El uso de la ciberarmas de día cero zero-day y su efecto en los sistemas de información militares en un conflicto armado internacional

Alfredo Miranda Capurro

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

EL USO DE LAS CIBERARMAS DE DIA CERO (ZERO-DAY) Y SU EFECTO EN LOS SISTEMAS DE INFORMACION MILITARES EN UN CONFLICTO ARMADO INTERNACIONAL

ALUMNO: TTE 1° (AP) ALFREDO MIRANDA CAPURRO

DIRECTOR: DR. CARLOS CASTAÑEDA MARROQUIN

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

EL USO DE LAS CIBERARMAS DE DIA CERO (ZERO-DAY) Y SU EFECTO EN LOS SISTEMAS DE INFORMACION MILITARES EN UN CONFLICTO ARMADO INTERNACIONAL.

Resumen

El ciberespacio viene siendo el medio por el cual los sistemas de información militares vienen integrando y gestionando información para la toma de decisiones. Las ciberarmas, como medios con los cuales se articulan ciber-operaciones ofensivas en ámbitos externos, son las desencadenantes de violencia, en y a través del ciberespacio, mediante el uso de la fuerza en una fuerza armada. La conjunción de ambos causa efectos adversos e incluso impredecibles, sobre todo si entran a tallar factores cambiantes de reglas de juego, como vienen siendo las vulnerabilidades de día cero y su exponente ofensivo a través de *exploits*. Las principales limitaciones, como es la falta de consenso en términos de aplicación ciberespacial y la ausencia de experiencias bélicas en ese campo, deja un vacío sobre cómo poder entender la peligrosidad e, importancia actual e incrementalmente futura que representa el conocimiento de vulnerabilidades de día cero y su militarización en un conflicto armado internacional frente a sistemas de información de índole militar.

La presente monografía de grado, busca representar dicha problemática a través de un marco referencia en donde se exponga el potencial uso que tienen las ciberarmas en el contexto antes propuesto. Dicha investigación, de tipo no experimental, impactará positivamente en la toma de decisiones sobre uso o adquisición de tecnología ciberespacial en aplicaciones no solo militares, sino también a otras áreas símiles gubernamentales con relación a la seguridad y defensa nacional, y las amenazas que afrontan.

Adicionalmente, se prevé que este marco, a través de su potencial adaptabilidad, otorgará elementos base para el desarrollo de modelos aplicables a la gestión de riesgos o incluso, elementos partícipes a tomar en cuenta al momento del desarrollo de operaciones ciberespaciales como parte del planeamiento operacional militar.

Palabras clave

día cero - ciberarma – ataques desconocidos – ciberdefensa – ciber-conflicto

Abstract

Cyberspace has been the vehicle by which military informational systems are integrating and managing information for decision making. Cyber weapons- as means where offensive cyberspace operations are articulate in external fields- are triggers of violence, in and through cyberspace, by the use of force in an armed force. The conjunction of both causes adverse effects and even unpredictable ones, mainly if some factors like a "game changer" get into it, as zero-day vulnerabilities and its offensive exponent known as zero-day exploits. The main limitations, as the lack of consensus in terms of cyberspace applicability and, the absence of war experiences in this field, leaves a gap between how to understand the danger that represents the knowledge of zero-day vulnerabilities and its military use in an international armed conflict against military informational systems.

This monograph tries to represent this issue presenting a framework that shows the potential uses that cyber weapons have in the context previously proposed. This research, of a non-experimental nature, will impact positively in the decision-making process regarding the use or acquisition of cyberspace technologies not only in military applications, but also, in other government sectors in relation with the national security and defense, and the threats they face.

Additionally, this framework, by its potential adaptability, will present base elements for the development of applicable models to the risk management or even inputs to take into account for the development of cyberspace operations as part of the military operations planning.

Keywords

zero-day – cyber weapon – unknow attacks – cyber defence – cyber conflict

Índices de contenido

Índice de Figuras

Listado de siglas y abreviaturas

ed.	edición
eds.	editores
ej.	ejemplar, ejemplo
et al.	*et alii*
etc.	etcétera
p.	página
pp.	páginas
p. ej.	por ejemplo

El uso de las ciberarmas de día cero (*zero-day*) y su efecto en los sistemas de información militares en un conflicto armado internacional.

0. Introducción

La evolución tecnológica de los últimos cuarenta años ha permitido a las fuerzas militares migrar desde un entorno mecánico y análogo hacia uno digital e informatizado. Dichas acciones, tanto en ámbitos administrativos como operacionales, ha conllevado a nuevos riesgos frente al uso y dependencia de estas nuevas tecnologías. Una forma de tratar estos riesgos ha sido a través del desarrollo de elementos tecnológicos defensivos que permitan proteger los sistemas de información bajo diversos perímetros de seguridad.

Estos enfoques conllevan a tener una perspectiva usualmente reactiva hacia nuevas amenazas descubiertas y, por ende, no prometen una protección contra vulnerabilidades desconocidas (Lyn, 2015). Son este tipo de vulnerabilidades las cuales vienen siendo materializadas a causa de fallos de codificación que la tecnología tiene a la hora de ser producida y que puede ser explotable por aquellos actores que la conocen; esto mediante la presencia de vulnerabilidades cuyo conocimiento público es de cero días o comúnmente conocidas como *zero-day* (Friedman y Singer, 2014).

El potencial armamentístico que tiene este tipo de vulnerabilidades y su aplicabilidad de uso en un Conflicto Armado Internacional (CAI) por una fuerza armada adversaria hacia los sistemas de información castrenses propios, permite inferir el gran valor que éstas pueden significar para el cumplimiento de objetivos militares. Dicha situación hace que sea una prioridad el poder tener un conocimiento base que pueda articular futuros marcos de riesgos técnicos y específicos frente a tecnología informacional militar adquirida o desarrollada.

La presente monografía de grado aborda esta problemática a través de la pregunta de investigación "¿Cómo las ciberarmas que explotan vulnerabilidades de día cero (*zero-day*) podrían afectar los sistemas de información militares en un conflicto armado internacional?". Todo esto bajo una línea concordante a la línea temática de investigación "Naturaleza de la Guerra, Terrorismo y Nuevas Amenazas" de esta Escuela Superior de Guerra.

Para dar respuesta a dicha pregunta, el objetivo general de este trabajo académico es representar esta situación a través de un marco de referencia o *framework*. Para tal fin, se desarrollan tres capítulos concordantes a los objetivos secundarios de la investigación, el primero comprende el estado del arte de los conceptos partícipes de la pregunta de investigación y su interrelación contextual. El segundo, provee un análisis de dos casos particulares y específicos que permitan aportar en la elaboración del escenario propuesto y, el tercero, la articulación de estos dos últimos a fin de componer el marco de referencia antes propuesto.

Finalmente, se presentan las conclusiones de este estudio y algunos trabajos futuros que puedan derivarse de éste.

1. Capítulo I

Los conceptos de ciberarmas, sistemas de información y ciber-operaciones aún se encuentran en elaboración o no tienen un consenso específico a nivel internacional. Dicha ausencia toma origen por la forma cómo el ciberespacio es conceptualizado y explotado en el campo militar por parte de países con mayor desarrollo de capacidades ciberespaciales.

Por tal motivo, este capítulo se divide en dos partes: una primera donde se introduce al lector en apartados referentes a los conceptos de vulnerabilidades de día cero, ciberarmas, sistemas de información y operaciones ciberespaciales militares; y una segunda, en la que se realiza una exposición de la relación que tienen estos tres últimos con las vulnerabilidades de día cero.

El objeto del mismo, será emplear el desarrollo de estos tópicos como elementos para la confección del marco de referencia a ser expuesto en el Capítulo III.

1.1. Elementos interactuantes.

1.1.1. *Vulnerabilidades de día cero.*

1.1.1.1. Vulnerabilidad.

Bajo el enfoque de la seguridad de la información, una vulnerabilidad es una "debilidad en un activo o control que puede ser explotada bajo una o más amenazas" (Joint Technical Committee ISO/IEC JTC 1/SC 27 IT Security techniques, 2018, p. 11). Estas debilidades tienen una multidimensionalidad que va desde lo tecnológico hasta lo humano, con causas que radican en fallos, deliberados o no, en el diseño, producción, remisión, configuración o durante el funcionamiento de los mencionados activos.

Bajo la dimensionalidad tecnológica que compone un sistema de información, el tipo de debilidades a las que se encuentra afecto son aquellas relacionadas al hardware, firmware y software. Desde el 2001 hasta el 2018 se han reportado un total de 108 685 vulnerabilidades (Özkan, 2019), y de éstas se observa, mediante Figura 1.1, que hay una tendencia al alza en cuanto a su cantidad y distribución de severidad.

Si bien la sola presencia de vulnerabilidades no necesariamente indica que pueden ser estas explotadas por parte de atacantes (Schneier, 2018), una vulnerabilidad de severidad alta (*high*) es

muy probable que si lo permita. Finalmente, éstas son remediadas mediante una acción reactiva realizada a través del despliegue y/o remisión de "parches"[1] por parte del fabricante (usualmente) hacia los usuarios finales.

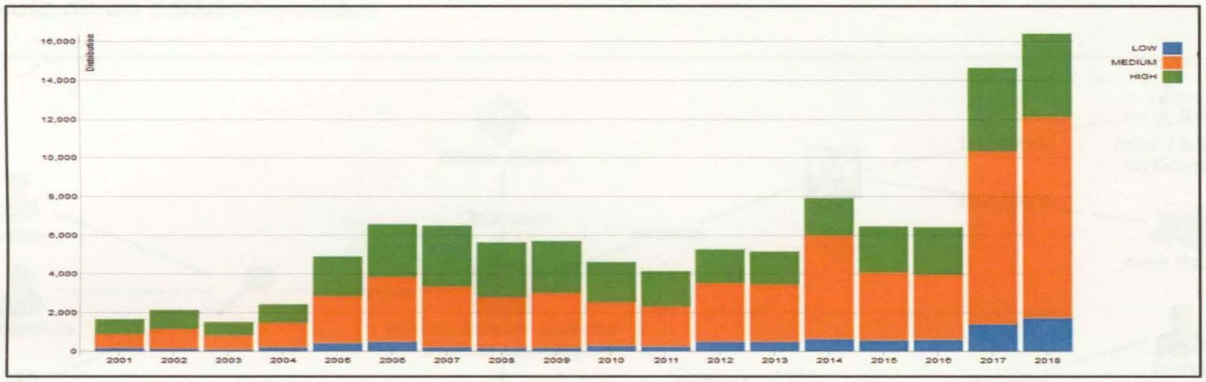

Figura 1.1 Distribución a través del tiempo de severidad CVSS.
Fuente: National Institute of Standards and Technology (2019).

1.1.1.2. Vulnerabilidades de día cero (zero-day) y detonador de día cero.

Una vulnerabilidad de día cero o *zero-day* es una vulnerabilidad cuyo parche no ha sido desarrollado, usualmente porque el desarrollador desconoce que se tiene esa vulnerabilidad (Libicki, Ablon y Webb, 2015). Como afectación, ésta no limita su presencia a sólo puntos finales de la red como vienen siendo los computadores de escritorio o portátiles, sino a todo sistema computacional que pueda verse afectado por fallos o errores sin importar la funcionalidad que cumpla, como puede ser un sistema de ciberseguridad, un sistema ciber-físico, un conmutador, etc.

El componente de detonación de estas vulnerabilidades desconocidas con fines perjudiciales se denomina *exploit* de *zero-day* o detonador de día cero, este hace referencia a la creación de código para aprovechar dicha vulnerabilidad con la finalidad de acceder a otras partes del sistema, ejecutar un código propio, actuar como administrador u otras acciones potencialmente perjudiciales (Ablon y Bogart, 2017). El modelo de trabajo con el cual se basan este tipo de *exploits* es a través del secretismo de su uso. Un mismo *exploit* de *zero-day* puede ser detonado paralelamente por diversos actores, incluso beligerantes entre sí, pero manteniéndose la particularidad de que éste no sea conocido públicamente.

[1] Modificación rápida de un programa, generalmente una sección de código que es superpuesto en un programa existente o sistema (Slade, 2006).

Los modos de obtención que se encuentran esquematizados en la Figura 1.2, dan a conocer cómo es que, a partir de ejes investigativos o de persuasión sobre un producto en particular, son detectadas / insertadas las vulnerabilidades y/o desarrollados o adquiridos los *exploits* de *zero-day* por parte de un Estado-Nación.

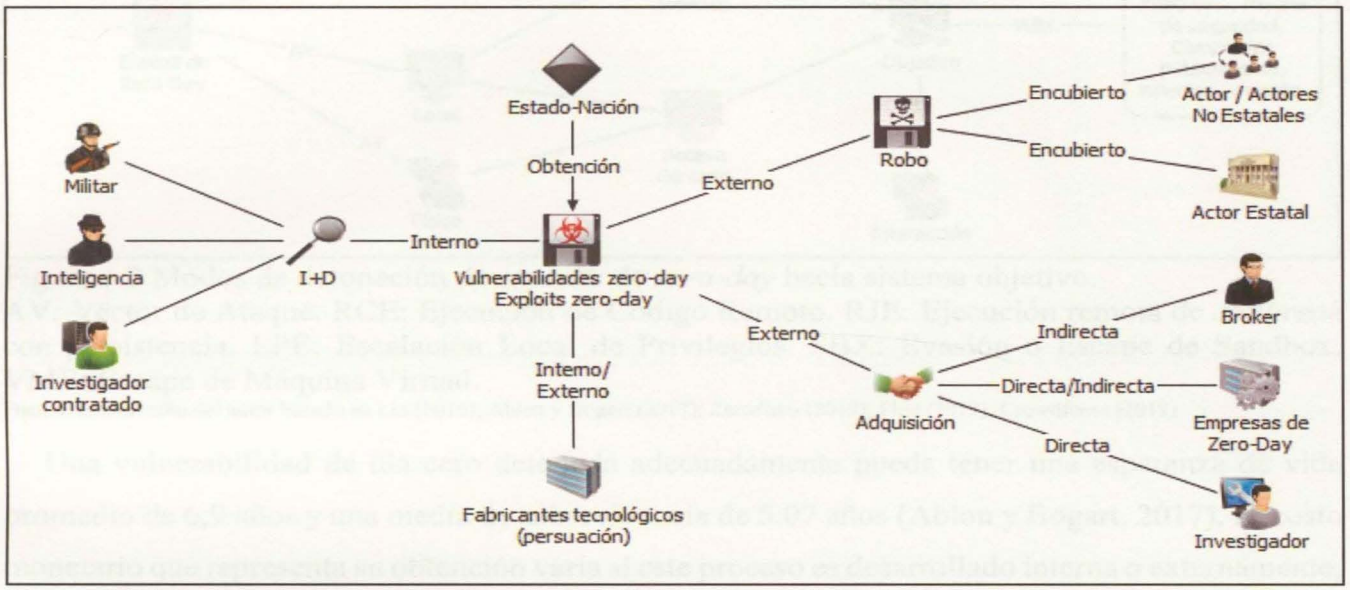

Figura 1.2 Modelo de obtención de vulnerabilidades y *exploits* de *zero-day* por parte de un Actor Estatal.

Fuente: Elaboración del autor basado en Herzog y Schmid (2016); Ablon y Bogart (2017); Lin (2010); Leonhard. (2017).

Los modos de detonación de un *exploit* de *zero-day* en el proceso de vulneración de un objetivo son subdivididos en vector de ataque, el tipo de acceso al objetivo y la interacción requerida para su activación; la descripción de estos se aprecia en la Figura 1.3.

Las acciones posteriores a esta detonación son definidas por el *payload* o carga útil que acompaña o descarga el *exploit* una vez este es desplegado. Es este *payload* el que se encarga de solidificar y mantener el acceso, así como de entregar efectos al sistema (Ablon y Bogart, 2017). Dichos efectos pueden ser medidos a través de los principios de la confidencialidad, integridad y disponibilidad o símiles accionables como la manipulación y negación.

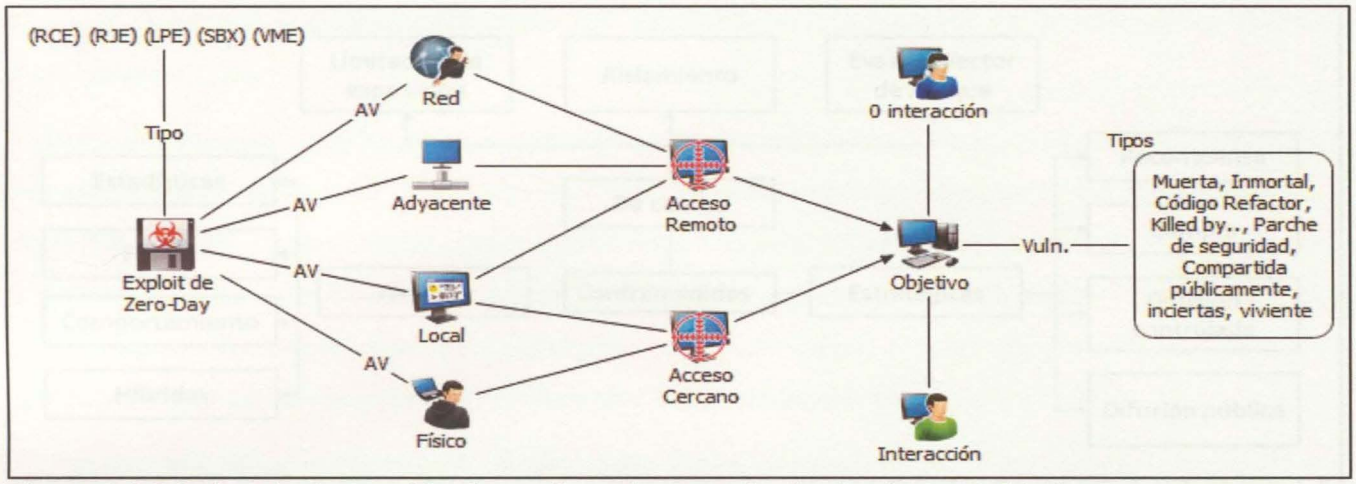

Figura 1.3 Modos de detonación de *exploits* de *zero-day* hacia sistema objetivo.
AV: Vector de Ataque. RCE: Ejecución de Código Remoto. RJE: Ejecución remota de *Jailbreak* con persistencia. LPE: Escalación Local de Privilegios. SBX: Evasión o Escape de Sandbox. VME: Escape de Máquina Virtual.
Fuente: Elaboración del autor basado en Lin (2016); Ablon y Bogart (2017); Zerodium (2019); First (2019); Crowdfense (2019).

Una vulnerabilidad de día cero detonada adecuadamente puede tener una esperanza de vida promedio de 6,9 años y una media de sobrevivencia de 5.07 años (Ablon y Bogart, 2017). El costo monetario que representa su obtención varía si este proceso es desarrollado interna o externamente; sólo la venta de vulnerabilidades de este último puede llegar a alcanzar los 3 millones de dólares (Crowdfense, 2019).

La variedad de factores combinables que representa la detonación de vulnerabilidades de día cero hace poco factible especificar cada escenario y contexto técnico, más aún si se considera la ausencia de casos no documentados de vectores de aproximación y el nulo conocimiento sobre aquellos *exploits (*de *zero-day)* activos. Características generales que guardan éstas están orientadas al paradigma de la invulnerabilidad de un sistema solo por el hecho de aplicarse medidas de seguridad estándar como son las actualizaciones en sus diferentes niveles, el *hardening* (endurecimiento) del sistema y la implementación de controles convencionales de seguridad.

1.1.1.3. Contramedidas.

Las contramedidas pueden ser clasificadas en tres modalidades cuya extensión se observa en el siguiente esquema (Figura 1.4). Las técnicas se encuentran orientadas a la reacción frente a un despliegue o detonación del *exploit*, mientras que las estratégicas a reducir su uso privado, y las de campo, orientadas a la disminución de la superficie de ataque del sistema frente al adversario.

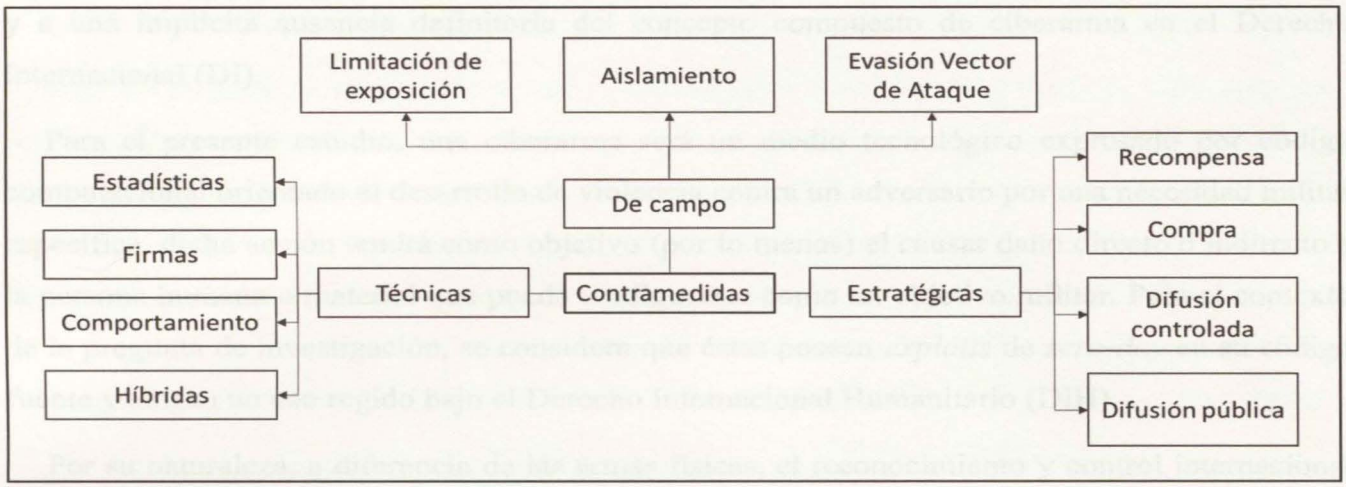

Figura 1.4 Contramedidas.
Elaboración del autor basado en Kaur y Singh (2014); Herzog y Schmid (2016).

Una vez que se hace pública la vulnerabilidad, actúa el desarrollador del activo vulnerado (si se cuenta con soporte técnico vigente), mediante la producción de un parche; de igual manera proveedores de sistemas de seguridad podrán desplegar paquetes de actualizaciones a fin de proveer detección sobre este tipo de vulnerabilidad. En menor medida organizaciones gubernamentales (p. ej. CERTs, CSIRT, etc.) o no lucrativas podrán proveer boletines informativos para de mitigación frente a la misma (p. ej. cerrar puertos, dar de baja servicios, etc.).

Hay problemáticas con respecto a la prioridad con la cual se crea un parche, un fabricante preferirá priorizar la creación de parches para un sistema más difundido frente a otro que, a pesar de tener el soporte técnico vigente, no lo considera prioritario. Una vez creado, la implementación inmediata de éste por parte de los usuarios de los sistemas puede, dependiendo de la complejidad del mismo, traer efectos negativos frente a la operatividad, como es la interferencia con otros sistemas o poner incluso en peligro éste a causa de su calidad, por lo que será necesario un análisis del impacto previo a su despliegue.

La suma de tiempo que conllevan estos factores de creación, despliegue, análisis e implementación, resultan en una ventana de tiempo en la cual es posible que la vulnerabilidad recientemente descubierta sea utilizada por una infinidad de actores que quieran explotarla.

1.1.2. *Ciberarmas.*

Hay ausencia de un acuerdo internacional para la definición del término de arma (Boothby, 2016), lo que conlleva a la dificultad de querer relacionar el dominio ciberespacial con las armas

y a una implícita ausencia definitoria del concepto compuesto de ciberarma en el Derecho Internacional (DI).

Para el presente estudio, una ciberarma será un medio tecnológico expresado por código computacional orientado al desarrollo de violencia contra un adversario por una necesidad militar específica, dicha acción tendrá como objetivo (por lo menos) el causar daño directo o indirecto a la persona humana o material que pueda configurarse como un objetivo militar. Para el contexto de la pregunta de investigación, se considera que éstas posean *exploits* de *zero-day* en su código fuente y tengan un uso regido bajo el Derecho Internacional Humanitario (DIH).

Por su naturaleza, a diferencia de las armas físicas, el reconocimiento y control internacional sobre estos medios es un problema de vigente complejidad. Su desarrollo o adquisición es realizado a través del secretismo propio de las herramientas de inteligencia, teniéndose la similitud adicional que supone el acceso clandestino a sistemas adversarios. De igual forma, la sola posesión de este tipo de ciberarmas (que detonan vulnerabilidades de día cero) significa que un determinado sistema es vulnerable, por lo que una declaración pública de tenencia alertaría tanto a aquellos poseedores de los sistemas afectados como a actores tecnológicos responsables frente a la toma de medidas para su corrección o neutralización.

Dicha característica dificulta a su vez la cuantificación de capacidades reales de una fuerza armada en un escenario de guerra. De igual manera, existe el riesgo que el adversario una vez las identifique realice acciones de contención y remediación de los activos vulnerados, generando su inutilidad, o en algunos casos, pudiendo ser usadas contra la propia fuerza; por lo que el despliegue de las mismas estará a razón de la conceptualización doctrinaria establecida por la fuerza.

Operacionalmente, la aplicación de este uso de fuerza a través de las ciberarmas significaría la eventual pérdida de una intrínseca capacidad de colección de información para la inteligencia, esto al tenerse el acceso y control del sistema cibernético objetivo. Por lo antes expuesto, su uso dependerá de la valoración que haga el Comandante con respecto al resultado proyectado frente al deterioro o pérdida de capacidad de vigilancia cibernética.

De acuerdo a su programación pueden funcionar de manera autónoma o bajo un comando y control; por lo que, en este último caso, se requerirá implícitamente de un medio (directo o indirecto), de comunicación externo.

1.1.3. *Sistemas de Información.*

Bajo un enfoque militar, un Sistema de Información corresponde a "toda la infraestructura, organización, personal y componentes para la colección, procesamiento, almacenamiento, transmisión, exhibición, diseminación y disposición de información" (Department of Defense, 2010, p. 176). Mientras que, bajo la perspectiva tecnológica, su definición corresponde a "un programa que se centra en los principios, el diseño y la aplicación de tecnología informática y de redes en el entorno militar" (Institute of Education Sciences, 2019). La clasificación de estos Sistemas de Información Militar (SIM) suele ser reservada, por lo que se proponen cinco tipos:

- Por funcionalidad: administrativos y operacionales.
- Por su propósito: p. ej. Comando y Control (C&C), logístico, etc.
- Por su clasificación de seguridad: p. ej. secreto, confidencial, etc.
- Por su criticidad: valor que representa su presencia en el desarrollo de operaciones militares en el contexto propuesto.
- Por su modalidad de producción o uso: Productos customizados y los productos fuera de caja (p. ej. COTS [*Commercial off-the-shelf*], GOTS [*Government off-the-shelf*], etc.).

Si bien el sector defensa ha tendido a crear su propio hardware, software y protocolos de comunicación desde el inicio de la cibernética, estos continuamente han venido integrándose a protocolos base estándar como es el Protocolo de Internet (IP) o, a hardware y software comercial cuyo doble uso, permite el soporte de la operación de sus sistemas de información. Esta tendencia de uso adaptativo de tecnología civil de madurez aplicable permite de igual manera, tener menores costos de operación y mantenimiento. Lo antes expuesto hace que la división de qué es de uso exclusivamente militar frente al civil este siendo cada vez más difusa.

Los SIM pueden compartir arquitectura o interactuar con otros tipos de sistemas como son los sistemas ciber-físicos[2]. Una de las problemáticas que han venido surgiendo es la incremental automatización digital a la cual han venido siendo objeto estos sistemas militares. Esto último es

[2] La U.S. Government Accountability Office (2018) los ejemplifica como aviones, buques, misiles, etc.; su comprometimiento genera afectación en mundos físicos, con consecuencias mayores que ataques a otros sistemas.

causante de incrementar la superficie de ataque que tiene una fuerza, sea a través de nodos de comunicación físicos o a través del espectro electromagnético.

Una característica que hace diferente un SIM frente a otros sistemas como un sistema de armas, es que la designación del primero aplica al correspondiente uso que se le dé y no primigeniamente al origen y/o al destino de su producción. Un SIM puede ser un software de servidor de correo, cuyo acceso tecnológico al mismo es tanto de uso civil como militar, mientras que un sistema de armas, como puede ser un sistema de defensa aérea, estará destinado a ser usado exclusivamente por una entidad militar.

1.1.4. *Operaciones ciberespaciales militares.*

1.1.4.1. Conflicto Armado Internacional.

Bajo la jurisprudencia internacional, el Tribunal Penal Internacional para la ex Yugoslavia (Comité Internacional de la Cruz Roja, 2008), afirma que "existe un Conflicto Armado Internacional (CAI) cuando se recurre a la fuerza armada entre dos o más Estados" (p.6).

Para el escenario propuesto de estudio, se requerirá de la presencia inequívoca de al menos dos a más actores estatales enfrentados, descartando un reemplazo (mas no una posible injerencia en la contienda) por aquellos no estatales y la respectiva proyección que estos tienen como ciber-amenazas bajo el ciberterrorismo, cibercrimen o el *hacktivismo* entre otros.

Es importante tener en cuenta que la presente investigación no se contextualiza necesariamente en un escenario de "ciberguerra" o ciber-conflicto como tal; sino únicamente en el uso de cierto tipo de ciberarma dentro de un CAI. Esto a razón de la poca homogeneidad que han venido teniendo estos términos por parte de diferentes autores y organismos.

1.1.4.2. Amenaza Ciberespacial – Estado-Nación.

Es fáctico determinar que las amenazas más sofisticadas y con mayor potencial de éxito sobre vulnerabilidades en activos cibernéticos son los Estados-Nación, y que cuya articulación de viabilidad requiere de los componentes de capacidad, acceso e intención (Jabbour y Devendorf, 2017).

Geopolíticamente el ciberespacio y su explotación en el campo militar tiende a ser visto y aplicado bajo los diversos enfoques que tengan estos Estados. Por ejemplo, Estados Unidos y parte

del bloque considerado como "occidente" conceptualizan al ciberespacio como un dominio separado, distinto de la guerra de la información y su asociación de aspectos psicológicos (Connell y Vogler, 2017).

El enfoque ruso expuesto por Kokoshin (Thomas, 2014), ve al aspecto de ciberguerra como un componente integral de la guerra de la información. Es decir, para ellos, las operaciones cibernéticas "no son una forma separada de guerra sino una herramienta de muchas dentro del marco más amplio de la guerra de información" (Creery, 2018). Mientras que, para China, su contexto doctrinario involucra a su equivalente militar, *computer network warfare*, como una parte principal dentro de las operaciones de información (Pollpeter, 2015).

La particularidad que tienen los Estados-Nación como amenaza es que "pueden conducir operaciones directamente o pueden tercerizarlas con terceras partes, incluyendo empresas de fachada, hackers patrióticos u otros sustitutos para alcanzar sus objetivos" (U.S. Joint Chiefs of Staff, 2018, pp. I-11). En relación con las vulnerabilidades, la Defense Science Board (2013) en la clasificación taxonómica que hace de ciber-amenazas, señala a éstos como actores que, en los niveles intermedios pueden descubrir vulnerabilidades y en niveles altos, crearlas usando todo espectro posible.

1.1.4.3. Ciber-operaciones.

Crowther (2017) manifiesta que hay cuatro conjuntos de actividades ciberespaciales que pertenecen al dominio militar: inteligencia, información, crimen y operaciones militares. Esta última (operaciones militares), como "actividades desarrolladas para cumplir una misión en el dominio militar" (Secretaría de Seguridad y Defensa Nacional, 2015, p. 113), vienen siendo adecuadas al concepto operacional ciberespacial mediante el término de ciber-operación. Schmitt y la NATO Cooperative Cyber Defence Centre of Excellence (2017), bajo la óptica del Derecho Internacional (DI), consideran a una ciber-operación como "el empleo de ciber capacidades para alcanzar objetivos en o través del ciberespacio" (p.564).

Este logro de objetivos es visto por Crowther (2017) mediante la habilitación de una operación (militar), o en su defecto siendo la operación en sí; sean éstas de tipo convencional o especiales, tal como se aprecia en la Figura 1.5. Finalmente, de acuerdo a sus efectos, estas ciber-operaciones

pueden orientarse a generar actividades propias de una ciber-explotación[3], ciber-sabotaje o de un ciberataque, siendo este último objeto del uso de una ciberarma.

Figura 1.5 Diagrama de relación entre el Ciberespacio y las Operaciones.
Fuente: Traducido de Crowther (2017).

1.1.4.4. Ciberataques.

Los ataques cibernéticos o ciberataques son considerados como "una ciber-operación, ya sea ofensiva o defensiva, que es razonablemente esperada para causar herida o muerte hacia personas o dañar o destruir objetos" (Schmitt y NATO Cooperative Cyber Defence Centre of Excellence, 2017, p. 415). Breedlove menciona que este inherente uso de la fuerza, puede llegar a tener consecuencias destructivas "tan devastadoras como las consecuencias de un ataque convencional..." (Caton, 2016, p. 10), por lo que tiende a considerarse su uso como parte de la capacidad de combate que puede desarrollar una fuerza armada.

Desde un punto de vista militar doctrinario, los ciberataques crean notables efectos de denegación en el ciberespacio o de manipulación que conlleva a efectos de denegación en los dominios físicos (U.S. Joint Chiefs of Staff, 2018). Se incluyen en éstas:

a. Denegación. Para prevenir el acceso a, operación de, o disponibilidad de la funcionalidad de un objetivo en un nivel específico para un tiempo específico, por:
   1. Degradación. - (...)
   2. Disrupción. - (...)

[3] Uso de acciones y operaciones para obtener información que de otro modo se mantendría confidencial y que es residente o está en tránsito a través de los sistemas computacionales o de redes del adversario (Lin, 2010).

3. Destrucción. - (...)

b. Manipulación. Como forma de ataque ciberespacial, controla o cambia información, sistemas de información y/o redes en ciberespacio rojo o gris para crear efectos físicos de denegación, usando decepción, señuelo, condicionamiento, *spoofing*[4], falsificación y otras técnicas similares. (U.S. Joint Chiefs of Staff, 2018, pp. II-7)

Las ciber-operaciones y el uso de sus medios armados, como son las ciberarmas, al tener un carácter ofensivo o de respuesta frente a una acción ofensiva, tienen una actuación orientada hacia la red adversaria y no la propia. Tanto la doctrina militar estadounidense como la china expresan el concepto de Ataque Ciberespacial (U.S. Joint Chiefs of Staff, 2018) y de Ataque de Redes de Computadores (Pollpeter, 2015) respectivamente como conceptos comunes cuyos fines son la interferencia o destrucción; coincidiendo ambos también en la trascendencia que tienen los SIM como son los Sistemas de Comando y Control y/o C4ISR en las fuerzas.

1.2. Relación conceptual.

Los siguientes párrafos expondrán la relación de las vulnerabilidades de día cero con los elementos antes desarrollados, esto con el fin de construir el entorno de la pregunta de investigación.

1.2.1. *Vulnerabilidad día 0 – SIM.*

Los Sistemas de Información Militar (SIM) representan el activo militar que se encuentra vulnerable frente a una posible detonación de una vulnerabilidad tecnológica desconocida. Las estrategias con respecto a la obtención de estas vulnerabilidades, dependerán de la manera como es que estos sistemas son adquiridos o desarrollados. La relación de las vulnerabilidades de día cero con el modo de detonación técnica en estos sistemas se encuentra resumido en la Figura 1.6, y de la cual se procederá a desglosar conceptos:

[4] Hacerse pasar por un recurso legítimo o usuario para ganar un acceso no autorizado en un sistema de información o para hacer que parezca que alguna otra organización o individuo inicie o emprenda cierta ciber actividad (Schmitt y NATO Cooperative Cyber Defence Centre of Excellence, 2017).

Figura 1.6 Modelo de vulnerabilidades en Sistemas de Información – Enfoque técnico.
Fuente: Elaboración propia basado en Jabbour y Devendorf, (2017); Lin, H. (2010); *U.S. Government Accountability Office.* (2018).

- Seguridad por tipo de código fuente: La relación de seguridad por código fuente abierto, cerrado o mixto, es un elemento técnico fundamental con respecto a la orientación del adversario frente a la detonación de este tipo de vulnerabilidades. Tanto la seguridad por código abierto como cerrado presentan su fortaleza en la publicación o no de éste; su utilidad dependerá del enfoque se tenga con respecto al beneficio de su auditoría por una comunidad de especialistas o caso contrario, de la aparente inexistencia del sistema. Independientemente de su elección, es muy improbable un desarrollo totalmente independiente, puesto que se dependerá directa o indirectamente de otras plataformas o sistemas de operación por parte de otros actores o sistemas tecnológicos para la creación de un SIM.

- Vulnerabilidades accidentales o deliberadas: Lin (2010) expresa que las vulnerabilidades en sistemas pueden ocurrir por causas accidentales o deliberadas. Para el primer caso, si bien no es factible garantizar un producto invulnerable, gran parte de las causas de esta situación radican en la adquisición o desarrollo de un producto no acreditado o validado que permita mitigar el riesgo de detonación. Para el segundo, existe el riesgo de la implementación deliberada de vulnerabilidades por presión de factores externos a la organización que los produce o de actores que interactúan en su entrega.

- Aproximación: Las aristas de aproximación hacia el SIM son dos, físicas (p.ej. conexiones ethernet, interfases de entrada y salida, etc.) o a través del espectro electromagnético (p. ej. redes WiFi, bluetooth, etc.). De dichas aristas devienen estrategias como es el aislamiento de sistemas, cuya efectividad se ha estado viendo reducida por acciones no cibernéticas como son las operaciones *HUMINT* (inteligencia humana), análisis de espectros como *TEMPEST*, etc.
- Interacción humana: Orientada a la activación (deliberadas o no) de vulnerabilidades, está basada en la cadena de proveedores y suministros, y en aquellos actores que realizan su configuración, así como el usuario final. El primero en base al diseño, producción, entrega y modificación del sistema, el segundo a través de una mala *praxis* al emitir alguna acción que devenga en la habilitación de la detonación de una vulnerabilidad (p.ej. un puerto abierto que permita la detonación de una vulnerabilidad), y el último en base a una interacción que pueda ser necesaria para la detonación de una vulnerabilidad.
- Vectores de detonación indirecta: Las vulnerabilidades de especificación hacen mención a que, por requerimiento de diseño, el sistema pueda ser vulnerable; mientras que las de arquitectura hacen referencia a un comprometimiento externo al sistema de información que permita su acceso a este (Jabbour y Devendorf, 2017). Con relación a esto último, los diversos canales de acceso e interacciones (propios de un sistema complejo y multifuncional) con otros sistemas permiten viabilizar vectores de ataque en los cuales el analista de seguridad no puede responder adecuadamente por responsabilidades externas.
- Vectores de detonación directa: Hardware, software y firmware vulnerable de acuerdo a características intrínsecas que las vulnerabilidades pueden conllevar.

Es necesaria una evaluación de riesgo que permita considerar todos estos axiomas con respecto a la amenaza que representa un Estado-Nación adversario en el contexto de un CAI. Conforme los SIM se vayan integrando al ciberespacio, éstos van a ser más propensos a su comprometimiento ya sea como parte de la Preparación Operacional del Campo de Batalla Ciberespacial (*Operational Preparation of the Cyber Battlefield*), como actividad de reconocimiento o vigilancia de un potencial adversario en tiempo de paz (Kehler, Lin, y Sulmeyer, 2017), a través de la denominada ciber-explotación o bien para el desarrollo de ciberataques en el mismo escenario propuesto.

De igual forma, dado el tiempo que toma la identificación de vulnerabilidades aprovechables y la generación de sus respectivos *exploits*; así como el alto dinamismo que tienen los CAI o incluso los *short-war,* es muy probable que el potencial adversario este desarrollando o adquiriendo vulnerabilidades desconocidas o *exploits* de *zero-day* para los sistemas de información identificados de la fuerza propia.

Finalmente, la interacción o conexión de los SIM con sistemas ciber-físicos incrementa el riesgo de daño ante una eventual manipulación de estos, como puede ser un uso no autorizado de un sistema de armas al cual se tenga acceso desde el SIM.

1.2.2. *Vulnerabilidad día 0 – Ciberarmas.*

Las ciberarmas para representar su éxito dependen en gran medida de la efectivad del código con el cual es posible vulnerar al SIM. El contar con código de detonación de una vulnerabilidad no conocida en el SIM adversario incrementa, dependiendo del tipo de *exploit* y la interacción que tiene éste con el entorno, significativamente la probabilidad de intrusión. La particularidad que estas tienen radica en su forma de desarrollo, obtención o adquisición por parte del adversario y la incertidumbre con respecto a los efectos de su empleo.

Se ha identificado que las ciberarmas que explotan vulnerabilidades de día cero afectan a los SIM de tres formas:

1. Daño directo físico-material correspondiente al SIM a través de la variación de sus rangos de trabajo.
2. Daño indirecto producto de la manipulación de la información o, a través de la disponibilidad o la negación de su uso, lo que influye al Comandante afectado en la toma de decisiones para la ejecución de órdenes en el teatro de operaciones y en la confianza sobre el SIM.
3. Daño indirecto físico a través del comprometimiento conexo de sistemas ciber-físicos.

El uso de estas ciberarmas depende mucho del actor que los explota y el objetivo trazado; dado al alto valor que significa su obtención y uso, y considerando la volatilidad que conlleva su inutilidad frente a su descubrimiento, dichos elementos tenderán a ser explotados racionadamente. China (Pollpeter, 2015), hace referencia a la capacidad armamentística que tiene el ciberespacio,

bajo el concepto de bala de plata o *assassin mace*, es decir bajo un uso único y en un escenario de guerra muy particular.

El uso o despliegue de las ciberarmas podrá realizarse previamente al inicio del conflicto o durante éste, existiendo el riesgo de detección de la detonación de la vulnerabilidad; puesto como se mencionó previamente, esta acción puede ser detectada bajo métodos reactivos, dependiendo en gran medida de los controles impuestos en el sistema y alrededor de éste.

Aún no se puede conocer el efecto final de este tipo de ciberarmas puesto que no se ha podido materializar su uso en las operaciones militares dentro de un CAI; de igual forma, mucho dependerá del efecto final deseado por el Comandante que las despliega y no por el que recibe dicho ataque.

Si bien hardware militar como aviones, barcos y tanques pueden tener una vida útil de más de 30 años, el cambio tecnológico computacional de un SIM es totalmente opuesto. Su dinámica, hace que un *exploit* que vulneraba un sistema de hace 30 años muy probablemente ya no se utilice o dicha vulnerabilidad ya haya sido descubierta y parcheada. Esto a razón del actual dinamismo que tienen los sistemas computacionales basado en su evolución tecnológica y economía en el mantenimiento, lo que representa su constante migración hacia productos actuales con soporte vigente.

La anterior situación demuestra el incierto tiempo de vida y funcionalidad que pueden tener estas ciberarmas. Otra problemática con respecto a su relación radica en las pruebas sobre la utilidad o efectividad que tienen éstas sobre sus objetivos, pues dependerán en algunos casos de la capacidad para simular la infraestructura o hacer un polígono del mismo. En este caso, simular un ataque a un sistema COTS o GOTS no ciber-físico no debería de tener mucha complejidad, esto al poder ser adquirido u obtenido relativamente fácil; mientras que sistemas ciber-físicos (p. ej. una planta de propulsión automatizada, una centrifugadora de uranio, etc.) si requerirán de una investigación más amplia y una puesta en escena de infraestructura, lo que incrementan tiempos de preparación para la ejecución de una operación.

Como se expuso anteriormente, existe la dicotomía en cuanto usar el *payload* de la ciberarma para infligir algún tipo de daño o en su defecto aprovechar las capacidades subrepticias de la ciber-explotación para poder tomar ventaja sobre el teatro de operaciones. La divergencia que hay entre

el área de las operaciones y la inteligencia es que impactan inversamente una con la otra en cuanto a sus capacidades.

1.2.3. *Vulnerabilidad día 0 – Ciber-operaciones.*

Las vulnerabilidades de día cero serán detonadas en un CAI a través del ejercicio de operaciones ciberespaciales por parte de una fuerza armada hostil. Los cuatro vectores de ataque anteriormente mostrados permiten identificar dos medios de aproximación: remoto y cercano, dos modos de activación de la detonación: con interacción y sin interacción, y dos arquitecturas posibles de sistema de información: aislado y conectado hacia otras redes.

Externamente, la proyección de una ciber-operación militar ofensiva hacia la fuerza propia se verá evidenciada por el auspicio del Estado-Nación adversario a través de su fuerza armada mediante sus miembros, o por actores no militares como habitantes en territorio ocupado que hacen parte de *levée masse*, actores civiles y mercenarios (Schmitt, 2017). Dicha interacción, sin importar los medios tecnológicos tendrá una parte responsable final humana perteneciente o articulable por una organización militar o gubernamental beligerante. La participación puede o no contar con la pública atribución o patrocinio de ésta, lo cual es una característica muy particular de estos medios de guerra.

El proceso de detonación puede incluir o contar con el apoyo, entre otros, de operaciones de inteligencia para la inserción de vulnerabilidades. La complejidad y naturaleza de las operaciones abocan a que el concepto de Preparación Operacional del Campo de Batalla Ciberespacial haga que la acción del comprometimiento del activo pueda suceder antes del CAI. Esto significaría que, en condiciones ideales, el activo debería encontrase comprometido previo a las operaciones militares, a la espera de la ejecución del *payload* que permita hacer uso efectivo del uso de la fuerza.

Por Figura 1.7 se presenta una esquematización sobre el modelamiento de una ciber-operación en la cual se considera el despliegue de una ciberarma que explote una vulnerabilidad de día cero.

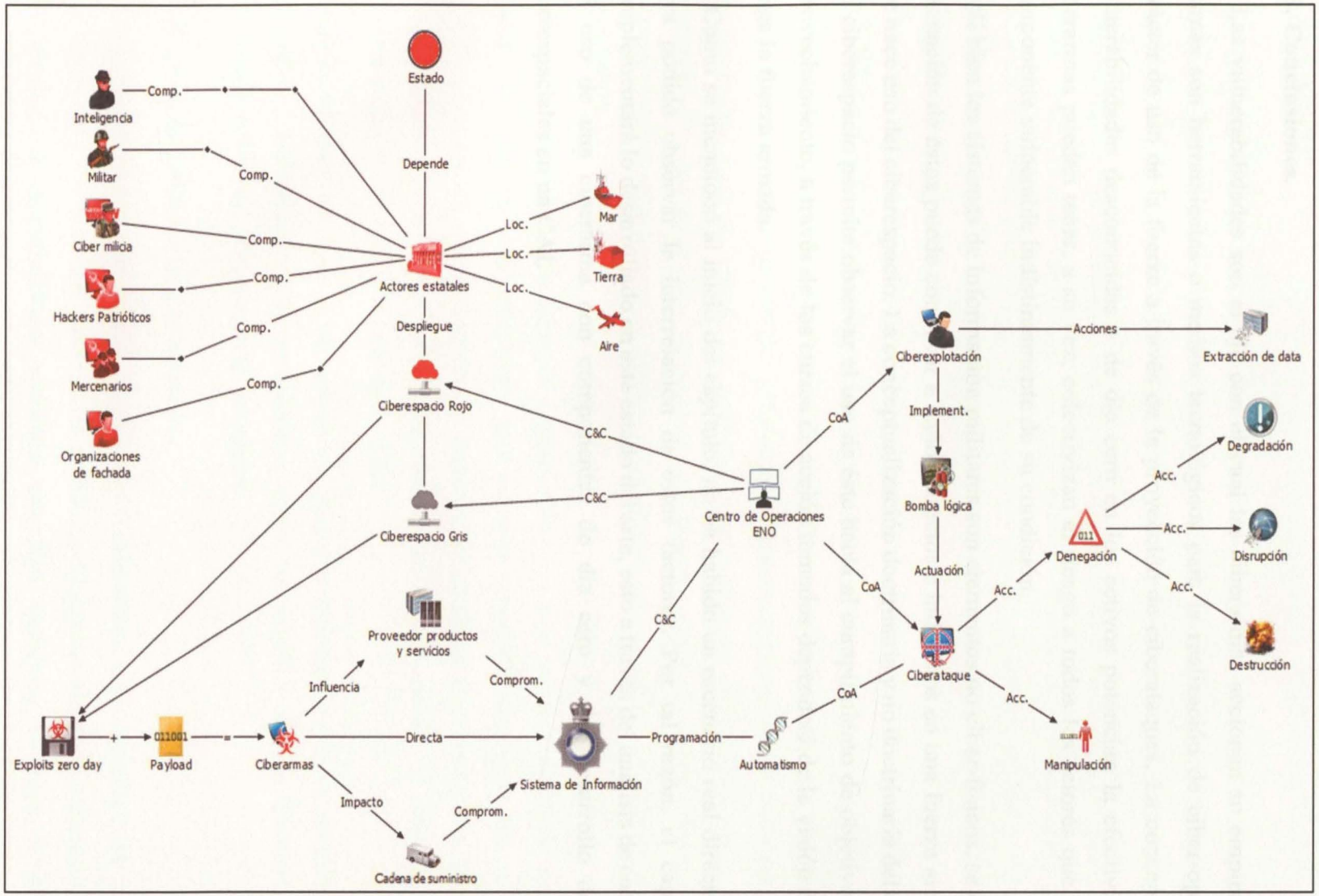

Figura 1.7 Diagrama de uso y detonación de vulnerabilidades de día cero en el contexto militar.

Acc.: Acción. CoA: Curso de Acción. C&C: Comando y Control. Comprom.: Comprometimiento. Comp.: Componente. Loc.: Localización. Implement.: Implementación.

Fuente: Elaboración del autor basado en Schmitt, M. y NATO Cooperative Cyber Defence Centre of Excellence, (2017); U.S. Joint Chiefs of Staff (2018); Lin (2010); Ablon y Bogart (2017).

1.3. Conclusiones.

Las vulnerabilidades son el eje con el cual las ciberarmas accionan su empleabilidad; estas últimas son herramientas o medios tecnológicos para la realización de ciber-operaciones con carácter de uso de la fuerza a través de la proyección de ciberataques. La conceptualización de vulnerabilidades desconocidas o de día cero en los activos potencian la efectividad que estas ciberarmas puedan tener, a su vez, colectivizan el riesgo a todos los actores que hacen uso del componente vulnerable indistintamente de su condición.

Si bien los sistemas de información militares son elementos no ciber-físicos, se observa que la detonación de éstos puede conllevar a daños directos e indirectos en una fuerza armada moderna que hace uso del ciberespacio. La conceptualización doctrinaria y no doctrinaria del empleo militar del ciberespacio permite observar el uso de éste hacia al cumplimiento de objetivos militares, su aprovechamiento, a través de los cursos de acción tomados dependerá de la visión doctrinaria que tenga la fuerza armada.

Como se mencionó al inicio del capítulo, no ha habido un escenario real directo en el cual se haya podido observar la interrelación de estos factores. Por tal razón, el capítulo entrante complementará lo desarrollado en este estado del arte, esto a través del análisis de casuísticas reales del uso de una ciberarma con componentes de día cero y del desarrollo de operaciones ciberespaciales en un CAI.

2. Capítulo II

En este capítulo se analizan dos casos, uno en el que se evidencia la proyección de un ciberataque que detona una vulnerabilidad de día cero y otro en el que se evidencian acciones ofensivas en el ciberespacio en un contexto de Conflicto Armado Internacional (CAI).

Para la realización de estos análisis, se presentan marcos de referencia (*frameworks)* aplicables al objeto de estudio; se seleccionan dos y se aplica el análisis correspondiente, presentándose al término conclusiones. El resultado de dicho procedimiento, al tratarse de casos reales, será insumo complementario para la composición del marco de referencia correspondiente al proceso asociativo del Capítulo III de esta monografía.

2.1. Casos.

No hay un escenario real histórico en el cual se pueda apreciar todos los factores componentes de la pregunta de investigación de "¿Cómo las ciberarmas que explotan vulnerabilidades de día cero (*zero-day*) podrían afectar los sistemas de información militares en un conflicto armado internacional?". Por tal motivo, como fuentes de soporte empírico, se han seleccionado dos casos o hechos históricos (únicos en su tipo) independientes pero complementarios para la formulación del problema.

El primero, la Operación *Olympic Games* o Stuxnet cuyo objeto de estudio serán los efectos causales del uso de una ciberarma que explota vulnerabilidades de día cero hacia una infraestructura crítica gubernamental. El segundo, el conflicto ruso-georgiano, bajo el objeto de las actividades u operaciones ciberespaciales desarrolladas previas al despliegue de fuerzas militares y durante éste en el marco de un CAI.

Ambos escenarios, cuyos responsables son muy probablemente actores estatales, responden a un nivel de sofisticación sin precedentes, como en aspecto técnico Stuxnet y de efectos coordinados militares, la guerra ruso-georgiana.

2.2. Marcos de Referencia y su selección.

La implementación de marcos de referencia orientados a la seguridad de la información, ciberseguridad y sus variantes, han venido siendo medios metodológicos y de estandarización que han permitido a organizaciones gestionar este tipo seguridad en base al conocimiento y

experiencias adquiridas. Con respecto a esto, Donaldson, Siegel, Williams, y Aslam (2015) enumeran 13 tipos principales de marcos.

Fuera de estos alcances, hay una limitada cantidad de marcos de referencia orientados a hacer un análisis sobre un incidente cibernético (o conjunto de éstos) de orientación académica que vaya más allá del aspecto organizacional y del cumplimiento de estándares. De acuerdo a los ejemplos anteriormente mostrados por Crowther en la Figura 1.5, es posible determinar que esta limitante evaluativa estratégica irá disminuyendo conforme siga incrementándose el uso que vienen dando los Estados a las herramientas cibernéticas como articuladores de intereses nacionales.

Considerando lo antes expresado, se identificaron y evaluaron marcos que permitan la aplicabilidad bajo un esquema de análisis *post mortem* de hechos sucedidos como son:

1. La *Cyber Kill Chain* desarrollada por Lockheed Martin (2018), como modelo de 7 pasos para el entendimiento de las tácticas, técnicas y procedimientos del adversario en el ámbito ciberespacial bajo la base del concepto militar *kill-chain*,
2. La modificación propuesta (de la *Cyber Kill Chain*) por Rutherford y White (2018), en la que se incluye los conceptos de colección de inteligencia y de movimientos fluidos una vez hecha la detonación,
3. El *PrEP: A Framework for Malware & Cyber Weapons* de Herr (2014), el cual propone un marco de referencia para la clasificación de malware y ciberarmas bajo 3 componentes,
4. El *System-Fault-Risk Framework for cyber attack classification* de Ye, Newman y Farley (2005), que provee un marco de referencia basado en la ingeniería de sistemas, la modelización de fallas y las teorías de evaluación de riesgos,
5. El *Cyber Conceptual Framework for Developing Military Doctrine* de Ormrod y Turnbull (2016), cuyo diseño se encuentra orientado al debate y análisis de ciber-conflictos para el desarrollo de doctrina, bajo el análisis de los efectos en cascada que representa un ciberataque, y
6. El *General Theoretical Framework* de Nacita y Reith, M. (2018), el cual brinda herramientas sobre cómo abordar ciber-amenazas específicas hacia la seguridad

nacional, esto mediante la aplicación de 6 preguntas orientadas a entender cualquier estrategia usada de manera anticipada al uso de fuerzas militares.

Si bien todos estos marcos cuentan con soporte académico sólido para poder efectuar análisis, sólo estos dos últimos tienen elementos adaptables únicos a la perspectiva investigativa de este trabajo de grado como es:

1. Un enfoque estratégico que permite centralizar el análisis en las consecuencias de las acciones ciberespaciales, permitiendo desarrollar procesos analíticos no parametrizados en ámbitos técnicos u organizacionales sino de nivel Estado-Nación.
2. Una aplicación del proceso analítico bajo un lenguaje y enfoque militar propio de autores pertenecientes al sector defensa y de revistas académicas provenientes de centros de educación superior militar, como el *Joint Services Command and Staff College* (Reino Unido) y la *Air University* (EEUU) respectivamente.
3. Una adaptabilidad del caso Stuxnet al *Cyber Conceptual Framework for Developing Military Doctrine* en razón de que el mencionado marco toma como eje el análisis de un ciberataque específico (como fue Stuxnet), permitiendo la medición de efectos, componentes, así como la escalabilidad y/o desarrollo de cadena de causalidad que éste genera a nivel país. La información actualmente disponible sobre esta ciberarma permite aplicar análisis en cada nivel y componente del referido marco, lo que permitirá mostrar el dimensionamiento que representa el uso de uno de estos artefactos bajo un escenario real.
4. Una adaptabilidad del escenario de guerra ruso-georgiano en el *General Theoretical Framework*, en razón a que en dicho conflicto hubo múltiples acciones ciberespaciales hacia diversos objetivos, por lo que es requerido un análisis interpretativo de la estrategia ciberespacial usada por parte de la fuerza militar beligerante. Dicho marco permite extensivamente hacer el análisis de dichas acciones ciberespaciales bajo la estrategia anticipatoria previa al uso de fuerzas militares.
5. Ninguno de estos marcos ha sido aplicado en los casos propuestos.

2.3. Primer Caso: Evidencia de uso de una ciberarma con componentes de día cero.

Stuxnet es el nombre de un malware de tipo gusano dado de manera no oficial por la combinación de nombres de archivos *.stub* y *MrxNet.sys* encontrados dentro del código fuente (Zetter, 2011). Debido a su diseño, funcionalidad y efectos creados, se estima que su intención fue, al menos, sabotear subrepticiamente las centrifugadoras de enriquecimiento de uranio de una planta nuclear iraní en Natanz. Esto era realizado a través de una reprogramación de los sistemas de control de las centrifugadoras (modelo P-1) hasta ocasionar un desgaste que de como resultado su inhabilitación.

Como malware, se calcula que tuvo una vida operacional desde noviembre de 2005 hasta junio de 2012, fecha en la cual se detuvieron las infecciones (McDonald, O Murchu, Doherty y Chien, 2013). Oficialmente no hay un responsable de la creación del mismo ni los daños que haya podido causar. La atribución propuesta por Sanger (2012), es que dicho elemento formaba parte de una operación llamada *Olympic Games,* en la que intervinieron, por lo menos, Estados Unidos e Israel.

Para efectos del análisis se tomará como punto de partida, los hechos sucedidos tanto en la referida planta como en el análisis superficial técnico del malware en mención. Adicionalmente, se tomará como supuesto el que Irán estuviese en la búsqueda activa de una capacidad armamentística nuclear, esto a través del enriquecimiento de uranio en la referida planta, como sugirió la Agencia Internacional de Energía Atómica (Heinrich y Holland, 2010).

Se aplicará el *Cyber Conceptual Framework Cyber-Attack Causal Chain* (Marco Cibernético Conceptual Cadena Causal de Ciberataque) presentado por Ormrod y Turnbull (2016) para el presente análisis; el antes mencionado está dividido en un marco conceptual de efectos y en uno de componentes.

2.3.1. *Marco conceptual de efectos de Ciberataque.*

Stuxnet fue un malware que tuvo versiones que van desde 0.500 hasta la 1.x, las cuales se diferenciaban por su agresividad, el marco de desarrollo y el empleo de diferentes tácticas de ataque (McDonald, O Murchu, Doherty y Chien, 2013). Como objeto de la aplicación del marco de referencia en el estudio, se analizará la versión 1. debido a que ésta fue la que finalmente desencadenó efectos cinéticos en las centrifugadoras.

Esta versión a la que denominaremos Stuxnet, tuvo la particularidad de ser un malware compuesto por 4 *exploits* de día cero y 2 certificados digitales (válidos) dentro de su código como medios de detonación y propagación. Una de las hipótesis de cómo es que el malware llegó a insertarse en los mencionados sistemas fue a través de la puesta de un dispositivo de almacenamiento externo comprometido dentro de la planta, y otra a través del despliegue de parches comprometidos por parte del fabricante.

La Figura 2.1 permite resumir los niveles de efectos producto del ciberataque aplicado al caso propuesto y que a continuación se describen:

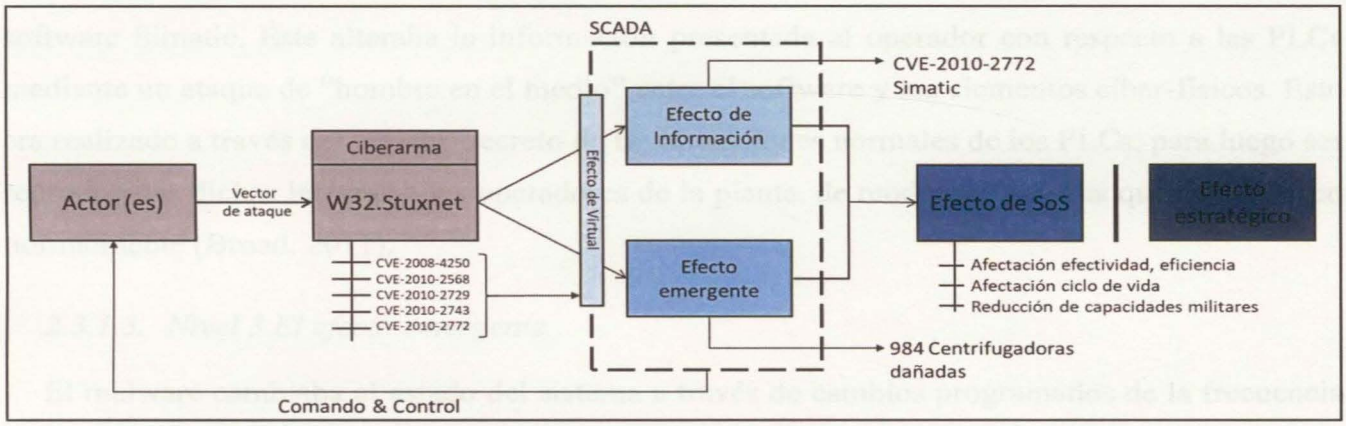

Figura 2.1 Diagrama de efectos Operación *Olympic Games*.
Fuente: Elaboración del autor basado en Ormrod y Turnbull (2016); Sood, Enbody y Loshin (2014); Broad (2011).

2.3.1.1. Nivel 1. El objeto de efecto virtual.

Hay comprometimiento en la confidencialidad, integridad y disponibilidad. Las vulnerabilidades específicas encontradas para la detonación de plataformas Windows en sus diferentes versiones fueron las CVE-2008-4250, CVE-2010-2568, CVE-2010-2729 y CVE-2010-2743 (Sood, Enbody y Loshin, 2014). De éstas cuatro, una (CVE-2010-2568) permitía la auto réplica a través de unidades extraíbles permitiendo una ejecución automática, dos (CVE-2008-4250 y CVE-2010-2729) estaban orientadas a la proliferación del malware en red local; y una cuarta (CVE-2010-2743) orientada a la obtención de privilegios locales. En el caso estuviese el software *Siemens Simatic WinCC Step7* (Simatic) en el host infectado, se detonaría una quinta vulnerabilidad (CVE-2010-2772), la cual permitiría sobrepasar la seguridad del software de gestión de los Controladores Lógicos Programables (PLC) de las centrifugadoras.

Con respecto a estas vulnerabilidades, la CVE-2010-2568 fue detonada anteriormente en el 2008 y la CVE-2010-2729 fue identificada en el 2009 por un magazine de seguridad (Falliere, O Murchu y Chien, 2011). En relación a la vulnerabilidad CVE-2010-2772, la clave de la base de datos estuvo publicada en un foro técnico de Siemens desde el 2008 (Zetter, 2010). A pesar de haber sido de conocimiento público dichas vulnerabilidades no se fabricó parche alguno por parte de los fabricantes hasta después del incidente con Stuxnet.

2.3.1.2. Nivel 2 El efecto de información.

Stuxnet tenía efectos en la información si en el host vulnerado se encontraba instalado el software Simatic. Éste alteraba la información presentada al operador con respecto a las PLCs mediante un ataque de "hombre en el medio" entre el software y los elementos ciber-físicos. Esto era realizado a través del registro secreto de las operaciones normales de los PLCs, para luego ser reproducidas dichas lecturas a los operadores de la planta, de modo que parezca que funcionasen normalmente (Broad, 2011).

2.3.1.3. Nivel 3 El efecto emergente.

El malware cambiaba el estado del sistema a través de cambios programados de la frecuencia de los convertidores, lo que incrementaba y reducía la velocidad de las centrifugadoras a fin de causar desgaste y daño. Dicha acción se complementaba subrepticiamente con los efectos informacionales expresados en el nivel precedente. Dichas acciones afectaban la toma de decisiones por parte del personal responsable con respecto a la gestión de las centrifugadoras.

2.3.1.4. Nivel 4. El efecto de Sistema de Sistemas (SoS).

Las acciones antes expuestas dieron como resultado efectos de diversa índole en la planta nuclear. Hubo una disrupción en el ciclo de vida de los componentes del sistema de enriquecimiento, esto ante el incremento del reemplazo de centrifugadoras debido al desgaste programado por el malware. Tanto la efectividad del sistema como su eficiencia se vieron afectadas por factores materiales y humanos.

Bajo el punto de vista material, de una base de 8700 centrifugadoras, que en condiciones normales se reemplazaban en promedio 800 por año (Zetter, 2011), Sanger (2012) expone que durante los meses del ciberataque cerca de 1000 centrifugadoras fueron puestas fuera de servicio,

mientras que Zetter (2011) entre 1000 a 2000. A nivel del recurso humano hubo despidos por parte del personal de planta (Sanger, 2012), lo que desencadenó en una pérdida de confianza con respecto al profesionalismo del personal participante.

En cuanto a la manifestación de estos sucesos en el Dominio Militar, dicho acontecimiento impactó la capacidad de Irán en cuanto al desarrollo de armas nucleares.

2.3.1.5. Nivel 5. El efecto estratégico.

El impacto a nivel nacional en cuanto a los mencionados eventos depende del punto de vista de los actores interactuantes, como es el país afectado, los posibles agresores y los organismos internacionales relacionados al evento. Bajo el presente marco de referencia se considera que no hubo impacto relacional en el ámbito estratégico. El país no se encontraba en un conflicto armado o realizando operaciones de combate. Al ser limitado el número de centrifugadoras dañadas y el rol que cumplía la planta, no se considera una afectación a funciones cívicas críticas, ni tampoco una afectación a la competitividad en el mercado global.

2.3.2. *Componentes del ciberataque.*[5]

2.3.2.1. Causalidad.

Los niveles interactúan desde el nivel 1 hasta el nivel 4. Todos los mencionados producen más de un efecto. La multiplicidad de las vulnerabilidades explotadas permitió al malware crear efectos en los niveles 2 y 3. Los resultantes del nivel 3 fueron observados en el nivel 4.

2.3.2.2. Intención.

No es posible determinar cuál fue el objetivo estratégico del iniciador al no haber un reconocimiento oficial del actor o actores que proyectaron dicho ciberataque. Una de las principales interrogantes es determinar el grado de sabotaje intencionado. Al considerarse que el mencionado malware formó parte de una operación (*Olympic Games*), es posible proyectar en el largo plazo una desclasificación del mismo y, por consiguiente, el conocimiento del objetivo u objetivos trazados.

---

[5] Provee un mecanismo para la identificación de un ciberataque y la metodología para medir su severidad (Ormrod y Turnbull, 2016).

Efectos inmediatos al término de operaciones de Stuxnet: A nivel técnico se determinó que el malware estuvo diseñado para sabotear una planta de enriquecimiento de uranio de características iguales a la de Natanz. A nivel político: El presidente iraní, Mahmoud Ahmadinejad, reconoció que el malware inhabilitó un limitado número de centrifugadoras (Anónimo, 2010). La Secretaria de Estado, Hillary Clinton, y el jefe saliente del Mossad, Meir Dagan, declararon de manera separada que creían que los esfuerzos iraníes se habían retrasado varios años (Broad, 2011).

Efectos posteriores al malware: Hubo acciones no cibernéticas orientadas a interrumpir el proceso de enriquecimiento de uranio, como sanciones económicas impuestas a Irán y la intensificación de atentados contra científicos participantes del programa nuclear. El escenario expuesto por Sanger (2018) da a entender que *Olympic Games* era solo una parte de un plan mayor denominado *Nitro Zeus*, por lo que la intención final es difusa.

Desenlace adverso al intencionado. - A inicios de febrero de 2011 Irán habría estado redoblando sus esfuerzos de enriquecimiento de uranio a través de la modernización de sus instalaciones nucleares (WSJ: Iran Redoubling Efforts To Enrich Uranium By Installing Faster Centrifuges - Diplomats, 2011). El ministro de relaciones exteriores iraní Mohammad Javad (Sanger, 2018), dijo a la contraparte estadounidense en Viena que "Al final, ¿qué lograron tus ingenieros? Nos hicieron más determinados que nunca a construir y construir más" (p.42). Es muy probable que los efectos finales intencionados con el ciberataque, tomando en consideración la cantidad de recursos utilizados para tal fin, no fueran los estimados. Esta situación permite validar lo expuesto por Nacita y Reith (2018), con respecto que el uso de poder cibernético tiene efectos difíciles de predecir.

Desenlace intencionado. – Después de estas acciones, Irán terminó negociando un acuerdo nuclear en el año 2015 a través del *Joint Comprehensive Plan of Action*. Israel fue crítico y opositor al mencionado acuerdo. Estados Unidos si bien fue firmante de éste, terminó retirándose en mayo de 2018.

2.3.2.3. Nivel de daño.

El nivel de daño fue superior al efecto informacional, lo que se considera como un ciberataque según los autores del marco de referencia. No se ha registrado lesión o muerte a personas, mientras que el daño material más acertado corresponde a 984 máquinas centrifugadoras reemplazadas

(Broad, 2011). Sanger (2018) conserva la óptica de que *Olympic Games* fue una operación liderada por una agencia de inteligencia diseñada para forzar a Irán a negociar.

2.3.2.4. Evento.

Se ocasionaron cambios en el comportamiento del sistema lo que resultó en daño físico. El efecto emergente de nivel 3 antes expuesto conlleva a la consideración de que se ejecutó un ciberataque.

2.3.3. *Reflexiones.*

Los efectos cascada del marco de referencia aplicado llegaron al nivel de Sistema de Sistemas (SoS) mediante el daño controlado y generalizado a sistemas ciber-físicos y las capacidades conexas que esto conlleva. La identificación del malware y las posteriores acciones de remediación, permitieron la continuación de las actividades de enriquecimiento de uranio.

Caso contrario es lo observado por operaciones militares de bombardeo hacia unas aparentes plantas nucleares en construcción en Siria (Operación Huerto - 2007) y en Iraq (Operación Ópera - 1981), cuyos efectos destructivos generalizados coadyuvaron a la negación de aspiraciones nucleares por parte de los países afectados.

El concepto de ciberataque que se concluye bajo el análisis del caso expuesto se ajusta a la concepción anteriormente dada en el Capítulo I. La interpretación de uso de malware como ciberarma y el efecto alcanzado por ésta permite determinar que el ciberataque fue exitoso. Los efectos finales deseados por parte del atacante, así como el grado de participación de actores no estatales en dicho proceso son aún inciertos.

2.4. Segundo Caso: Acciones ofensivas en el ciberespacio en un contexto de CAI.

La denominada "Guerra ruso-georgiana" fue un CAI entre los países de Georgia y Rusia, y con la interacción de las autoproclamadas repúblicas de Osetia del Sur y Abkhazia. Este CAI de intervenciones militares a gran escala, tuvo lugar entre el 7 y 12 de agosto de 2008, y tiene la particularidad de ser única en su tipo, ya que contempló la presencia de incidentes cibernéticos precedentes a la campaña militar (Maness y Valeriano, 2016).

Al haber sido negada responsabilidad alguna de estos incidentes por parte de Rusia (Interfax, 2013) y, ante lo trascendente que fueron las acciones ciberespaciales ocurridas en contra de

Georgia en el contexto militar, el análisis se realizará bajo el supuesto de que Rusia haya tenido responsabilidad de estas operaciones cibernéticas.

Se aplicará para el análisis de los eventos ciberespaciales ocurridos las preguntas expuestas en el *General Theoretical Framework* presentado por Nacita y Reith (2018), esto bajo una perspectiva rusa. Se responderán dichas preguntas en base a los hechos registrados a fin de dar un entendimiento de la estrategia adoptada y los cursos de acción desplegados.

El estudio no centrará su análisis bajo las doctrinas y tanques de pensamiento actuales rusos, sino en la concepción más próxima que se tenía del ciberespacio y la guerra como tal al momento del desarrollo de las operaciones, esto a razón de que hubo reformas militares profundas (Bryce-Rogers, 2013) debido a las deficiencias operacionales y organizacionales rusas en ese conflicto (Connell y Vogler, 2017).

2.4.1. *Análisis ciberespacial.*

Rusia conceptualiza al ciberespacio como un elemento informacional (Connell y Vogler, 2017). La aplicación bélica de ésta última (guerra de información) en tiempo de guerra radica en alcanzar la superioridad o dominancia de la información sobre el enemigo, ganando y manteniendo una ventaja informacional, pero a su vez protegiendo la propia (Heickero, 2010).

Las operaciones ciberespaciales sucedidas tuvieron la particularidad de no explotar todo el potencial cibernético, ser ejecutadas (en parte) por actores no militares y funcionar como marco de prueba sobre los efectos del ciberespacio en las operaciones de información. La Figura 2.2 que a continuación se muestra expone una guía introductoria diagramada del análisis a ser desarrollado en los próximos párrafos.

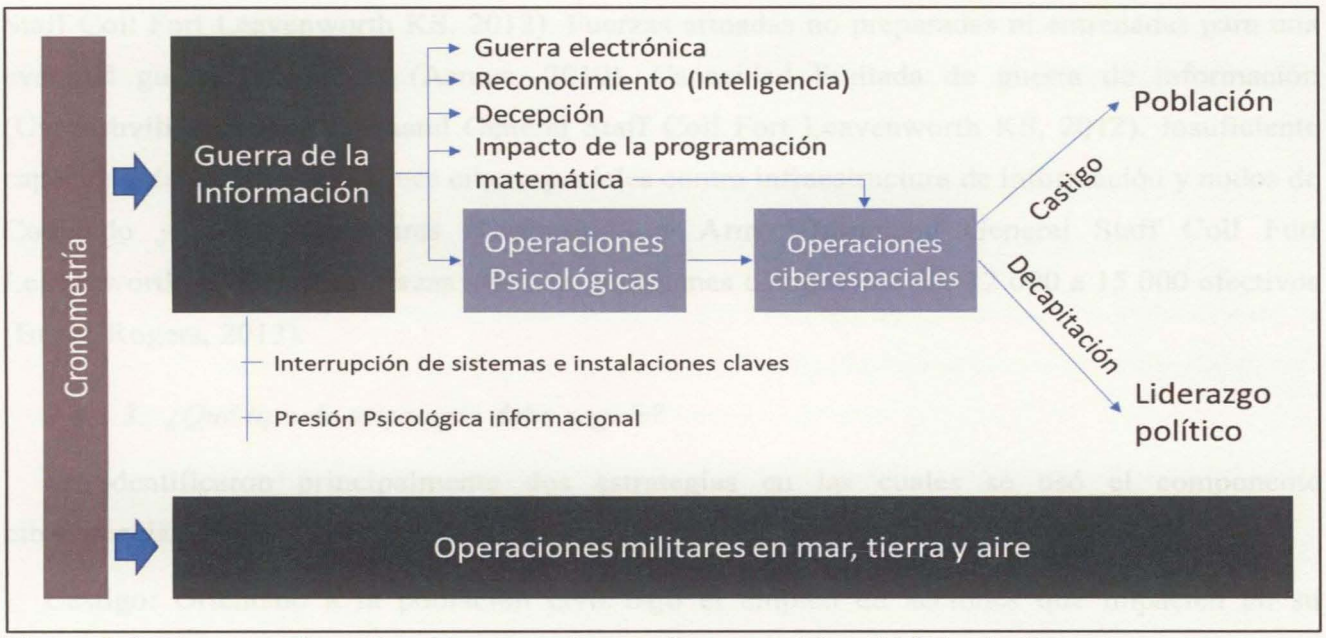

Figura 2.2 Diagrama de aplicación operaciones ciberespaciales CAI Rusia-Georgia.
Fuente: Elaboración del autor basado en Nacita y Reith (2018) ; Heickero (2010).

2.4.1.1. ¿Qué resultado estoy buscando?

En el ámbito ciberespacial, apoyar al cumplimiento de objetivos de la campaña militar a través de la realización y/o coordinación de operaciones ciberespaciales orientadas a obtener superioridad de la información. Evaluar el impacto de las acciones ciberespaciales efectuadas contra el adversario. Políticamente, mantener el *statu quo* de las repúblicas (parcialmente reconocidas) de Osetia del Sur y Abkhazia.

2.4.1.2. ¿Cuáles son mis capacidades político-militares específicas y las del adversario?

Rusia: Ejecución de acciones políticas para desestabilizar el gobierno georgiano (Asmus, 2010). Aplicación de tácticas militares basadas en doctrina militar del año 2000 (Sokov, 2007). Preparación ante una eventual guerra con Georgia (Bryce-Rogers, 2013). Guerra de información implementada en los niveles estratégicos, operacionales y tácticos (Limno y Krysanov, 2003). Ejecución de operaciones ofensivas en el ciberespacio por parte de la fuerza propia y a través de otros actores (personas, grupos, etc.). Negación de atribución. Fuerzas militares rusas y aliadas compuestas por 35 mil a 40 mil efectivos (Bryce-Rogers, 2013).

Georgia: Bajo liderazgo presidencial (Asmus, 2010). Aplicación de tácticas militares basadas en doctrina militar de las ex fuerzas armadas soviéticas (Usenashvili y Army Command General

Staff Coll Fort Leavenworth KS, 2012). Fuerzas armadas no preparadas ni entrenadas para una eventual guerra con Rusia (Asmus, 2010). Capacidad limitada de guerra de información (Usenashvili y Army Command General Staff Coll Fort Leavenworth KS, 2012). Insuficiente capacidad de defensa de ataques ciberespaciales contra infraestructura de información y nodos de Comando y Control militares (Usenashvili y Army Command General Staff Coll Fort Leavenworth KS, 2012). Fuerzas armadas georgianas compuestas por 12 000 a 15 000 efectivos (Bryce-Rogers, 2013).

2.4.1.3. ¿Qué tipo de estrategia debo seguir?

Se identificaron principalmente dos estrategias en las cuales se usó el componente ciberespacial, castigo y decapitación:

Castigo: Orientado a la población civil bajo el empleo de acciones que impacten en su psicología, esto a través de la generación de pánico y confusión (Hollis, 2011). Se dificultó la comunicación de ésta con las autoridades, y por ende la aplicación de respuestas efectivas por parte del gobierno georgiano. Se indispuso la figura de liderazgo (presidencial) en medios oficiales gubernamentales. Para tal fin se ejecutaron actividades disruptivas a sistemas de comunicaciones y servicios web relacionados a gobierno y finanzas, entre otros, y acciones de *defacement*[6] a servicios web, todo esto mediante vectores de detonación no sofisticados (DDoS, Sql Injection, etc.). Se preservó el acceso a servicios vitales sociales (agua, energía eléctrica, etc.) y no se proyectaron ciberataques o acciones cibernéticas que hayan causado muerte o daño material.

Decapitación: Aislamiento del liderazgo gubernamental georgiano (centro de gravedad) mediante la degradación de comunicación con la ciudadanía y la comunidad internacional. Se estima que un 35 % de las redes georgianas fueron incomunicadas durante los ataques (Kaska, Tikk y Vihul, 2010).

2.4.1.4. ¿Qué blancos u objetivos son los más importantes?

[6] Resultado de una detonación a un servidor web (usualmente) con el fin de modificar su contenido (Ruef, Shakarian y Shakarian, 2013).

Aspectos que deben ser atacados: sitios web que impacten en el modo que la población accede a la información sea gubernamental o privada, banca e internet. Industria de telecomunicaciones a través de los proveedores locales.

Estrategia genérica: indirecta a través de la denegación, degradación y disrupción de medios informacionales tecnológicos de uso de la sociedad civil y su interacción gubernamental.

Nivel de destrucción: ninguno que tenga como origen las acciones ciberespaciales, la orientación se basó en la interrupción de sistemas y presión psicológica, esto en base a acciones que no atenten contra la vida humana o daño material.

2.4.1.5. ¿Qué mecanismos espero que desencadene mi operación?

Confusión en masa por parte de la población (georgiana) que pueda coadyuvar al sentir de ineficacia del gobierno para poder defender la soberanía nacional. Disminución de la voluntad de lucha por parte del personal militar. Frustración del gobierno al no poder articular canales adecuados de comunicación interna y externa. Todas estas acciones en el ciberespacio fueron aparentemente habilitadoras para las fuerzas convencionales (Connell y Vogler, 2017), siendo éstas últimas las que finalmente permitieron obtener una victoria militar rusa frente a Georgia. Se descarta que un solo uso de operaciones ciberespaciales *per se* haya podido detener el avance georgiano a Osetia del Sur.

2.4.1.6. ¿Cómo debo cronometrar mis acciones?

Hubo acciones simultáneas de coordinación entre las operaciones ciberespaciales, alineadas con las operaciones de información, con las operaciones militares convencionales (previo al bombardeo aéreo a Gori se interrumpió el acceso de esa localidad a sitios web de gobierno y noticias). Hubo coordinación con actores no estatales como hackers patrióticos, milicia cibernética, grupo cibercriminales y demás, para la proyección de acciones cibernéticas hacia objetivos georgianos (p. ej. se habilitaron sitios web con instructivos para realizar incursiones cibernéticas y listados de objetivos cibernéticos georgianos). Dichas acciones permitieron negar atribución gubernamental, a pesar de estar relacionadas en tiempo con las operaciones militares aéreas y de tierra.

2.4.2. *Reflexiones.*

Se utilizó el ciberespacio como parte del esfuerzo bélico, mediante la ejecución de operaciones ciberespaciales de índole ofensivo en beneficio principalmente ruso. Las mencionadas acciones fueron en el contexto de una campaña militar hacia ciber infraestructura civil, como parte de la guerra informacional bajo la perspectiva rusa.

No se descartan actividades ciberespaciales en contra de objetivos cibernéticos militares georgianos, sobre todo los relacionados a sistemas de información, pues la falta de manifestación y evidencia es congruente con la reserva y naturaleza propia militar, caso contrario de los medios cibernéticos de uso social.

No hubo muertos ni daño material a causa de las actividades cibernéticas antes descritas, por lo que, a diferencia del caso anterior, estas operaciones de índice no violento no son consideradas como ciberataques. El no uso de todo el potencial ciberespacial hacia sistemas cibernéticos militares, de cual forman parte las ciberarmas que explotan vulnerabilidades de día cero, pudo ser a causa de no exponer tácticas, técnicas o procedimientos frente a adversarios de menor complejidad.

Se observó la ejecución de operaciones previas al despliegue de fuerzas como parte de la Preparación Operacional del Campo de Batalla Ciberespacial. Dicho espectro (ciberespacio) fue adaptado al cumplimiento de objetivos doctrinarios de tipo militar, esto mediante la aplicación de intrusiones a objetivos que representen centros de gravedad dentro del marco de operaciones psicológicas.

La participación de personal no militar como entes ejecutores de operaciones ciberespaciales fue una nueva variable en este tipo de conflictos. Dicha participación presenta nuevos retos relacionados a la anonimidad, el involucramiento de terceras partes y la exposición frente las acciones enemigas.

2.5. Conclusiones.

En ambos escenarios se ejecutaron operaciones ciberespaciales como un componente más dentro de las estrategias generales de cada actor, el primero tuvo como objeto un ciberataque, mientras que el segundo acciones orientadas a la guerra de la información. En estos dos casos, la disposición del poder ciberespacial por sí solo, distó de ser el único medio necesario para alcanzar

un objetivo estratégico de acción militar. La presencia de este si bien coadyuvó (o no) al cumplimiento del objetivo estratégico, su sola efectividad en una hipotética unilateralidad de uso tendría efectos muy limitados.

En el primer caso, el empleo del *payload* fue subrepticio, prolongado y delimitado tanto en daño como en amplitud de acciones, proveyendo efectos diluidos en tiempo hasta llegar al término de su ciclo de vida con su neutralización. Bajo esta experiencia, una aplicación más agresiva de la entrega de efectos de cadena causal, incluso de nivel 5 (del Marco Cibernético Conceptual Cadena Causal de Ciberataque), a otro tipo de infraestructura crítica es factible y alcanzable, pudiendo desencadenar incluso un conflicto armado.

El empleo operacional de una ciberarma como la de este tipo en un CAI requerirá de igual forma de recursos y trabajos previos para lograr sus efectos. Romper la barrera de acceso hacia este nivel puede significar años de preparación (dependiendo del o los sistemas), por lo que será una tendencia cada vez más marcada el despliegue subrepticio, en tiempo de paz, de malware que logre estos efectos en activos críticos militares y civiles como parte de la denominada preparación de campo de batalla y su activación en ciberarmas.

Para el segundo caso, si bien no hubo un ciberataque o el empleo de ciberarmas bajo la conceptualización determinada en el Capítulo I, hubo el empleo del ciberespacio dentro de la estrategia informacional armada rusa y la participación de actores no militares. Con respecto a esto último, la multidimensionalidad de estos actores interactuantes y coordinantes, tanto en la fase de preparación como ejecución de las ciber-operaciones, mostró una asimetría no antes observada con respecto a la participación de personal no militar en el contexto del CAI.

Las operaciones ciberespaciales rusas antes expuestas, demostraron que no se requiere tener una connotación de alta sofisticación técnica para poder ser efectivas, de igual forma, para efectos funcionales no requirieron de un componente específicamente militar para ser adaptadas o ejecutadas.

En ambos casos, el pragmatismo que representa el innato anonimato del ciberespacio se ve reducido por el contexto en el cual las operaciones son ejecutadas, lo que permite atribuir un responsable directo tácito beneficiario frente a éstas.

A diferencia de las operaciones militares convencionales, cada curso de acción ciberespacial tomado expone a detalle métodos y medios al adversario y terceras partes. El uso de ciberarmas, como Stuxnet, y los recursos empleados para su creación, trajo consigo la reducción del arsenal militar ciberespacial y herramientas de colección de inteligencia cibernética disponibles por parte del Estado-Nación responsable. Los cursos de acción tomados contra Georgia generan la ampliación de la visión doctrinaria de protección de los activos ciberespaciales nacionales en un CAI.

Finalmente, la inherentemente característica de "un solo uso" que representan las ciberarmas obliga un prudente despliegue de las mismas, dicha acción fue expuesta por el accionar ruso y su decisión de no utilizar este tipo de elementos sofisticados frente a un adversario en desigualdad de condiciones o de no imperativa necesidad operacional.

3. Capítulo III

El presente capítulo tiene por finalidad asociar el concepto de ciberarmas con componente de día cero y su uso contra sistemas de información en el contexto bélico internacional. Para tal fin, se presentará un marco de referencia que permita denotar esta asociación mediante la representación de este potencial uso en el contexto propuesto, presentándose al término un ejemplo de su aplicación y reflexiones sobre el mismo. Se utilizó como insumo los conceptos relacionados a los cuatro componentes de estudio y el análisis de los casos anteriormente vistos.

3.1. Marco de referencia.

Se exponen dos escenarios, uno sobre la esquematización del uso de una ciberarma y otro relacionado a los componentes que permiten describir un escenario de ésta a través del marco de referencia como tal.

3.1.1. *Esquematización de uso.*

Es iniciado por la determinación y/o elección del SIM objetivo en correlación directa a su valoración como objetivo militar, siendo esto realizado idealmente previo al escenario de un CAI. El objeto de dicho proceso corresponde al posterior desarrollo o adquisición de vulnerabilidades de día cero que permitan su detonación con una mayor tasa de éxito en comparación a otros cursos de acción.

El despliegue del *exploit* de *zero-day* y su configuración como una herramienta de ciber-explotación, así como de su potencialidad como ciberarma, radican en la forma en que éste es entregado hacia el objetivo y el *payload* que tenga o permita obtener. Estas acciones corresponden (y en algunos casos se entrelazan) a las capacidades de inteligencia y las operaciones militares *per se*. La cronología de dichos actos es variable y dependen de la catalogación de la amenaza extranjera que se tenga, Sánchez (2013) mide esta última en función de las variables de capacidad y voluntad. De igual manera, todo este proceso puede ser realizado en pleno CAI o idealmente, previamente a éste, durante el estado de agresión, crisis o anteriores, los cuales conforma parte del proceso de Preparación Operacional del Campo de Batalla Ciberespacial (POCBC).

La configuración final obtenida de todo este proceso como ciberarma será generar el efecto final deseado de violencia, como se aprecia por Figura 3.1.

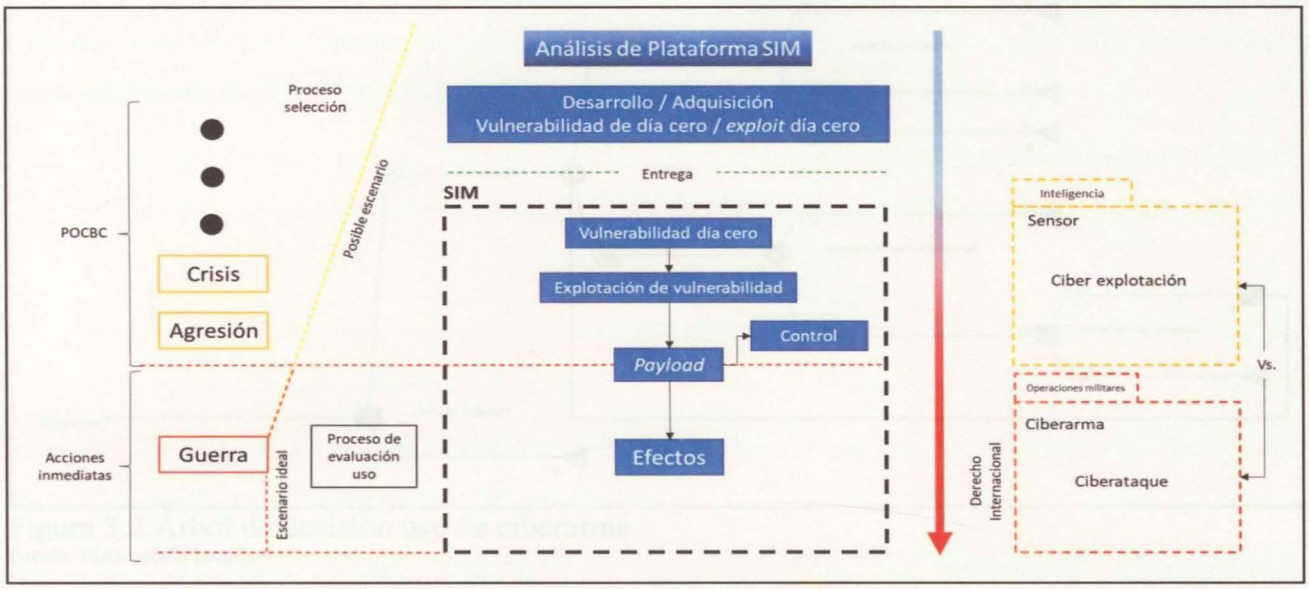

Figura 3.1 Esquema uso ciberarma.
Elaboración propia.

El despliegue de esta ciberarma contará por tanto con dos elementos de tiempo, uno en el cual previamente se vulnera el SIM y otro en el que desarrolla la entrega de efectos; sólo cuando el empleo de efectos es realizado y permita cuantificar un impacto en daño, sea directo o indirecto, será posible determinar la aplicación de una ciberarma, y por ende el desencadenamiento de un ciberataque bajo el uso de la fuerza.

El proceso de evaluación de uso dependerá de la capacidad técnica de la misma con respecto a los efectos que pueda tener y las autorizaciones de uso en razón de las reglas de enfrentamiento. La valoración de los cursos de acción a tomar con el mencionado despliegue corresponderá a las estimaciones de los factores probabilísticos de éxito y la afectación del poder combativo de la fuerza adversaria o al incremento de la propia. Dicho proceso se ve expuesto en el árbol de decisión presentado en la Figura 3.2, en donde el factor probabilístico del azar es expuesto en porcentajes (%) y el impacto del valor del poder combativo en un factor numérico (positivo o negativo) acorde a las fórmulas internas de cada fuerza para dicho cálculo.

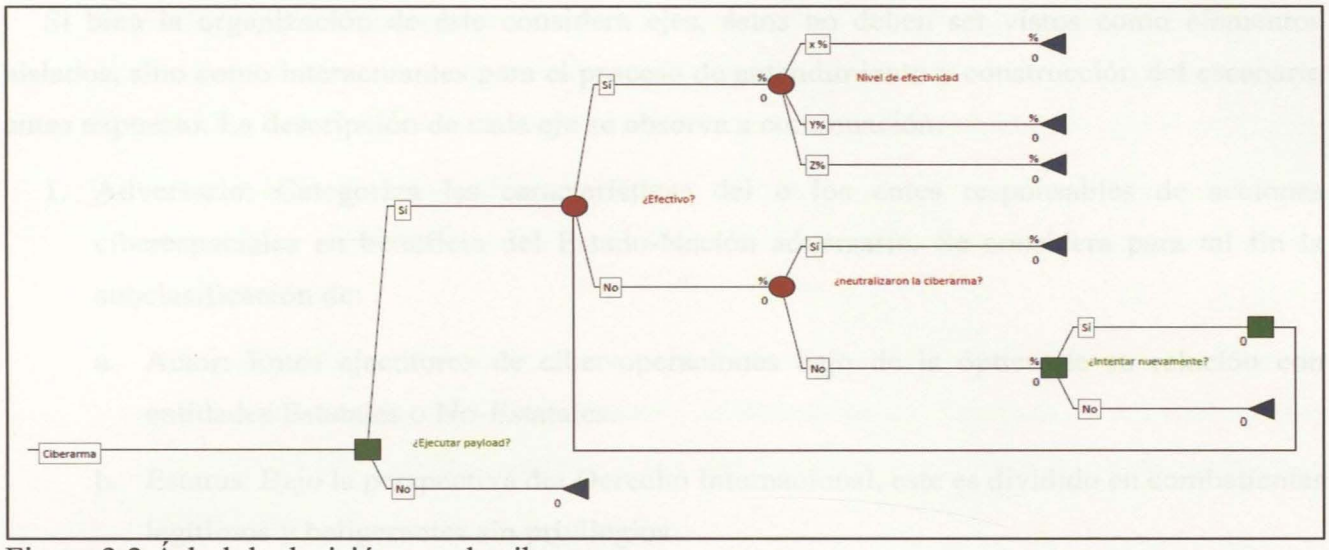

Figura 3.2 Árbol de decisión uso de ciberarma.
Fuente: Elaboración propia.

3.1.2. *Composición.*

Este marco, cuyo objeto es describir el escenario objeto del problema, se divide en 4 ejes interrelacionados, cuyo resumen del mismo se observa a través de la siguiente matriz (Figura 3.3).

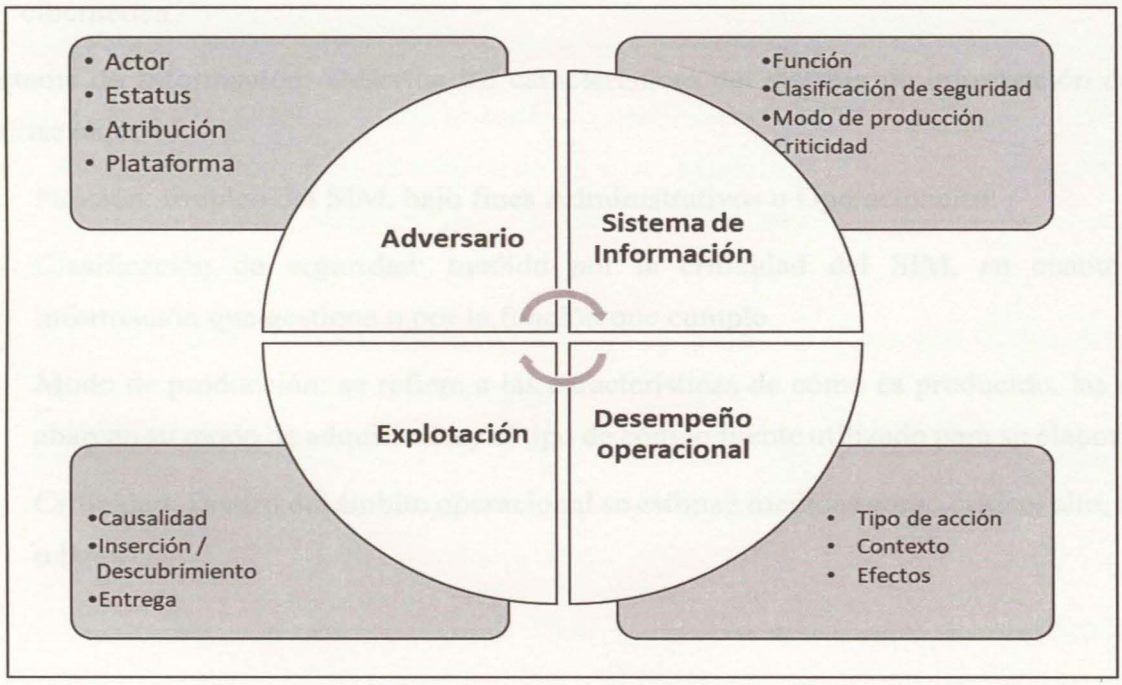

Figura 3.3 Matriz "Ciberarmas que detonan vulnerabilidades de día cero en Sistemas de Información Militar en un Conflicto Armado Internacional".
Elaboración propia.

Si bien la organización de éste considera ejes, éstos no deben ser vistos como elementos aislados, sino como interactuantes para el proceso de entendimiento y construcción del escenario antes expuesto. La descripción de cada eje se observa a continuación:

1. Adversario: Categoriza las características del o los entes responsables de acciones ciberespaciales en beneficio del Estado-Nación adversario. Se considera para tal fin la subclasificación de:
    a. Actor: Entes ejecutores de ciber-operaciones bajo de la óptica de su relación con entidades Estatales o No-Estatales.
    b. Estatus: Bajo la perspectiva del Derecho Internacional, este es dividido en combatientes legítimos y beligerantes sin privilegios.
    c. Atribución: Como capacidad de responsabilizar las actividades ciberespaciales ejecutadas, se divide en atribuible (origen Infraestructura Cibernética Adversaria) y no atribuible (proveniente de Ciberespacio Gris[7])
    d. Plataforma: Elemento físico del cual es geográficamente es proyectada la operación cibernética.
2. Sistema de Información: Describe las características del sistema de información de tipo militar objetivo.
    a. Función: Empleo del SIM, bajo fines Administrativos u Operacionales.
    b. Clasificación de seguridad: medido por la criticidad del SIM, en cuanto a la información que gestiona o por la función que cumple.
    c. Modo de producción: se refiere a las características de cómo es producido, las cuales abarcan su modo de adquisición y el tipo de código fuente utilizado para su elaboración.
    d. Criticidad: Dentro del ámbito operacional se estiman medidas como crítico, alto, medio o bajo.

[7] Aquel que no corresponde al ciberespacio propio ni del enemigo (U.S. Joint Chiefs of Staff, 2018).

3. Modalidad de detonación: Expone las características del proceso de detonación de la ciberarma, considera características básicas de la vulnerabilidad bajo el contexto de su detonación, la detonación *per se* y el modo en que ejecuta instrucciones.
    a. Causalidad de detonación: Considera el motivo de las acciones que activan la ciberarma, se divide en causales deliberadas y no deliberadas, bajo contextos internos y externos.
    b. Inserción / Descubrimiento: Considera escenarios en los cuales las vulnerabilidades fueron insertadas y bajo qué escenario. El descubrimiento se basa en el conocimiento de la vulnerabilidad desconocida, si fue esta descubierta internamente o adquirida hacia un externo.
    c. Entrega: Considera la manera en cuanto la ciberarma es desplegada, contempla aspectos de aproximación (directa o indirecta), vectores de ataque utilizados, el elemento de aproximación, el tipo de detonación tecnológica y la forma de activación.
    d. Funcionamiento: Por medio del tipo de funcionamiento, esta puede operar autónomamente a través de la programación de instrucciones previas al despliegue o, recibir éstas a través de un enlace de comunicación directo o indirecto con el adversario.
4. Desempeño operacional: describe el contexto operacional del despliegue de la ciberarma. Se parte del hecho de que, al ser una ciberarma, se encuentran acciones relacionadas al uso de la fuerza o a un ciberataque *per se*, y no otras actividades ciberespaciales conexas como guerra de información o inteligencia.
    a. Tipo de acción: Accionar del adversario en razón de un Ofensiva o Contraofensiva a una acción realizada por la fuerza propia.
    b. Contexto: Busca identificar si la operación tiene relación con otras operaciones militares convencionales en su conjunto o es una acción aislada previa al conflicto o durante este.
    c. Efectos: Estos pueden ser bajo el nivel de efectos alcanzados de la ciberarma, el impacto del *payload* (sea directo o indirecto) y por las consecuencias finales expuestas en factores humanos y materiales.

La extensión de los diferentes elementos y configuraciones que componen estos ejes se encuentra expuestos en el marco de referencia que se presenta por Anexo. Esta última considera una base general de los conceptos descriptivos relevantes para la composición de cualquier situación que permita representar el potencial uso de este tipo de ciberarmas en el contexto propuesto, independientemente del medio y técnica usada.

La interdependencia, demostración y composición de estos podrá ser apreciada a través de un caso de uso propuesto en párrafo siguiente.

3.2 Ejemplo de uso.

Se plantea la detonación de un hipotético sistema de C4I[8] en una unidad naval que conlleve a consecuencias de fratricidio. La finalidad de este ejemplo, será exponer de manera práctica y concisa dicha situación mediante el marco de referencia propuesto y sus componentes de uso. La trascendencia que tiene este tipo de sistema de información (C4I) en una fuerza armada permitirá exponer uno de los escenarios más dañinos y extremos que tiene el empleo de una ciberarma que detone una vulnerabilidad de día 0 de un SIM en un CAI

3.2.1. *Caso: Ciberataque a Sistema de C4I.*

El país A se encuentra en conflicto armado con el país B. El país B proyectó un ciberataque al país A por medio de una ciberarma. La presentación de la catalogación de dichas acciones es expuesta por el siguiente cuadro (Figura 3.4):

1. Adversario: País A

1.1. **Actor**: Estatal miembro de una Fuerza Armada: Cibercomando.
1.2. **Estatus:** Combatientes legítimos.
1.3. **Atribución:** No atribuible.
1.4. **Plataforma:** Tierra.

2. Sistema de Información: C4I

2.1. **Función:** Operacional
2.2. **Clasificación de seguridad:** Secreto
2.3. **Modo de producción:** Producto de mercado adquirido como Mil COTS para el software de aplicación; COTS para el hardware, firmware y sistema operativo. Tipo de código mixto.

[8] Comando, Control, Comunicaciones, Computación e Inteligencia.

2.4. **Criticidad:** Alta

3. Modalidad de detonación

3.1. **Causalidad de denotación:** No deliberada, un usuario final del sistema ejecutó un archivo no autorizado.

3.2. **Inserción / Descubrimiento:** Se tiene conocimiento de la venta de dicha vulnerabilidad por empresa investigadora externa.

3.3. **Entrega:**

Aproximación: Directa. - Hacia los componentes del SIM

Vector de Ataque: Red

Elemento de aproximación: Conexiones físicas

Tipo de detonación tecnológica: Software

Activación: Con interacción humana

3.4. **Funcionamiento:** Enlace de comunicación con adversario directo a través de canales de comunicación IP.

4. Desempeño operacional

4.1. **Tipo de acción:** Ofensiva

4.2. **Contexto:** Acción como parte del desarrollo de operaciones militares.

4.3. **Efectos:**

Nivel alcanzado: SoS, se generaron blancos erróneos al reprogramar como enemigo un contacto naval de la propia fuerza.

Impacto del *Payload:* Indirecto. - Afectación de la integridad de la información del SIM. Influencia en la toma de decisiones y desconfianza en el SIM. Se indujo a acciones ofensivas hacia la fuerza propia.

Consecuencias: Pérdida de una unidad de combate por medio de su destrucción y la posterior muerte y lesión de un aún indeterminado número de combatientes. Inoperancia del SIM.

Figura 3.4 Ejemplo de uso de marco de referencia con relación al uso de ciberarmas con componente de día cero en un conflicto armado internacional.

3.2.2. *Reflexiones.*

El ejemplo antes expuesto demostró la aplicabilidad del marco de referencia en la representación del caso propuesto, permitiendo el entendimiento de las aristas que abarcan el uso de estas ciberarmas bajo una conceptualización estratégica de escenarios tanto hipotéticos como reales. Esto a través de la capacidad de construcción de cualquier escenario que se desee simular, transmitir o explicar con respecto al uso armado de este tipo de vulnerabilidades de día cero y su correlación con los conceptos interactuantes de sistemas de información, ciberarmas y ciber-operaciones, propios de la pregunta de investigación.

De igual forma es posible ampliar significativamente su aplicabilidad a otros escenarios operacionales a través de la implementación de los campos "tipo de vulnerabilidad" (conocida, desconocida) y "tipo de operación" (guerra de información, colección de inteligencia, etc.) en el marco de referencia propuesto en el Anexo. Esto último permite complementar significativamente el espectro de opciones disponibles para la ejecución de operaciones en el ciberespacio, aumentando el alcance de este trabajo académico en el campo militar.

Finalmente, se estima un uso potencial de este marco como herramienta para el desarrollo de modelos aplicables a la gestión de riesgo y para el proceso de planeamiento de operaciones ciberespaciales. El primero, en cuanto al aporte del conocimiento sobre la detonación de vulnerabilidades de día cero, el cual debido a la extrema complejidad que radican sus componentes ha venido teniendo una muy limitada contextualización en el teatro de operaciones para las fuerzas y sus escenarios de riesgos frente amenazas de mayor sofisticación como son los Estados-Nación.

Para el segundo, el planeamiento, como proceso deliberado del balance de opciones, medios y riesgos para alcanzar estados finales deseados (U.S. Joint Chiefs of Staff, 2017), requiere de elementos paramétricos para el diseño de operaciones militares en el ámbito ciberespacial. El marco de referencia provee de herramientas e insumos base para dicho proceso coadyuvando tanto al planeamiento como la ejecución de operaciones de este tipo.

4. Conclusiones y trabajo futuro

4.1. Conclusiones.

La demostrada complejidad que viene teniendo la protección de sistemas informáticos radica en el cambio de paradigma que significan las vulnerabilidades no conocidas, su tratamiento subrepticio en *exploits* y su posterior detonación en activos y sistemas propios de una organización. La actual confianza en tecnología, tanto adquirida como desarrollada, así como la dependencia externa que se viene teniendo de ésta, ha venido dejando de lado el reconocimiento de cuán vulnerable realmente es y la problemática que representa una multi vectorial defensa frente aquello que es desconocido.

Las ciberarmas y su proyección más dramática realizada por los Estados-Nación, han permitido mostrar el verdadero dimensionamiento de esta situación, muchas veces también limitado por el secretismo que representa este tipo de arsenal y la actual orientación que vienen teniendo estudios y soluciones tecnológicas hacia amenazas de menor proporción como la ciberdelincuencia y la congruente proyección de intrusiones menos sofisticadas.

El marco de referencia propuesto, contribuye a disminuir esta problemática, al poder representar óptimamente el potencial uso que tienen las ciberarmas que explotan vulnerabilidades de día cero hacia sistemas de información militares en un Conflicto Armado Internacional. Lo anterior, a su vez, responde la pregunta de investigación y da cumplimiento al objetivo general de la presente monografía, ambos expuestos en la introducción.

Dicho entregable, presentado en el Capítulo III y detallado por Anexo (numeral 6), es de igual manera una contribución cognitiva frente a la escasez de marcos y hechos históricos fuente relacionados al potencial uso que tienen las ciberarmas con estas características. De igual manera, se suple en parte la necesidad estratégica de presentar un estudio académico sobre un escenario bélico en particular y de común proyección bajo una orientación no-técnica de aplicabilidad militar. Esto permitirá brindar una guía neutral de conocimiento de la amenaza que representan las vulnerabilidades de día cero en el contexto antes dado y como parte de su proyección en ámbitos operacionales frente a actores estatales.

Como se mencionó en la introducción, la motivación principal de esta investigación es exponer al tomador de decisión el conocimiento sobre esta problemática frente a la limitada concienciación

que se viene teniendo con respecto a la adquisición y uso de tecnología. Estas acciones han permitido colateralmente, exponer lo vulnerable que puede llegar a ser el uso de tecnología ciberespacial que cumple una función vital en una fuerza, como es la gestión de la información en el desarrollo de operaciones militares y lo compleja que significaría su protección.

El escogimiento del sistema objetivo, en este caso un Sistema de Información, no debe significar una limitante frente al alcance o proyección del estudio. Es factible adaptar la aplicación del marco a cualquier otro tipo de sistema informático o tipo de ciber-operación, así como a las necesidades propias de cada organización que enfrente retos similares.

El intrínseco dinamismo, propio del avance y uso de la cibernética tanto en aplicaciones militares como civiles, traerá como consecuencia la necesidad de modificaciones del marco de referencia. La implementación de nuevos estudios complementarios basados en nuevos sucesos y progresos tecnológicos serán necesarios para mantener su actual vigencia.

De igual forma, la sola consideración de este marco permitirá la implementación de controles organizacionales que posiblemente no era dilucidados anteriormente, habilitando el desarrollo de cada de eje de manera granular de acuerdo a requerimientos propios de las instituciones.

4.2. Trabajo futuro.

La capacidad de producir un sistema invulnerable en todas sus instancias y dependencias es al momento inalcanzable. De igual manera, la presente monografía de grado no tiene como finalidad el brindar modelos de protección frente a este tipo de ciberarmas. Trabajos futuros podrían considerar la utilización de este marco como herramienta base para el desarrollo de modelos de riesgos cuantitativos frente a este tipo de acciones particularmente exclusivas a un Estado-Nación y ser aplicables a las infraestructuras críticas nacionales, así como de su de viniente tratamiento como parte del proceso de la gestión de riesgos.

Otros futuros trabajos podrán centrarse en el desarrollo de herramientas de simulación que permitan proyectar o validar procedimientos de respuesta frente a la conjunción de los elementos expuestos, o en el desarrollo del proceso del planeamiento operacional militar en el ámbito ciberespacial, así como, en la evaluación de posibles cursos de acción a ser tomados en el proceso de ejecución de ciber-operaciones que engloben los elementos del referido marco.

5. Referencias bibliográficas

Ablon, L., & Bogart, T. (2017). *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits.* Santa Mónica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1751.htm

Anónimo. (2010). International: Yet to turn; The Stuxnet worm. *The Economist*, p. n/a.

Asmus, R. (2010). *A little war that shook the world : Georgia, Russia, and the future of the West* (First ed.). New York: Palgrave Macmillan.

Boothby, B. (2016). Cyber weapons. In K. Friis, & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 165-174). London; New York: Routledge, Taylor & Francis Group.

Borghard, E., & Lonergan, S. (10 de Septiembre de 2018). *What Do the Trump Administration's Changes to PPD-20 Mean for U.S. Offensive Cyber Operations?* Obtenido de Council on Foreign Relations: https://www.cfr.org/blog/what-do-trump-administrations-changes-ppd-20-mean-us-offensive-cyber-operations

Broad, W. (2011, Enero 15). Israel Tests on Worm Called Crucial in Iran Nuclear Delay. *The New York Times*, pp. 1-8.

Bryce-Rogers, A. (2013). Russian Military Reform in the Aftermath of the 2008 Russia-Georgia War. *Demokratizatsiya, 21*(3), 339-368.

Caton, J. (2016). *NATO cyberspace capability : A strategic and operational evolution.* Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press.

Comité Internacional de la Cruz Roja. (2008, Marzo). *Cuál es la definición de "conflicto armado" según el derecho internacional humanitario?* Retrieved from https://www.icrc.org/spa/assets/files/other/opinion-paper-armed-conflict-es.pdf

Connell, M., & Vogler, S. (2017, Marzo). *Russia's Approach to Cyber Warfare.* Retrieved from CNA: https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf

Creery, M. (2018, Diciembre 5). *Russia Strategic Understanding of Cyber: Not an Information War – A War on Information*. Retrieved from Georgetown Security Studies Review: http://georgetownsecuritystudiesreview.org/2018/12/05/russia-strategic-understanding-of-cyber-not-an-information-war-a-war-on-information/#_edn8

Crowdfense. (2019). *Bug bounty program*. Retrieved from https://www.crowdfense.com/bug-bounty-program.html

Crowther, G. (2017). The Cyber Domain. *The Cyber Defense Review, 2*(3), 63-78.

Defense Science Board. (2013, Enero). *Task Force Report: "Resilient Military Systems and the Advanced Cyber Threat.* Retrieved from Defense Technical Information Center: https://apps.dtic.mil/dtic/tr/fulltext/u2/a569975.pdf

Department of Defense. (2010, Noviembre). *Department of Defense Dictionary of Military and Associated Terms.* Retrieved from Homeland Security Digital Library: https://www.hsdl.org/?view&did=11391

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2015). *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats.* Berkeley, CA: Apress.

Falliere, N., O Murchu, L., & Chien, E. (2011, Febrero). *W32.Stuxnet Dossier, version 1.4.* Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-w32-stuxnet-dossier-11-en.pdf

First. (2019). *Common Vulnerability Scoring System Version 3.0 Calculator*. Retrieved from https://www.first.org/cvss/calculator/3.0 /

Friedman, A., & Singer, P. (2014). *Cybersecurity and cyberwar : What everyone needs to know.* New York, NY: Oxford University Press.

Heickero, R. (2010, Marzo). *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations.* Retrieved from http://www.highseclabs.com/data/foir2970.pdf

Heinrich, M., & Holland, S. (2010, Febrero 18). *IAEA fears Iran working now on nuclear warhead* . Retrieved from https://www.reuters.com/article/us-nuclear-iran-iaea/iaea-fears-iran-working-now-on-nuclear-warhead-idUSTRE61H4EH20100218

Herr, T. (2014). Prep: A framework for malware and cyber weapons. *Journal of Information Warfare, 13*(1), 87-106.

Herzog, M., & Schmid, J. (2016). Who pays for zero-days? In K. Friis, & J. Ringsmose (Eds.), *Conflict in cyber space: Theoretical, strategic and legal perspectives* (pp. 99-115). London; New York: Routledge, Taylor & Francis Group.

Hollis, D. (2011, Enero 6). *Cyberwar Case Study: Georgia 2008.* Retrieved from Small Wars Journal: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf

Institute of Education Sciences. (2019). *Military Information Systems Technology*. Retrieved from National Center for Education Statistics: https://nces.ed.gov/ipeds/cipcode/cipdetail.aspx?y=55&cipid=89486

Interfax. (2013, Mayo 30). *Russian Foreign Ministry denies cyber-attacks on Georgia during South Ossetian conflict.* Retrieved from Newswire, Interfax: Russia & CIS Military: http://ezp-prod1.hul.harvard.edu/login?url=http://search.ebscohost.com/login.a

Jabbour, T., & Devendorf, E. (2017). Cyber Threat Characterization. *The Cyber Defense Review, 2*(3), 79-93.

Joint Technical Committee ISO/IEC JTC 1/SC 27 IT Security techniques. (2018). *ISO/IEC 27000:2018(E), Information technology — Security techniques — Information security*

management systems — Overview and vocabulary. Geneva, Switzerland: International Organization for Standardization.

Kaska, K., Tikk, E., & Vihul, L. (2010). *International Cyber Incidents: Legal Considerations.* Retrieved from Cooperative Cyber Defence Centre of Excellence (CCD COE): https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Kaur, R., & Singh, M. (2014). Efficient hybrid technique for detecting zero-day polymorphic worms. *2014 IEEE International Advance Computing Conference (IACC)*, (pp. 95-100). Haryana, India.

Kehler, R., Lin, H., & Sulmeyer, M. (2017). Rules of Engagement for Cyberspace Operations: A View from the United States. *Journal of Cybersecurity, 3*(1), 1-30.

Leonhard, W. (2017, Mayo 16). *Shadow Brokers threaten to release even more NSA-sourced malware.* Retrieved from Computerworld: https://www.computerworld.com/article/3196836/shadow-brokers-threaten-to-release-even-more-nsa-sourced-malware.html

Libicki, M., Ablon, L., & Webb, T. (2015). *The defender's dilemma : Charting a course toward cybersecurity.* Santa Monica, Calif: RAND Corporation. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1024/RAND_RR1024.pdf

Limno, A., & Krysanov, M. (2003). Information warfare and camouflage, concealment and deception. *Military Thought, 12*(2), 181-185.

Lin, H. (2010). Offensive cyber operations and the use of force. *Journal of National Security Law & Policy, 4*(1), 63-86.

Lin, H. (2012). Operational Considerations in Cyber Attack and Cyber Exploitation. In D. Reveron (Ed.), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (pp. 37-56). Washington, DC: Georgetown University Press.

Lin, H. (2016). Attribution of malicious cyber incidents: from soup to nuts. *Journal of International Affairs, 70*(1), 75-137.

Lockheed Martin. (2018). *The Cyber Kill Chain®.* Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lyn, K. (2015, Agosto). Classification of and resilience to cyber-attacks on cyber-physical systems. USA. Retrieved from https://smartech.gatech.edu/bitstream/handle/1853/53926/LYN-THESIS-2015.pdf?sequence=1&isAllowed=y

Maness, R., & Valeriano, B. (2016). Cyber spillover conflicts. In K. Friss, & J. Ringsmose (Eds.), *Conflict in Cyber Space : Theoretical, Strategic and Legal Pespectives* (pp. 45-64). London: Routledge.

McDonald, G., O Murchu, L., Doherty, S., & Chien, E. (2013, Febrero 26). *Stuxnet 0.5: The Missing Link, version 1.0.* Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf

Ministerio de Defensa. (2010, Mayo 21). *Manual de Derecho Internacional Humanitario y Derechos Humanos para las Fuerzas Armadas.* Retrieved from https://www.mindef.gob.pe/informacion/documentos/manual_ddhh_ffaa_2010.pdf

Nacita, I., & Reith, M. (2018). Cyber War and Deterrence: Applying a General Theoretical Framework. *Air & Space Power Journal, 32*(2), 74-83.

National Institute of Standards and Technology. (2019). *CVSS Severity Distribution Over Time.* Retrieved from National Vulnerability Database: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time

Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies, 16*(3), 270-298.

Özkan, S. (2019, Abril 1). *Current CVSS Score Distribution For All Vulnerabilities*. Retrieved from https://www.cvedetails.com

Pollpeter, K. (2015). Chinese Writings on Cyberwarfare and Coercion. In J. Lindsay, T. Cheung, & D. Reveron, *China and cybersecurity : Espionage, strategy, and politics in the digital domain* (pp. 138-162). New York: Oxford University Press.

Ruef, A., Shakarian, J., & Shakarian, P. (2013). *Introduction to cyber-warfare : A multidisciplinary approach.* Waltham, MA: Syngress.

Rutherford, J., & White, G. (2018). Cyber Kill Chain Model Needs A Makeover. *Signal, 72*(6), 41-42.

Sánchez, H. (2013). *En la mente de los estrategas ¿Conoce usted su curva de rendimiento estratégico?* Bogotá: Escuela Superior de Guerra.

Sanger, D. (2012, Junio 1). Obama Order Sped Up Wave Of Cyberattacks Against Iran. *New York Times (1923-Current File)*, p. A1.

Sanger, D. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age* (First ed.). New York : Crown, an imprint of the Crown Publishing Group.

Schmitt, M. & NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (Second ed.). Cambridge, United Kingdom: Cambridge University Press.

Schmitt, M. (2017). Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. *Harvard National Security Journal, 8*, 239-282.

Schneier, B. (2018). *Click here to kill everybody : Security and survival in a hyper-connected world* (First ed.). New York: W.W. Norton & Company.

Secretaría de Seguridad y Defensa Nacional. (2015). *Doctrina de Seguridad y Defensa Nacional.* Lima.

Slade, R. (2006). *Dictionary of information security.* Rockland, MA: Syngress.

Sokov, N. (2007). The origins of and prospects for Russian nuclear doctrine. *The Nonproliferation Review, 14*(2), 207-226.

Sood, A., Enbody, R., & Loshin, P. (2014). *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware.* Waltham, Massachusetts: Syngress.

Thomas, T. (2014). Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies, 27* (1), 101-130.

U.S. Government Accountability Office. (2018, Octubre). *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities.* Retrieved from https://www.gao.gov/assets/700/694913.pdf

U.S. Joint Chiefs of Staff. (2017, Junio 16). *Joint Planning Joint Publication 5-0.* Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf

U.S. Joint Chiefs of Staff. (2018, June 8). *Cyberspace Operations Joint Publication 3-12.* Retrieved from Joint Chiefs of Staff: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

Usenashvili, D. & Army Command General Staff Coll Fort Leavenworth KS. (2012). A Strategic Capability Review of the Georgian Armed Forces.

WSJ: Iran Redoubling Efforts To Enrich Uranium By Installing Faster Centrifuges - Diplomats. (2011, Febrero 18). *Dow Jones Institutional News*. Retrieved from http://search.proquest.com.ezp-prod1.hul.harvard.edu/docview/2157831713?accountid=11311

Ye, N., Newman, C., & Farley, T. (2005). A System-Fault-Risk Framework for cyber attack classification. *Information, Knowledge, Systems Management, 5* (2), 135-151.

Zerodium. (2019). *Our Exploit Acquisition Program*. Retrieved from https://zerodium.com/program.html

Zetter, K. (2010). *SCADA System's Hard-Coded Password Circulated Online for Years*. Retrieved from https://www.wired.com/2010/07/siemens-scada/

Zetter, K. (2011). *How digital detectives deciphered Stuxnet, the most menacing malware in history*. Retrieved from https://arstechnica.com/tech-policy/2011/07/how-digital-detectives-deciphered-stuxnet-the-most-menacing-malware-in-history/

6. Anexo

Marco de Referencia Extendido "Ciberarmas que detonan vulnerabilidades de día cero en Sistema de Información Militar en un Conflicto Armado Internacional".

1. Adversario

1.1. **Actor**
- 1.1.1. Estatales
  - 1.1.1.1. Miembros de Fuerzas Armadas
    - A) Cibercomandos y/o Comandos Operacionales Cibernéticos
    - B) Organismos de inteligencia militar
    - C) Áreas técnicas de soporte informático
  - 1.1.1.2. Agencias de Inteligencia gubernamentales
  - 1.1.1.3. Otros organismos de Estado
- 1.1.2. No-Estatales
  - 1.1.2.1. Milicias cibernéticas
  - 1.1.2.2. Hackers patrióticos
  - 1.1.2.3. Civiles no expertos de una de las partes o neutrales
  - 1.1.2.4. Mercenarios
  - 1.1.2.5. Organizaciones[9]
  - 1.1.2.6. Contratistas privados

1.2. **Estatus**
- 1.2.1. Combatientes legítimos
  - 1.2.1.1. Miembros de Fuerzas Armadas (puede incluir paramilitares y fuerzas del orden) de una de las partes y miembros de milicias o cuerpos voluntarios que forman parte de esas fuerzas armadas.
  - 1.2.1.2. Miembros de otras milicias y miembros de otros cuerpos voluntarios, incluyendo miembros organizados movimientos de resistencia (de una de las partes de conflicto).
  - 1.2.1.3. Habitantes parte de un *levée en masse.*
- 1.2.2. Beligerantes sin privilegios
  - 1.2.2.1. Mercenarios
  - 1.2.2.2. Civiles (no miembros de fuerzas armadas o grupos asimilados a las fuerzas armadas ni participantes en *levée en masse*)

1.3. **Atribución**
- 1.3.1. Atribuible
- 1.3.2. No atribuible

1.4. **Plataforma**

[9] Personas jurídicas, prestadoras de bienes y/o servicios, colaboradoras con el adversario.

1.4.1. Aire
1.4.2. Mar
1.4.3. Tierra
1.4.4. Espacio

2. Sistema de Información

2.1. **Función**
2.1.1. Administrativa[10]
2.1.2. Operacional[11]
2.2. **Clasificación de seguridad**
2.2.1. Reservado
2.2.2. Confidencial
2.2.3. Secreto
2.2.4. Público
2.3. **Modo de producción**
2.3.1. Adquisición
2.3.1.1. Diseño customizado[12]
A) Interno
B) Tercerizado
2.3.1.2. Producto de mercado
A) COTS
B) GOTS
C) Mil COTS[13]
2.3.2. Tipo de código fuente
2.3.2.1. Cerrado[14]
2.3.2.2. Abierto[15]
2.3.2.3. Mixto[16]
2.4. **Criticidad**
2.4.1. Alta
2.4.2. Media
2.4.3. Baja

3. Modalidad de detonación

3.1. **Causalidad de detonación**
3.1.1. Deliberada

[10] Orientada al sostenimiento administrativo de la organización.
[11] Con relación directa a la ejecución/sostenimiento de las operaciones militares.
[12] Diseño realizado bajo especificaciones del usuario, sea por parte de personal perteneciente a la organización o externo a ésta.
[13] Producto fuera de caja con orientación de uso militar.
[14] De solo conocimiento por parte del desarrollador y/o de un determinado grupo de actores.
[15] Cuyo conocimiento está disponible públicamente.
[16] Contiene partes de código cerrado y partes de abierto en su composición.

3.1.1.1. Interno
A) *Insiders*[17]
B) Espías (y derivados)[18]
3.1.1.2. Externo
A) Actores del adversario[19]
3.1.2. No deliberada
3.1.2.1. Internos
A) Usuarios finales
B) Personal soporte técnico
C) Implementadores
D) Desarrolladores tecnológicos propios
E) Terceras partes dentro del Sistema de Sistemas
3.1.2.2. Externos
A) Proveedor productos/servicios
B) Cadena de suministro[20]

3.2. **Inserción / Descubrimiento**
3.2.1. Inserción
3.2.1.1. Previa entrega
A) Fase diseño[21]
B) Fase manufactura[22]
C) Fase envío[23]
3.2.1.2. En producción/funcionamiento
A) Modificaciones tecnológicas
a) Fabricante (parches / actualizaciones)[24]
b) Inserción de componentes[25]
3.2.2. Descubrimiento[26]
3.2.2.1. Interno
3.2.2.2. Externo

3.3. **Entrega**
3.3.1. Aproximación

---

[17] Miembros de la organización que guardan un fin contrario a los intereses organizacionales, pero sin la necesidad de responder a un actor específico.
[18] Como agentes que responden a los intereses de un actor adversario.
[19] Descritos en el acápite 1.1 del marco de referencia.
[20] Actores intervinientes en el despacho del sistema o componente de éste, desde su centro de producción hacia el adquiriente y/o contratante.
[21] Inserción de la vulnerabilidad en su fase de diseño para su posterior inclusión en su manufactura.
[22] Inserción de la vulnerabilidad durante el proceso de manufactura, no estando considerada dicha vulnerabilidad en su fase de diseño.
[23] Inserción de la vulnerabilidad durante la remisión del activo.
[24] Mediante el despliegue de una modificación al sistema que conlleve a la creación o explotación de una vulnerabilidad no habilitada anteriormente.
[25] Inserción de nueva tecnología que compromete al sistema a nivel de hardware, software y firmware.
[26] Descubierta por personal adscrito o no a la organización, ver Figura 1.2.

3.1.1.1. Directa
3.1.1.2. Indirecta[27]
3.3.2. Vector de Ataque
3.3.2.1. Red[28]
3.3.2.2. Adyacente[29]
3.3.2.3. Local[30]
3.3.2.4. Físico[31]
3.3.3. Elemento de aproximación
3.3.3.1. Conexiones físicas
3.3.3.2. Conexiones inalámbricas
3.3.4. Tipo de detonación tecnológica
3.3.4.1. Hardware
3.3.4.2. Software
3.3.4.3. Firmware
3.3.5. Activación[32]
3.3.5.1. Con interacción humana
3.3.5.2. Sin interacción humana

3.4. **Funcionamiento**
3.4.1. Autónomo[33]
3.4.2. Enlace de comunicación con adversario[34]
3.4.2.1. Directo
3.4.2.2. Indirecto

4. Desempeño operacional

4.1. **Tipo de acción**
4.1.1. Ofensiva
4.1.2. Contraofensiva
4.2. **Contexto**
4.3. **Efectos**

---

[27] Mediante otro elemento externo del sistema, sea dependiente o interdependiente, que permita una posterior afectación.

[28] Vulnerabilidad usualmente denominada como "explotable remotamente". El componente vulnerable está enlazado con la pila de red, la ruta del atacante está a través de la capa 3 del modelo OSI (capa de red). Se considera como un ataque que se puede explotar en uno o más saltos de red (First, 2019).

[29] El componente vulnerable esta unido a la pila de red, sin embargo, el ataque está limitado a la misma red física (p. ej. Bluetooth, IEEE 802.11) o lógica (p. ej. subred local IP), y no se puede realizar a través del límite de capa 3 OSI (p. ej. un enrutador) (First, 2019).

[30] El componente vulnerable no está unido a la pila de red, y la ruta del atacante es vía capacidades de lectura, escritura, ejecución. En algunos casos, el atacante puede conectarse localmente a razón de explotar la vulnerabilidad, de otro modo, ésta puede depender de la interacción del usuario para ejecutar el código malicioso.

[31] Requiere que el atacante toque o manipule físicamente el componente vulnerable. La interacción física puede ser breve o persistente (First, 2019).

[32] Como la necesaria interacción o no de la persona para detonar la vulnerabilidad.

[33] Que tiene programada instrucciones posteriores a la explotación que involucran un efecto deseado.

[34] Recibe instrucciones por parte del C&C adversario para ejecutar acciones.

4.3.1. Nivel alcanzado
- 4.3.1.1. Emergente[35]
- 4.3.1.2. SoS[36]
- 4.3.1.3. Estratégico[37]

4.3.2. Impacto del *Payload*
- 4.3.2.1. Directo
  - A) Daño físico al hardware[38]
- 4.3.2.2. Indirecto
  - A) Denegación
  - B) Influencia
    - a) Toma de decisiones[39]
    - b) Desconfianza[40]
  - C) Control sobre elementos ciber-físicos[41]

4.3.3. Consecuencias
- 4.3.3.1. Personas
  - A) Lesión
  - B) Muerte
- 4.3.3.2. Objetos
  - A) Daño
  - B) Destrucción

Marco de Referencia "Ciberarmas que detonan vulnerabilidades de día cero en Sistemas de Información Militar en un Conflicto Armado Internacional".

Elaboración propia basado en Schmitt y NATO Cooperative Cyber Defence Centre of Excellence (2017); Ormrod y Turnbull (2016); U.S. Joint Chiefs of Staff (2018); First (2019) ; Lin (2016).

[35] Efecto en el tomador de decisión, algoritmo o el sistema ciber-físico conectado (Ormrod y Turnbull, 2016).

[36] Sistema de Sistemas: efecto en sistemas físicos grandes al nivel de personas, organizaciones, gobiernos y sociedad (Ormrod y Turnbull, 2016).

[37] Degrada la voluntad o habilidad nacional para la lucha, el desarrollo de operaciones de combate, la provisión de funciones críticas cívicas o competir en el mercado global (Ormrod y Turnbull, 2016).

[38] A través de la variación de sus parámetros de funcionamiento.

[39] A través de la modificación de interfases de información humanas que conllevan a la toma de una decisión errada.

[40] Basado en la inutilización del sistema a causa de la puesta en riesgo de su legitimidad de uso en la fuerza.

[41] Control derivado del sistema inicialmente vulnerado que permite acceso sobre otro sistema, en este caso, un sistema ciber-físico, del cual permite proyectar un efecto cinético (p. ej. control sobre un montaje, un sistema misilístico, etc.).