

**Omnium contra omnes**  
*Análisis político-militar  
de la guerra  
en el ciberespacio*

\* \* \* \* \*

*Joan Soriano Aguilar*

© Joan Soriano Aguilar, 2021

© De esta edición:

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

Nau Llibres apoya las leyes de propiedad intelectual que protegen a los creadores de contenido, fomentan la diversidad de ideas, estimulan la creatividad y favorecen el desarrollo de nuestra sociedad. Gracias por comprar una edición autorizada de este libro y por no reproducir, escanear ni distribuir ninguna parte de esta obra por ningún medio sin autorización previa. De esta forma, usted está respaldando a los autores y permitiendo que Nau Llibres continúe publicando libros. Diríjase a CEDRO (Centro Español de Derechos Reprográficos) si necesita utilizar algún fragmento de esta obra ([www.conlicencia.com](http://www.conlicencia.com); 91 702 19 70 / 93 27204 45).



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**

<b>1. Definiciones</b> .....	23
1. Nuevos medios para la guerra .....	23
2. El concepto de ciberguerra.....	24
3. Inicio y fin de la ciberguerra .....	29
<b>2. El por qué de la ciberguerra</b> .....	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
<b>3. Lo virtual</b> .....	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
<b>4. El ciberespacio como teatro de guerra</b> .....	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**

<b>5. La ciberguerra como conflicto asimétrico</b> .....	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
<b>6. Elementos del escenario bélico</b> .....	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
<b>7 Estrategia de ciberguerra</b> .....	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
<b>8 Estructura del ataque</b> .....	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

<b>9. Contrainsurgencia</b> .....	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
<b>Conclusiones</b> .....	181
<b>Anexo</b> .....	183
<b>Referencias</b> .....	203