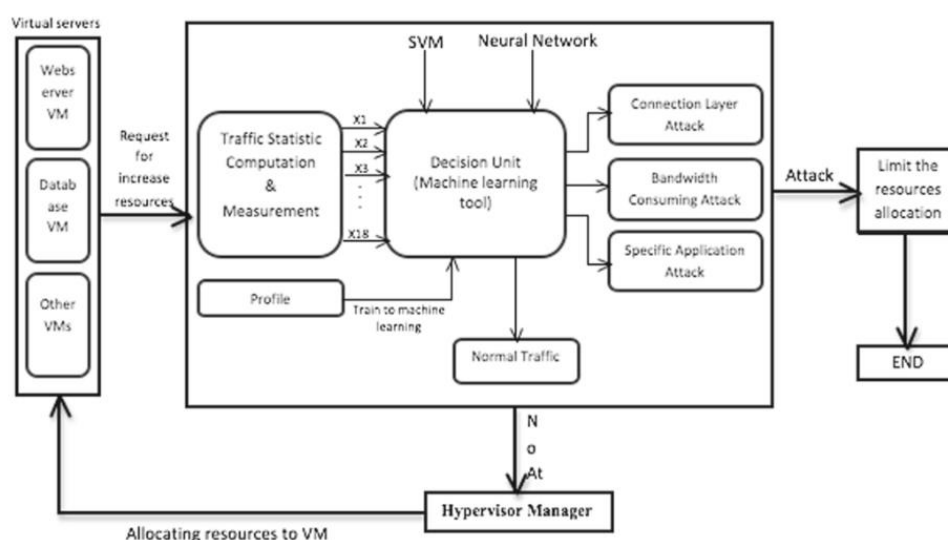


Figura 1.- Arquitectura de la herramienta de protección propuesta

2.2.5. TACTICAL DENIAL OF SUSTAINABILITY (TDOS)

Los ataques TDoS constan de poner en peligro la sostenibilidad de una *Tactical Cloud* [30], impactando así las funciones de esta, influyendo de esta manera en la toma de decisiones de la víctima.

Un ejemplo de ataque EDoS que provoca TDoS sería el que se puede ver en (Figura 2) procedente de [24]:

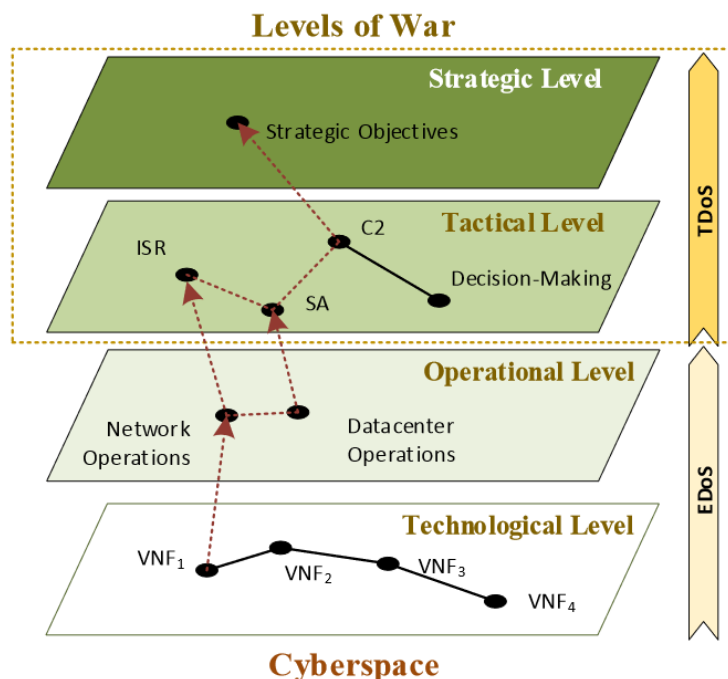


Figura 2.- Ejemplo de propagación vertical de una amenaza TDoS

Como se puede ver en (Figura 2), existen varias *Virtual Network Functions* (VNFs) desplegadas. Según la *European Telecommunications Standards Institute* (ETSI) [31], una *Network Function* (NF) es un bloque funcional dentro de una infraestructura de red con unas interfaces y un comportamiento definidos y una VNF consiste en separar las NFs del hardware en el que se ejecutan usando herramientas de abstracción de hardware virtual.

En la figura se puede observar que, en este caso, las VNFs se encuentran en el nivel tecnológico y son la base de operaciones que red, datos y comando y control. Si el atacante realiza un I-EDoS como los que se explicaron anteriormente, el atacante forzaría la creación de un gran número de VNFs que no son necesarias, por lo que la infraestructura no tendrá los recursos computacionales necesarios para las VNFs que soportan las operaciones vitales de la *Tactical Cloud*.

De esta manera un ataque EDoS ha impactado en las funciones de una *Tactical Cloud*, por lo que se podría decir que mediante un EDoS se pueden realizar TDoS. Sin embargo, en [24] se muestra cómo, a pesar de que ataques EDoS pueden provocar situaciones TDoS, existen otras maneras de provocar TDoS que no tienen ninguna relación con ataques EDoS.

Existen dos tipos de TDoS, *Maintenance-based Tactical Denial of Sustainability* (U-TDoS) y *Deployment-based Tactical Denial of Sustainability* (D-TDoS). [24]

U-TDoS sucede cuando el coste de mantenimiento de un servicio sufre un gran incremento en un momento inesperado. En el caso de D-TDoS, este consiste en un gran e inesperado incremento de las VNFs en las que se basa un servicio.

En [32] se proponen dos medidas de defensa contra ataques TDoS en función del tipo de ataque. Ambas se basan en modelos de estados como el de (Figura 3):

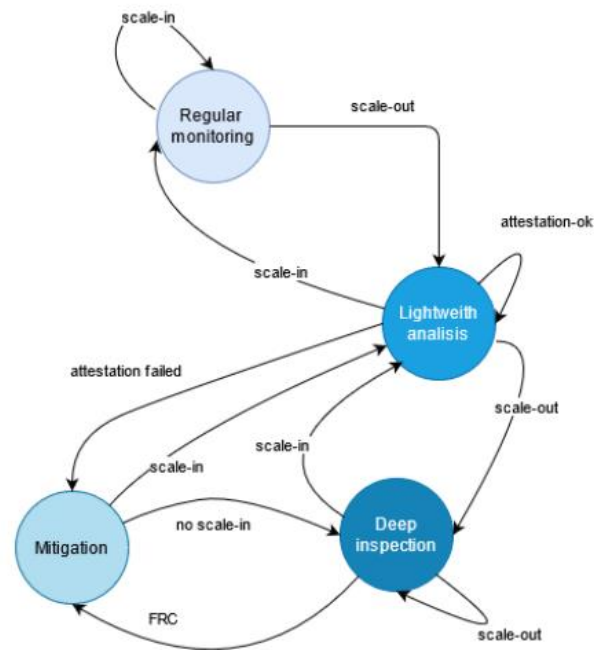


Figura 3.- Modelo de estados para la defensa de ataques TDoS

En este modelo se comienza en la fase de *Regular Monitoring*. En este estado se utiliza una mínima cantidad de recursos para monitorizar el uso del sistema. En el caso de que el sistema de defensa detecte una anomalía, se pasa al *Lightweight Analysis*, estado en el cual se busca a los grupos de usuarios causantes de dicha anomalía.

Si se encuentran, el sistema cambia al estado de *Mitigation*, para así poder tomar las medidas pertinentes para desconectar a los usuarios maliciosos del servicio y redistribuir los recursos que se están utilizando de manera que solo se utilicen aquellos que sean necesarios.

En caso contrario, el sistema pasa al estado de *Deep Inspection*, en el que se utiliza un nodo de análisis separado del resto del sistema para hacer un análisis profundo. Esto conlleva un alto coste en cuanto a recursos, por lo que se reserva para situaciones excepcionales. En cuanto se encuentren a los usuarios causantes del ataque, el sistema pasará al estado de *Mitigation* como se describió anteriormente.

2.3.CORRELACIÓN

Se entiende como correlación el grado y tipo de relación que puede existir entre dos o más variables. En cuanto a la correlación de eventos, se trata de un proceso en el que se analizan series de eventos con el propósito de detectar grupos de eventos que suceden en ventanas de tiempo predefinidas. [33]

Generalmente, los sistemas de correlación tienen una arquitectura parecida a la expuesta en (Figura 4) procedente de [34]:

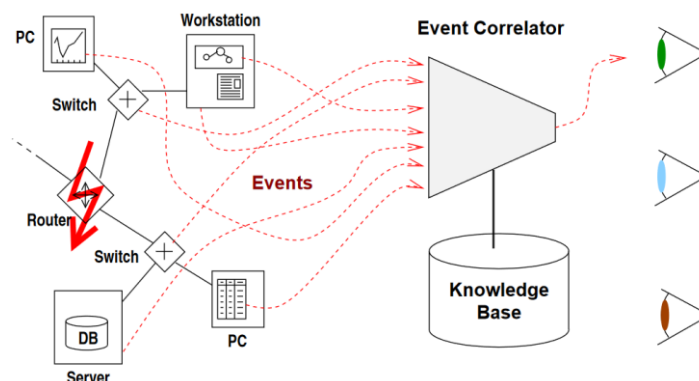


Figura 4.- Esquema genérico de un correlador de eventos

En este modelo, se puede ver que los datos de entrada del correlador proceden de una variedad de dispositivos de diferentes tipos. El correlador trata de averiguar cuando los eventos están relacionados entre sí gracias a los datos guardados en la *Knowledge Base*. El correlador devuelve datos más concretos para que sean más fáciles de entender por los administradores.

También existen sistemas de monitorización y correlación de eventos como el de [35] en los que se incluye un monitor que detecta los eventos que suceden en un sistema y produce una serie de datos en base a dichos eventos. Estos eventos se guardan en una base de datos usando un lenguaje que expresa los eventos siguiendo un *Event Pattern Language* (EPL).

En el caso de [35], se recomienda usar *Formal Language For Expressing Assumptions* (FLEA), ya que incluye varios patrones comunes de eventos a los cuales se les puede añadir reglas y relaciones entre eventos adicionales que desee el usuario. De esta manera se definen las condiciones que han de cumplirse para que el sistema detecte una correlación.

Los patrones y relaciones de eventos especificados se compilan en una base de datos usando un compilador de eventos. De esta manera, cuando existe una correlación entre los eventos detectados, el sistema nos avisará de ello.

Otro sistema de correlación de eventos es [36], destacable porque, a diferencia del sistema explicado anteriormente, basado en patrones de reglas, este utiliza matrices aleatorias y análisis de similitud basado en grafos para encontrar correlaciones. De esta manera, los eventos son representados mediante grafos en redes de correlación y los datos en la *Knowledge Base* son comparados con los eventos mediante técnicas de comparación de grafos.

Ahora procederemos a explicar en mayor detalle el funcionamiento de este sistema, cuyas partes aparecen descritas en (Figura 5):

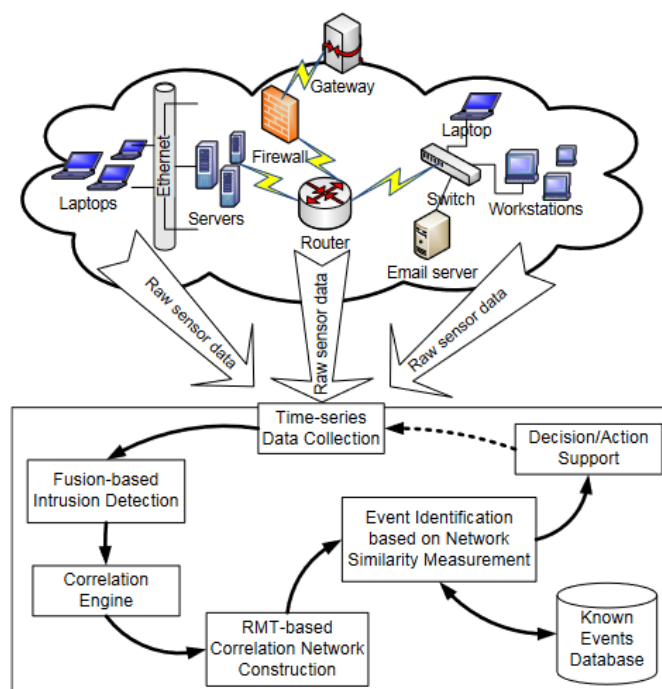


Figura 5.- Esquema del sistema de correlación de eventos

Este sistema utiliza varios sensores presentes en varios sistemas y redes para recoger eventos. De manera autónoma y en base a los eventos recogidos, cada sensor decide si hay una amenaza presente en la red y reporta su decisión al *Time Series Data Collection* presente en la figura anterior.

Basándose en las decisiones tomadas por cada sensor, el *Fusion-based Intrusion Detection* decide si está sucediendo una intrusión. En caso afirmativo, el *Correlation Engine* se activa y construye una matriz de correlación de eventos en base a los datos recogidos por los sensores.

Seguidamente, y basándose en esta matriz, la *RMT-based Correlation Network Construction* construye una red de correlación de eventos y, como hemos dicho anteriormente, los eventos se comparan con la base de datos de eventos mediante técnicas de comparación de grafos. Tras esto pueden suceder dos posibilidades:

- a) Si se encuentra una red de correlación en la base de datos similar al recogido, el sistema toma las medidas de defensa pertinentes e informa al sistema de la coincidencia entre eventos para así poder refinar los indicadores de eventos o redesplegar los sensores.
- b) Si no se encuentran coincidencias, la red de correlación se añade a la base de datos como futura referencia.

Por último, es interesante mencionar a los *Security Information and Event Management* (SIEMs), los cuales recogen eventos de varios sistemas diferentes en una red, los convierte a un formato común y detectan correlaciones. [37] Sin embargo, estos sistemas suelen tener problemas cuando el volumen de eventos aumenta, ya que en ese momento también aumentan los falsos positivos y la cantidad de almacenamiento necesaria para guardar los eventos.

2.3.1. MODELOS DE CORRELACIÓN

Un ejemplo de modelo de correlación es el *Run-Time Correlation Engine* presente en [38]. Se puede ver un esquema de este modelo en [Figura 6]:

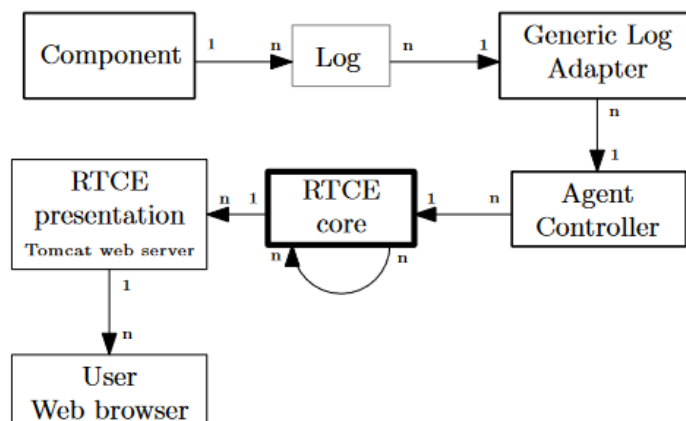


Figura 6.- Arquitectura del Run-Time Correlation Engine

Como se puede ver en la figura, cada uno de los elementos analizados por el modelo envía sus logs al *Generic Log Adapter* que convierte esos logs al formato *Common Base Events* (CBE) [39]. Para cada elemento analizado existe un *Agent Controller* (AC), un intermediario entre los adaptadores y el *RTCE core*.

El *RTCE core* está conectado a todos los AC y se encarga de recoger todos los eventos que suceden y procesarlos. La manera en la que los eventos son procesados depende del contexto usado. El contexto define que componentes se van a monitorizar, el nivel de filtrado usado y otras propiedades específicas del host. Estos contextos resultan especialmente útiles en grandes redes en las que se despliegan varias aplicaciones.

El *RTCE presentation* se despliega en un servidor web Tomcat junto al *RTCE core* para así poder aceptar peticiones de los usuarios y mostrar toda la información correlada en el navegador web del usuario.

2.4. GUERRA HÍBRIDA

Frank Hoffman fue el primer autor en utilizar el término “Guerra Híbrida” [40] para describir conflictos que mezclan elementos de lucha por la influencia sobre la población (lo que también se conoce como guerra irregular) y de conflictos de estado. Para Hoffman, el término “Híbrido” también se refiere a la organización de las partes beligerantes, que mezclan estructuras jerárquicas con células descentralizadas interconectadas entre sí.

Esta estrategia militar se ha ido volviendo más prevalente en Occidente durante los años recientes debido a factores como la falta de amenaza de un conflicto a gran escala y el poco conocimiento de los líderes políticos sobre las consecuencias de una guerra convencional. [41]

Algunos de los ejemplos que se suelen usar para describir la Guerra Híbrida son la Guerra de Vietnam [42] y la Guerra de la Independencia Española (las guerrillas españolas cooperaron con el ejército inglés) [43].

En cuanto a ejemplos más actuales, Rusia es un país sospechoso de haber estado involucrado en varios ciberataques conocidos públicamente y en el caso de los ciberataques realizados a Ucrania, estos han existido en un contexto de guerra híbrida, ya que recientemente se han visto combinados con la invasión del territorio ucraniano.

En este trabajo destacaremos los diversos ataques cibernéticos que el país ruso a realizado a Estados Unidos y la existente guerra híbrida entre Rusia y Ucrania, debido a su relevancia en la situación geopolítica actual.

A pesar de ello, es importante recalcar que se cree que Rusia ha realizado un número considerable de ciberataques adicionales en los cuales no profundizaremos.

Entre ellos se encuentran países como Francia, víctima de un ciberataque en el que se filtraron emails de Emmanuel Macron [44] con la intención de dañar su reputación 2 días antes de las elecciones a la presidencia de Francia en el año 2017. Como veremos más adelante, este ataque se asemeja a la filtración de emails sucedida en las elecciones presidenciales estadounidenses de 2016, ya que ambos se realizaron en circunstancias similares.

Otra de las elecciones en las que se acusa a Rusia de haber intervenido fueron las elecciones al parlamento alemán en 2021. [45] La Comisión Europea acusó a Rusia de apoyar al grupo de hackers Ghostwriter, responsables de varios ciberataques a miembros del parlamento y del gobierno alemán, además de políticos, periodistas y civiles mediante el acceso a sus ordenadores y el robo de sus datos personales.

2.5. ATAQUES CIBERNÉTICOS DE RUSIA A EE. UU.

Durante los últimos años, Rusia ha realizado múltiples ciberataques a países de Occidente, como el ciberataque que realizó a varias agencias federales de Estados Unidos en 2020, todas las ramas militares del ejército estadounidense y 425 corporaciones del Fortune 500. Se cree que este ataque comenzó con Rusia atacando a la empresa SolarWinds desde al menos octubre de 2019 [46] y que alrededor de marzo de 2020 los rusos consiguieron acceder a las agencias estadounidenses. El ataque no fue detectado hasta el 13 de diciembre de 2020. [47]

El éxito de este ciberataque radicó en el hecho de que cerca de 18000 usuarios descargaron una actualización modificada por los delincuentes rusos que introducía vulnerabilidades en los productos de monitorización Orion de la compañía SolarWinds. [48] [49]

Esto entra dentro de un contexto de Guerra Híbrida entre Estados Unidos y Rusia en la que también se puede destacar la intervención rusa en las Elecciones Presidenciales de Estados Unidos en el año 2016, que consistió principalmente en la creación de cuentas falsas en redes sociales que apoyaban posiciones políticas radicales y la filtración de los correos electrónicos de oficiales de campaña de Hillary Clinton para la posterior publicación de información que desprestigiase la imagen de la candidata demócrata. [50]

Por último, cabe destacar la intervención rusa en las elecciones de 2020. Ya desde el mes de agosto la *United States Intelligence Community* informó [51] que países como Rusia, China y hasta Irán tratarían de influenciar en el resultado de las elecciones estadounidenses. En el caso del país chino, estos buscaban la victoria de Joe Biden mientras que Rusia prefería una victoria del candidato republicano. En el caso de Rusia, en el informe se menciona que su metodología consistía en la filtración de llamadas de teléfono y difundir información falsa como por redes sociales como por canales de televisión.

2.6. CONFLICTO RUSO-UCRANIANO

Durante los últimos meses el conflicto ruso-ucraniano iniciado por la invasión rusa de Crimea en 2014 [52] se ha reactivado y ha ido escalando. En cuanto al ciberespacio se refiere, el grupo de hackers Armageddon, clasificado tanto como el gobierno ucraniano como la empresa Mandiant como una APT, ha estado operando desde al menos el año 2014 y ha realizado ataques a organismos del gobierno ucraniano. Esta organización usa métodos como el phishing o las vulnerabilidades CVE-2018-20250 de WinRAR, que permite introducir archivos en el disco local de la víctima y CVE 2017-0199 de Microsoft Office, que permite la ejecución remota de código. [53] [54]

Otro ataque destacable fue el ataque a la red eléctrica ucraniana en el año 2015, el cual se conoce como el primer ataque exitoso a una red eléctrica. [55] Se le atribuye este hackeo al grupo ruso Sandworm, el cual uso el malware BlackEnergy3 para este propósito. Se cree que este programa estuvo instalado en

los sistemas de red eléctrica 6 meses antes del ataque. Para instalar el malware, Sandworm comenzó realizando ataques de phishing a las oficinas de las compañías eléctricas. Estos emails infectados incluían ficheros adjuntos con macros que permitían a los hackers tomar control de las máquinas. Tras tomar control, adquirirían las credenciales de las VPNs usadas por los operadores del sistema eléctrico para acceder a los sistemas de control de red eléctrica. [56]

Como se puede ver, incluso antes del comienzo de la guerra, los ciberataques eran constantes. Más concretamente, es importante recalcar el hecho de que la SSU ha neutralizado más de 2000 ciberataques a organismos del gobierno en el año 2021. [57]

El 14 de enero de 2022, se realizó un ataque a docenas de páginas web del gobierno ucraniano, en el cual se cambió el texto de estas por un texto en ucraniano, ruso y polaco que alegaba que algunos datos personales habían sido filtrados. Sin embargo, la agencia de seguridad nacional ucraniana, *Security Service of Ukraine* (SSU), declaró que los datos de los usuarios no se vieron afectados. [58]

El 22 de febrero, dos días antes de la invasión rusa de Ucrania, se formó un equipo de respuesta contra ciber amenazas cuyos miembros proceden de varios países de Europa como Lituania, Croacia, Polonia, Rumanía, Países Bajos y Estonia. Esto se debió a los continuos ataques sufridos por Ucrania y al hecho de que las tropas rusas se encontraban aún en la frontera con dicho país. [59]

En el día siguiente, el 23 de febrero, un ataque DDoS fue realizado sobre páginas web del gobierno y el ejército ucraniano, además de varias páginas web de bancos. La mayoría de estas webs fueron restauradas tras unas horas, debido a que estaban preparadas para mitigar estos ataques. [60]

Tras la invasión, los ciberataques se incrementaron. Según el informe [61], los ataques a ucranianos se incrementaron hasta 10 veces más que en otros países europeos. Estos datos fueron proporcionados por la compañía Quad9 [62]. Quad9 es una plataforma de DNS recursivo (lo que quiere decir que realiza consultas a otros servidores DNS para encontrar direcciones IP) y gratuito que bloquea las peticiones DNS a sistemas maliciosos.

Al inicio de la invasión, las peticiones procedentes de Kiev disminuyeron notablemente, debido probablemente a cortes de luz o de fibra, pero como se puede ver en (Figura 7), ha habido un crecimiento grande en las peticiones maliciosas procedentes de Kiev y Varsovia:

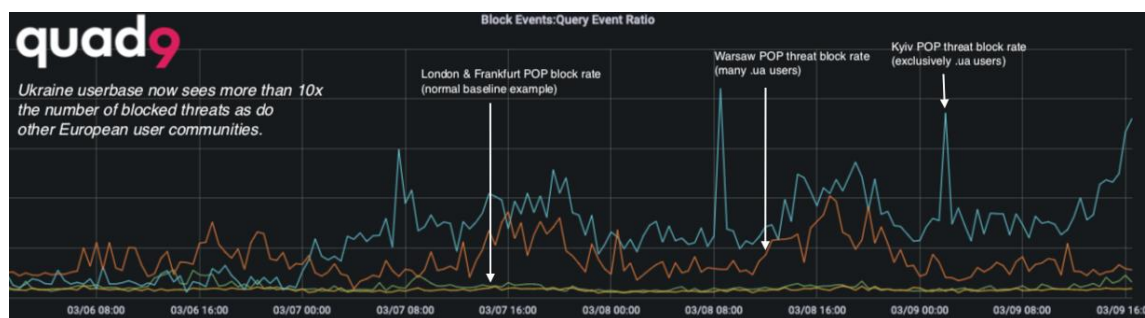


Figura 7.- Incremento en el tráfico malicioso dirigido a usuarios ucranianos alrededor del 8 de marzo

Se cree que el incremento de tráfico procedente de Varsovia ha sido provocado por ciudadanos ucranianos que huyeron al país vecino.

Para dar datos más concretos, John Todd, dirigente de Quad9 declaró que el 16 de febrero, Quad9 bloqueó 118 millones de peticiones en todo el mundo, y que 1,4 millones de esas peticiones procedían de Polonia y Ucrania (un 1,2% aproximadamente con respecto del total). El 9 de marzo Quad9 bloqueó 121 millones de peticiones en todo el mundo, y 4,6 millones de procedían de Ucrania o Polonia (un 3,8% respecto del total), lo cual es 3,28 veces mayor que los bloqueos ocurridos en febrero.

3. DISEÑO DEL PROTOTIPO

En esta parte se comenzará con el objetivo principal de este Trabajo de Fin de Grado, que es la elaboración de un modelo de correlación.

En primer paso, será necesario realizar un modelo de información para cada uno de los dos entornos que se desean correlar, estableciendo una serie de activos y amenazas para cada uno de ellos.

Tras la elaboración del modelo, se efectuará un análisis de riesgos en el que identificaremos vulnerabilidades de nuestros activos. Más tarde, los riesgos serán cuantificados y priorizados conforme a una serie de criterios que se explicarán posteriormente.

Después, los riesgos se tratarán siguiendo una de las siguientes estrategias: transferirlos, eliminarlos, asumirlos o mitigarlos.

Seguidamente se realizará una prueba de concepto para cada uno de los dos modelos, en la que se mostrará el riesgo final que tiene cada par activo-amenaza.

Posteriormente, se desarrollará un esquema de definición de correlaciones en el que se establecerán los coeficientes de correlación entre las amenazas de activos de un entorno y los activos del otro entorno, de manera que, por ejemplo, se podrá ver como el impacto de un misil a uno de los servidores pertenecientes al ejército afecta a los soldados en el campo de batalla, ya que la caída del servidor podría haber dañado los datos disponibles sobre el enemigo o los sistemas de comunicaciones, lo cual afecta al rendimiento de las tropas.

3.1. ENTORNO CIS

3.1.1. MODELO DE INFORMACIÓN

A la hora de realizar este modelo de información, se ha usado el modelo MARGERIT v3 [63], ya que está diseñado para el análisis y gestión de riesgos de sistemas de información, por lo que ayudará a la hora de identificar y clasificar activos y amenazas y realizar un análisis de riesgos.

ACTIVOS

Para la definición de activos se han consultado artículos como [64] en los que ya se han establecido una serie de activos y amenazas. A pesar de que el susodicho artículo este orientado hacia entornos de *cloud computing*, es posible adaptarlo al entorno militar, ya que, como se mencionó en el apartado de Tactical Clouds, es posible utilizar elementos de *cloud computing* en el campo de batalla.

En la elaboración de este modelo, se ha partido de la suposición de que todos los activos se encuentran en el mismo edificio, para así poder simplificar el análisis de riesgos.

En base a la información expuesta en el artículo ya mencionado, junto a información adicional que encontramos durante la búsqueda de información y que se mencionará más adelante, se ha decidido que los activos de nuestro modelo de información serán los siguientes:

- Sistema para *Cloud Based Internet Isolation* (CBII)
- Servidor proxy
- Router de acceso a Internet
- Cortafuegos
- Balanceador de carga
- Servidor web para usuarios externos
- Servidor web para usuarios pertenecientes a la red
- Terminales de usuarios

- Servidor de aplicación de uso interno que interactúa con la base de datos. Por ejemplo, una aplicación que realiza cálculos de algún tipo en función de la información en la BD.
- Servidor de base de datos
- Servidor de copias de seguridad
- Servidor de almacenamiento de datos, que incluye documentos confidenciales
- Fuentes de alimentación y cableado eléctrico

Con excepción del CBII, la mayoría de estos elementos son bastante comunes en los entornos de *cloud computing*.

En cuanto al CBII, se trata de un sistema que se apoya en la tecnología de *Browser Isolation*, que se basa en el cual el usuario navega por internet a través de un navegador que se está ejecutando en un entorno virtual como puede ser un contenedor o una máquina virtual. [65] Este entorno virtual se ejecuta en un servidor aislado al resto de la red, por lo que la exposición directa de los usuarios a las vulnerabilidades se reduce.

Esta tecnología fue reconocida por Gartner [66] como una de las tecnologías más importantes en el campo de la ciberseguridad en 2017. Algunos ejemplos de software que utilizan esta tecnología son WEBGAP y Silo, este último desarrollado por la compañía Authentic8.

El ejército de Estados Unidos comenzó a utilizar sistemas CBII en junio de 2021. [67] Según ellos, gracias a CBII se han reducido los tiempos de carga en un 50%, ya que las actividades relativas a la seguridad de los usuarios se ejecutan en el *cloud*, de manera que estas actividades están aisladas del resto de la red. Como anteriormente se realizaban en puntos de acceso a Internet de la red, la congestión del ancho de banda se ha reducido.

Otra de las ventajas que explicó el Departamento de Defensa de los Estados Unidos fue el hecho de que, con CBII, actualizar las versiones de los navegadores se convierte en una tarea más sencilla, ya que no tienen que preocuparse de problemas de compatibilidad, al encontrarse los navegadores aislados de los usuarios. [68]

Como se acaba de explicar, estos sistemas se encontrarían en nuestro modelo en un entorno aislado de los demás activos. A pesar de ello, y como se demostrará más adelante, CBII es un activo al tener en cuenta a la hora de establecer las correlaciones, ya que su mal funcionamiento causaría problemas de acceso a información a los activos en el entorno de Misión.

Según el modelo MARGERIT v3, es posible clasificar nuestros activos en varios tipos:

- **Activos esenciales:** Estos marcan los requisitos de seguridad para todos los demás componentes del sistema. Se considera que tanto la información como los servicios presentes en un sistema de información son activos esenciales. Es posible clasificar la información en varios tipos:
 - Datos de interés para la administración pública
 - Datos vitales (registros de la organización), cuya carencia o daño afectaría inmediatamente a la existencia de la organización: Algunos ejemplos son aquellos que permiten que la organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas (tareas, servicios o sistemas cuyo fallo causaría que todo el proceso de negocio se interrumpa [69]) y aquellos que sustentan la naturaleza legal o los derechos financieros de la Organización o sus usuarios.
 - Datos de carácter personal
 - Datos clasificados

- **Arquitectura del sistema:** Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
 - Punto de acceso al servicio: Establece una frontera entre la prestación de un servicio (proveedor) y el usuario.
 - Punto de interconexión: Establece una frontera entre dos sistemas que se interconectan para intercambiar información.
 - Proporcionado por terceros: Establece una frontera interior en el caso de que necesitemos de un tercero para proporcionar nuestros servicios.
- **Datos u Información:** Incluye ficheros, copias de respaldo, archivos de configuración, credenciales...
- **Claves criptográficas:** Esenciales para asegurar que los sistemas criptográficos funcionan correctamente. Se incluyen en este apartado los certificados de clave pública, las claves de cifra para el cifrado de soportes de información y las claves de cifrado de canales de comunicaciones.
- **Servicios:** Función que satisface una necesidad de sus usuarios. Estos servicios pueden ser ofrecidos al público general, a usuarios externos bajo una relación contractual o de manera interna.
- **Software – Aplicaciones Informáticas:** Tareas que han sido automatizadas para su desempeño por un equipo informático. No se incluye el código fuente porque se considera este como una serie de datos de interés comercial. Algunos ejemplos de aplicaciones informáticas son el sistema de backup, el antivirus o el sistema operativo.
- **Equipamiento informático (hardware):** Son los medios materiales destinados a soportar directa o indirectamente los servicios que presta la organización. Es en este tipo donde se clasifican los terminales usados en la organización y los elementos de soporte de la red como *switches*, *routers* o cortafuegos.
- **Redes de comunicaciones:** Medios de transporte que llevan datos de un sitio a otro. Se incluyen tecnologías como WiFi, LAN o comunicaciones por satélite.
- **Soportes de información:** Dispositivos físicos que permiten almacenar información.
- **Equipamiento auxiliar:** En este tipo clasificamos elementos como fuentes de alimentación, equipos de climatización, cableado...
- **Instalaciones:** Lugares donde se hospedan los sistemas de información y comunicaciones.
- **Personal:** Personas relacionadas con los sistemas de información.

Ahora se procederá a la clasificación de activos según su tipo, ya que de esta manera MARGERIT nos podrá ayudar a identificar las amenazas que afectan a cada tipo de activo. La clasificación se puede contemplar en [Figura 8]:

Servicio	Equipamiento informático	Software	Soporte de información	Equipamiento auxiliar
CBII	Router de acceso a Internet	Servidor de aplicación de uso interno	Servidor de BD	Fuentes de alimentación y cableado eléctrico
Proxy	Cortafuegos		Servidor de copias de seguridad	
Servidor web externo	Balanceador de carga		Servidor de almacenamiento de datos	
Servidor web interno	Terminales de usuarios			

Figura 8.- Tabla de clasificación de activos CIS

AMENAZAS

Se han usado las amenazas que aparecen en el catálogo de tipos de amenazas que incluye la metodología MARGERIT v3.

Debido a la gran cantidad de amenazas que presenta este documento, hemos decidido escoger únicamente algunas de ellas, las cuales son:

- **Explosiones, derrumbes o incendios:** Aunque algunas de estas amenazas pueden ocurrir de manera natural o debido a la actividad industrial, afectan a todos los activos, ya que afecta a toda la infraestructura física sobre la que se basan los activos del modelo. Afecta a la disponibilidad de la información.
- **Contaminación electromagnética:** Este puede ser provocado por una gran variedad de dispositivos eléctricos [70] y puede afectar a los sistemas informáticos [71]. Afecta a la disponibilidad de la información.
- **Corte de suministro eléctrico:** El cese de la alimentación de potencia implicaría el fin del funcionamiento de todos nuestros activos en el entorno CIS, ya que todos dependen de energía eléctrica para funcionar. Afecta a la disponibilidad de la información.
- **Ocupación enemiga:** Causado por la invasión de locales lo que conlleva la pérdida de control sobre los medios de trabajo.
- **Fuga de información:** Esto puede ser causado mediante ataques intencionados de agentes externos tanto como por negligencia por parte del personal. Afecta a la confidencialidad de la información.
- **Destrucción de información:** Al igual que la fuga de información, esto puede ser causado mediante ataques intencionados de agentes externos tanto como por negligencia por parte del personal. Afecta a la disponibilidad de la información.

- **Denegación de servicio:** En esta categoría se encuentran los diferentes ataques de denegación de servicios que se explicaron en apartados anteriores de este trabajo, como puede ser el DDoS, el TDoS o el EDoS. Afecta a la disponibilidad de la información.

3.1.2. ANÁLISIS DE RIESGOS

Ahora comenzaremos con la elaboración de un Análisis de Riesgos según la metodología descrita por el Instituto Nacional de Ciberseguridad en su página web [72]:

1. Definir el alcance
2. Identificar los activos
3. Identificar las amenazas
4. Identificar vulnerabilidades y salvaguardas
5. Evaluar el riesgo
6. Tratar el riesgo

En cuanto a los tres primeros apartados, estos ya han sido realizados con anterioridad. El alcance de este análisis es el modelo de información que hemos definido anteriormente, con sus activos y amenazas.

IDENTIFICAR VULNERABILIDADES Y SALVAGUARDAS

Para la realización de este análisis se ha partido de la suposición que no existían medidas de seguridad implantadas con anterioridad aparte del servidor proxy, el cortafuegos y el servidor de copias de seguridad. Estas medidas se conocen como salvaguardas. Se ha optado por introducir estas medidas en el modelo al finalizar el análisis de riesgos, para que así puedan ser aplicadas a la hora de tratar los riesgos.

En cuanto a las vulnerabilidades, no se van a tener en consideración ya que no se definieron con suficiente precisión los activos para poder averiguar sus puntos débiles o vulnerabilidades como pueden ser el uso de software desactualizado y la falta de mantenimiento o soporte por parte del fabricante.

EVALUAR EL RIESGO

En este paso se estimará para cada par activo-amenaza a probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. Tras esto, el riesgo será calculado en base a estas dos probabilidades.

Para ello primero se decidirá que activos son afectados por cada una de las amenazas descritas anteriormente:

- **Explosiones, derrumbes o incendios:** Como se ha explicado anteriormente cuando se establecieron las amenazas, esto podría llegar a afectar a todos los activos, en función de la magnitud del desastre acontecido, ya que todos ellos necesitan de una infraestructura física para funcionar.
- **Contaminación electromagnética:** Esta amenaza también afecta a todos los activos, incluso al suministro eléctrico, incluso a las fuentes de alimentación [73].
- **Corte de suministro eléctrico:** Al igual que las dos amenazas anteriores, esta afecta a todos los activos puesto que todos necesitan electricidad para funcionar.
- **Ocupación enemiga:** Puesto que, como hemos dicho anteriormente, todos nuestros activos se encuentran en el mismo edificio, la ocupación enemiga de ese edificio conllevaría la pérdida de acceso a todos nuestros activos.

- **Fuga de información:** Esto afecta a todos nuestros activos pertenecientes al grupo “Soporte de la Información”, es decir, nuestro servidor de BD, servidor de copias de seguridad y servidor de almacenamiento de datos. También a nuestra aplicación de uso interno, ya que como se mencionó a la hora de definir los activos, esta hace uso de la base de datos.
- **Destrucción de información:** Afecta a los mismos activos que la amenaza anterior.
- **Denegación de servicio:** Afecta a nuestros activos localizados en los grupos de “Servicio”, “Equipamiento informático”, “Software” y “Soporte de información” puesto que es posible sobrecargar todos estos activos mediante el envío de un gran número de peticiones.

En [Figura 9] aparecen representados los activos afectados por cada una de las amenazas:

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	X	X	X	X			X
Proxy	X	X	X	X			X
Servidor web externo	X	X	X	X			X
Servidor web interno	X	X	X	X			X
Router de acceso a Internet	X	X	X	X			X
Cortafuegos	X	X	X	X			X
Balanceador de carga	X	X	X	X			X
Terminales de usuarios	X	X	X	X			
Servidor de aplicación de uso interno	X	X	X	X	X	X	X
Servidor de BD	X	X	X	X	X	X	X
Servidor de copias de seguridad	X	X	X	X	X	X	X
Servidor de almacenamiento de datos	X	X	X	X	X	X	X
Fuentes de alimentación y cableado eléctrico	X	X	X	X			

Figura 9.- Activos afectados por cada amenaza CIS

Ahora se estimará la probabilidad que tienen las amenazas de materializarse y el impacto que pueden llegar a tener de forma cuantitativa. Se asignará un valor numérico a cada pareja activo-amenaza cuyo valor será directamente proporcional a la probabilidad o el impacto de cada amenaza.

En cuanto a la probabilidad, ya que se supuso que no existían más medidas salvaguardas aparte del proxy, el cortafuegos y el servidor de copias de seguridad con antelación a este análisis de riesgos, varios activos tendrán la misma posibilidad de materializarse para algunas amenazas, como por ejemplo la amenaza “Explosiones, derrumbes o incendios”. Debido a ello será necesario fijarse también en el impacto que tienen estas amenazas al materializarse para poder averiguar que riesgos son los que hay que tratar con mayor urgencia.

El criterio usado para asignar valores numéricos a las probabilidades será el propuesto por INCIBE en [72], el cual se puede ver en [Figura 10]:

Valor	Descripción
1	La amenaza se materializa a lo sumo una vez cada año.
2	La amenaza se materializa a lo sumo una vez cada mes.
3	La amenaza se materializa a lo sumo una vez cada semana.

Figura 10.- Criterio para el análisis cuantitativo de probabilidad

Ahora se asignarán estos valores a cada uno de los pares activo-amenaza como se puede ver en [Figura 11]:

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	2	2	1			3
Proxy	1	2	2	1			3
Servidor web externo	1	2	2	1			3
Servidor web interno	1	2	2	1			2
Router de acceso a Internet	1	2	2	1			3
Cortafuegos	1	2	2	1			3
Balanceador de carga	1	2	2	1			3
Terminales de usuarios	1	2	2	1			2
Servidor de aplicación de uso interno	2	2	2	1	2	2	2
Servidor de BD	2	2	2	1	2	2	2
Servidor de copias de seguridad	2	2	2	1	2	2	2
Servidor de almacenamiento de datos	2	2	2	1	2	2	2
Fuentes de alimentación y cableado eléctrico	2	2	2	1			

Figura 11.- Probabilidad de pares activo-amenaza CIS

Cabe destacar que para los activos relacionados con la amenaza “Denegación de servicio” se ha otorgado una menor probabilidad a aquellos activos a los que no se pueda acceder directamente desde el exterior.

También se ha decidido dar una mayor probabilidad para los activos “Servidor de aplicación de uso interno”, “Servidor de BD”, “Servidor de copias de seguridad”, “Servidor de almacenamiento de datos” y “Fuentes de alimentación y cableado eléctrico” para la amenaza “Explosiones, derrumbes o incendios” ya que estos tienen un mayor riesgo de cortocircuitarse o sobrecalentarse que el resto de los activos.

Para el cálculo del impacto seguiremos el siguiente criterio, también proveniente de [72] y que se puede observar en [Figura 12]:

Valor	Descripción
1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Figura 12.- Criterio para el análisis cuantitativo de impacto

Ahora se asignarán estos valores a cada uno de los pares activo-amenaza como se puede ver en [Figura 13]:

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	1	1	1			1
Proxy	1	1	1	1			1
Servidor web externo	1	1	1	1			1
Servidor web interno	1	1	1	2			1
Router de acceso a Internet	1	1	1	1			1
Cortafuegos	1	1	1	1			1
Balanceador de carga	1	1	1	1			1
Terminales de usuarios	1	1	1	2			1
Servidor de aplicación de uso interno	2	2	2	3	3	2	2
Servidor de BD	2	2	2	3	3	2	2
Servidor de copias de seguridad	2	2	2	3	3	2	2
Servidor de almacenamiento de datos	2	2	2	3	3	2	2
Fuentes de alimentación y cableado eléctrico	3	3	3	3			

Figura 13.- Impacto de pares activo-amenaza CIS

Como se puede observar, algunos activos como el CBII, el proxy o las fuentes de alimentación no son de vital importancia en el entorno CIS en un contexto militar, pues en este contexto la organización

sufre un mayor daño si los riesgos afectan a activos relacionados con la información almacenada, especialmente si el enemigo consigue hacerse control de la inteligencia.

Se ha estimado que aquellos activos a los cuales se puede acceder más fácilmente desde el exterior no manejarían datos importantes ni servicios críticos, por lo que se les ha dado una baja importancia.

Riesgos relacionados con el servidor interno o los terminales de usuarios pueden producir consecuencias reseñables para la organización si los riesgos están relacionados con la ocupación física del territorio en el que se encuentran los activos, pues el enemigo podría hacer uso de estos elementos para hacer más daño al bando aliado o, por ejemplo, podría encontrar documentos confidenciales en los terminales de usuario que los usuarios hayan descargado del servidor de datos. En el resto de los riesgos no se considera que su impacto sea tan grande, por lo que se les ha otorgado una importancia menor.

Elementos auxiliares como los balanceadores de carga tienen menos importancia que las fuentes de alimentación, puesto que, ya que todos los elementos necesitan electricidad para funcionar, el mal funcionamiento de las fuentes de alimentación y el cableado podría implicar que ningún activo pudiese funcionar correctamente.

Por último, la pérdida de copias de seguridad por sí sola no conlleva una gran repercusión, ya que se pueden volver a hacer copias fácilmente, pero si esas copias caen en manos del enemigo o si se pierden las copias de seguridad a la vez que perdemos los datos originales los daños serían graves. Debido a ello, y como se verá más adelante, aplicar medidas que aislen al servidor de copias del resto de activos del entorno nos será de gran ayuda para tratar los riesgos.

Finalmente, procederemos a calcular el riesgo para averiguar los riesgos que hemos de tratar con mayor urgencia de manera cuantitativa, utilizando la siguiente fórmula:

$$\text{Riesgo} = \text{Probabilidad} \cdot \text{Impacto}$$

Los resultados son visibles en [Figura 14]:

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	2	2	1			3
Proxy	1	2	2	1			3
Servidor web externo	1	2	2	1			3
Servidor web interno	1	2	2	2			2
Router de acceso a Internet	1	2	2	1			3
Cortafuegos	1	2	2	1			3
Balanceador de carga	1	2	2	1			3
Terminales de usuarios	1	2	2	2			2
Servidor de aplicación de uso interno	4	4	4	3	6	4	4
Servidor de BD	4	4	4	3	6	4	4
Servidor de copias de seguridad	4	4	4	3	6	4	4
Servidor de almacenamiento de datos	4	4	4	3	6	4	4
Fuentes de alimentación y cableado eléctrico	6	6	6	3			

Figura 14.- Riesgo de pares activo-amenaza CIS

TRATAR EL RIESGO

Hemos decidido que trataremos todos los riesgos cuya puntuación sea igual o superior a 4. Según [72] y como se dijo anteriormente, existen cuatro estrategias principales a la hora de tratar riesgos:

- **Transferir** el riesgo a un tercero, por ejemplo, con la contratación de un seguro. Cabe destacar que esto no transfiere la responsabilidad de este.
- **Eliminar** el riesgo con medidas como la prohibición de acciones que pudieran dar lugar a que se produjera tal riesgo.
- **Asumir** el riesgo, es decir, aceptar de manera consciente y objetiva el riesgo de manera justificada, proporcionando evidencias claras del cumplimiento con la política de la organización y los criterios de aceptación de los riesgos.
- **Mitigar** el riesgo, mediante la aplicación de controles apropiados para reducir los riesgos.

Debido a la posición de responsabilidad en la que se encontrarían los responsables de seguridad de este modelo en un entorno militar, no resulta muy creíble que el riesgo se pudiera transferir a un tercero, por lo que descartaremos esa posibilidad y usando el mismo razonamiento es posible afirmar que asumir el riesgo tampoco es una opción viable.

Se ha considerado que los activos que tienen riesgos iguales o mayores de 4, es decir, el servidor de aplicación de uso interno, el servidor de BD, el servidor de copias de seguridad, el servidor de almacenamiento de datos y las fuentes de alimentación y cableado eléctrico; son esenciales en este entorno CIS, por lo que eliminar el riesgo tampoco es una opción.

En conclusión, la única medida que es posible tomar frente a estos riesgos es mitigarlos.

Una de las medidas salvaguarda que se usará para mitigar el impacto los riesgos es la instalación de un grupo electrógeno para que suministre energía a nuestros activos críticos en caso de un corte de electricidad. Con ello, se podrá reducir el impacto de la amenaza “Corte del suministro eléctrico” en el activo “Fuentes de alimentación y cableado eléctrico” y en los activos que reciban energía del grupo electrógeno, que son: “Servidor de aplicación de uso interno”, “Servidor de BD”, “Servidor de copias de seguridad” y “Servidor de almacenamiento de datos”.

Esto también conllevará que el impacto de cualquier amenaza sobre “Fuentes de alimentación y cableado eléctrico” se reduzca, ya que los activos más importantes que necesitan electricidad tienen el grupo electrógeno disponible.

Otra medida a aplicar será aislar el servidor de copias de seguridad del espacio físico en el que se encuentran el resto de los activos a un lugar que esté a 50 km de distancia como mínimo. Con esto se podrán reducir los riesgos asociados a activos de la clase “Soporte de la información”, ya que, de esta manera, será menos probable que un riesgo pueda afectar al servidor de copias de seguridad y al resto de activos relacionados con el almacenamiento de información.

También se usarán de sistemas de detección y prevención de intrusos (IDS/IPS) como los que expuestos anteriormente en el trabajo para reducir la posibilidad de que el riesgo “Denegación de servicio” se materialice.

Para reducir el impacto de la contaminación electromagnética se tomarán medidas como el uso de cables apantallados, que son cables eléctricos de uno o más conductores los cuales están aislados entre sí y se recubren por una capa común conductora. De esta manera, se produce un efecto de jaula de Faraday mediante el cual se evitan las interferencias tanto del exterior hacia al cable como del cable al exterior. [74] También se aislarán nuestros servidores de aplicación de uso interno, de BD, de copias de seguridad y de almacenamiento de datos en jaulas de Faraday para reducir el efecto de las interferencias en estos.

Para tratar las explosiones, derrumbes e incendios, se instalará un sistema antincendios en todo el edificio y un sistema de ventilación en las habitaciones con los servidores de aplicación de uso interno, de BD, de copias de seguridad y de almacenamiento de datos para reducir las posibilidades de que suceda un incendio.

En cuanto a la amenaza “Fuga de información”, se incrementará la seguridad en todo el edificio con controles de seguridad en la entrada y salida y se utilizarán sistemas de autenticación basado en DIAMETER para así poder tener un servidor de autenticación centralizado y así poder incrementar la seguridad, al no guardarse las credenciales de los usuarios en sus terminales.

3.1.3. PROOF OF CONCEPT

Tras haber instalado las salvaguardas necesarias, vamos a recalcular el riesgo. Los resultados se pueden ver en [Figura 15], [Figura 16] y [Figura 17].

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	2	2	1			3 → 2
Proxy	1	2	2	1			3 → 2
Servidor web externo	1	2	2	1			3 → 2
Servidor web interno	1	2	2	1			2 → 1
Router de acceso a Internet	1	2	2	1			3 → 2
Cortafuegos	1	2	2	1			3 → 2
Balanceador de carga	1	2	2	1			3 → 2
Terminales de usuarios	1	2	2	1			2 → 1
Servidor de aplicación de uso interno	2 → 1	2	2	1	2 → 1	2	2 → 1
Servidor de BD	2 → 1	2	2	1	2 → 1	2	2 → 1
Servidor de copias de seguridad	2 → 1	2	2	1	2 → 1	2	2 → 1
Servidor de almacenamiento de datos	2 → 1	2	2	1	2 → 1	2	2 → 1
Fuentes de alimentación y cableado eléctrico	2 → 1	2	2	1			

Figura 15.- Probabilidades corregidas activo-amenaza CIS

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	1	1	1			1
Proxy	1	1	1	1			1
Servidor web externo	1	1	1	1			1
Servidor web interno	1	1	1	2			1
Router de acceso a Internet	1	1	1	1			1
Cortafuegos	1	1	1	1			1
Balanceador de carga	1	1	1	1			1
Terminales de usuarios	1	1	1	2			1
Servidor de aplicación de uso interno	2	2 → 1	2 → 1	3	3	2 → 1	2
Servidor de BD	2	2 → 1	2 → 1	3	3	2 → 1	2
Servidor de copias de seguridad	2	2 → 1	2 → 1	3	3	2 → 1	2
Servidor de almacenamiento de datos	2	2 → 1	2 → 1	3	3	2 → 1	2
Fuentes de alimentación y cableado eléctrico	3 → 2	3 → 2	3 → 2	3 → 2			

Figura 16.- Impacto corregido activo-amenaza CIS

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
CBII	1	2	2	1			~~3~~ → 2
Proxy	1	2	2	1			~~3~~ → 2
Servidor web externo	1	2	2	1			~~3~~ → 2
Servidor web interno	1	2	2	2			~~2~~ → 1
Router de acceso a Internet	1	2	2	1			~~3~~ → 2
Cortafuegos	1	2	2	1			~~3~~ → 2
Balanceador de carga	1	2	2	1			~~3~~ → 2
Terminales de usuarios	1	2	2	2			~~2~~ → 1
Servidor de aplicación de uso interno	~~4~~ → 2	~~4~~ → 2	~~4~~ → 2	3	~~6~~ → 3	~~4~~ → 2	~~4~~ → 2
Servidor de BD	~~4~~ → 2	~~4~~ → 2	~~4~~ → 2	3	~~6~~ → 3	~~4~~ → 2	~~4~~ → 2
Servidor de copias de seguridad	~~4~~ → 2	~~4~~ → 2	~~4~~ → 2	3	~~6~~ → 3	~~4~~ → 2	~~4~~ → 2
Servidor de almacenamiento de datos	~~4~~ → 2	~~4~~ → 2	~~4~~ → 2	3	~~6~~ → 3	~~4~~ → 2	~~4~~ → 2
Fuentes de alimentación y cableado eléctrico	~~6~~ → 2	~~6~~ → 4	~~6~~ → 4	~~3~~ → 2			

Figura 17.- Riesgo corregido de pares impacto-amenaza CIS

3.2. ENTORNO MISIÓN

3.2.1. MODELO DE INFORMACIÓN

ACTIVOS

Ahora se comenzará a definir el modelo información para el entorno de misión. Para decidir que activos serán utilizados en el modelo se tomará como referencia el equipamiento actual de los ejércitos de tierra, mar y aire de Estados Unidos. [75]

Se ha optado por utilizar activos genéricos que representen a un tipo de equipamiento en lugar de activos más concretos. Por ejemplo, usaremos el activo “Avión de combate” en lugar de un activo como “B-2 Spirit” que representa un avión de combate concreto.

Los activos del modelo del entorno de misión son los siguientes:

- **Dispositivos de comunicaciones:** Esenciales para el intercambio de información entre el personal del ejército y para el acceso a información presente en los activos del entorno CIS.
- **Soldado:** Este activo encapsula a todos los soldados presentes en los ejércitos de tierra, mar y aire, por lo que será afectado por los riesgos pertenecientes a cualquiera de los tres dominios.
- **Artillería:** Este activo representa a armas como morteros, obuses, artillería de cohetes y equipamiento de defensa aérea.
- **Vehículo terrestre:** En este activo se encuentran medios de transporte como camiones y vehículos ligeros como otros con una capacidad ofensiva mayor como los tanques.
- **Transporte terrestre:** Son utilizadas para transportar tropas, armamento y equipamiento militar. Tienen menor capacidad ofensiva que los tanques, por lo que son más vulnerables frente a ataques enemigos, pero, al estar más lejos del frente que los tanques es menos probable que los riesgos asociados a este activo se materialicen.
- **Transporte marítimo:** Similar al transporte terrestre, pero en el dominio marítimo.
- **Transporte aéreo:** Similar al transporte terrestre, pero en el dominio aéreo.
- **Avión de combate:** Pueden defenderse más fácilmente de ataques enemigos debido a su equipamiento, pero tienen una mayor probabilidad de que sus riesgos se materialicen debido a su cercanía al frente.
- **Vehículo aéreo no tripulado:** Pueden realizar misiones tanto de reconocimiento como de ataque [76]. Al no estar tripulados, los riesgos asociados a estos vehículos no afectan a los soldados.
- **Submarino:** Es un buque capaz de navegar tanto sobre la superficie del agua como debajo de esta.
- **Buque de superficie:** En este activo se consideran tanto buques grandes (portaaviones, destructores...) como embarcaciones ligeras (lanchas) que, como el nombre de este activo indica, navegan en la superficie del agua.

- **Base militar:** Es una instalación propiedad del ejército o una de sus ramas. Sirve para almacenar material y acoger personal militar. También posee instalaciones para entrenamiento y operaciones.

Ahora, de manera similar a como se hizo con los activos del entorno CIS, se clasificarán estos activos según la dimensión de la guerra a la que pertenezcan:

Tierra	Mar	Aire
Soldado		
Dispositivos de comunicaciones		
Artillería	Transporte marítimo	Transporte aéreo
Vehículo terrestre	Submarino	Avión de combate
Transporte terrestre	Buque de superficie	Vehículo aéreo no tripulado
Base militar		

Figura 18.- Tabla de clasificación de activos Misión

Se ha considerado que la artillería pertenece a la dimensión terrestre ya que, a pesar de que algunos buques de guerra tengan armamento como lanzamisiles este armamento es simplemente un elemento del buque de guerra, por lo que sería mejor no separar al armamento del buque y simplemente considerarlo todo como el activo “buque de superficie”.

AMENAZAS

Se ha decidido que las amenazas correspondientes a este modelo de información serán las siguientes, según la información presente en [75]:

- **Impacto de misil:** Los misiles pueden estar presentes como armamento en aviones de combate, buques de superficie o pueden ser utilizados con equipamiento más especializado, que permita su lanzamiento desde distancias como 50km como miles de kilómetros de distancia.
- **Ataque por ondas electromagnéticas:** Se realiza con equipamiento capaz de generar altas cantidades de energía electromagnética que destruye dispositivos eléctricos y electrónicos.
- **Revelación de secretos:** Consiste en la obtención por parte del enemigo de información clasificada, ya por robo de identidad, espías infiltrados en el bando aliado...
- **Activación de mina:** Como se ha dicho anteriormente, solo afecta a activos localizados en tierra o mar.
- **Sabotaje:** Afecta a todos los activos directamente con excepción de los soldados. Cabe destacar que, a pesar de ello, como los soldados dependen del equipamiento para el éxito de las operaciones militares, los soldados también serían afectados de una manera indirecta.
- **Asalto a base militar:** Como su nombre indica, afecta a las bases militares. Sin embargo, al haber soldados presentes en ellas, estos también se ven afectados. Se ha decidido no tener en cuenta ninguno de los otros activos a pesar de que estos pudiesen estar presentes en una base militar ya que el número tanto como la variedad de equipamiento militar que puede estar presente en una base puede variar fuertemente en función de su localización geográfica y de su importancia.

3.2.2. ANÁLISIS DE RIESGOS

A pesar de que este entorno es diferente al CIS, se optará por usar la misma metodología usada para el entorno CIS anteriormente ya que es fácilmente adaptable para este entorno.

IDENTIFICAR VULNERABILIDADES Y SALVAGUARDAS

Al igual que en el entorno CIS, no se van a tener en consideración posibles vulnerabilidades ya que los activos no se definieron con suficiente precisión para poder averiguar sus puntos débiles o vulnerabilidades.

En cuanto a las medidas salvaguardas ya presentes, cabe destacar que el activo “Artillería”, así como el activo “Buque de superficie” poseen medidas de defensa antiaérea. Esto les podrá ayudar contra los aviones de combate enemigos que tengan incorporados misiles en su armamento, reduciendo así la probabilidad de que un misil impacte.

También cabe destacar que las bases militares están fuertemente protegidas contra asaltos enemigos, por lo que el impacto de los asaltos enemigos será menor.

EVALUAR EL RIESGO

Al igual que en el entorno CIS, en este paso se estimará para cada par activo-amenaza a probabilidad de que la amenaza se materialice y el impacto sobre el modelo que esto produciría. Tras esto, el riesgo será calculado en base a estas dos probabilidades.

Primero se decidirá que activos son afectados por cada una de las amenazas descritas anteriormente.

- **Impacto de misil:** Esta amenaza puede afectar a todos los activos salvo a los submarinos, ya que los misiles pueden impactar contra objetivos en tierra, en la superficie del mar y en el aire. Sin embargo, los activos de transporte, al estar más lejos del frente de batalla, tendrán una menor probabilidad de sufrir este riesgo.
- **Ataque por ondas electromagnéticas:** De manera similar a la amenaza “Contaminación electromagnética” del entorno CIS, esta amenaza afecta a todos los dispositivos eléctricos y electrónicos.
- **Revelación de secretos:** Afecta tanto a los dispositivos de comunicaciones como a las bases militares, ya que en esos activos se trata con información clasificada. También afecta a los soldados, ya que es posible que el bando enemigo consiga información privilegiada a través de ellos.
- **Activación de mina:** Produce una explosión de manera similar a un misil, sin embargo, solo afecta a activos con capacidad de movimiento localizados en tierra o mar, ya que las minas no se pueden localizar en el aire.
- **Sabotaje:** Consiste en el daño o deterioro de equipamiento por parte del enemigo para obstruir el funcionamiento de las operaciones.
- **Asalto a base militar:** Sucede cuando se efectúa una ofensiva contra una de las bases militares aliadas. En esta ofensiva se pueden utilizar algunas de las amenazas mencionadas previamente.

En [Figura 19] aparecen representados los activos afectados por cada una de las amenazas:

Amenazas Activos	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Soldado	X		X	X		X
Dispositivos de comunicaciones	X	X	X		X	
Artillería	X	X			X	
Vehículo terrestre	X	X		X	X	
Transporte terrestre	X	X		X	X	
Base militar	X	X	X		X	X
Transporte marítimo	X	X		X	X	
Submarino		X		X	X	
Buque de superficie	X	X		X	X	
Transporte aéreo	X	X			X	
Avión de combate	X	X			X	
Vehículo aéreo no tripulado	X	X			X	

Figura 19.- Activos afectados por cada amenaza Misión

Al igual que como se realizó en el entorno CIS, ahora se estimará la probabilidad que tienen las amenazas de materializarse y el impacto que pueden llegar a tener de forma cuantitativa. Se asignará un valor numérico a cada pareja activo-amenaza cuyo valor será directamente proporcional a la probabilidad o el impacto de cada amenaza.

Al igual que en el entorno CIS, el criterio usado para asignar valores numéricos a las probabilidades será el propuesto por INCIBE en [72], el cual se puede ver en [Figura 10].

Ahora se asignarán estos valores a cada par activo-amenaza como se puede ver en [Figura 20]:

Amenazas Activos	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Soldado	3		2	3		2
Dispositivos de comunicaciones	2	3	3		2	
Artillería	2	3			2	
Vehículo terrestre	3	3		3	2	
Transporte terrestre	2	2		2	1	
Base militar	2	2	1		1	2
Transporte marítimo	2	2		2	1	
Submarino		3		3	2	
Buque de superficie	2	3		3	2	
Transporte aéreo	2	2			1	
Avión de combate	3	3			2	
Vehículo aéreo no tripulado	3	3			1	

Figura 20.- Probabilidad de pares activo-amenaza Misión

Como se puede ver en la tabla, por lo general la probabilidad de las amenazas asociadas a los activos “Base militar” y a los activos de transporte es menor debido a su lejanía del frente de batalla.

También, como se ha dicho anteriormente, los activos “Artillería” y “Buque de superficie” tienen medidas antiaéreas, por lo que tanto estos dos activos como los soldados presentes en ellos tendrán una probabilidad menor de sufrir un impacto de misil.

En cuanto al cálculo del impacto, se procederá de manera similar a como se hizo en el entorno CIS, proveniente de [72] y que se puede observar en [Figura 12].

Ahora se asignarán estos valores a cada uno de los pares activo-amenaza como se puede ver en [Figura 21]:

Amenazas Activos	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Soldado	1		1	1		1
Dispositivos de comunicaciones	2	2	2		2	
Artillería	1	1			1	
Vehículo terrestre	1	1		1	1	
Transporte terrestre	2	2		2	2	
Base militar	2	2	3		2	2
Transporte marítimo	2	2		2	2	
Submarino		1		1	1	
Buque de superficie	1	1		1	1	
Transporte aéreo	2	2			2	
Avión de combate	1	1			1	
Vehículo aéreo no tripulado	1	1			1	

Figura 21.- Impacto de pares activo-amenaza Misión

Debido a la gran cantidad de soldados y equipamiento militar, generalmente estos activos tienen una baja probabilidad. Se ha dado una mayor probabilidad a los activos de transporte porque estos se encargan del transporte de suministros y al activo “Base militar” porque se ocupa de su almacenamiento.

Para los activos “Soldado” y “Base militar” se ha tenido en cuenta la gran cantidad de defensas que tendrá la base militar, por lo que su riesgo tiene una puntuación de 2 para el activo “Base Militar” y de 1 para el activo “Soldado”.

Por último, cabe destacar que para la amenaza “Revelación de secretos”, se ha dado una menor importancia al soldado, ya que este no suele conocer información importante. Se ha considerado que esta se encuentra en los mensajes transportados en las redes de comunicaciones y en las bases militares.

Para finalizar con la evaluación de los riesgos, se calculará el riesgo multiplicando la probabilidad y con el impacto para cada par activo-amenaza como se puede ver en [Figura 22]:

Amenazas Activos	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Soldado	3		2	3		2
Dispositivos de comunicaciones	4	6	6		4	
Artillería	2	3			2	
Vehículo terrestre	3	3		3	2	
Transporte terrestre	4	4		4	2	
Base militar	4	4	3		2	4
Transporte marítimo	4	4		4	2	
Submarino		3		3	2	
Buque de superficie	2	3		3	2	
Transporte aéreo	4	4			2	
Avión de combate	3	3			2	
Vehículo aéreo no tripulado	3	3			1	

Figura 22.- Riesgo de pares activo-amenaza Misión

TRATAR EL RIESGO

En este caso, hemos decidido tratar los riesgos con puntuación mayor o igual que 6. Esto es debido a que creemos que es natural que la actividad en este entorno conlleve un mayor riesgo que en el entorno CIS.

Esto nos deja con dos amenazas para el activo “Dispositivos de comunicaciones”, que son “Ataque por ondas electromagnéticas” y “Revelación de secretos”.

En primer lugar, para la amenaza “Ataque por ondas electromagnéticas”, no nos queda más remedio que asumir el riesgo, ya que, al contrario que hicimos en el entorno CIS, no es posible aislar nuestros sistemas de comunicación de las interferencias electromagnéticas ya que, si se aíslan, sería imposible la comunicación, al realizarse esta mediante ondas electromagnéticas.

Sin embargo, es posible mitigar el riesgo “Revelación de secretos” mediante el uso de cifrado en las comunicaciones. De esa manera, aunque el enemigo consiga averiguar la frecuencia en la que se transmiten los mensajes no podrá averiguar su contenido. De esta manera, y como se verá más tarde en el *Proof of Concept*, la probabilidad de que la vulnerabilidad “Revelación de secretos” se materialice se reducirá.

Al contrario que en el entorno CIS, ya que únicamente se ha tratado una amenaza que afecta a un activo, no se incluirán las tablas con las probabilidades y el impacto corregidas, sino que simplemente se mostrará los valores finales del riesgo en el *Proof of Concept*.

3.2.3. PROOF OF CONCEPT

Como se comentó anteriormente, hemos reducido la probabilidad de la amenaza “Revelación de secretos” para el activo dispositivos de comunicaciones de un 3 a un 2, lo que ha causado que el riesgo pase de ser 6 a valer 4, como se puede ver en [Figura 23]:

Amenazas Activos	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Soldado	3		2	3		2
Dispositivos de comunicaciones	4	6	~~6~~ → 4		4	
Artillería	2	3			2	
Vehículo terrestre	3	3		3	2	
Transporte terrestre	4	4		4	2	
Base militar	4	4	3		2	4
Transporte marítimo	4	4		4	2	
Submarino		3		3	2	
Buque de superficie	2	3		3	2	
Transporte aéreo	4	4			2	
Avión de combate	3	3			2	
Vehículo aéreo no tripulado	3	3			1	

Figura 23.- Riesgo corregido de pares activo-amenaza Misión

3.3.ESQUEMA DE DEFINICIÓN DE CORRELACIONES

En este apartado definiremos la probabilidad de que, tras la materialización de una amenaza en un entorno, se materialice otra amenaza en el otro entorno. Se estimará esta probabilidad según los datos obtenidos en los análisis de riesgos realizados. Se comenzará con el cálculo de $P(\text{Riesgo CIS} | \text{Riesgo Misión})$. Para calcular este valor aplicaremos la siguiente fórmula:

$$P(\text{Riesgo CIS} | \text{Riesgo Misión}) = \frac{P(\text{Riesgo CIS} \cap \text{Riesgo Misión})}{P(\text{Riesgo Misión})}$$

$P(\text{Riesgo Misión})$ se ha calculado como la media de todas las probabilidades que un riesgo tiene para todos los activos en [Figura 20], por lo que únicamente necesitamos saber $P(\text{Riesgo CIS} \cap \text{Riesgo Misión})$. Esta probabilidad se refiere a la probabilidad de que ambos eventos sucedan de manera próxima en el tiempo. Para este trabajo se ha decidido estimar esta probabilidad debido a la falta de información en este aspecto. Los valores estimados se pueden ver en [Figura 24]:

Riesgo Misión Riesgo CIS	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Explosiones, derrumbes o incendios	0,33	0	0	0	0,12	0,28
Contaminación electromagnética	0	0,37	0	0	0,12	0
Corte de suministro eléctrico	0,24	0,26	0	0	0,12	0,28
Ocupación enemiga	0	0	0	0	0,06	0,12
Fuga de información	0	0	0,12	0	0,06	0,12
Destrucción de información	0,05	0	0	0	0,03	0,04
Denegación de servicio	0	0	0	0	0,12	0,20

Figura 24.- $P(\text{Riesgo CIS} \cap \text{Riesgo Misión})$

Los resultados finales se pueden ver en [Figura 25].

Riesgo Misión Riesgo CIS	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
Explosiones, derrumbes o incendios	0,7	0	0	0	0,4	0,7
Contaminación electromagnética	0	0,7	0	0	0,4	0
Corte de suministro eléctrico	0,5	0,5	0	0	0,4	0,7
Ocupación enemiga	0	0	0	0	0,2	0,3
Fuga de información	0	0	0,3	0	0,2	0,3
Destrucción de información	0,1	0	0	0	0,1	0,1
Denegación de servicio	0	0	0	0	0,4	0,5

Figura 25.- $P(\text{Riesgo CIS} \mid \text{Riesgo Misión})$

En cuanto a las probabilidades asociadas al impacto de misil, se ha supuesto que la probabilidad de daños en la infraestructura es de un 0,7. Se ha dado una probabilidad algo menor al corte de suministro eléctrico ya que hay zonas en el entorno CIS que podrían ser dañadas por una explosión y no afectar al suministro eléctrico.

La probabilidad $P(\text{Destrucción de información} \mid \text{Impacto de Misil})$ tiene un valor muy bajo dado a que tanto los servidores de información como los servidores de copias de seguridad deberían de ser inutilizados para que la información se pierda. Por tanto, lo que debería suceder es que uno de esos dos servidores este inutilizado previamente al impacto del misil y que el misil consiga destruir el otro servidor para que la información se pueda considerar como perdida.

Como se mencionó en el Análisis de Riesgos en el entorno CIS, las fuentes de alimentación y el cableado eléctrico pueden verse afectados por contaminación electromagnética, por lo que se ha establecido una probabilidad $P(\text{Corte del suministro eléctrico} \mid \text{Ataque por ondas electromagnéticas})$.

“Revelación de secretos” tiene una probabilidad de 0,3 cuando se establece como condición para “Fuga de información”, ya que no toda la información que posea un activo del entorno Misión puede afectar a activos CIS. Por ejemplo, la revelación de secretos relacionados con el armamento no afecta a activos CIS, pero secretos como credenciales si afectan.

Como una mina no se puede activar en un entorno CIS, ya que las minas se encuentran el campo de batalla, se considera que las probabilidades condicionadas relacionadas con “Activación de Mina” son 0.

En cuanto al riesgo “Sabotaje”, se ha puesto una menor probabilidad para la probabilidad condicionada asociada al riesgo “Destrucción de información” debido a la existencia de servidores de copias de seguridad.

Por último, “Asalto a la base militar” es un riesgo que, en caso de que el asalto tenga éxito, causaría que se materializase la amenaza “Ocupación enemiga”, pero, ya que no todos los asaltos son exitosos, la probabilidad es distinto de 1.

Como se pudo ver en los Análisis de Riesgos realizados previamente, los riesgos tienden a afectar a cada activo de una manera diferente, por lo que los riesgos en un campo tienen probabilidades diferentes de afectar a los activos del otro en función de la naturaleza de cada activo. Usando [Figura 25] y los resultados del análisis de riesgos se ha elaborado [Figura 26] en la que se puede ver las probabilidades de que cada amenaza del entorno Misión afecte a los activos CIS.

Para calcular la probabilidad que cada activo CIS tiene de sufrir los riesgos calculados anteriormente se ha supuesto que $P(\text{Riesgo CIS} | \text{Riesgo Misión})$ y $P(\text{Activo sufre riesgo CIS})$ son independientes, por lo que multiplicando ambas probabilidades se puede calcular $P(\text{Activo sufre riesgo CIS} \cap (\text{Riesgo CIS} | \text{Riesgo Misión}))$, que es lo que calcularemos a continuación.

Por lo general, se ha optado por multiplicar las probabilidades calculadas en [Figura 25] por 0,2 si en el Análisis de Riesgos se había establecido la probabilidad de la amenaza como 1, 0,4 si el valor de la probabilidad es 2 y 0,6 si es 3. En este caso nos hemos fijado en los valores de probabilidad de [Figura 11]. En ocasiones puede suceder que una amenaza del entorno de Misión provoque varias amenazas CIS, por lo que en ese caso se sumarán las probabilidades en los activos. Los resultados se pueden ver en [Figura 26].

Amenazas Activos						
	Impacto de misil	Ataque por ondas electromagnéticas	Revelación de secretos	Activación de mina	Sabotaje	Asalto a base militar
CBII	0,34	0,48	0	0	0,68	0,78
Proxy	0,34	0,48	0	0	0,68	0,78
Servidor web externo	0,34	0,48	0	0	0,68	0,78
Servidor web interno	0,34	0,48	0	0	0,6	0,68
Router de acceso a Internet	0,34	0,48	0	0	0,68	0,78
Cortafuegos	0,34	0,48	0	0	0,68	0,78
Balanceador de carga	0,34	0,48	0	0	0,68	0,78
Terminales de usuarios	0,34	0,48	0	0	0,6	0,68
Servidor de aplicación de uso interno	0,52	0,48	0,4	0	0,8	0,86
Servidor de BD	0,52	0,48	0,4	0	0,8	0,86
Servidor de copias de seguridad	0,52	0,48	0,4	0	0,8	0,86
Servidor de almacenamiento de datos	0,52	0,48	0,4	0	0,8	0,86
Fuentes de alimentación y cableado eléctrico	0,48	0,48	0	0	0,52	0,62

Figura 26.- Probabilidades Amenazas Misión - Activos CIS

Ahora es necesario calcular $P(\text{Riesgo Misión} \mid \text{Riesgo CIS})$. A la hora de calcularlo usando el mismo $P(\text{Riesgo CIS} \cap \text{Riesgo Misión})$ que el que se ve en [Figura 24] se puede ver que el resultado no es el mismo que $P(\text{Riesgo CIS} \mid \text{Riesgo Misión})$, por lo que ambos sucesos no son independientes.

Esto tiene sentido, ya que, $P(\text{Explosiones, derrumbes o incendios} \mid \text{Impacto de misil})$ no tiene el mismo valor que $P(\text{Impacto de misil} \mid \text{Explosiones, derrumbes o incendios})$, ya que el impacto de un misil puede causar una explosión, pero el hecho de que algo explote no tiene que implicar que un misil vaya a impactar más adelante.

Los resultados de estas probabilidades se pueden ver en [Figura 27].

Riesgo CIS Riesgo Misión	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
Impacto de misil	0,13	0	0,10	0	0	0,02	0,13
Ataque por ondas electromagnéticas	0	0,18	0,13	0	0	0	0
Revelación de secretos	0	0	0	0	0	0	0
Activación de mina	0	0	0	0	0	0	0
Sabotaje	0,09	0,09	0,09	0,04	0,04	0,02	0,09
Asalto a base militar	0,22	0	0,22	0,09	0,09	0,03	0,22

Figura 27.- $P(\text{Riesgo Misión} \mid \text{Riesgo CIS})$

Se considera que varios de los riesgos CIS pueden venir acompañados de medidas de sabotaje, por ende, “Sabotaje” es un riesgo presente en varias probabilidades condicionales.

Otra probabilidad que resulta interesante de explicar es $P(\text{Asalto a base militar} \mid \text{Fuga de información})$. Esta probabilidad se ha razonado como que primero el bando enemigo ha conseguido averiguar información sobre las bases militares, como puede ser su localización o medidas defensivas, por lo que realizan un ataque aprovechando que tienen la ventaja.

Usando [Figura 20] y [Figura 27] se realizará [Figura 28], de la misma manera que calculamos los valores en [Figura 26].

Amenazas Activos	Explosiones, derrumbes o incendios	Contaminación electromagnética	Corte de suministro eléctrico	Ocupación enemiga	Fuga de información	Destrucción de información	Denegación de servicio
Soldado	0,17	0,00	0,14	0,04	0,04	0,02	0,06
Dispositivos de comunicaciones	0,09	0,14	0,15	0,02	0,02	0,02	0,03
Artillería	0,09	0,14	0,15	0,02	0,02	0,02	0,03
Vehículo terrestre	0,11	0,14	0,17	0,02	0,02	0,02	0,03
Transporte terrestre	0,07	0,09	0,11	0,01	0,01	0,01	0,02
Base militar	0,16	0,09	0,19	0,05	0,05	0,02	0,08
Transporte marítimo	0,07	0,09	0,11	0,01	0,01	0,01	0,02
Submarino	0,03	0,14	0,11	0,02	0,02	0,01	0,03
Buque de superficie	0,09	0,14	0,15	0,02	0,02	0,02	0,03
Transporte aéreo	0,07	0,09	0,11	0,01	0,01	0,01	0,02
Avión de combate	0,11	0,14	0,17	0,02	0,02	0,02	0,03
Vehículo aéreo no tripulado	0,10	0,12	0,15	0,01	0,01	0,02	0,02

Figura 28.- Probabilidades Amenazas CIS - Activos Misión

4. ELABORACIÓN DEL PROTOTIPO

Para la elaboración del prototipo se ha utilizado el software MATLAB y su funcionalidad *MATLAB App Designer*, la cual permite desarrollar la interfaz de usuario y la lógica de una aplicación.

Este prototipo se encarga de simular los efectos que puede provocar una amenaza por correlación, es decir, los efectos que puede tener una Amenaza CIS en activos de misión. Para ello utiliza las probabilidades presentes en [Figura 26] y [Figura 28], calculadas en el apartado anterior.

El funcionamiento del prototipo es el siguiente. Al inicio, en el prototipo aparecen todos los activos con el estado “OK”. Al seleccionar y simular una amenaza, se marcan como “Vulnerable” los activos que pertenecen al mismo dominio que la amenaza y se considera que pueden ser afectados por ella. Los activos que pueden ser afectados por cada amenaza se pueden ver en [Figura 9] para las amenazas CIS y [Figura 19] para las amenazas Misión.

También, usando las probabilidades mencionadas anteriormente, el prototipo calcula la posibilidad de que los activos del otro dominio se vean afectados. En el caso de que lo estén, se marcan esos activos como “Afectado por correlación”.

Se puede resumir el funcionamiento del prototipo en el siguiente esquema:

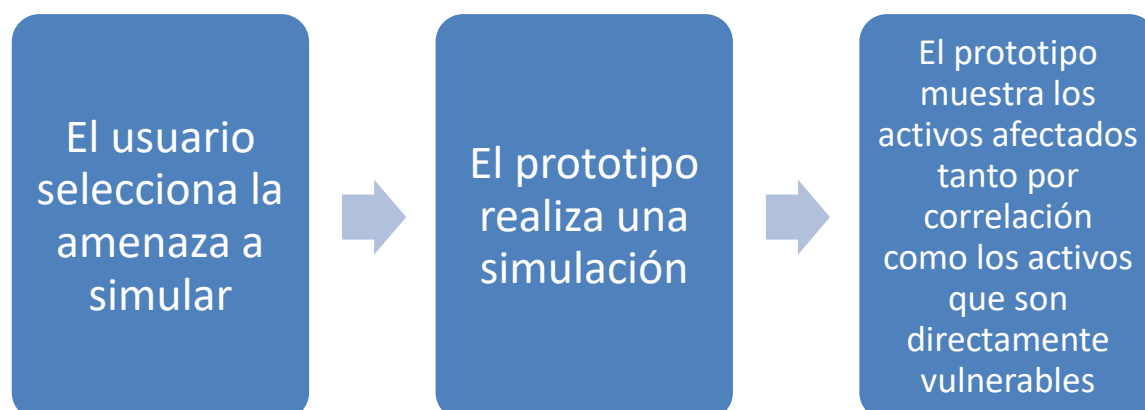


Figura 29.- Funcionamiento del prototipo

Ahora se mostrarán algunas capturas de pantalla de la interfaz gráfica del prototipo. En [Figura 30] se puede ver la interfaz gráfica del prototipo antes de simular una amenaza:

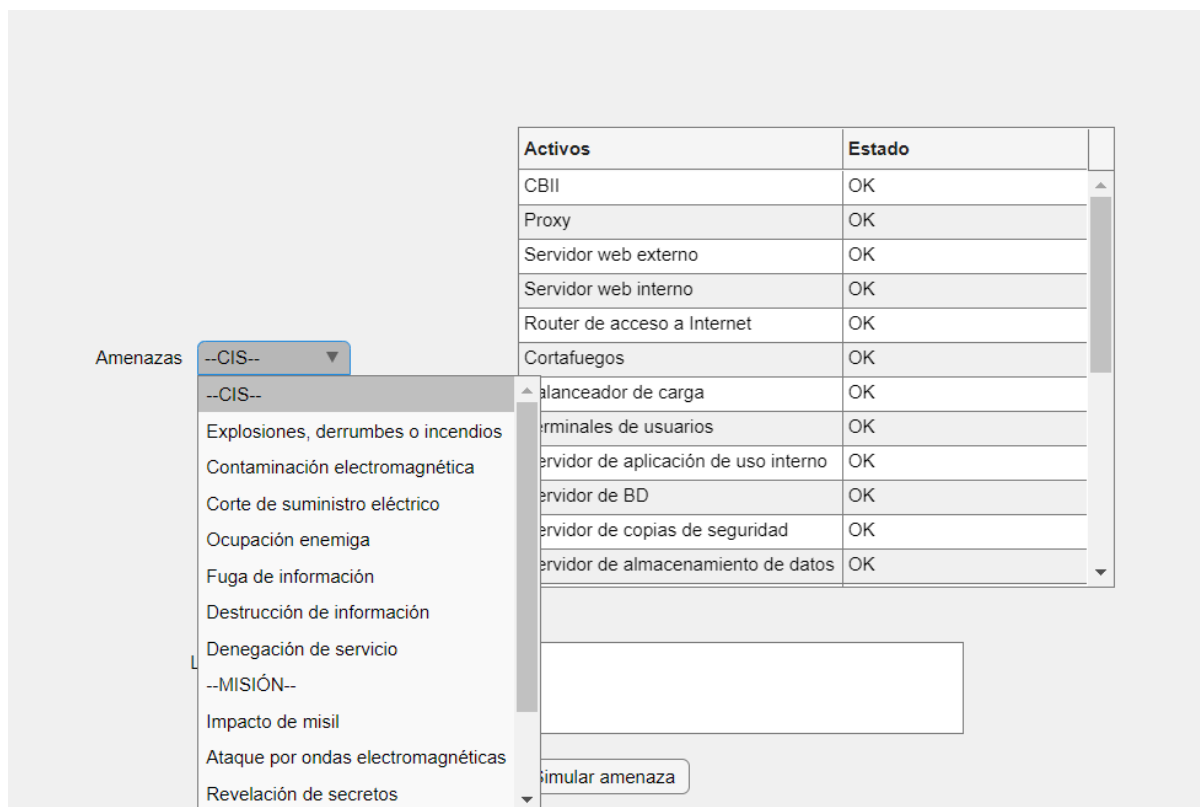


Figura 30.- Interfaz gráfica del prototipo

Como se puede ver en la imagen, es una interfaz muy sencilla, que consta de un menú en el cual se puede seleccionar la amenaza que se quiere simular, una tabla que muestra los activos y su estado, un botón que simula la amenaza seleccionada y un área de texto en el que se reportan los cambios sucedidos.

Tras seleccionar una amenaza y dar clic al botón el prototipo tendrá un aspecto similar al de [Figura 31]:

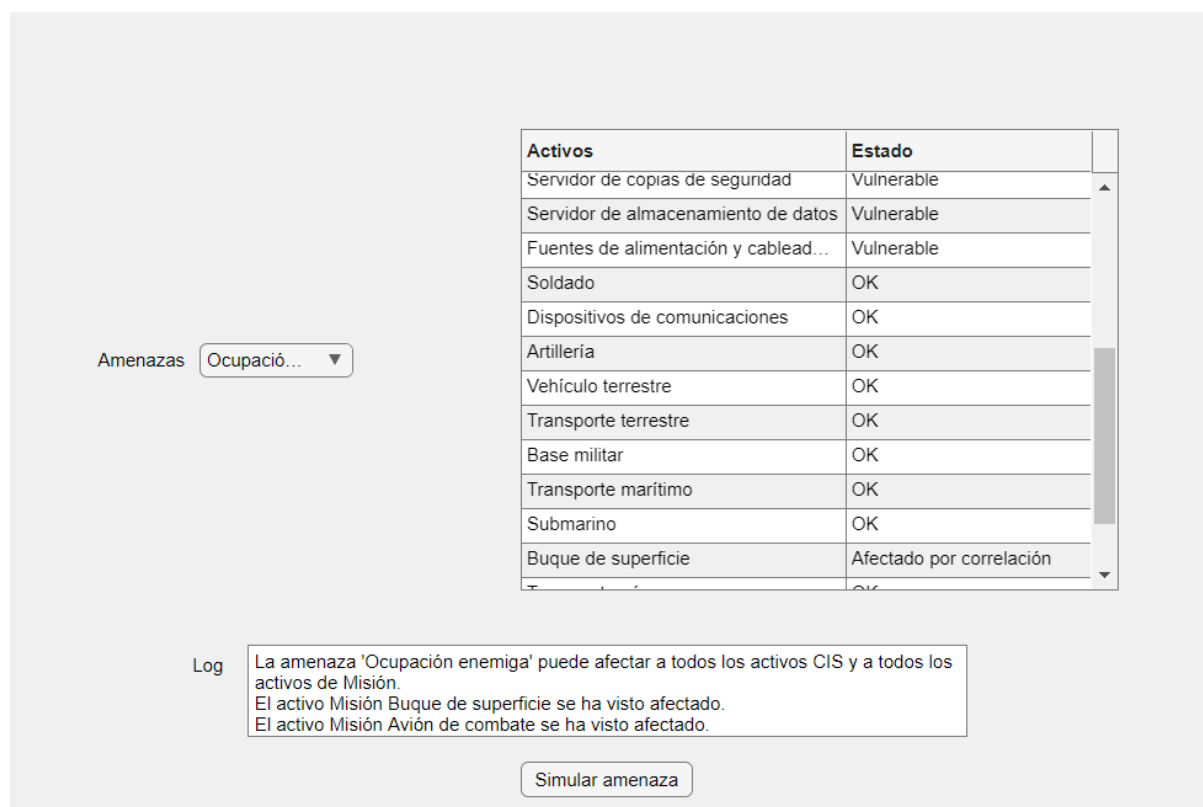


Figura 31.- Estado del prototipo tras simular una amenaza

En este caso, se simuló una amenaza perteneciente al Modelo CIS, por lo que se marcaron los activos CIS que pueden ser afectados por esa amenaza como vulnerables.

En cuanto a los activos de Misión, el prototipo, utilizando las probabilidades mencionadas anteriormente, simula la materialización de la amenaza e indica que activos se han visto afectados. Cabe destacar que, como se trata de un suceso aleatorio, los activos que se verán afectados por correlación cambiarán en cada ejecución.

Tanto las probabilidades como los modelos de información de ambos entornos están guardados en el código de la aplicación, por lo que para modificarlos es necesario modificar el código del archivo mlapp.

Se ha considerado como una de las líneas de investigación futuras la elaboración de un programa más elaborado que permita la agregación de ficheros de configuración y que tenga la capacidad de poder cambiar tanto las probabilidades de que suceda una correlación como los activos y amenazas desde la interfaz gráfica.

5. CONCLUSIONES Y LÍNEAS FUTURAS

5.1. CONCLUSIONES

En este proyecto se ha realizado un análisis del Estado del Arte en cuanto a ciberseguridad y ciberdefensa se refiere. También se han explicado en qué consisten las guerras híbridas y se han enlazado estos conceptos con conflictos reales.

Más tarde, se procede a la realización de dos modelos de información (Misión y CIS) con la intención de poder comprender mejor como las amenazas presentes en el ciberespacio pueden afectar a activos más cercanos al campo de batalla y como las amenazas propias del campo de batalla pueden afectar a activos relacionados con las tecnologías de la información.

Finalmente, se procede a la elaboración de un prototipo que nos ayuda a visualizar estas correlaciones.

Tras la finalización de este trabajo, se cree que dichas correlaciones existen, pero las probabilidades exactas de que sucedan son difíciles de cuantificar de una manera exacta debido a la falta de información, especialmente en cuanto al modelo de Misión se refiere, por lo que en este trabajo se han tenido que realizar varias suposiciones.

5.2. LÍNEAS FUTURAS

Como se ha mencionado en el apartado anterior, existen importantes limitaciones y mejoras que se proponen como trabajos futuros:

- Realizar cálculos de las probabilidades de correlación más precisos, a través de simulaciones con redes neuronales artificiales.
- Mejorar los modelos de información propuestos, con activos más similares a los usados por las unidades militares y amenazas que se asemejen a las que se materializan en conflictos militares.
- Implementar el sistema en un entorno de simulación con los modelos de información CIS y Misión con el objetivo de poder extraer información de los modelos y así poder tener una mayor conciencia de lo que está sucediendo en ese momento.

5.3. VALORACIÓN PERSONAL

Se considera que este trabajo ha realizado una aproximación inicial a la correlación existente entre eventos que suceden en el ciberespacio y eventos que suceden en el campo de batalla. Debido a ello, ha sido necesario realizar estimaciones en algunas partes del trabajo, por lo que el cálculo más preciso de las probabilidades de que estos eventos estén correlacionados se deja para trabajos posteriores. También se cree que los modelos de información expuestos en este trabajo son genéricos y que para su aplicación en un entorno real sería necesario especificar más detalles de los activos.

Sin embargo, se cree que la idea general expuesta en este trabajo es la correcta y que en efecto existen relaciones entre eventos que suceden en las dos dimensiones.

En cuanto al prototipo, se considera que este es un prototipo muy básico y que se podrían realizar mejoras, como la posibilidad de que el prototipo utilice ficheros de configuración permitiendo de esta manera que el usuario pueda cambiar tanto los activos, como amenazas y probabilidades.

6. BIBLIOGRAFÍA

- [1] N. Giatrakos, E. Alevizos, A. Artikis, A. Deligannakis y M. Garofalakis, «Complex event recognition in the Big Data era: a survey,» *The VLDB Journal* 29, p. 313–352, 2020.
- [2] N. Stanton, P. Chambers y J. Piggott, «Situational awareness and safety,» *Safety Science*, vol. 39, nº 3, pp. 189-204, 2001.
- [3] M. P. J. Tremblay, «Shaping and adapting: Unlocking the power of Colonel John Boyd's OODA Loop,» 2015.
- [4] V. Lenders, A. Tanner y A. Blarer, «Gaining an Edge in Cyberspace with Advanced Situational Awareness,» *EEE Security & Privacy*, vol. 13, nº 2, pp. 65-74, 2015.
- [5] A. Horneman, «Situational Awareness for Cybersecurity: An Introduction,» Carnegie Mellon University, 9 Septiembre 2019. [En línea]. Available: <https://insights.sei.cmu.edu/blog/situational-awareness-for-cybersecurity-an-introduction/>.
- [6] S. Mukkamala, A. Sung y A. Abraham, «Cyber Security Challenges: Designing Efficient Intrusion Detection Systems and Antivirus Tools,» *Enhancing Computer Security with Smart Technology*, vol. I, nº 1, pp. 125-163, 2005.
- [7] A. L. Buczak y E. Guven, «A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,» *IEEE Communications Surveys & Tutorials*, vol. 18, nº 2, p. 1153–1176, 2015.
- [8] Berkeley, «LBNL Power Data,» 2016. [En línea]. Available: <https://secpriv.lbl.gov/project/powerdata/>.
- [9] J. McHugh, «Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory,» *ACM Transactions on Information and System Security*, vol. 3, nº 4.
- [10] R. D. Medenou, V. M. C. Mayo, M. G. Balufo, M. P. Castrillo, F. J. G. Garrido, A. L. Martinez, D. N. Catalán, A. Hu, D. S. Rodríguez-Bermejo y J. M. Vidal, «CYSAS-S3: a novel dataset for validating cyber situational awareness related tools for supporting military operations.,» de *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20)*, New York, NY, USA, 2020.
- [11] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník y J. Komárková, «CRUSOE: A toolset for cyber situational awareness and decision support in incident handling,» *Computers & Security*, vol. 115, nº 1, 2022.
- [12] United States Department of Defense, «Department of Defense Dictionary of Military and Associated Terms,» 12 Abril 2007. [En línea]. Available: <https://wikileaks.org/w/images/a/a7/Jp1-02.pdf>.
- [13] D. Raymond, T. Cross, G. Conti y R. Fanelli, «A Control Measure Framework to limit collateral damage and propagation of cyber weapon,» de *2013 5th International Conference on Cyber Conflic*, Tallinn, Estonia, 2013.
- [14] B. Thompson y R. Harang, «Identifying Key Cyber-Physical Terrain,» de *CODASPY '17: Seventh ACM Conference on Data and Application Security and Privacy*, Scottsdale, Arizona, USA, 2017.

- [15] P. Price, N. A. Leyba, M. Gondree, Z. Staples y T. Parker, «Asset Criticality in Mission Reconfigurable Cyber Systems and its Contribution to Key Cyber Terrain,» de *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii, 2017.
- [16] A. Kim y M. H. Kang, «Determining Asset Criticality for Cyber Defense,» 23 Septiembre 2011. [En línea]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.958.3955&rep=rep1&type=pdf>.
- [17] G. Bertoli y S. Raio, «The Elusive Nature of “Key Cyber Terrain”,» *Journal of the Cyber Security & Information Systems Information Analysis Center*, vol. 6, nº 2, pp. 40-47, 2018.
- [18] O. S. Oubbati, A. Lakas, F. Zhou, M. Güneş y M. B. Yagoubi, «A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs),» *Vehicular Communications*, vol. 10, nº 1, pp. 29-56, 2017.
- [19] J. N. Wang, A. Narula-Tam y R. Bhan, «Interconnecting Heterogeneous MANET Networks at the Tactical Edge,» de *2014 IEEE Military Communications Conference*, 2014.
- [20] W. Smith, G. Kuperman, M. Chan, E. Morgan y N. Nguyen, «Cloud computing in tactical environments,» de *2017 IEEE Military Communications Conference (MILCOM)*, 2017.
- [21] F. Chi, X. Wang, W. Cai y V. C. Leung, «Ad-Hoc Cloudlet Based Cooperative Cloud Gaming,» *IEEE Transactions on Cloud Computing*, vol. 6, nº 3, pp. 625-639, 2018.
- [22] 3GPP, «3rd Generation Partnership Project, Technical Specification Group Radio Access Network (E-UTRAN), Self-configuring and self-optimizing network (SON) use cases and solutions (Release 9),» Marzo 2011. [En línea]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2581>.
- [23] B.-N. Cheng, G. Kuperman, P. Deutsch, L. Mercer y A. Narula-Tam, «Group-centric networking: addressing information sharing requirements at the tactical edge,» *IEEE Communications Magazine*, vol. 54, nº 10, pp. 145-151, 2016.
- [24] J. M. Vidal y M. A. S. Monge, «Denial of sustainability on military tactical clouds,» de *15th International Conference on Availability, Reliability and Security (ARES '20)*, New York, NY, USA, 2020.
- [25] C. Hoff, «Cloud Computing Security: From DDoS (Distributed Denial Of Service) to EDoS (Economic Denial of Sustainability),» 27 Noviembre 2008. [En línea]. Available: <https://www.rationalsurvivability.com/blog/2008/11/cloud-computing-security-from-ddos-distributed-denial-of-service-to-edos-economic-denial-of-sustainability/>.
- [26] C. Hoff, «A Couple Of Follow-Ups On The EDoS (Economic Denial Of Sustainability) Concept...,» 23 Enero 2009. [En línea]. Available: <https://www.rationalsurvivability.com/blog/2009/01/a-couple-of-follow-ups-on-the-edos-economic-denial-of-sustainability-concept/>.
- [27] G. Somani, M. S. Gaur, D. Sanghi y M. Conti, «DDoS attacks in cloud computing: Collateral damage to non-targets,» *Computer Networks*, vol. 109, pp. 157-171, 2016.
- [28] M. A. S. Monge, J. M. Vidal y G. M. Pérez, «Detection of economic denial of sustainability (EDoS) threats in self-organizing networks,» *Computer Communications*, vol. 145, nº 1, pp. 284-308, 2019.
- [29] H. Abbasi, N. Ezzati-Jivan, M. Bellaiche, C. Talhi y M. R. Dagenais, «Machine Learning-Based EDoS Attack Detection Technique Using Execution Trace Analysis,» *Journal of Hardware and Systems Security*, vol. 3, pp. 164-176, 2019.

- [30] Z. Zhou, L. Qian y H. Xu, «Intelligent Decentralized Dynamic Power Allocation in MANET at Tactical Edge based on Mean-Field Game Theory,» de *2019 IEEE Military Communications Conference (MILCOM)*, 2019.
- [31] ETSI, «ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV,» Enero 2020. [En línea]. Available: https://www.etsi.org/deliver/etsi_gr/NFV/001_099/003/01.05.01_60/gr_NFV003v010501p.pdf.
- [32] M. A. S. Monge, J. M. Vidal y R. D. M. Choumanof, «Adaptive Mitigation of Tactical Denial of Sustainability,» de *16th International Conference on Availability, Reliability and Security (ARES 2021)*, New York, NY, USA, ARES 2021.
- [33] X. Larriva-Novó, M. Vega-Barbas, V. A. Villagrà, D. Rivera, M. Sanz y M. Álvarez-Campana, «Dynamic risk management architecture based on heterogeneous data sources for enhancing the cyber situational awareness in organizations,» de *Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20)*, New York, NY, USA, 2020.
- [34] B. Gruschke, «A New Approach for Event Correlation based on Dependency Graphs,» de *5th Workshop of the OpenView University Association*, 1998.
- [35] N. Krishnamurthy y T. Deborah, «US-6629106-B1 - Event Monitoring and Correlation System,» 29 Septiembre 2003. [En línea]. Available: <https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=06629106&IDKey=&HomeUrl=%2F>.
- [36] Q. Wu, D. Ferebee, Y. Lin y D. Dasgupta, «An integrated cyber security monitoring system using correlation-based techniques,» de *2009 IEEE International Conference on System of Systems Engineering (SoSE)*, Albuquerque, NM, USA , 2009.
- [37] S. Bhatt, P. K. Manadhata y L. Zomlot, «The Operational Role of Security Information and Event Management Systems,» *IEEE Security & Privacy*, vol. 12, n° 1, pp. 35-41, 2014.
- [38] W. Holub, T. Parsons, P. O'Sullivan y J. Murphy, «Run-time correlation engine for system monitoring and testing,» de *6th international conference industry session on Autonomic computing and communications industry session*, New York, NY, USA, 2009.
- [39] IBM, «Common base event format,» IBM, 13 Octubre 2021. [En línea]. Available: <https://www.ibm.com/docs/en/cics-ts/5.3?topic=formats-common-base-event-format>.
- [40] F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, Virginia: Potomac Institute for Policy Studies, 2007.
- [41] A. Bratko, D. Zaharchuk y V. Zolka, «Hybrid warfare – a threat to the national security of the state,» *Revista de Estudios en Seguridad Internacional*, vol. 7, n° 1, pp. 147-160, 2021.
- [42] W. Murray y P. R. Mansoor, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, 2012, pp. 254-288.
- [43] F. G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington: Potomac Institute for Policy Studies, 2007, pp. 20-22.
- [44] CNBC, «Macron campaign says it is the victim of massive, coordinated hacking campaign,» CNBC, 5 Mayo 2017. [En línea]. Available: <https://www.cnbc.com/2017/05/05/macron-campaign-says-it-is-the-victim-of-massive-coordinated-hacking-campaign-reuters.html>.
- [45] V. Cotovio, «Russia accused of 'Ghostwriter' cyberattacks ahead of German election,» 24 Septiembre 2021. [En línea]. Available: <https://edition.cnn.com/2021/09/24/europe/russia-accused-ghostwriter-cyberattacks-german-election-intl>.

- [46] E. Kovacs, «SolarWinds Likely Hacked at Least One Year Before Breach Discovery | SecurityWeek.Com,» 18 Diciembre 2020. [En línea]. Available: <https://www.securityweek.com/solarwinds-likely-hacked-least-one-year-breach-discovery>.
- [47] C. Bing, «Suspected Russian hackers spied on U.S. Treasury emails - sources | Reuters,» Reuters, 13 Diciembre 2020. [En línea]. Available: <https://www.reuters.com/article/us-usa-cyber-treasury-excluive-idUSKBN28N0PG>.
- [48] A. Sebenius, K. Mehrotra y M. Riley, «U.S. Agencies Exposed in Attack by Suspected Russian Hackers - Bloomberg,» 13 Diciembre 2020. [En línea]. Available: <https://web.archive.org/web/20201216002322/https://www.bloomberg.com/news/articles/2020-12-14/u-s-government-agencies-attacked-by-hackers-in-software-update>.
- [49] D. E. Sanger, N. Perlroth y E. Schmitt, «Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit - The New York Times,» 14 Diciembre 2020. [En línea]. Available: <https://web.archive.org/web/20201218062201/https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>.
- [50] R. S. Mueller, «Report On The Investigation Into Russian Interference In The 2016 Presidential Election,» Marzo 2019. [En línea]. Available: <https://www.justice.gov/archives/sco/file/1373816/download>.
- [51] Office of the Director of National Intelligence, «Statement by NCSC Director William Evanina: Election Threat Update for the American Public,» 7 Agosto 2020. [En línea]. Available: <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.
- [52] T. D. Grant, «Annexation of Crimea,» *American Journal of International Law*, vol. 109, nº 1, pp. 98-95, 2015.
- [53] Security Service of Ukraine, «Gamaredon/Armageddon Group,» 4 Noviembre 2021. [En línea]. Available: <https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armageddon.pdf>.
- [54] D. McWhorter, «APT28: A Window into Russia's Cyber Espionage Operations? | Mandiant,» Mandiant, 27 Octubre 2014. [En línea]. Available: <https://www.mandiant.com/resources/apt28-a-window-into-russias-cyber-espionage-operations>.
- [55] N. Kostyuk y Y. M. Zhukov, «Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?,» *Journal of Conflict Resolution*, vol. 63, nº 2, pp. 317-347, 2019.
- [56] D. Park y M. Walstrom, «Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks - The Henry M. Jackson School of International Studies,» 11 Octubre 2017. [En línea]. Available: <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks>.
- [57] Security Service of Ukraine, «SSU neutralizes over 2,000 cyber attacks on government resources in 2021,» Security Service of Ukraine, 18 Enero 2022. [En línea]. Available: <https://ssu.gov.ua/en/novyny/za-mynulyi-rik-sbu-neitralizuvala-ponad-2-tysiachi-kiberatak-na-uriadovi-resursy-ukrainy>.
- [58] Security Service of Ukraine, «SSU investigates Russian involvement in cyber attacks on Ukrainian government websites,» Security Service of Ukraine, 14 Enero 2022. [En línea]. Available: <https://ssu.gov.ua/en/novyny/sbu-rozsliduie-prychetnist-rosiiskikh-spetssluzhb-dohodnishnoi-kiberatky-na-orhany-derzhavnoi-vlady-ukrainy>.
- [59] J. Tidy, «Ukraine: EU deploys cyber rapid-response team,» BBC, 22 Febrero 2022. [En línea]. Available: <https://www.bbc.com/news/technology-60484979>.

- [60] J. Tidy, «Ukraine crisis: 'Wiper' discovered in latest cyber-attacks,» BBC, 24 Febrero 2022. [En línea]. Available: <https://www.bbc.com/news/technology-60500618>.
- [61] B. Krebs, «Report: Recent 10x Increase in Cyberattacks on Ukraine,» 11 Marzo 2022. [En línea]. Available: <https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/>.
- [62] Quad9, «Quad9 and Your Data,» 13 Marzo 2018. [En línea]. Available: <https://www.quad9.net/news/blog/quad9-and-your-data/>.
- [63] Ministerio de Hacienda y Administraciones Públicas, «MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.
- [64] L. B. A. Rabai, M. Jouini, A. B. Aissa y A. Mili, «A cybersecurity model in cloud computing environment,» *Journal of King Saud University - Computer and Information Sciences*, vol. 25, nº 1, pp. 63-75, 2013.
- [65] J. Witts, «How Does Browser Isolation Work?,» Expert Insights, 28 Marzo 2022. [En línea]. Available: <https://expertinsights.com/insights/how-does-browser-isolation-work/>.
- [66] Gartner, «Gartner Identifies the Top Technologies for Security in 2017,» Gartner, National Harbor, MD., 2017.
- [67] J. DeHaan, «New IT initiative promises safer, faster web browsing experience for DoD employees,» U.S. Army, 16 Junio 2021. [En línea]. Available: https://www.army.mil/article/247605/new_it_initiative_promises_safer_faster_web_browsing_experience_for_dod_employees.
- [68] J. Miller, «Cloud based internet isolation initiatives to give DoD new kind of cyber protections,» Federal News Network, 15 Octubre 2020. [En línea]. Available: <https://federalnewsnetwork.com/ask-the-cio/2020/10/cloud-based-internet-isolation-initiatives-to-give-dod-new-kind-of-cyber-protections/>.
- [69] W. Kenton, «Mission Critical,» 18 Septiembre 2021. [En línea]. Available: <https://www.investopedia.com/terms/m/mission-critical.asp>.
- [70] C. A. Schmidt, Complete CompTIA A+ Guide to PCs, 6th Edition, Pearson IT Certification, 2013.
- [71] Piotrowski, «Susceptibility of PC to electromagnetic interference,» de *Electromagnetic Compatibility Symposium Adelaide*, Adelaide, 2009.
- [72] Instituto Nacional de Ciberseguridad, «¡Fácil y sencillo! Análisis de riesgos en 6 pasos,» 16 Enero 2017. [En línea]. Available: <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo>.
- [73] J. Zhang y Y. Lv, «High Frequency Impedance and Electromagnetic Interference Suppression of Lithium-Ion Power Battery Pack,» de *WCX SAE World Congress Experience*, Detroit, 2019.
- [74] K. Armstrong, «EMC techniques in electronic design Part 2 - Cables and Connectors,» 2009. [En línea]. Available: https://www.emcstandards.co.uk/files/part_2_text_and_graphics_21_may_09.pdf.
- [75] The International Institute for Strategic Studies, *The Military Balance 2021*, London: Routledge Journals, 2021.

- [76] D. Axe, «Strategist: Killer Drones Level Extremists' Advantage,» WIRED, 17 Juni 2009. [En línea]. Available: <https://www.wired.com/2009/06/strategist-killer-drones-level-extremists-advantage/>.
- [77] P. Taylor, Text-to-Speech Synthesis, Cambridge University Press, 2009.
- [78] Zen, H., Tokuda, K., & Black, A. W., «Statistical parametric speech synthesis,» *Speech Communication*, 51(11), pp. 1039-1064, 2009.
- [79] Pardo, J.M., Giménez de los Galanes, F.M., Vallejo, J.A., Berrojo, M.A., Montero, J.M., Enríquez, E., Romero, A., «Spanish text-to-speech, from prosody to acoustics,» de *International Congress of Acoustics*, 1995.
- [80] «Portal web de la ETSIT UPM,» [En línea]. Available: <http://www.etsit.upm.es/>.

ANEXO A: ASPECTOS ÉTICOS, ECONÓMICOS, SOCIALES Y AMBIENTALES

A.1 INTRODUCCIÓN

Este proyecto permitirá poder detectar correlaciones entre eventos que sucedan en el ciberespacio y en el campo de batalla, por lo que ayudará a calcular las posibilidades de que sucesos aislados en estos dos dominios terminen causando un conflicto a gran escala.

A.2 DESCRIPCIÓN DE IMPACTOS RELEVANTES RELACIONADOS CON EL PROYECTO

Se considera que el impacto de este trabajo abarca varias áreas, ya que puede ayudar a predecir posibles guerras, las cuales tienen un impacto tanto a nivel social como económico o ambiental.

En cuanto al nivel social, estos conflictos terminan cobrándose la vida de varias personas y con muchas otras exiliadas. Por lo que al nivel económico se refiere, algunos de los países beligerantes pueden recibir sanciones económicas de la comunidad internacional o tener sus relaciones comerciales bloqueadas con otros países. Por último, cabe destacar el impacto en el medio ambiente, debido a que en estos conflictos se utilizan varias armas que afectan a este.

A.3 ANÁLISIS DETALLADO DE ALGUNO DE LOS PRINCIPALES IMPACTOS

Se considera que el impacto a nivel social es el principal impacto para analizar debido a que las guerras tienen grandes consecuencias en esta dimensión.

Más concretamente, las guerras tienen consecuencias a nivel social como provocar la muerte de varios soldados y civiles y el exilio de un gran número habitantes en ambos bandos, provocando la separación de bastantes familias.

Con este proyecto, los gobiernos podrán predecir estos conflictos, ayudándoles a tomar medidas preventivas que garanticen la seguridad de su población.

A.4 CONCLUSIONES

Los impactos relacionados con este proyecto descritos anteriormente otorgan un valor adicional a este trabajo, ya que son muestra de la importancia que tiene continuar con esta línea de investigación para poder ayudar a paliar los efectos propios de los conflictos armados descritos anteriormente.

ANEXO B: PRESUPUESTO ECONÓMICO

		horas	Precio/hora	TOTAL
COSTE DE MANO DE OBRA (coste directo)		350	15 €	5.250 €
COSTE DE RECURSOS MATERIALES (coste directo)				
	Precio de compra	Uso en meses	Amortiz. en años	TOTAL
Ordenador personal (Software incluido).....	1.500,00 €	6	5	150,00 €
Impresora láser	300,00 €	6	5	30,00 €
Otro equipamiento				
TOTAL				180,00 €
GASTOS GENERALES (costes indirectos)	15%	sobre CD		814,50 €
BENEFICIO INDUSTRIAL	6%	sobre CD+CI		374,67 €
MATERIAL FUNGIBLE				
Impresión				100,00 €
Encuadernación				50,00 €
SUBTOTAL PRESUPUESTO				6.769,17 €
IVA APLICABLE			21%	1.421,53 €
TOTAL PRESUPUESTO				8.190,70 €