

Advanced Sciences and Technologies for Security Applications

Manousos E. Kambouris

# Hybrid Warfare 2.2

Where Biothreats Meet Irregular  
Operations and Cyber Warriors in the  
21st Century

 Springer

# **Advanced Sciences and Technologies for Security Applications**

## **Editor-in-Chief**

Anthony J. Masys, Associate Professor, Director of Global Disaster Management, Humanitarian Assistance and Homeland Security, University of South Florida, Tampa, USA

## **Advisory Editors**

Gisela Bichler, California State University, San Bernardino, CA, USA

Thirimachos Bourlai, Department of Computer Science and Electrical Engineering, West Virginia University, Multispectral Imagery Lab (MILab), Morgantown, WV, USA

Chris Johnson, University of Glasgow, Glasgow, UK

Panagiotis Karampelas, Hellenic Air Force Academy, Attica, Greece

Christian Leuprecht, Royal Military College of Canada, Kingston, ON, Canada

Edward C. Morse, University of California, Berkeley, CA, USA

David Skillicorn, Queen's University, Kingston, ON, Canada

Yoshiki Yamagata, National Institute for Environmental Studies, Tsukuba, Ibaraki, Japan

## Indexed by SCOPUS

The series *Advanced Sciences and Technologies for Security Applications* comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)


Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

Manousos E. Kambouris

# Hybrid Warfare 2.2

Where Biothreats Meet Irregular Operations  
and Cyber Warriors in the 21st Century

Manousos E. Kambouris   
Department of Pharmacy  
University of Patras  
Patras, Greece

ISSN 1613-5113 ISSN 2363-9466 (electronic)  
Advanced Sciences and Technologies for Security Applications  
ISBN 978-3-031-60018-0 ISBN 978-3-031-60019-7 (eBook)  
<https://doi.org/10.1007/978-3-031-60019-7>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

*To the wilderness feline that marked my life*

*This book is dedicated to my precious Goldie  
for being inspiration, comfort and assistance*

# Foreword

This book is written less as an academic textbook and more as a guide to factuality or prospects, due to the widespread interest of concerned individuals active in all fields of everyday life regarding security, defense and the hitherto ignored *bio-* dimension. It is meant also to instigate a more specialized interest within the security community, taken in the widest possible context, who developed, especially after the COVID-19 an interest on biological issues pertaining their sectors and fields of interest, which is perhaps a fitting definition for biosecurity. The different aspects of biosecurity as causally interacting and interrelating with actual and emerging defense and security issues are the main issue here; such aspects have been up to now examined in a most passing and casual way within the original and innovative concepts of biosecurity. As a result, the book focuses on the assets, liabilities, synergies and incompatibilities of the different sectors expected to define the hybrid threat from now on. These include, without being restricted to, missile-centric warfare, the explosive development of drones of every kind and size and the increased dependence on IT amenities. The defense issues may be approached easily through the Internet in a basic search and are thus used with the least development. On the contrary, the bioscientific issues need some deeper knowledge to pursue and are thus more meticulously referenced.

Patras, Greece

Manousos E. Kambouris

# Preface

The setting of hybrid warfare, a contemporary description of an ages-long approach to warfare and power struggles, changes dramatically due to emerging technologies. This has always been so. The current iteration, though, allows unprecedented destructiveness, as it integrates potent conventional weapons, biological agents, cyber-operations in the virtual and real world and the classical leverage of displaced/moving populations, possibly enhanced with cultural warfare endeavors and false-flag or secret operatives of the private -or otherwise beyond the state- sphere. The combination of all these attributes allows for a range of options for both state and non-state players that may escalate to extinction-level events, these being GCBR as has been the COVID-19, or other similar or dissimilar events. And the possibility of escalation increases due to the interdependence of the different attributes of entities such as all-out war, terrorism, proxy-war or the other-than-war operations (a euphemism for international policing/enforcement).

The nanotechnology allows, if applied to biowarfare context, the dispersed or focused contamination of targeted populations by the delivery of propagating or non-propagating agents, or by enhancing the normal dissemination of contagious diseases to levels unattainable by natural events. The noise in surveillance policies and patterns caused by mass illegal immigration perplexes the problem of vigilance, identification and, most of all, of containment. The deterioration or outright destruction of infrastructures by conventional or asymmetric effectors may amplify naturally occurring biorisks out of proportion, as happened in Iraq in the 90s; with *engineered* biothreats this may only worsen.

Last but not least, cybernetics may tap onto public health networks and databases, manipulating identification, diagnosis and treatment protocols and the prescription routines, or falsifying the electronic health files of patients. This may lead to multiple, untraceable events of erroneous and possibly fatal administration of drugs, with



enormous monetary cost for whole societies and massive disruptive effect, ultimately leading to real-life endangerment the physical, and social, survival of multi-million populations.

Patras, Greece

Manousos E. Kambouris

**Acknowledgements** To Prof. George P. Patrinos and Senior Researcher Yiannis Manoussopoulos, for their active support. Without them this endeavor would have been unaccomplished

# Contents

<b>1</b>	<b>Introduction: Hybrid Warfare 2.2</b>	<b>1</b>
1.1	Introduction	1
1.2	Hybrid Warfare 1.0	2
1.3	Hybrid Warfare 2.0	4
1.4	Hybrid Warfare 2.1	6
1.5	Hybrid Warfare 2.2	8
	References	9
 <b>Part I The Impact of Bioagents in Irregular Warfare</b>		
<b>2</b>	<b>Irregular Operations and the Biothreat</b>	<b>13</b>
2.1	Introduction	13
2.2	Contemporary Examples	17
2.3	The Cliff Straight Ahead	19
2.4	The Hybrid Operators Aspect	23
	2.4.1 Special and Secret Warfare Operatives	23
	2.4.2 Non-state Affiliated Agents	25
	References	27
<b>3</b>	<b>Cyber Warfare and the Biothreat</b>	<b>31</b>
3.1	Introduction	31
3.2	The Liabilities and Threat Potential	33
3.3	Areas of Convergence and Liabilities	35
3.4	Something to Mull and Ponder	40
	References	41

**Part II The Bioagent in Conventional and New Age Warfare**

**4 Conventional Operations and Means Incorporating Bioagents as Partial Effectors** ..... 47

4.1 Introduction ..... 47

4.2 Offensive Options and Delivery Practices and Means ..... 50

    4.2.1 Infection Techniques ..... 51

    4.2.2 Contamination Techniques ..... 52

    4.2.3 Dispersion Patterns ..... 53

    4.2.4 Dispersion Means ..... 54

4.3 Prevention-Intervention ..... 56

    4.3.1 ISR Drones ..... 58

    4.3.2 Decon(tamination) Drones ..... 58

    4.3.3 Interceptor Drones ..... 59

    4.3.4 Drug Delivery Imitated ..... 60

4.4 The Run for Diagnostics ..... 61

References ..... 64

**5 Introducing the Nano-dimension: The Biote-Bot Hybrid** ..... 69

5.1 Introduction ..... 70

5.2 Controlled Release Patterns ..... 72

5.3 The Cybernetic Dimension (Bot) ..... 72

5.4 The Microbiote (Biote) ..... 75

5.5 Defying Bio-surveillance and Diagnostics ..... 77

5.6 Countermeasures: Contemplating the Options ..... 78

References ..... 83

**Part III An Infernal Match-Making**

**6 Integrating the Two: A Technical Aspect** ..... 91

6.1 Introduction ..... 91

6.2 The Means ..... 92

    6.2.1 The IXD Revolution ..... 92

    6.2.2 Patch Deliveries of Toxins ..... 95

    6.2.3 AI-Enabled Personalized Bioassaults ..... 96

    6.2.4 Dogs, Sharks and Birds ..... 98

6.3 The Operator/Warrior ..... 99

    6.3.1 Hybrid Warfare Operatives/Warriors ..... 100

    6.3.2 The NBC Troops ..... 102

    6.3.3 The Biowarrior ..... 103

6.4 Binary Assets ..... 111

    6.4.1 Homologous Binary Assets ..... 112

    6.4.2 Heterologous Binary Assets ..... 114

6.5 Nightmare or Just Dystopia? ..... 116

References ..... 117

- 7 Integrating the Two: An Operational and Strategic Aspect** ..... 123
  - 7.1 Introduction ..... 123
  - 7.2 The Matrix Effect ..... 124
  - 7.3 The Epidemic Dimension ..... 126
    - 7.3.1 The Frangible Threat: Shooting Death ..... 127
    - 7.3.2 The Rabid Menace ..... 130
    - 7.3.3 The Lever(Age) ..... 132
  - References ..... 135

**Part IV Beyond the Current**

- 8 The GCBR After COVID-19** ..... 143
  - 8.1 Introduction ..... 143
  - 8.2 Setting the Object ..... 145
    - 8.2.1 Globality, Universality or Something Planetary? ..... 146
    - 8.2.2 Singularity Versus Multiplicity ..... 148
  - 8.3 Enter Biology ..... 152
    - 8.3.1 Specifics, Characteristics and Iterations of Life ..... 152
    - 8.3.2 A Gap—or a Matter—of Generations ..... 153
    - 8.3.3 Defining Priorities and Semantics: Generations, Categories, Classes and Abbreviations ..... 159
    - 8.3.4 A List Too Long... or Not Long Enough? ..... 165
  - 8.4 How Bad is a Catastrophe? ..... 167
  - 8.5 Preparedness and Response ..... 168
  - 8.6 A Matter of Community or Individual(s)? ..... 170
  - 8.7 To the Next X-demic ..... 172
  - References ..... 175

- 9 Reforming the Past** ..... 187
  - 9.1 Introduction ..... 188
  - 9.2 Recasting the Past ..... 191
    - 9.2.1 The Historic Background of Foreigners in Greek Battlefields ..... 192
    - 9.2.2 Genography and Actuality ..... 196
    - 9.2.3 Rejecting the Obvious ..... 198
    - 9.2.4 The Winning Hand ..... 199
    - 9.2.5 An Exercise in Revisionism ..... 201
  - 9.3 Turning the Ploughs into Swords and the Keyboards to Explosives ..... 203
  - References ..... 205

# Chapter 1

## Introduction: Hybrid Warfare 2.2



**Abstract** The notion of hybrid warfare, implying the use of means not counted amongst the weapons already known or conventionally accepted, or even understood, has been a steady tendency in human history since the earliest recorded struggles. But both its means and the degree of their integration to normal policy and warfare practices change. From paid agents and spies through special operators and assassins, the first iteration was concluded with the advent of international bodies claiming impartiality but favoring selected players. The addition of the cyber dimension, which dissociates operations from spatial limitations regarding distance in 3-D settings and the insertion of the new guise of bioagents, with the full force of synthetic biology, which democratized/dispersed genetic engineering and xenobiology, unmistakably create a much more risky and complex operational continuum that exponentially increases possibilities, opportunities and global risk.

**Keywords** Financial warfare · Special warfare · Government toppling · Regime change · NGO · International organizations · Biowarfare · Cyberwarfare · Electronic warfare

### 1.1 Introduction

The term *Hybrid Warfare*, incorporating all forms of war and all non-war and other-than-war approaches in succumbing a prospective contestant's will to refuse a given agenda, is rather new; it coincides with the other-than-war/humanitarian/peace support operations that started in the 90s that established the (western) rules of the new world order over the unipolar world that surfaced once the Cold War had died out [15].

## 1.2 Hybrid Warfare 1.0

The concept though is much older, as there are similar ideas and concepts throughout history. Tainting missiles, mainly arrows and javelins, with animal or plant poisons for hunting is lost into the mists of time, along with the use of the occult, either to raise morale or to precipitate submission. The Seven Military Classics of ancient China [23] provide ample examples: the first book, the Tai Kung, is a veritable handbook for undermining societies to effect a regime change. The Sun Tzu directly instructs to use agents (the term “spies” is perhaps a suboptimal translation, given the meaning) near the enemy sovereign, not only to learn his mind but also to affect his judgment. In the Bible similar practices are mentioned in the campaign against Jericho, where spies were introduced to make contact with disgruntled social strata (Rahab, a whore) so as to facilitate the undermining of the defenses (Joshua 2:1).

Leveraging the public of a foreign state to attain acceptance or submission is within the methods to be used for regime change, since the myth of Danaus (Apollod 2.1,4) and for submission of enemy polities or to sow discord and blunt an enemy: in the Trojan war lore, the Hero Palamedes was wrongfully but believably accused (actually framed) as a Trojan agent (Apollod E.3,8). Later literature makes clear how bribes and enforcers were used by the Persian Empire for conscripting social and political agency to subdue its enemies and promote its interests and influence, as were the bribes that sparked the Corinthian War as a diversion to the Spartan invasion under King Agesilaus in 394 BC (Xen Hell 3.4,1) and the notorious *hetera* Thargelia who brought about the Medism of Thessaly with no blow exchanged just before the invasion of Xerxes in 480 BC [26].

Such practices went on throughout written history in all latitudes and longitudes, with the European paradigm being none other than Niccolo Machiavelli, with his two works, *The Prince* (1513) and *The Art of War* (1519–20). Being usually assigned to political science (at least “*The Prince*”), these two works interrelate to delineate how unscrupulousness would make a polity successful in (formal) war and peace, and thus dwell in the hard core of the Hybrid Warfare concept; with more or less success in terms of immediate and long—term results. Occasionally, the two differ greatly; a near-term success was proving counterproductive in the long run. The most blatant such case must have been the support of the Bolsheviks by Imperial Germany to make the Russian Empire succumb and then accept defeat in 1917 and sign the Brest-Litovsk treaty [27] which crippled Russia, only to find the new communist regime fighting against its reborn Nazi spawn in the WW II.

All these could be classified under Hybrid Warfare (HW) 1.0. Different methods and ideas were usual, but never changed the basic idea: an interplay (or fighting) of polities and governments, possibly by proxies and in many cases by fifth columnists. But the actors were state entities (*sensu lato*). The statehood could be actual, as happened in most cases (the subversion of North Vietnam against the South Vietnam was a contest between two fully formed and internationally recognized, sovereign states) or prospective (as in revolutionaries, rebels and insurgents; them being secessionist as the Confederates in the 1860s’ American Civil War; or not, as the Greek

Communists in the great insurgency of 1944–49). But somehow the actors were affiliated to a state—or sub-state—entity, actual or prospective.

The notion of Information Warfare [25] is equally ancient, possibly primordial in inception and focuses on creating convenient realities to attain one's purpose through the active assistance, support or at the very least tolerance of others. In different times and polities it is described by the diminutive but very suitable term “propaganda”. Propaganda wars were always an integral part of the hostilities, especially in wars waged by Empires. The propaganda has to belittle the enemy, to muster public support for a given cause and thus proactively quell public discontent and wariness for sacrifices of all kinds, prevent drop of morale, discourage cooperation or even tolerance for the enemy and embed a notion of discipline. It is also expected to do exactly the opposite to enemy audiences, both military and civilian, and although modern equipment and methods are light-years more advanced and effective, there were mechanisms, as for example the monumental architecture, that were driving such messages home. Splendor and grandness were just two... The culturomics in their humanities' version (not the microbiological one) were also employed. The cry “Infidel” from both clashing contestants, Christendom and Islam, had a precedent, with one side slandering the morals, the culture, the achievements and the beliefs and customs of the other; the Behistun inscription shows such a monarch, Darius I, launching religious libels to insurgents.

The HW 1.0 uses every deviousness of the human political and technical genius but for the EM spectrum and the globalist intervention, and thus is still in widespread use, whenever an interested party does not partake in the latter and does not excel in the former. The short-lived but remarkable Wagner Mutiny (or Prigozin mutiny, by the name of the head of the Private Military Company “Wagner”) in 2023 [6] was nothing essentially different from Byzantine plots, or the notorious incident of the Silver Shields of Eumenes of Cardia at Gabiene, 316 BC favoring Antigonus the one-eyed (Diod 19.42–43); had it been genuine. Had it been a hoax, it stems directly from the pages of Herodotus, as in the stratagem of Zopyrus (Hdt 3.153–158) and the lore of the Trojan War (Apollod E.5,14–18).

The other-than-war operations were very old inventions too. Achaemenid Persia, Athens, Rome, the Ottoman Empire, planted nuclei of own citizens to the lands of subjects, as did the Russians; it was an internal colonialism to ensure the occupation. This refers not to the satisfaction of land hunger, which meant the migration of social strata (as in the 2<sup>nd</sup> colonial wave of the Greeks in the eighth-sixth centuries BC) or of whole peoples, as the Sea Peoples in twelfth century BC according to the Egyptian records, but to controlling occupied territories. Rather than planting forts and garrisons, as did the US Army at the Forts that dotted the frontiers in the nineteenth century, and the British Army throughout the Empire, a social cell was transplanted, granted civic status and provided garrison and expeditionary troops with local knowledge, affiliations and very low cost for the public coffers; they were supported by the economic activity they were engaged into, and procreated locally a next generation of subjects and troops.

The environmental attacks, in practical and symbolic versions, have also been an element of HW 1.0. The wildfires and urban fires burning rampant the last years are

occasionally attributed to external subversion or internal undermining; one of the most hardly hit countries in both respects had been Greece, with one foreign power claiming openly responsibility for at least the great fires in east Aegean islands in the 80's and 90s<sup>1</sup> and another considered culprit for arson in four important native corporations in the 80s in urban environment.<sup>2</sup> The double fiery attacks, of 2008 against the forestry and rural environment, with some 100 dead, and of 2009, in the city of Athens, may be linked to foreign instigators and some imported agents but the actual operational base, in terms of personnel, equipment, planning and basing/facilities/refuges and lairs qualifies for nothing but native agency; although *sensu lato*, due to the possibility of large numbers of illegal immigrants participating in both events. Whether the California fires and the Australian bushfires (of 2020 and 2019–2020 respectively) qualify for asymmetric warfare, as was the case in Greece during the 80s, is to be resolved by the local authorities. But the desertification was understood as an act of total war, both in ancient Greece [12] and medieval Europe, with Attila allegedly declaring “From where I pass not even grass ever grows after”.<sup>3</sup> Similarly, massive incendiary attacks in urban, rural or natural environments were considered irregular operations, the causality of which must be denied as is the case of Sphacteria (Thuc 4.30,2) or incurs violent retribution, divine in the case of the Spartan King Cleomenes I who incinerated the sacred Argive grove (Hdt 6.75) or human, as was the burn of Athens by Xerxes I to avenge the burning of Sardis by the Ionian rebels and their Athenian allies (Hdt 5.100–102), and the burning of Persepolis by Alexander III the Great to avenge the burning of Athens (Diod 17.70–72).

### 1.3 Hybrid Warfare 2.0

Thus, the Hybrid Warfare 2.0 that may be dubbed “Unipolar Anarchy” emerged at the end of the twentieth century, when shadowy NGOs with no obvious or direct country affiliations (as the name implies) but occasionally aligning to some state player [3] joined the previously available, multi-nation sanctioned international organizations that offered a globalized network of covert power projections by engineering civil unrest or, in less cases, by actually assisting a population. The subversive dynamics however seem to favor assisting a given social group within a state or a population, either to annex it or to cause some kind of social and political friction. The idea to subvert national sovereignty for some or other international or anational directorate, to be true, had been already tried, at first by international alliances such as the Holly

---

<sup>1</sup> *Former Turkish PM's arson admission fuels anger* (2011) *ekathimerini*. Available at: <https://www.ekathimerini.com/news/137956/former-turkish-pms-arson-admission-fuels-anger/>.

<sup>2</sup> *Fire gutted two of Greece's largest department stores today* (1980) *United Press International*,. Available at: <https://www.upi.com/Archives/1980/12/19/Fire-gutted-two-of-Greeces-largest-department-stores-today/3890346050000/>

<sup>3</sup> <https://www.sutori.com/en/story/attila-the-hun--zaSpr9ne2P9yZLUV1kaHG4Hd>.



Alliance in the nineteenth century<sup>4</sup> to be followed by “societies” and “communities” of nations: from the League of Nations of the early twentieth century to the UN and its tail of “World” organizations.<sup>5</sup> Perhaps the original case of Hybrid Warfare 2.0 is the Korean War, where no multinational alliance went to war for the westernizers; but an international organization (the UN) did so, manipulated by a (group of) state(s) that intervened openly, officially and militarily<sup>6</sup>—nothing short of a formal declaration of war between states.

As this kind of constitutional aggression was followed only 40 years later, with the coalition of the Second Gulf War of 1991, the recipe had not been very successful in a bipolar world bristling with nuclear weapons. On the other hand, with the danger of a massive escalation gone, it was evolved and adjusted after the end of the said period. First in 1999 in Kosovo, with the instrumentalization of a minority that was attempting secession in favor of a hostile state. The case was too similar to the US colonists of Texas in the late nineteenth century, who, after being established in Mexican territory, decided that they wanted to be under US flag and sovereignty, they and *their* lands and estates which were in the realm of Mexico. But in the 1999 case it was not the state sponsor of the separatists that attacked in their support. A international alliance (NATO) foreign to both parts went to unprovoked aggression against a sovereign state by self-assuming the role of international policeman, and finally enforced the secession.

A further iteration came by NGOs manipulating regime changes through ingenious application of social mechanics, or simply bringing chaos, to targeted nations. The regime change cases are exemplified by the Color revolutions of the first decade of the twenty-first century in former Soviet republics and with the Arabian Spring of the second decade. The chaos caused dwarfs the riots in Athens, Greece, in December 2008 by native anarchists supported by similar groups from abroad entering the country massively, especially through Italy by ferry boats, following—perhaps incidentally—an obviously too Russophilic policy of the then Greek administration.

Another round of incidents was instrumentalizing massive populations of immigrants. Migrations of sixth century AD and of eleventh century BC were destructive to some polities; but were not orchestrated by some foreign mastermind. On the contrary, in 2019–20 there was a state sponsored wave—almost a direct, open and violent invasion—of many thousands of Asian immigrants from Turkish soil to the northern and eastern Greek territories, reminiscent of scenes of direct assault. Still of undeclared mastermind are the repeated riots—to the point of failed revolutions—in France, first in 2005 and then in 2023, by second and third generation immigrants. Much less intensive but extremely tell-tale were the pro-Ukrainian riots occurring in 2022 in European countries by Ukrainian refugees and immigrants who were actively assaulting whoever was unsupportive to Ukraine.

And the most asymmetric is of course the use of private and financial establishments. Although the West India Company had a peer- to -statehood position in

---

<sup>4</sup> <https://www.britannica.com/topic/Holy-Alliance>.

<sup>5</sup> <https://www.un.org/en/about-us/un-system>.

<sup>6</sup> <https://www.unc.edu/History/1950-1953-Korean-War-Active-Conflict/>

the eighteenth century, the multinational corporations of the twentieth century that effected regime changes and wholesale wars [16] were something new. This is especially true if they are apperceived as a trading-credit complex with an ever-pervasive network of banks and other financial institutions that may carry out financial wars on an unprecedented scale [5]. The well-orchestrated such war of Alexander the Great against the most powerful weapon of the achaemenid empire, its huge gold reserves [14], dwarfs in comparison to twentieth century such operations of the US against communist Cuba, Iran and North Korea [20] and the twenty-first century—rather ineffective but massive—sanctions since 2022 against Russia [9].

## 1.4 Hybrid Warfare 2.1

The Hybrid Warfare 2.1 refers to the abject space. In essence it started with the radiowaves that shortened the physical dimensions of the battlefield, but they just shrank them, and not uniformly; a grunt has still the same means to cover a given distance on foot. The radiowaves are invisible, but abide to spatial rules, such as dispersion, scatter, dying out/decaying, distance covered per time etc. Thus, the electronic warfare is a different kind, not a different dimension of warfare with the literary meaning of the word “dimension”, as used in the “3-D world”.

What is really a paradigm change is the creation of cyberspace, which in essence twists the conventional space. It is not something concerning “remoteness”, but something creating another space altogether. A power facility can be blown not by remote guiding some terminal effector, but by simply de-calibrating its control elements through network attacks. Firewalls do not exist nor do they produce any kind of smoke in reality, no one can pinpoint them with map or GPS. They exist in the cyberspace. When there were mainframes and desktops and local networks, a part of the cyberspace could be folded into the circuitry of the related machines. Once world-wide web nets and, more importantly, Clouds came on-line, the Cyberspace became even more abstract.

Conventional wisdom puts the beginning of the Electronic Warfare to WW II, regarding both intelligence (as with interception of radiosignals, especially of communications) and sensor systems, with the RADAR (RADio Detection And Ranging) being the most prominent but not the only one. Guidance systems were also developed, with the German *Knickebein* and *X-Gerät*<sup>7</sup> remote navigation for bombers, based on the convergence of two different radiosignals over the target in early WW II. The electric propulsion of torpedoes does not fall in this category, as there were no interception, apprehension, jamming or decision functions. On the contrary, the introduction of remotely operated missiles, as the wireless German F-X guided bomb<sup>8</sup> and robot vehicles, as the explosives—laden wire-guided German

<sup>7</sup> <https://www.balsi.de/weltkrieg/waffen/sonderwaffen/luftwaffe/xgeraet+knickebein.htm>

<sup>8</sup> [https://airandspace.si.edu/collection-objects/bomb-guided-ruhrstahl-fritz-X-X-1/nasm\\_A19710760000](https://airandspace.si.edu/collection-objects/bomb-guided-ruhrstahl-fritz-X-X-1/nasm_A19710760000).

“Goliath”,<sup>9</sup> coupled to the progress in fuzing and guidance systems, counts: examples range from the German magnetic sea bottom mines to the proximity-fuzed AA ammunition of the Allies<sup>10</sup> which were fired under radar fire control and were set electronically. Actually, these interactions rather than simple functions define the existence of Electronic Warfare, and as a result the most prominent applications in WW II were the signal interception and jamming techniques (with radar receivers, active jammers and chaff dispensers for the radar, and with paints absorbing the IR signal, such as used in German subs) and the massive demagnetization provisions in Allied ships and German tanks.

In all honesty, it may be argued that if the last aspect is taken, the first instance of Electronic warfare might have occurred much earlier: during the 1912 First Balkan War, a crewmember (most probably officer) of a French ship moored at the port of Thessaloniki (while still part of the Ottoman Empire) tuned in to the frequencies used by the Hellenic Royal Navy, at the time a pioneer in using wireless telegraph for fleet communications, and by producing loud mechanical noise effectively interrupted such communications. The incident is very ill-documented, almost to the verges of legend, but some details of the naval operations in that very war lend it credibility.

After WW II and during the Cold War the HW 2.1 came to age. Computers, being introduced during the war but in a local fashion, became networked and thus, by combining electronics (not mechanics, as in older calculating and computing systems) with telecommunications came the cyberspace during the 80s as a parallel universe to the known 3-D one. In between, but definitely post WW-II there was the autonomy revolution, where autonomous robots (such as the early drones, with pre-arranged course and mission parameters) and the self-guided missiles (with onboard processors and decision logic) constituted an early form of smart machines. The alleged almost automated aerial interception by manned fighters which would be controlled from GCI<sup>11</sup> facilities with the pilot simply overseeing the process and only occasionally intervening [11], if accurate a description, was definitely a most illustrative example. The support, protection and optimization of such processes and, on the other hand, any possibility to interrupt them created the combined electronic and cyber warfare spectrum, the former coinciding with the 3D spatiotemporal continuum as we apperceive it and live in it, the latter in a virtual, parallel universe with relaxed (but rigid, nevertheless) spatiotemporal association with the former. The “relaxed but rigid” clause should be understood as the rigid need of processing and input amenities, even to access the Infosphere; these amenities exist within the 3-D reality. On the other hand, what happens at someplace, for example the 2003 NE blackout (a massive failure of the electricity networks over North America<sup>12</sup>), may have been caused by an event either far away, to some remote server, or in the virtual world, where information and commands exist in cyberspace.

---

<sup>9</sup> <https://www.warhistoryonline.com/weapons/goliath-tracked-mine.html>.

<sup>10</sup> <https://www.historynet.com/proximity-fuze/>

<sup>11</sup> <https://academic-accelerator.com/encyclopedia/ground-controlled-interception>

<sup>12</sup> <https://www.electricchoice.com/blog/worst-power-outages-in-united-states-history/>

Within HW 2.1 one may recognize an ever-enhanced strive for more complicated trans-domain concepts, beyond the, but possibly interacting with, cyberspace. These are within the 3D volume and world, but they cause some challenges due to their peculiarities. Such domains include subterranean warfare, extreme environments, space, and deep sea/seabed confrontation.

## 1.5 Hybrid Warfare 2.2

The Hybrid Warfare 2.2 incorporates the biological factor. It has been done before, with spiking wells (Thuc 2.48, 1–2.) or releasing rats carrying tularemia [2, 7]; not to mention poisoned arrows, the infamous “Parthian shot” [21]. It is recorded since the earliest myths; the Greek arch-hero Hercules painted with poisonous biotoxins—as opposed to venomous ones [17, 21]—the points of his arrows (Apollod 2.5). The practice was discontinued and embargoed into the next generation, as suggested in the *Odyssey* (Hom ii-259/263), but with some exceptions, as was Hercules’ follower Philoktetes who inherited and used in combat his tainted arrows (Hyginus Fab 114; Hom II-718; Apollod E.3,27). This is comfortably well beyond the tenth century BC. Similarly, the same epic tradition refers to abrupt outbursts of epidemics, for the treatment of which physicians took exorbitant rewards, including large parts of the secular powers of a given polity, as is the case with the seer Melampus (blackfoot) in Argos [22]. The concept directly implies the use of some intoxicant and then its remedy, the latter being either the discontinuation of the use of the agent, if it was operating in a dose-dependent decaying curve manner; or by the introduction of its antidote. Similar epidemics-on-order are reported in the *Iliad* (Hom I-35/53), not to forget the Plagues of Egypt (Exodus 9:1-12 and 11:1-12.36). Thus the use of bioagents within the full context of the hybrid warfare is nothing new, and the military dimension in countering epidemics (of natural or perpetrated causes) is a given [4].

What is new is the current iteration of hybrid warfare and how it may incorporate bioattacks. It is the first time that the biological factor is used on top of the HW which had just expanded into the cyber dimension and off the state of the unipolar anarchy. The biotic effectors may target every living entity but also materiel of diverse origin and manufacture [10]. Without ever raising a syrx, natural procedures, conceivably not even of infective nature, may culminate to massive health casualties through the use of bioscientific knowledge and intelligence through digital effectors only [13]. The scale of artificial life, as in Xenobiology, is unprecedented and allows many sinister thoughts and dark temptations [1, 8, 18, 24]. Last and most exotic, but by no means least, is the combination of BW agents with cyborgs [19]. This could well become a most sinister but, unfortunately, indispensable tool for Other-Than-War operations where lethal scale of violence is regularly authorized but needs to be applied subtly, discreetly and, still, extremely massively and effectively.

## References

1. Acevedo-Rocha CG, Budisa N (2016) 'Xenobiotechnology: a roadmap for genetic code engineering. *Microbial Biotechnol.* John Wiley and Sons Ltd 9(5):666–676. <https://doi.org/10.1111/1751-7915.12398>
2. Alibek K, Handelman S (1999) *Biohazard: the chilling true story of the largest covert biological weapons program in the world—Told from inside by the man who ran it.* Random House, New York, NY
3. Banks N, Hulme D, Edwards M (2015) NGOs, states, and donors revisited: still too close for comfort? *World Dev* 66:707–718. <https://doi.org/10.1016/j.worlddev.2014.09.028>
4. Biselli R et al (2022) A historical review of military medical strategies for fighting infectious diseases: from battlefields to global health. *Biomedicines.* <https://doi.org/10.3390/biomedicines10082050>
5. Bracken P (2007) *Financial Warfare*, Foreign Policy Research Institute. Available at: <https://www.fpri.org/article/2007/09/financial-warfare/>
6. Clarke C (2023) Following Prigozhin's aborted mutiny, what will happen to the Wagner Group? Foreign Policy Research Institute. Available at: <https://www.fpri.org/article/2023/07/following-prigozhins-aborted-mutiny-what-will-happen-to-the-wagner-group/>
7. Croddy E, Krčálová S (2001) Tularemia, biological warfare, and the battle for Stalingrad (1942–1943). *Military Med.* Association of Military Surgeons of the US, pp 837–838. <https://doi.org/10.1093/milmed/166.10.837>
8. Diwo C, Budisa N (2018) Alternative biochemistries for Alien life: basic concepts and requirements for the design of a robust biocontainment system in genetic Isolation. *Genes.* MDPI AG 10(1). <https://doi.org/10.3390/genes10010017>
9. Elliott L (2023) The west's tightening of Russian sanctions is a sign of failure. *The Guardian*, 21 May
10. Gottschalk R, Preiser W (2005) Bioterrorism: is it a real threat? *Med Microbiol Immunol* 194(3):109–114. <https://doi.org/10.1007/s00430-004-0228-z>
11. Ground-controlled-interception (no date) academic-accelerator. Available at: <https://academic-accelerator.com/encyclopedia/ground-controlled-interception>
12. Hanson V (2006) *A war like no other.* Random House Publishing Group
13. Hatzis I et al (2023) Cyberbiodsecurity: the threat of the sages. In: Kambouris ME (ed) *Biosecurity in the making: the threats, the aspects and the challenge of readiness*, 1st edn. Taylor & Francis Ltd, pp 119–132
14. Hiliopoulos GZ (2003) *The unknown alexander.* Communications SA, Athens
15. Hoffman F (2007) *Conflict in the 21st century: the rise of hybrid wars.* Potomac Institute for Policy Studies, Arlington, Virginia
16. Jansen K (2023) Banana wars and the multiplicity of conflicts in commodity chains. *Revista Europea de Estudios Latinoamericanos y del Caribe/European Review of Latin American and Caribbean Studies.* In: Striffler S et al (ed) *Centrum voor Studie en Documentatie van Latijns Amerika (CEDLA)*, (81), pp 97–113
17. Jared C, Mailh-Fontana P, Antoniazzi M (2021) Differences between poison and venom: an attempt at an integrative biological approach. *Acta Zoologica.* Wiley 102(4):337–350. <https://doi.org/10.1111/azo.12375>
18. Kambouris M (2021) Bio-offense: black biology. In: Kambouris M (ed) *Genomics in biosecurity*, 1st edn. Elsevier Academic Press, London, pp 109–126
19. Kambouris ME et al (2023) The biote-bot hybrid. The ultimate biothreat merging nanobots, AI-enabled cybernetics and synthetic biology. *Future Medicine AI.* *Future Med* 1(1):FMAI4. <https://doi.org/10.2217/fmai-2023-0008>
20. Kessler E (2022) Working paper: Chicago Council on Global Affairs
21. Mayor A (2008) *Greek fire, poison arrows, and scorpion bombs.* The Overlook Press, New York