Omnium contra omnes

Análisis político-militar de la guerra en el ciberespacio

* * * * *

Joan Soriano Aguilar

NAUllibres

Nau Llibres

Periodista Badía 10. 46010 València
Tel.: 96 360 33 36
Fax: 96 332 55 82
E-mail: nau@naullibres.com
web: www.naullibres.com

Diseño y maquetación:
Pablo Navarro y Artes Digitales Nau Llibres

Ilustración de la cubierta:
[Tohey22] / Depositphotos.com

ISBNs Nau Llibres

ISBN_papel: 978-84-18047-54-1
Depósito Legal: V-1362-2021
ISBN_ePub: 978-84-18047-55-8
ISBN_mobi: 978-84-18047-56-5
ISBN_PDF: 978-84-18047-57-2

Impresión: Podiprint

Gracias a mi madre, que me ha dado todo. A mi padre, que me enseñó a pensar y que ha sido parte fundamental en la estructuración de este estudio. Por supuesto, también a mi hermano, y al resto de la familia, por siempre estar ahí para todo.

A S2 Grupo, que no sólo ha sido el motor de la publicación, sino también el lugar donde he aprendido la práctica totalidad de mis conocimientos sobre ciberseguridad. Un lugar especial gracias a las personas que lo componen, jefes, compañeros y amigos, cuya familiaridad y cercanía permite que uno se enorgullezca de formar parte.

Finalmente, gracias a Antonio Villalón, por los consejos y la ayuda que me ha dado durante todo el proceso.

Índice

Prólogo 11

Consideraciones previas 13

Introducción 15

Primera parte
De lo político

1. Definiciones 23
1. Nuevos medios para la guerra 23
2. El concepto de ciberguerra 24
3. Inicio y fin de la ciberguerra 29

2. El por qué de la ciberguerra 31
1. El inicio del equilibrio internacional 31
2. La guerra de Foucault 36
3. Ciberguerra como elemento político 39
4. Victoria no clausewitziana 42

3. Lo virtual 45
1. El sujeto del escenario virtual 47
2. El objeto del escenario virtual. La ciberarma 48
3. El medio en lo virtual 50
4. El tiempo en lo virtual 52
5. El ciberespacio 54
   5.1. Ciberespacio como tecnología de la información y la comunicación 55
   5.2. Traslación del Estado al ciberespacio 56

4. El ciberespacio como teatro de guerra 65
1. Anonimato 65
   1.1. Hacia el realismo político 67
2. No dependencia del factor humano 75
   2.1. Eje sociopolítico 75
   2.2. Eje militar 81
   2.3. La ciberguerra como guerra de la razón 87

Segunda parte
De lo militar

5. La ciberguerra como conflicto asimétrico 95
1. Lawrence de Arabia 98
2. El control en posiciones de guerra asimétrica 101
3. Sun Tzu 103
4. Posiciones asimétricas en el conflicto convencional 106
5. Victoria en el conflicto asimétrico 108

6. Elementos del escenario bélico 111
1. Enemigo 111
2. Grupo operativo 112
3. Sistemas de mando y control 113
4. Ciberarmas 115
5. Territorio 116
6. Objetivos 119
7. Teatro de la guerra 120

7 Estrategia de ciberguerra 123
1. Dualidad de ámbito en la estrategia 124
2. Táctica 125
3. Técnica y procedimiento 126
4. Elementos condicionantes de la estrategia 127
   4.1. Inteligencia 127
   4.2. Disposición táctica y movilidad 136
   4.3. Psicología 145
   4.4. Otras cuestiones sobre lo virtual y lo político 152

8 Estructura del ataque 159
1. Antecedentes 160
2. Reconocimiento 161
3. Militarización 161
4. Entrega y abuso 162
   4.1. Entrega y abuso por vía remota 163
   4.2. Entrega y abuso por vía física 164
5. Colocación 165
6. Mando y control 166
7. Acciones sobre el objetivo 168

9. Contrainsurgencia 171
1. Definición de contrainsurgencia 171
2. Teoría clásica 172
2.1. David Galula 172
2.2. Robert Thompson 173
2.3. David Kilcullen 174
3. El trilema de la contrainsurgencia 174
4. Contrainteligencia en el ciberespacio 175
4.1. Contrainteligencia defensiva 175
4.2. Contrainteligencia ofensiva 178
5. Reinicio de las hostilidades 179

Conclusiones 181

Anexo 183

Referencias 203

Prólogo

Excmo. Sr GD Rafael García Hernández,
Comandante Jefe del Mando Conjunto
del Ciberespacio

¿Qué tienen que ver los dioses griegos Ares y Atenea con la ciberguerra? ¿Y Carl von Clausewitz con la doctrina Gerasimov?

¿Influye la Guerra de los 30 años y las campañas de Napoleón en la preparación de los ataques realizados por las APTs (Amenazas avanzadas persistentes)?

¿Fue Sun Tzu quién teorizó sobre la defensa y ataque asimétrico como en la ciberguerra?

Para contestar a estas y otras muchas preguntas, el autor nos coloca en un tablero de ajedrez con un eje político-económico y otro eje militar para intentar encontrar una definición teórica de lo que es la ciberguerra.

Apoyándose en marcos económicos, diplomáticos y comerciales nos va definiendo las características del ciberespacio tal como lo conocemos hoy: un dominio casi infinito,

con límites y fronteras poco definidas, en el que infinidad de actores utilizan armas y técnicas específicas, en un entorno legal muy complejo y sobre el que no hay control armamentístico ninguno.

La ciberguerra es un conjunto de acciones que puede afectar a todas las actividades del Estado y acerca la zona de combate al corazón de una Nación. Nunca hasta ahora se había aplicado en toda su extensión ese lema tan conocido de *"La guerra es la continuación de la política por otros medios"*.

El libro nos trata de acercar al concepto mediante un repaso histórico de las teorías de la guerra para confluir en los ciberataques actuales, un modelo asimétrico de conflicto con unas técnicas, tácticas y procedimientos propios, en los que no hay que olvidar los aspectos de la inteligencia.

Aborda, siempre desde un punto de vista teórico, todas las capacidades de una guerra en red, con los apoyos de la guerra sicológica y la ingeniería social para repasar la estructura de un ataque, con ejemplos vigentes como el uso de la "Kill Chain" usada por los grupos de las citadas APTs, con saltos continuos atrás y adelante en la historia.

Todo un ensayo teórico para finalizar con la utilización del ciberespacio como teatro de una guerra asimétrica por parte de las naciones como un marco de competición sin fronteras.

Una guerra de todos contra todos.

Consideraciones previas

El siguiente análisis ha nacido con el objetivo de profundizar en el ámbito táctico de la ciberguerra más allá del aspecto técnico. Para ello, a partir del estudio de la ciencia militar que precede al ámbito de la seguridad informática, se han concretado ciertas tesis para abordar un hipotético escenario teórico.

En la primera parte del texto se define el concepto de ciberguerra como punto de partida, acotando, de este modo, las acciones con objetivo político desde medios tecnológicos que pueden considerarse bajo el planteamiento teórico expuesto. Durante el análisis de los elementos que rodean las operaciones cibernéticas, es cuando se detecta su ineludible vinculación con un escenario político, y se encuentra la metodología de la ciberguerra como heredera de un contexto diplomático. Así, dado que su mera existencia se debe a la superposición política y económica en las relaciones internacionales, aparecen una serie de particularidades que impiden analizar ambos conceptos como independientes.

La dependencia entre el ámbito político y el militar es bidireccional, pues las posibilidades de la ciberguerra también han alterado las posiciones políticas asumidas dentro del equilibrio westfaliano. Por lo tanto, ha sido necesario incidir tanto en las premisas como en las consecuencias resultantes a través de dos partes diferenciadas del estudio, posiciones que permiten tomar distancia respecto al idealismo político planteado por Kant y Wilson.

Las ideas extraídas de dicho análisis permiten entender que las capacidades virtuales establecen un nuevo paradigma de las operaciones en el ciberespacio, apareciendo un tipo de conflicto que diferencia significativamente la parte atacante y la parte defensora, quedando definido como de corte asimétrico y, en consecuencia, llevándose a cabo una asociación entre el amplio aspecto teórico desarrollado en este tipo de conflicto y el mundo virtual. Esta cuestión permite poder enmarcar las estrategias de ciberguerra dentro de tesis planteadas por teóricos como Lawrence de Arabia.

Finalmente, se debe incidir en que, debido a la especial velocidad con la que las nuevas herramientas inciden dentro del ciberespacio, en este texto se ha optado por posiciones puramente teóricas, dejando de lado el aspecto práctico con el objetivo de impedir una pronta obsolescencia del mismo.

Introducción

La mitología griega ha permitido que llegara a nuestros días la brillante perspectiva de la cultura clásica, cultura que sentaría las bases de la civilización occidental en los diferentes ámbitos que rodean a la existencia humana. También sobre la dualidad del ser humano. Ese animal racional que describía Aristóteles queda reflejado en los dos aspectos fundamentales que definen al individuo: pasión y razón. Ambas tienen cabida en el ser humano durante gran parte de su devenir existencial, social e histórico. Y ambas han quedado reflejadas también en su percepción de la guerra.

Cada uno de los aspectos vitales quedó personificado dentro del amplio abanico de divinidades que conformaría la tradición helénica. La guerra, como uno de los ámbitos más importantes para los griegos, cuenta con un matiz especialmente relevante, pues existen dos deidades diferentes asociadas a ella, Ares y Atenea, cada una representando los aspectos más humanos de todo conflicto bélico.

Ares representaba al héroe guerrero y su habilidad y valentía, pero también la brutalidad de las batallas y sus horrores. Era el lado emocional del conflicto. Atenea, por su parte, complementaba las características de Ares: nacida de la frente de Zeus y también diosa de la sabiduría, representaba la parte racional de la guerra a través de la estrategia. Así pues, la guerra se concebía bajo la misma dualidad que el ser humano.

Aunque, evidentemente, los griegos contemplaron esta dualidad dentro de un concepto clásico de guerra, ¿tendría sentido hablar también de dualidad en la guerra del ciberespacio?

A lo largo de la historia de la humanidad, todas las estrategias y tácticas de guerra han quedado obsoletas o susceptibles de reinterpretación ante la aparición de nuevas tecnologías aplicadas a la guerra. En concreto, en los últimos años han surgido un gran número de nuevas metodologías sobre las cuales se ejercen acciones de guerra. Dichas metodologías se han basado, fundamentalmente, en las nuevas tecnologías de la información y la comunicación, siendo el ciberespacio el último de los avances tecnológicos, cuyas repercusiones resultan similares a las que ya había.

Desde la innovación de la *sarissa*[1] y su aplicación en la falange macedonia para la superación de la formación hoplítica espartana, hasta la posibilidad de la estructuración nodal de los ejércitos creada por el mariscal de campo Moltke[2], la aplicación de los nuevos avances tecnológicos en la estrategia militar han resultado cruciales. Del mismo modo que estas, las condiciones en el ciberespacio han permitido una nueva comprensión del conflicto bélico y lo han convertido en un nuevo campo de aplicación de estrategias militares.

1 Ver punto 1 del Anexo.

2 Helmuth Von Moltke, mariscal de campo alemán (1800-1891).

Primera parte

De lo político

1 Definiciones

1. Nuevos medios para la guerra

Heráclito afirmó que la guerra es el padre de todo y el rey de todas las cosas. La conclusión del filósofo griego permite entender la magnitud de la importancia que ha tenido la guerra a lo largo de la historia, y por qué la utilización de la gran mayoría de las evoluciones tecnológicas ha conducido a nuevas metodologías para abordar la interactuación entre las naciones a través de métodos hostiles. También ha sido así con las tecnologías de la información y la comunicación, lo que motivó que, en la cumbre de Varsovia de 2016, se considerase el ciberespacio como el quinto dominio de las operaciones militares[4].

Desde la segunda mitad del siglo XX, lo virtual ha confluido con las metodologías de guerra convencionales, pues las posibilidades que ofrece la interconexión a nivel global permiten la potenciación de muchas de las capacidades ya

4 La OTAN clasifica el ciberespacio como el dominio global virtual compuesto tanto por las redes interconectadas como por las redes y sistemas aislados o independientes.

existentes, como son la incorporación de la automatización en el manejo de las armas o la aparición de las tecnologías dron, resultando compleja la diferenciación de ciertos conceptos tras la evolución digital.

Por lo tanto, dado que las posibilidades del ciberespacio son innumerables, ¿tendría cabida toda acción no consentida a través de un elemento digital como parte del ámbito de la guerra virtual? ¿Cuál es el límite de participación de las tecnologías de la información y la comunicación para que sea considerada como ciberguerra?

Para la elaboración de un marco teórico militar de la guerra en el ciberespacio, resulta fundamental establecer los límites de su aplicación, de cara a poder crear metodologías más concretas en función de la tipología de la operación.

2. El concepto de ciberguerra

De las implicaciones tecnológicas comentadas y de su utilización con un objetivo político, nació una de las definiciones más genéricas para este tipo de conflictos: la Guerra Híbrida. Esta metodología de guerra se define como "la utilización de toda clase de medios y procedimientos para la realización de un impacto sobre el enemigo, especialmente a través de la influencia sobre la población" (Hoffman, 2012). Es en esta definición donde se encuentra la inclusión de guerra asimétrica y diferentes contextos de combate, como el político, el comunicativo o el tecnológico, pero teniendo también cabida las metodologías convencionales de guerra.

Una de las más famosas implementaciones de Guerra Híbrida se encuentra en la doctrina Gerasimov. El general ruso Valeri Vasilievich Gerasimov estableció la importancia de la colaboración público-privada en la ejecución de opera-

2 El por qué de la ciberguerra

Durante los últimos años se ha visto cómo el número de intervenciones por parte de grupos presumiblemente asociados a intereses políticos ha ido en aumento. Y es que, a pesar de existir conflictos entre naciones en el ámbito del ciberespacio o guerras subsidiarias, desde la segunda mitad del siglo XX no se han producido enfrentamientos directos entre dos naciones del primer mundo. Es precisamente la utilización de métodos de ciberguerra, y no de otros, lo que resulta definitorio en sí mismo, pues la ciberguerra ofrece una serie de particularidades como conflicto que permiten adecuarse de manera acorde a las relaciones internacionales contemporáneas.

1. El inicio del equilibrio internacional

Muchos historiadores han establecido la guerra como la más antigua de las relaciones entre pueblos o naciones.

A pesar de que actualmente el timón de dichas relaciones habría quedado, en la mayoría de los casos, al margen de los métodos violentos y dentro de un marco diplomático y comercial, no hay que olvidar que, históricamente, el auge y caída de los grandes imperios ha dependido de sus posibilidades bélicas. De este modo, la guerra ha sido el principal medio sobre el que se ha conformado el *status quo* actual de equilibrio internacional.

El marco diplomático del que se dispone hoy en día apenas cuenta con cuatrocientos años de vida, pues no siempre ha existido equilibrio alguno del cual formar parte. Desde el Imperio Macedonio, pasando por el Romano o el Español, todos han actuado sin intención de respetar la soberanía de los pueblos sometidos[10]. Los imperios aspiraban a ser ellos mismos la representación del equilibrio, aplicando una autoridad común para regir el mundo bajo unas mismas leyes y partiendo de una legitimidad basada en su poder militar, su economía, su cultura o su religión.

Fue tras la Guerra de los Treinta Años cuando los Estados se encontraron con la necesidad de estructurar unas bases para las relaciones entre las naciones, acuerdos conocidos como la Paz de Westfalia, que fueron firmados en 1648. Dicho documento es considerado como el origen de la diplomacia moderna debido a que es el primer escrito donde se encuentra el concepto de equilibrio entre Estados soberanos, reconociendo así su coexistencia, prohibiendo la intromisión en los asuntos internos de otra nación, y aspirando a conseguir una igualdad de poder entre ellas.

Sin embargo, la dificultad de llevar a la práctica esta idea motivó la redacción de un complejo entramado de acuerdos de control entre las naciones firmantes que permitía incluso la intervención del resto de ellas si alguna vulneraba algún

10 Ver punto 5 del Anexo.

3 Lo virtual

La teoría militar en el ciberespacio cuenta, sin duda, con la ventaja de que parte de más de 2.500 años de estudio dentro de este ámbito, y sus análisis pueden tomarse como base para el establecimiento del conjunto de referencias teóricas para la conformación de una teoría estratégica para la ciberguerra. Sin embargo, es en el momento de analizar las formaciones de ataque o las metodologías de movimiento de tropas, cuando se detecta una serie de limitaciones que dificultan la traslación de todos estos conceptos de manera directa a los actores y herramientas que constituyen la guerra en el ciberespacio.

Mientras que la guerra convencional tiene una serie de características que vienen limitadas por las leyes físicas, el ciberespacio las ha superado. Dichos cambios podrían clasificarse en dos grupos. Por una parte, se tendrían aquellos derivados de la aparición de un medio que proporciona nuevos principios de actuación y, por otra, aquellos que dependen de

todas las características del medio físico y que no es posible trasladar al ciberespacio.

El escenario de guerra convencional tiene límites orográficos, es decir, montañas y océanos que se deben tener en cuenta en la logística del desplazamiento de tropas o el diseño de la estrategia de batalla, y otros, como las condiciones climatológicas. En la misma línea, las herramientas que intervendrán en la ejecución de las acciones de guerra están basadas en los recursos e infraestructura que tenga una nación, disponibles en función de las capacidades económicas, y que confieren a las naciones que las poseen un *status quo* de superioridad respecto a sus rivales. Pero, sobre todo, las guerras convencionales estaban ceñidas a un contexto espacio-temporal particular que las hacía diferentes unas de otras, con implicaciones económicas, sociales y políticas que podían ser muy diferentes. No es necesario insistir demasiado en que, en el paradigma virtual, estas características desaparecen.

A pesar de que el medio en el ciberespacio es el fruto de las necesidades de comunicación del ser humano, este ha resultado ser en sí mismo un nuevo medio al margen de sus mismas capacidades. Dicho escenario resulta conformado por la generación de señales a través de sistemas digitales, materializando la representación de los valores discretos, conocidos como bits, en conjuntos de datos cuyo proceso e interpretación quedan incluidos dentro de la idea de información, concepto elemental que dotará de su naturaleza al conflicto en el ciberespacio. Así pues, al establecer como punto central la idea de la información, una particularidad concreta resulta del medio virtual en contraposición al físico, y es que la información no solo constituye el medio donde tienen lugar las acciones del ciberespacio, y por ende de la ciberguerra, sino que también forma el resto de elementos que conforman las interacciones bélicas.

4 El ciberespacio como teatro de guerra

En el capítulo anterior se han analizado las particularidades del ciberespacio como medio por sus capacidades vinculadas a lo virtual. Sin embargo, las repercusiones más importantes a nivel político vienen determinadas por ser el medio donde tienen lugar las acciones de ciberguerra. Esto se debe a las posibilidades de realización de actos a través de un medio virtual, pero es también consecuencia de la superación de ciertas construcciones que como sociedad se habían elaborado dentro de los medios de regulación.

1. Anonimato

Lo más relevante de un escenario bélico es que las acciones de guerra no son ejecutadas por una nación en sí, sino por entes que actúan de manera anónima motivados por una serie de cuestiones desconocidas a priori por el Estado objeto del mismo. Esta cuestión no afecta simplemente a las

metodologías de la guerra en sí, sino también a las implicaciones sobre el cálculo de costos sobre el que está construido el sistema legal en la sociedad.

La posibilidad de realizar una acción en el ciberespacio de manera anónima viene motivada por la dificultad de traslación, desde el impacto recibido en una organización en particular, hasta el origen de la misma. Esta problemática resulta de la consecución de atribuciones a diferentes niveles.

En primer lugar, aparecería la dificultad de crear un perfil virtual a un actor asociado a una nación en particular simplemente por la utilización de ciertas tácticas, técnicas y procedimientos en diferentes campañas[24].

En segundo lugar, se tendría la asociación del actor modelado a través de sus procedimientos al interés de una nación en particular. La existencia de múltiples conflictos mundiales proviene del mutuo interés de diferentes actores en la consecución de un objetivo particular, por lo que el número de posibles *casus belli* aumenta de manera exponencial respecto a un conflicto convencional. Si bien es cierto que actualmente existen un número reducido de países (al menos presumiblemente) capaces de realizar estas acciones en el ciberespacio, todo apunta a que cada vez más naciones están adquiriendo la madurez suficiente para realizar campañas de alta sofisticación.

La siguiente problemática sería la trazabilidad de un actor asociado a los intereses de una nación con las personas que realizan dichas acciones. Los nodos intermedios, además de la infraestructura ubicada en Estados con jurisdicciones más laxas en el ámbito del ciberespacio, dificultará la trazabilidad del origen de las acciones.

24 Ver punto 11 del Anexo.

Segunda parte

De lo militar

5 La ciberguerra como conflicto asimétrico

La definición de ciberguerra sobre la que hicieron hincapié los oficiales Raymond C. Parks y David P. Dungan en su estudio *Principies of Cyber-warfare*, hace referencia a la necesidad de la existencia de un impacto cinético proveniente e iniciado en el ciberespacio. De este modo, la ciberguerra ha quedado definida como una guerra entre dos tipos de medios, cada uno con sus características propias. Mientras que, tal y como se ha detallado, la acción en el medio virtual queda asociado a un potencial de fuego basado en la información, esta no deja de ser susceptible de ser intervenida a un nivel físico en donde las capacidades virtuales puedan ser inofensivas.

Indagando a lo largo de la historia, el enfrentamiento entre dos medios ya tuvo lugar en uno de los episodios bélicos más icónicos, las Guerras del Peloponeso.

Este acontecimiento se inició con la brillante implementación táctica que supuso la Batalla de Salamina[33], que, junto a la batalla de Platea, supondría un punto de inflexión en la Segunda Guerra Médica. Tras la victoria de los griegos contra los persas de Jerjes I, la coalición helénica se encontró en posición de conformar una contraofensiva.

Atenas, ciudad que apenas veinte años antes había quedado devastada tras la invasión persa en la Primera Guerra Médica, ahora se encontraba en posición de conformar un imperio. Tras liberar Tracia, Jonia y las islas del Egeo, se conformó de la mano de Arístides la Liga de Delos. Con Pericles como gobernante, Atenas se posicionó como la más importante ciudad griega, consiguiendo una hegemonía sobre las demás ciudades de la liga, cuyo poder resultaría una provocación para la otra gran ciudad griega, Esparta, naciendo lo que más tarde el politólogo estadounidense Graham Allison bautizaría como la "trampa de Tucídides"[34].

Como consecuencia del cambio en el paradigma político griego, el conflicto entre ambas ciudades-estado de intereses e influencia sobre el resto de polis griegas condujo a que la Liga del Peloponeso, liderada por Esparta, se enfrentara a la Liga de Delos en la que sería conocida como Guerra del Peloponeso, cuyas crónicas quedarían para la posteridad a través de los escritos de Tucídides.

La divergencia en cuanto al entendimiento del conflicto aparece en el tipo de ejército que había conformado cada potencia. Atenas, poco antes de la Primera Guerra Médica, durante el arcontado de Temístocles en el 493 a.C., inició una fuerte inversión para aumentar su poderío naval, que acabaría siendo crucial para el devenir de los acontecimientos, y que propiciaría la victoria en Salamina. Por otra parte,

33 Ver punto 19 del Anexo.

34 Ver punto 20 del Anexo.

6 Elementos del escenario bélico

Tras establecer el punto de partida en cuanto a la consideración de las partes en el escenario de batalla de la ciberguerra, debe definirse la disposición táctica, que resulta de la disposición de una serie de medios. Por ello es fundamental definir los elementos que conforman el conjunto de las posibilidades de la guerra en el ciberespacio.

1. Enemigo

Dentro del ámbito belicista se considera al enemigo como la entidad que permite particularizar una amenaza (Cottam, Mastors, Preston y Dietz, 2016). Por lo tanto, desde la perspectiva de la ciberguerra, estas fuerzas armadas serían el conjunto de sistemas tecnológicos de información, así como también las capacidades humanas que hacen frente en una operación del ciberespacio.

La particularización de a quién o a qué se considera enemigo en un escenario de ciberguerra va cambiando según la perspectiva que tenga del mismo una u otra de las partes. Un ejemplo sería el factor humano pues, mientras que la parte defensora no puede identificar al ente físico que realiza el ataque, la parte atacante sí puede considerar objetivos a personas concretas. Esta condición la tiene exclusivamente el atacante pues, si el receptor de una ataque cibernético iniciara acciones contra los sistemas del atacante y obtuvieran información sobre el mismo, esto supondría una inversión de roles, y sería de nuevo el atacante quien, por la superioridad que le confiere la asimetría del conflicto, obtuviera información del defensor.

Por lo tanto, el defensor quedaría limitado únicamente al conocimiento de identificadores de la infraestructura de carácter virtual, hashes, dominios, direcciones IP o artefactos de red o host que permitieran la identificación única de la campaña, es decir, los Indicadores de Compromiso. Además de este tipo de información, el atacante podrá conocer de manera adicional información personal asociada a los recursos humanos, la cual permite un análisis más en profundidad del contexto de la operación, ampliando los vectores ataque y facilitando el éxito de la operación.

2. Grupo operativo

Se va a considerar grupo operativo al conjunto de elementos humanos que ejecutan o programan las acciones de ciberguerra, que podría entenderse como una particularización del personal técnico del concepto de enemigo, tanto del lado atacante como del defensor. Debido a su carácter no virtual, introduce el factor del azar, tanto por sus imperfecciones como por sus condicionantes emocionales.

7 Estrategia de ciberguerra

Durante la primera parte del texto se ha podido determinar la aparición de un nuevo contexto donde ejercer una competición entre naciones, primero a través del ámbito diplomático y comercial y, más tarde, de manera imprevista para los ideólogos del equilibrio internacional post Segunda Guerra Mundial, también bajo el escenario virtual. Estas premisas parten de las posibilidades de interconexión en tiempo real y de una codependencia económica, pero también de un escenario donde impera la razón y, con ello, la posibilidad de una mayor planificación de las acciones a llevar a cabo.

Por lo tanto, entendiendo la guerra en el ciberespacio como un modelo asimétrico de guerra heredado de la teoría de Lawrence de Arabia, se va a fundamentar el marco teórico en los principios del control intangible, considerando la inteligencia, la movilidad y la psicología como elementos clave dentro de la guerra en el ciberespacio.

1. Dualidad de ámbito en la estrategia

Los capítulos 5 y 6 han permitido entender que la ventaja de la guerra en el ciberespacio respecto de otras metodologías de guerra reside, fundamentalmente, en una mayor posibilidad de continuación del conflicto en el ámbito político. Por lo tanto, la elaboración de un marco teórico debe basarse en dicha consideración para la definición de la estrategia.

Clausewitz estableció el concepto de estrategia como el conjunto de operaciones que tienen como objetivo la consecución de un éxito político. Por ello, si tal y como se ha establecido, la ciberguerra es parte intrínseca de un marco político, se estaría ante una posible divergencia de planos de actuación, pues esta dualidad en la consideración del conflicto en el ciberespacio quedaría en función del contexto en donde se aplicara.

Considerando que en una guerra política las naciones llevan a cabo una serie de acciones para la obtención de un rédito que mejore su situación internacional, la ciberguerra sería una de esas acciones, del mismo modo que podrían utilizar capacidades del ámbito diplomático, comercial o incluso de guerra convencional. La definición de este plano de estrategia quedaría alineada con la idea de Guerra Híbrida.

También dentro de la estrategia política tendría cabida una parte de las posibilidades del escenario del ciberespacio, pues existe una dependencia de la innovación y el desarrollo en las posibilidades de ejecutar en un momento determinado una acción en el ciberespacio. Para ello, la nación debe contar con las capacidades necesarias, que incluyen la previa inversión en este campo.

Sin embargo, en la particularización necesaria para el establecimiento de un marco más concreto de actuación, un segundo eje de análisis podría centrarse en considerar la ciberguerra como un marco teórico en sí sobre el cual llevar

8 Estructura del ataque

En consonancia con las conclusiones extraídas en los capítulos anteriores, debe establecerse una estructura del ataque contra una organización utilizando como base la aproximación de guerrillas. Aunque sí que se tomarán como referencia la utilización de sus elementos clave, como la inteligencia, la movilidad o la psicología, el ámbito teórico desarrollado al respecto, como por ejemplo el de Mao (1937), no facilitan una correlación de escenarios. Sin embargo, sí que se han desarrollado diferentes implementaciones en la teoría de la ciberseguridad, por lo que se utilizará como base parte de estas ideas.

El modelo más conocido es la modificación realizada por la corporación Lockheed Martin del concepto tradicional de kill chain[59]. También en esta línea apuntarían el estándar de MITRE ATT&CK[60] framework o modelos mixtos como

59 The Cyber kill chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

60 https://attack.mitre.org/

puede ser la Kill Chain unificada[61]. En las próximas líneas se va a utilizar la Cyber Kill Chain con alguna modificación. Además, la ejemplificación de las posibilidades dentro de las fases se utilizará con lo que MITRE ATT&CK define bajo la idea de "táctica"[62].

Así pues, se va a llevar a cabo un desarrollo de una operación de ciberguerra, pero contemplando también la participación de acciones físicas en ciertos contextos, como son los posibles métodos de la fase de entrega. Debe considerarse que el carácter dual de la ciberguerra obliga a considerar el contexto político que subyace a la operación como parte de ciertas fases del ataque.

1. Antecedentes

Una operación de ciberguerra no nace por sí sola, sino que proviene de una necesidad concreta en el escenario geopolítico. Dicha necesidad también conlleva la imposibilidad de ejecutar un impacto grave sobre el objetivo, y contempla la utilización de metodologías de ciberguerra como medio para la obtención del rédito político. Por lo tanto, es dentro de una estrategia política donde se deben planificar las necesidades que se pueden plantear ante posibles escenarios de operaciones de ciberguerra.

61 The Unified Kill Chain. https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf.

62 Ver punto 34 del Anexo.

9 Contrainsurgencia

El establecimiento del paradigma teórico del ciberespacio como una guerra de guerrillas permite estudiar la defensa de una organización bajo el escenario de la contrainsurgencia. De este modo, deben ser analizadas las posibilidades que tiene la parte defensora respecto a las posibilidades de control intangible que dispondría la guerrilla.

A lo largo del capítulo se van a analizar los elementos teóricos necesarios para aplicar una teoría para la defensa de la organización basada en los métodos de contrainsurgencia.

1. Definición de contrainsurgencia

La contrainsurgencia es el conjunto de técnicas y prácticas aplicadas por los Estados con el objetivo de detectar y destruir a los miembros y bases de apoyo de los grupos insurgentes.

Tras el incremento de la utilización de las tácticas de guerrilla y la difusión de sus metodologías a través de diferentes escritos, surgió una respuesta, también teórica, sobre las medidas de contrainsurgencia a llevar a cabo. La posterior sustitución del conflicto convencional por la lucha asimétrica también provocó un aumento de su estudio.

Utilizando la conocida frase del general francés Louis Hubert Lyautey *ganar corazones y mentes*, se pueden clasificar las acciones de contrainsurgencia bajo dos tipologías: por un lado, las operaciones militares, policiales y de inteligencia que actúan sobre la insurgencia, y, por otro, las acciones de apoyo a la población civil.

Del mismo modo que el aspecto biológico de Lawrence quedaba sin aplicación, su homólogo en la contrainsurgencia respecto al respaldo de la población carecería de sentido. A continuación se detallará el encaje del modelo de contrainsurgencia por parte de la defensa de una organización.

2. Teoría clásica

A raíz de la explosión de las revoluciones durante la segunda parte del siglo XX y su inspiración en las tácticas defendidas por Lawrence de Arabia, los Estados se vieron en la necesidad de abordar un nuevo concepto de guerra no convencional, donde dos ejércitos no se enfrentan de manera directa y donde los estudios de corte clausewitziano habían dejado de ser aplicables.

2.1. David Galula

El militar francés David Galula, que participó en la guerra de Argelia como oficial, utilizó las teorías de Mao como base

Conclusiones

En este texto se han planteado las posibilidades militares nacidas de la utilización del ciberespacio como teatro de guerra. Al profundizar en el análisis, se ha podido observar que conceptos asociados a lo cinético, como son los vinculados a lo numeral o espacial, se han dejado de aplicar en la misma medida que lo hacen en la guerra convencional.

Pero, en este espacio, es posible definir las acciones bélicas como un conflicto de corte asimétrico, posibilitando, por tanto, el desarrollo de una metodología de ciberguerra basada en la guerra de guerrillas. El desarrollo de acciones de ocultación, el cambio en los conceptos de control de la situación y potencia de fuego basados en el conocimiento de información son ejemplos de los ejes de acción de un nuevo paradigma basado en lo virtual. Y es que, la aplicación de este modelo no solo permite indagar en la explotación de las tácticas de guerrilla en las diferentes tipologías de operaciones en el ciberespacio, sino que también permite asociar un modelo teórico para la seguridad de una organización.

No cabe duda de que la innovación y el desarrollo de los medios virtuales está conduciendo hacia un mundo donde el conocimiento de la realidad mediante los sentidos está viéndose reducido a medida que lo virtual converge con el mundo cinético. La verdad puede quedar modificada o alterada cuando esta es procesada por medios virtuales. En este nuevo escenario, no solo aparece la dificultad de ser conocedor de estar bajo un ataque por parte de una nación extranjera, sino que, en muchos casos, puede ser incluso imposible comprender el motivo originario de dicho acto, lo que impide responder al mismo. Dicha cuestión se ve agravada por la aparición de posibilidades comerciales entre Estados de todo el mundo, lo que provoca que existan múltiples motivos para llevar a cabo una acción bélica contra cualquier nación.

Por lo tanto, las naciones han encontrado en el ciberespacio un marco de competición en la lucha por conseguir posiciones de ventaja política y económica, un marco donde no existen fronteras para las relaciones entre naciones y donde el coste de participación militar se ve minimizado respecto a su equivalente cinético, hecho que facilita la participación en un número de acciones políticas mucho mayor, y cuyo resultado es un complejo entramado político y comercial donde los Estados son aliados y enemigos entre sí. Una guerra de todos contra todos.

Anexo

[1] Se le atribuye a Filipo II la creación de la falange macedonia, formación que permitió las grandes conquistas de su hijo, Alejandro Magno, y que nació con el objetivo de hacer frente al sistema hoplítico espartano. Filipo dotó a los piqueros de una lanza más larga que la convencional llamada *sarissa*, de unos cuatro metros y medio, que junto a la aplicación de una velocidad de carga mayor causaría graves problemas a las defensas griegas que hicieron frente a la falange. Las posibilidades de victoria de esta nueva formación se veían reforzadas dado que este tipo de armamento tenía un coste mucho menor, lo que permitía dotar de equipo a un mayor número de soldados. También resultó fundamental la implementación de la táctica militar conocida como el martillo y el yunque, que potenciaba las ventajas que ofrecía la *sarissa*.

La maniobra del yunque y el martillo quedaba constituida con una formación móvil, en este caso la caballería, la cual rodeaba al debía ser similar al del oponente. La personificación del yunque quedaba conformado por la falange y la infantería macedonias, que eran las encargadas de bloquear a las fuerzas enemigas. De este modo, la caballería empujaba

a los enemigos desde los flancos hacia la falange, donde las fuerzas quedaban sin opción de escapar.

[2] La doctrina Gerasimov parte de la premisa de establecer un enfoque gubernamental a través de la sincronización del ámbito militar con otras agencias. De este modo establece seis etapas en las que se pueden diferenciar los conflictos del siglo XXI.

El inicio de las acciones por parte del atacante se llevaría a cabo de modo encubierto mediante la transmisión de información que permitiera la influencia en la opinión pública y el respaldo de la oposición. Tras ello, la escala de tensiones y las repercusiones a nivel diplomático y económico podrían provocar el inicio de actividades militares dentro del Estado. Sería, dentro de este estado de crisis, donde el atacante podría intervenir militarmente alegando razones humanitarias, las cuales le permitirían en el futuro restablecer la paz en consonancia con sus intereses.

[3] Existen diferentes aproximaciones sobre qué considerar una APT. Entre las de ámbito más común se tendría la clasificación como un actor con capacidades muy sofisticadas. Sin embargo, otra perspectiva es considerar una APT como un actor con motivaciones políticas[68].

Esta cuestión resulta de gran importancia, sobre todo a la hora de establecer ciertos actores como podría ser FIN7, cuyas capacidades son muy sofisticadas, pero cuyo objetivo resultaría de índole económico. Otro tipo de grupos, como APT-C-36, serían actores con motivaciones políticas y con procedimientos más genéricos y menos dirigidos. Dado que este estudio va a considerar los actos de ciberguerra como parte de un contexto de equilibrio westfaliano, se va a considerar APT aquellos grupos cuyos intereses sean de ámbito político, independientemente de su sofisticación.

[4] La existencia de grupos empresariales con valores de mercado comparables al Producto Interior Bruto de naciones del primer mundo hace que las conocidas como GAFAM deban

68 Definición utilizada en la Guía STIC 817 del CCN Cert

Referencias

Allison, Graham. (2017). The Thucydides Trap. https://foreignpolicy.com/2017/06/09/the-thucydides-trap/

Aristóteles. (IV a.C.). Política.

Arquilla, John y Ronfeldt, David (1997). *Cyberwar is Coming!* https://www.rand.org/pubs/reprints/RP223.html.

Ayrault Dodge, Theodore (2012). *Hannibal: A History of the Art of War among the Carthaginians and Romans down to the Battle of Pydna*.

Barlow, John Perry (1996). *Declaración de Independencia del Ciberespacio*. Davos (Suiza): Foro Económico Mundial. Disponible en

BBC News. (2020). UK says Russia's GRU behind massive Georgia cyber-attack. https://www.bbc.com/news/technology-51576445.

Bloomerg. (2018).The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Calugareanu, Ilinca. (2014). Chuck Norris contra el comunismo.

Carr, Jeffrey. (2009). Inside Cyber Wafare: Mapping the Cyber Underworld.

Clarke, Richard A. y Knake, Robert K. (2011). *Guerra en la red. Los nuevos campos de batalla*. Barcelona: Ariel.

Clausewitz, Carl von (2005). *De la Guerra*. Madrid: La Esfera de los Libros.

Colom Piella, Guillem. (2018), La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo. Revista Ejército nº933. https://www.seguridadinternacional.es/?q=es/content/la-doctrina-gerasimov-y-el-pensamiento-estrat%C3%A9gico-ruso-contempor%C3%A1neo

Cottam, Martha L.; Mastors, Elena; Preston, Thomas y Dietz, Beth (2016). *Introduction to Political Psychology*. New York: Routledge.

Dodge, Theodore Ayrault (2012). *Hannibal: A History of the Art of War among the Carthaginians and Romans down to the Battle of Pydna*.

Earle, Edward Mead. (1997). *Creadores de la estrategia moderna*. Buenos Aires: Escuela de guerra naval.

Habermas, Jürgen. (1997). La idea kantiana de paz perpetua. Desde la distancia histórica de doscientos años. *Isegoría*, 16, 61-90. https://doi.org/10.3989/isegoria.1997.i16.184

Heródoto (2006). *Historias*. Madrid: Cátedra.

Hesíodo. Teogonia.

Heuer, Richards J. Jr. (2013). *Psychology of Intelligence Analysis*. Martino Fine Books.

Higgins, Kelly Jackson. (2018). *Chinese APT Backdoor Found in CCleaner Supply Chain Attack*. https://www.darkreading.com/endpoint/privacy/chinese-apt-backdoor-found-in-ccleaner-supply-chain-attack/d/d-id/1331250

Hobbes, Thomas. (2018). *Leviatán*. BNarcelona: Ariel.

Hoffman, Frank G. (2012). *Hybrid vs compound war. The Janus choice: Defining today's multifaceted conflict*. https://www.semanticscholar.org/paper/Hybrid-vs-.-com-

SOC PRIME (2017). PETYA.A / NOTPETYA IS AN AI-POWERED CYBER WEAPON, TTPS LEAD TO SANDWORM APT GROUP. *SOC PRIME*, 2 de Julio. https://socprime.com/blog/petya-a-notpetya-is-an-ai-powered-cyber-weapon-ttps-lead-to-sandworm-apt-group/.

Stanton, Neville A.; Baber, Chris y Harris, Don (2008). *Modelling Command and Control: Event Analysis of Systemic Teamwork*. CRCPress.

Sun Tzu (2018). *El arte de la guerra*. https://www.amazon.es/El-Arte-Guerra-Sun-Tzu/dp/148407291X.

Symantec. (2010). W32.Stuxnet Dossier. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

Tanase, Stefan (2015). Satellite Turla: APT Command and Control in the Sky. *Securelist. Kaspersky's cyberthreat research and reports*. https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/.

Tucídides (1989). *Historia de la Guerra del Peloponeso*. Madrid: Akal.

United Nations, Office on Drugs and Crime. (2007). Definitions of Terrorism. https://web.archive.org/web/20071012230930/http://www.unodc.org/unodc/terrorism_definitions.html

Villalón, Antonio. (2016). *Amenazas Persistentes Avanzadas*. Valencia: Nau Llibres.

Wikipedia. Sarisa. https://es.wikipedia.org/wiki/Sarisa.

Wikipedia. Sarzana. https://es.wikipedia.org/wiki/Sarzana

Wilson, Thomas Woodrow. (1918). *Los Catorce Puntos*. https://www.dipublico.org/3669/catorce-puntos-del-presidente-wilson-1918/El texto anterior sólo ha sido posible gracias a una serie de personas, a las que quiero dedicar las siguientes palabras.