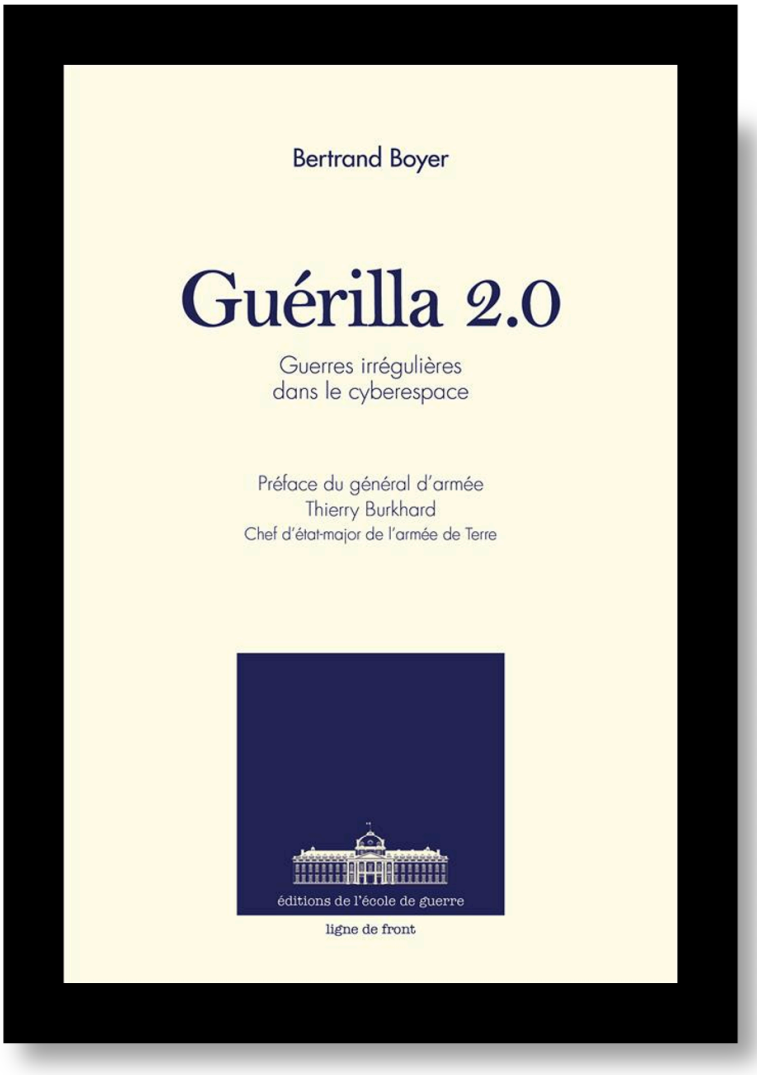
February 2025

BOOK OF THE MONTH

Security & Defence



Reviewed by : ***Julien Debidour Lazzarini***

Summary :

In *Guérilla 2.0*, Colonel Bertrand Boyer analyzes the evolution of modern conflict in the digital age. Cyberspace has become a strategic battlefield where information manipulation, cyberattacks, psychological actions and operations in cognitive fields are interwoven through the semantic layer of cyberspace

Inspired by French military doctrines and the history of guerrilla warfare, this new form of warfare, dubbed *digital guerrilla warfare*, exploits the vulnerabilities of connected societies to spread panic and weaken political cohesion.

This book highlights the importance of adopting an offensive posture, exploiting the opportunities offered by technology to counter these threats. The development of a doctrine of *counter-guerrilla warfare 2.0*, making it possible to infiltrate, neutralize and disrupt adversary networks while protecting critical infrastructures, is vital, as is international cooperation and strategic adaptability, in order to master this new environment and respond effectively to the challenges posed by hybrid and asymmetric warfare.

Key words :

Cyberspace, digital guerrilla warfare, disinformation, cyberattacks, psychological action, counter guerrilla 2.0, hybrid warfare.

Table of contents

Introduction to Guerrilla 2.0 **4**
A pioneering work : contextualizing the new paradigms of warfare in the digital age **5**
I. Biography **7**
a. An operational and technical curriculum, from Saint-Cyr to Télécom ParisTech *8*
b. A pioneering role in shaping cyber « à la française *8*
c. A return to field command after his years on the staff *9*
II. Writing context **10**
a. Hybrid warfare or hybrid threat : a revolution in confrontation? 11
b. The digital technostructure, a lever of power at the heart of geopolitical rivalries *14*
c. A necessary response to technological and societal changes, and the need for a legal framework for allocation *17*
III. Author's thesis **22**
a. Cyberspace as a hybrid strategic battlefield *23*
b. Guerrilla warfare 2.0 : a digital extension of historical insurgencies *29*
c. The invariants of warfare and their adaptation to the digital age *34*
IV. Food for thought **34**
a. The need for national resilience and the integration of a digital counter-guerrilla strategy *35*
b. Modernizing legal and organizational frameworks as a key to national security *37*
c. Investing in education, innovation and shaping tomorrow's military doctrines in the age of cyberspace *38*
Conclusion **39**
References **40**

Introduction to Guerrilla 2.0

« Guerrilla warfare 2.0 is not a substitute for traditional methods of war or protest, but rather a complement to them, opening up a new field of conflict for modern armies. [...] More than ever, Colonel Bertrand Boyer invites our armies to think of cyberspace as a new environment of confrontation, where the principles of war as we know them must be applied. [...] Beyond classic, kinetic actions, we must now be able to combine our effects with cyberspace and the information field ».

Colonel Bertrand Boyer's third book opens with these words from General Thierry Burkhard, then *Chief of Staff of the French Army (CEMAT)*. There is no doubt that this avant-garde work, published in 2020 and exploring the tactical and strategic dimensions of immaterial fields and *irregular operations below the threshold*, is in line with the innovative strategic vision of Army General Burkhard, appointed *Chief of Staff of the Army (CEMA)* on July 22, 2021, notably within his famous triptych entitled *Competition - Contestation - Confrontation.*

Winner of the Cyber 2021 Book Prize awarded by the *International Cybersecurity Forum* and published by *the École de Guerre*, *Guérilla 2.0: guerres irrégulières dans le cyberespace (Guerrilla 2.0: irregular warfare in cyberspace*) by Chef de Corps Bertrand Boyer is a work perfectly in tune with the times. With 10 chapters spread over 347 pages, this dialectical handbook develops a well-argued historical analysis, blending human and social science concepts with cybernetic tools, with a view to providing a clear vision of what *a « counter-guerrilla 2.0 »* strategy might look like.

A pioneering work : contextualizing the new paradigms of warfare in the digital age

« War is a simple art of execution », Napoleon Bonaparte [1].

Following the military operation launched by Russia in Ukraine on February 24, 2022*; emblematic of the evolution of warfare towards hybrid operations (mixing military and paramilitary actions);* or irregular conflicts between Israel and terrorist organizations such as *Hamas* or *Hezbollah ; symbol of the war of the weak against the strong ;* this dense treatise explores the nature of new modes of confrontation, the emergence of threats and conflicts fostered by information and communication technologies *(ICTs)*, and the new frontiers imposed by the information society and social networks, such as digital battlegrounds.

Immaterial fields, and within these mainly cyberspace, are today increasingly preponderant battlefields at the heart of modern conflicts. At the crossroads of digital, psychological and technological dimensions, actions in the cyber field enable militant protagonists or militant groups, though materially and

demographically weaker, to act in a blurred environment where geographical and political boundaries are broken.

Colonel Boyer describes this era *in* which *« the battle is no longer fought on a closed field, where armed forces clash, but in the heart of the population, under the gaze of cameras and influencers ».*

The observation is simple but powerful : the rise of new *(digital)* technologies and information and communication *technologies (NICT)* has overturned the rules of the operative art of war. Irregular warfare is redefining the paradigms of confrontation: instead of traditional military confrontations, technological tools are expanding the spaces of confrontation.

Cyberspace is not just a complementary tool for traditional conflicts, but a terrain in its own right, where a variety of actors clash, ranging from states to terrorist and criminal organizations, activists *(or hacktivists*) or isolated individuals seeking to satisfy their own indignities. In short, this metamorphosis in the nature of war is not limited to technical attacks on information systems; it also encompasses psychological, economic and political actions aimed at manipulating populations and destabilizing institutions, notably through the use of operations in the cognitive layer of cyberspace.

This reference book is therefore aimed at a wide audience : military strategists, political decision-makers, cyber experts, academics and, above all, citizens keen to understand the stakes of this new era and the technical workings of the *Technopolitics [2]* described by Asma Mhalla. Through a rigorous, historical analysis and methodical exploration of the tactics and consequences of the actions of the guerrilla *2.0*, Colonel Boyer invites us to rethink the way we approach our understanding of information systems, security and warfare in the 21st century.

Adopting a progressive, structured approach, this book is easy to read, revealing its trans-disciplinary concepts in an assembly-like fashion as it progresses. Beginning with the bricks of doctrinal definition and the necessary historical feedback, it then goes on to address possible response scenarios in the face of irregular adversaries, and is divided into five main sections :

1. *Digital combat and hybrid approaches to warfare, the new matrix of irregularity ?*
2. *The nature of insurgent combat throughout history : between irregular adversaries (ADIR), small-scale warfare and revolutionary guerrilla warfare*
3. *Direct and indirect methods of digital guerrilla warfare*
4. *Information as a key component of guerrilla tactics 2.0 : a weapon for both state actors and terrorist organizations*
5. *A sketch of digital counter-insurgency and informational counter-guerrilla warfare*

After a brief introduction to the author, our analysis will focus on the main thrusts and themes of this methodological treatise on *counter-guerrilla 2.0*. Secondly, we will highlight the underlying ideas that structure and enrich the author's approach in the light of recent events, and examine the implications and perspectives it raises. Finally, we will conclude this study with some food of thoughts, in which we will share our overall appreciation of his work.

I. Biography

Colonel Bertrand Boyer is the current Chief of Staff of *CIAE (Centre Interarmées des Actions sur l'Environnement), « the organization [responsible for] increasing the capacity of the French armed forces to influence the human environment of operations. » [3]*

a. An operational and technical curriculum, from *Saint-Cyr* to *Télécom ParisTech*

Colonel Boyer is more than just a field soldier. As a Saint-Cyrien, his time at *the École de guerre*, after his command and *overseas operations (OPEX*) stripes, and his involvement in various think tanks such as the *M82 Project (a not-for-profit association aiming to build, lead and develop a network of players and experts in the field of cybersecurity, cyberdefense and the fight against information manipulation [4])* on strategic issues have consolidated his reputation as a clear-sighted analyst.

After an initial career in operational units abroad, as an officer in the navy and as a Saint-Cyrien, he specialized in telecommunications and cybersecurity before graduating from *the École de Guerre* and *Télécom ParisTech*. He adopts holistic and historical approaches to irregular warfare, while integrating innovative technological approaches adapted to cyberspace.

b. A pioneering role in shaping cyber *« à la française*

One of the first officers to imagine tomorrow's conflicts in cyberspace, his many skills have led him to publish several notable works, including :

- *Cyberstratégie, l'art de la guerre numérique* (2012) *[5]*, a book that bridges the gap between the strategist and the technician, exposing technical concepts without drowning the uninitiated in esoteric vocabulary,

and raising questions about the possibility of transposing classical strategic principles into hypothetical digital warfare.

- *Cybertactique, conduire la guerre numérique* (2014) *[6]*, winner of the 2014 Cyber / FIC *(Forum International de la Cybersécurité)* book award, in which Colonel Boyer explores the similarities between the fundamental principles of warfare and military strategy and electronic warfare, and discusses the different forms of digital tactics and the challenges of digital warfare on decision-making, management and intelligence.
- *Dictionary of cybersecurity and networks* (2015) *[7],* aimed at making computer security and digital culture concepts accessible.

c. A return to field command after his years on the staff

He thus played a pioneering role in the structuring of French cyberdefense. His military career, punctuated by missions in complex conflict zones between humanitarian and military missions *(Democratic Republic of Congo)*, enabled him to develop unique expertise in new forms of guerrilla warfare.

Colonel Boyer is constantly moving back and forth between classical strategic principles and their application to cyberspace. His in-depth knowledge of guerrilla dynamics both on the ground and historically, combined with an acute understanding of technological developments, has made him a notable reference in irregular operations *« made in France ».*

Between 2012 and 2023, he was successively Head of the Cyber Defense Sector, Head of the Operations & Anticipation Office at the *Centre Interarmées des Actions sur l'Environnement (CIAE)* and Head of the Cyber Cell at the French Army *[8]*.

In July 2024, at the dawn of his career specializing in new forms of conflict, Colonel Boyer was appointed Chief of Staff of the *Centre Interarmées des Actions sur l'Environnement (CIAE)*, thanks to his knowledge of action from the weak to the strong and cybernetic operations.

II. Writing context

Modern warfare is characterized by a fundamental transition : it is no longer limited to direct, kinetic confrontations between states, and the means and spaces of confrontation have radically evolved.

Guerrilla 2.0 was published against a backdrop of profound changes in the nature of armed conflict - *mainly kinetic* - from conventional state confrontations to so-called *« hybrid » (in reference to the doctrine*

described by Gerasimov [9]), « irregular » [10], « fourth-generation » or « composite » wars *[11]* or operations *« other than war »* , characteristics to which we'll return later.

Far beyond *« symmetrical »* wars between states employing *« regular »* modes of action, these new forms of confrontation rely on the disruptive *NBIC [12]* technologies described below, which redefine the rules of warfare through *techno-scientific power*.

- *Nanotechnology (all miniaturized technologies operating on the nanometer scale) ;*
- *Biotechnology (the marriage of science and technology applied to living organisms and all their externalities);*
- *Computer science (science of information processing) ;*
- *Cognitics (science of automatic knowledge processing and related techniques) ;*

What characterizes the possibilities offered by these new technologies is the cost-benefit ratio of their *militarization* and *the « strategic asymmetry » (« the use of any difference to gain an advantage over the adversary » [13])* they offer to competing states - or non-state actors - who possess them in the face of other world powers, in order to upset the established order through a certain technological deterrence *(as in the case of Taiwan and the importance of its semiconductor industry)*

a. *Hybrid warfare or hybrid threat : a revolution in confrontation?*

Although, according to the author, conflicts of *an « asymmetrical »* nature have existed for hundreds of years, ranging *« from the lion against the gnat (Jean de la Fontaine's fable of the lion and the gnat) to the Taliban, from FARC to the barbudos »*, the proliferation of digital and technological tools is undermining the established ascendant order of constituted states in the face of rebel groups or various militias.

Well-known asymmetrical operations *(sabotage, doxxing, domestic opposition, clandestine actions, hacktivism or online indignation, slacktivism or indirect action)* thus enable these - often non-state actors *(terrorism, ideological militantism, non-governmental organizations)* to level the enemy's superiority - numerical, conventional, historical - in combat. These actions, most often based on surprise and unpredictability, contrast with an open declaration of war and a conventional confrontation : they are the very archetype of so-called *« sub-threshold »* actions.

This mutation of the battlefield has been amplified by the emergence of immaterial fields *(cyberspace, electromagnetic fields, cognitive fields)*, offering an operating terrain where traditional balances of power have been turned on their head. Which, incidentally, is a characteristic taken into account and expressed by the current French *Multi-Milieux Multi-Champs* (*M2MC)* doctrine for responding to actions in these fields of competition, contestation or irregular confrontation *[14]*.

Cyberspace, whose penetration rate *[15] (percentage or numbers of users having used a product or service over a given period)* is growing exponentially in the 21st century, has become a multiplier of propaganda and non-kinetic actions of all kinds *(although actions in cyberspace should not be reduced to non-kinetic actions, these do have direct consequences on the functioning of an information system or a national or private communications network).*

This enables minority players to exert disproportionate influence over states or entire coalitions. Since the late 2000s, several events have marked this transformation towards a ubiquitous battlefield :

The Stuxnet attack (2010) [16]

This cyberattack *(*a *worm allegedly designed by the National Security Agency [NSA] in collaboration with an Israeli cyber unit 8200),* which targeted Iran's nuclear infrastructure, has become an emblematic example of the use of cyberspace for strategic military purposes. It demonstrated for the first time *(in the court of public opinion)* that a strictly digital offensive operation could cause tangible damage to critical installations *(in this case, so-called SCADA systems - Supervisory Control And Data Acquisition [17] - or real-time control and data acquisition systems)*, without requiring direct physical intervention, thus redefining the dynamics of modern conflicts and the nature of threats for all of this century's rivals and competitors.

Russia's annexation of Crimea (2014) [18]

By combining limited military action with massive cyber-attacks on Ukrainian systems, Russia has illustrated the effectiveness of hybrid strategies for territorial gain, combining conventional forces on the ground, information manipulation, intelligence, demoralization *(deceptions)*, and cyber-attacks on Ukrainian state information systems of an intensity equivalent to the symbolic *Stuxnet* attack, the first for a non-US actor

Massive information manipulation campaigns (known to public opinion since 2016)

Cases of information manipulation during national or regional elections have been coming thick and fast for years. Since the Cambridge Analytica scandal *[19] (data economics at the service of manipulation),* the *Brexit* and the case of Sino-Russian and Iranian interference in the 2016, 2020 and 2024 US election campaigns, many elections have experienced massive informational campaigns on social networks aimed at undermining public opinion and altering democratic processes, such as the cancellation of the first round of the Romanian presidential election following the revelation of a large-scale influence operation on Tiktok, thanks to the declassification of national intelligence information *[20]*. These examples underline the growing impact of the influence and techno-power of the *guerrilla 2.0*, mastering the codes of action of the 21st century

Today, every conceivable modern actor - *states, terrorist organizations and hacktivists* - is exploiting these new opportunities to disrupt the established international order or, on the contrary, support it.

b. The digital technostructure, a lever of power at the heart of geopolitical rivalries

« Digital guerrilla warfare, in addition to its ability to mobilize, must develop and maintain a capacity to produce effects, to act and strike blows at its adversary, in the same way as traditional movements.

Colonel Boyer's book comes at a time when information and communication technologies are omnipresent, transforming not only human interactions at the heart of society, but also military tactics and strategies. Indeed, the blurred nature of immaterial fields in the designation of an actor's responsibility for action in these *« gray«* spaces, and the absence of easy zone control through access/area denial *[21] (anti-access/area denial or A2/AD),* make control of the operational environment that is cyberspace more and more complicated.

Thus, the term *« gray zone«* has emerged to describe the turmoil of confrontational spaces such as these, defined by the *Special Operations Command (SOC)* as*: « Below the threshold of open conflictuality, a particular situation in which hostile intent fails to be clearly discerned and/or the attribution of responsibility to a major actor remains unclear, or even uncertain, in a context of instrumentalization of the law.«*

From cyberattacks crippling critical energy infrastructures to information manipulation campaigns destabilizing the neutrality of state content published during elections in targeted countries, cyberspace therefore offers unprecedented opportunities to wage *« sub-threshold«* wars at the heart of the irregularity matrix

Powers such as Russia and China have thus resorted to campaigns estimated by Western analyses as *« hybrid«* *[22], [23]* to weaken their adversaries while strengthening their global influence and using cyberspace as a major strategic lever in particular through their state social networks *(Telegram, VK, TikTok)* but also foreign *(Facebook, Twitter/X, Instagram, Odyssey...)*

Here are a few examples of contemporary players who illustrate this irregular civil-military use of cyberspace for all kinds of purposes.

The Russian Federation and the spectre of the hybrid « octopus

Russian strategy is based on a sophisticated combination of conventional civil-military military action and aggressive cyber and information operations. Crippling infrastructure cyberattacks, such as those carried out against Estonia *(2007)* or Ukraine *(2014 - ?) [24],* demonstrate how Moscow uses cyberspace to disrupt critical infrastructures and intimidate decision-makers in competitor countries opposed to its ambitions. Here, the use of information *« supports«* traditional military operations, as a complementary tool for action.

These - *often digital* - offensives do more than just disrupt critical infrastructures; they also aim to undermine public confidence, sow confusion and intimidate political decision-makers in targeted nations. In this way, the Russian Federation exploits these hybrid tactics to blur the boundaries between wartime and peacetime, making it difficult to attribute attacks directly and complicating the responses - *diplomatic, economic or political* - that can be envisaged.

China and digital economic warfare (a continuation of the « unrestricted » warfare[25])

China, for its part, is focusing on economic and industrial espionage, in line with its rise in both technological and commercial power over the past thirty years. Massive hacking campaigns carried out by groups like *APT10*, often linked to the Chinese state, aim to steal sensitive technologies and extend Chinese influence, notably as part of the New *(Digital)* Silk Roads *or Belt and Road Initiative (B.R.I.)*. Initially called *« One Belt, One Road » [26],* this is a project of strategic importance initiated by China in 2013, aimed at economically linking *(and a fortiori extending its influence)* China to Europe, by crossing Central Asia thanks to a vast network of rail, road and telecommunications corridors.

Non-state actors

Various terrorist groups such as *Daesh*, *al-Qaeda, al-Nosra*, *Hamas* and *Hezbollah [27]* have demonstrated their ability to take advantage of digital networks to recruit, disseminate their ideology and coordinate attacks, even at a sometimes continental distance. Similarly, the use of *« reflexive »* attacks aims to coordinate several technical and informational acts in order to hit its target *(often a state-owned one in this case)* by rebound. Environmentalists *(Extinction Rebellion, the Vinci affair),* anti-capitalists *(Occupy New York),* human rights activists *(Amnesty International)*, freedom fighters *(cryptoanarchists and cyberpunks)*, *hacktivists (Anonymous)* and organized crime groups have already used similar means to challenge state powers *on a weak-to-strong* basis and achieve their own ideological or militant objectives.

Colonel Boyer emphasizes that the use of these technologies is not neutral. Actively used by our strategic competitors and many of their proxies, they are shaping the way conflicts are fought, favoring decentralized approaches, actions from the weak to the strong, and distributing power among a multitude of state and non-state actors.

These dynamics are profoundly transforming international relations, blurring the boundaries between peace and war and rendering obsolete the traditional analytical continuum *of peace/crisis/war*.

c. A necessary response to technological and societal changes, and the need for a legal framework for allocation

Faced with these disruptive phenomena in the evolution of our relationship with the veracity of facts, the nature of threats and the mechanisms of *social engineering (a set of manipulation techniques aimed at extorting information about a target from an individual via social interaction)*, the absence of clear *(global)* regulation in cyberspace implies the plausibility of a cyber *Far-West*. Unlike traditional armed conflicts, wars over knowledge and narratives in cyberspace escape all norms, rules and international conventions, opening the way to uninhibited misuse and uncontrolled escalation of tension.

As a result, cyberspace is no longer just a support area for traditional conflicts, but a battlefield in its own right. Without concerted action to establish bodies of international regulation in intangible fields, it will be impossible to regulate the behavior of public and private players in cyberspace.

As a result, cyberspace increasingly resembles an arena where powerful competitors *(often state or institutional)* can be targeted at low cost - or with disproportionate returns. Conflicts of a digital nature are likely to become a critical destabilizing factor, both nationally and internationally, not least because of the ease with which attacks can be deployed and the difficulty of identifying offensive actors. Our times are thus marked by the mutation of armed conflicts and military operations in conventional environments *(land, sea, air, outer space, cyber)* towards irregular *(unconventional)* and hybrid wars, integrating all the possibilities and modes of action offered by *informational*, *electromagnetic* and *cognitive* fields.

Social networks, a digital battleground for influence

Today, our societies are being profoundly transformed by *new information and communications technologies (NICTs)*, making states, companies and individuals ever more dependent on digital information systems. This dependence, both material *[28] (physical components and assemblies of digital tools)* and psychological *[29] (Pavlovian/classical or Skinnerian/responsive conditioning mechanisms)* creates vulnerabilities that can be exploited for malicious purposes by actors hostile to our interests, both on a societal level, by targeting .

Digital platforms such as *Facebook*, *Twitter* and *TikTok [30]* play a key role in *narrative warfare* between competitors seeking to develop their own ideals and perspectives on a world in crisis. They enable malicious actors to rapidly disseminate narratives of strategic importance, polarize societies targeted by influence campaigns or sow discord. Disinformation campaigns, such as those associated with the Covid-19 pandemic, show how cyberspace can be used to manipulate perceptions and undermine trust in state institutions

Renewed propaganda methods

Moreover, recent events support the hypothesis of a *« Russianization » [31] of* information manipulation, similar to the operating methods used in China and the Philippines. This can be seen in the

transition in the valence of propaganda methods used on a massive scale to persuade, orient perceptions or deception *[32]*.

Historically, this involved the use of historically defensive positive propaganda about a government, regime or country *(id este propaganda designed to promote the values of the influence campaign actor),* often illustrated by *« conative »* action *(in psychology, one of the components of action, the impulse to act)* on its own population to retain its support, coupled with positive propaganda *(informational interference)* within other countries *[33]*.

An example of this method is American strategy during the *Cold War*, which combined internal defensive propaganda with external informational interference.

Internally, media and educational campaigns *(American soft power)* promoted democratic values and the superiority of the American way of life to mobilize popular support, using cultural media *(film and television productions)*, patriotic symbols *(often anti-communist)* and incentives for concrete actions, such as voting or supporting the military effort.

Abroad, initiatives such as *Voice of America [34]* broadcast pro-democracy programs in the local languages of communist countries, while cultural exchanges *(jazz tours)* presented the United States as a free and progressive society. This two-pronged approach was designed to consolidate support at home, while at the same time sparking emulation, dissent and even insurrection abroad - a method of operation highlighted by Colonel Boyer in his book.

Today, as the efficiency of the defensive method has been called into question, the use of negative offensive propaganda *[35]* is more in vogue, targeting a government, a state or an institution. This is an external action of attack and degradation of a competitor's image, aimed at altering the decision-making capacities of individuals, decision-makers or economic leaders *(what we might call cognitive interference [36])*. This type of action is particularly common in electoral processes.

During the 2016, 2020 and 2024 US presidential elections, information manipulation campaigns on social networks, often attributed to foreign actors *(Russia, Iran, China)*, aimed to polarize public opinion and discredit certain candidates through the use of false information *(pizzagate [37])*.

Similarly, the year 2024 was marked by notable foreign interference in electoral processes *(Moldova, Georgia, Romania [38])* of rare intensity and notable effectiveness, using social networks like *Tiktok* as a catalyst for information operations. These campaigns targeted decision-makers and the electorate, sowing doubt and political instability, with the aim of weakening confidence in the democratic system, and directing voting according to primary survival mechanisms, like instinctive reactions to fear, the unknown or threat. This type of cognitive interference exploits informational vulnerabilities to alter the strategic decision-making processes of a given country or state.

Finally, another modus operandi is tending to develop *(or be reborn)* with the exponentiation of interconnections in our modern societies, namely purely conative actions: the aim in this method is to act by seeking to produce a desired end state *(in the operative art, the attainment of the desired end state or EFR [39])* on a competitor or its population, with an action that will spur the opponent or target into action *(typical of reflexive control)*. A concrete example of this mode of action lies in foreign interference during large-scale demonstrations, *(the Gilets Jaunes movement in France, the Arab Spring, the Color Revolutions in Eastern European countries)*.

By amplifying certain stories on social networks via *bots (software that performs automated, repetitive and predefined tasks, generally imitating or replacing the behavior of human users [40])* or anonymous accounts, external actors sought to polarize public opinion and incite specific groups to intensify their protests. These actions aimed to push the target population to act in a predictable way, creating pressure on legitimate authorities to react in a direction desired by the instigator.

The « milicianization of war » [41]

Since the 2000s, non-state groups such as *Daesh* and *Anonymous* have been exploiting technology for guerrilla warfare. Cyberspace offers these asymmetrical actors, such as terrorist groups or weak states, tools capable of competing with well-established military powers, sometimes reversing the relationship between the weak and the strong.

A well-designed cyberattack on a critical infrastructure, such as a power grid, a submarine telecommunications cable, or a health or financial system, can paralyze an entire nation without mobilizing a single soldier. The massification of *NICTs* has turned military strategies on their head.

Today, the cybernetic tool - *or weapon* - affects critical infrastructures, minds and social dynamics, redefining the notion of a *« war zone »* . The author wishes to draw attention to the importance of structuring an appropriate response to adversaries operating in a borderless space, where the lines between civilians, armies and hacktivists *(ethical or otherwise)* are blurred.

III. Author's thesis

« The battlefield is everywhere »

Bertrand Boyer argues that cyberspace is a fundamentally different theater of war from traditional battlefields. Irregular warfare in this domain is not based on direct confrontation, but on indirect strategies aimed at exploiting the structural, psychological and technological vulnerabilities of adversaries. It is this difference in the nature of the confrontation that enables players who are sometimes negligible in the balance of power to take advantage of asymmetrical offensive means.

The author suggests adopting an *opportunistic*, *proactive* approach to the hybrid threat in cyberspace, rather than limiting ourselves to a merely *reactive* posture. He stresses the importance of leveraging our forces *(of the French army where appropriate)* and exploiting the opportunities offered by digital technology to achieve strategic and operational objectives.

This strategy is based on the ability to shape the digital environment, using consumer tools to prepare and control the terrain, while anticipating and countering adversary actions. It also advocates the integration of accessible digital tools into the military arsenal to neutralize enemy narratives, influence opinion, and exploit adversary vulnerabilities.

Finally, Colonel Boyer stresses the need for controlled hybridization, combining civilian and military technologies to enhance the effectiveness of *information (propaganda, recruitment and intelligence)* and *counter-guerrilla operations* in cyberspace.

a. Cyberspace as a hybrid strategic battlefield

« First in last out » : occupying cyberspace

Colonel Boyer begins by revisiting the nature of modern warfare and explaining its contemporary hybridity. Modern warfare combines classic military actions *(strategic and tactical armed forces on land and at sea, air strikes, actions in outer space)* and digital strategies *(for the French Army, the cyber-offensive doctrine - LIO - / cyber-defensive doctrine - LID - / Lutte Informatique d'Influence - L2I - [42])*.

This enables both state and non-state actors to conduct influence campaigns and *Multi-Domain* Operations *(MDOs)* while remaining below the threshold of declared war. This peculiarity quickly raised the question of defining a *« threshold »* above which an action could be qualified as *an act of war,* thus justifying an adjustment of strategic posture in the face of a strategic competitor.

How, then, can we neutralize actions *that* remain below a formal threshold of harm - *involving neither civilian casualties nor the direct compromise of information systems* - but which are primarily aimed at undermining the political cohesion of an adversary by sowing panic or instilling doubt about the official information of the political regime in place?

Whether we're talking about cyberattacks on critical infrastructures *(such as Stuxnet)*, manipulations of the information spectrum orchestrated via social networks to polarize public opinion, or operations in *gray zones*, the problem of operational response to these *« sub-threshold »* actions always arises.

The grey zone : the antechamber of irregular combat

Indeed, *grey zones* represent legally ambiguous spaces *(specific territories where power rivalries are particularly heightened, notably at the heart of the law of the sea, cyberspace and parts of the web that are not listed - deep web - or accessible using specific connection protocols - dark web -)* where states hesitate to intervene or cannot legislate directly, leaving room for non-state or semi-state actors, such as terrorist groups or hacktivists.

Examples include attacks *on* submarine telecommunications cables *(C-Lion1 in the Baltic Sea between Sweden and Lithuania, and Germany and Finland [43]),* submarine power cables *(EstLink2 in the Baltic Sea between Estonia and Finland [44])*, and submarine gas pipelines *(Nord Stream 2 in the Baltic Sea between Russia and Germany [45])*.

Similarly, the relatively inexpensive access to cyberspace facilitates the development of online propaganda campaigns, anonymous hacking or indirect sponsorship of malicious activities by states via indirect actors *(proxies)* using very specific social networks *(Telegram in particular)* that researcher in cyber-strategy of jihadist groups, Laurence Bindner, describes as *« a kind of jihadotheque«* . This mode of action is similar to the relocation of direct offensive operations by the *Islamic Republic of Iran*, which for several years has been arming and training proxies it more or less controls *(Hamas, Hezbollah, Houthis [46])*.

The use of proxies : diversity and convergence of players

These terrorist groupings can thus be described as proxies in the sense that they have varying degrees of autonomy while aligning themselves with major Iranian positions and objectives, and act both in immaterial fields *(online propaganda and recruitment)* and kinetically on the ground *(Hamas terrorist attack on Israeli territory on October 7, 2023)*.

Colonel Boyer underlines the growing role of non-state actors in irregular warfare in cyberspace. Whereas traditional conflicts mainly pitted national armies against each other, cyberspace is a domain where individuals, criminal organizations and militant groups can compete with states *(see above)*.

The image of the mujahid, initially perceived as that of a fighter or resistance fighter, is gradually spreading in the West, particularly through digital social networks.

It evolves to embody a warrior of faith committed to jihad. Radical Islamists from the Arabian Peninsula and the Caucasus join the ranks of fighters on the ground, helping to shape the mythical figure of the soldier of faith, ready to wage a fierce and uncompromising struggle to defend and preserve his ideal through a new *digital jihad*.

Numerous examples are cited where cyberattacks attributed to anonymous groups have had major geopolitical consequences. The *NotPetya* attack *(data-destroying wiper malware, but appearing as ransomware)* in 2017, for example, caused billions of dollars in economic damage worldwide, demonstrating that a single well-coordinated operation can have global impacts. These new players, often motivated by economic, political or ideological interests, blur the lines between war, crime and activism.

The growing role of human psychology at the heart of algorithms and informational attacks

Colonel Boyer also emphasizes the importance of psychological actions *(unplanned and not necessarily aimed at an objective)* and operations *(a series of planned actions determined by a goal to be achieved)* in this type of numerical and irregular combat. Among the mediums used in information manipulation campaigns are :

- *demoralization techniques : demoralizing enemy troops, undermining their discipline, depressing troop morale and the morale of a population*.
- *deception techniques* : *using deliberate misrepresentations of reality to gain a competitive advantage through concealment or camouflage, intoxication (rumors, bluffing) or simulation (decoy effect).*
- *psychological operations* on social networks *(planned psychological activities in times of peace, crisis and war, directed at enemy, friendly and neutral audiences to influence their attitudes and behavior so as to affect the achievement of political and military objectives)*

The aim of this operative art is to undermine public confidence in institutions, creating an environment where a country's internal stability can be jeopardized. This form of *« information warfare »* and *« psychological warfare »* is a powerful lever for irregular actors, who are often more agile and creative than states in this field, states constrained by legal regulations and bearing a responsibility to a certain ethic preached by their claimed status as democracies.

The interconnection of technological and human operational dimensions

Wars are no longer confined to the physical arena. Economic, psychological and digital dimensions are intertwining to multiply the pressure points on the adversary. Colonel Boyer suggests adopting a collective and adaptive response to counter the hybrid threat in cyberspace, by exploiting the diversity of skills offered by international coalitions. He recommends leveraging the linguistic, cultural and technical capabilities of partners to neutralize the actions of hybrid actors on specific targets, while developing false-flag strategies to infiltrate their networks.

This approach is based on anticipated and massive occupation of digital space, using propaganda tools and virtual robots *(bots)* to saturate the environment and provoke exploitable adversary reactions. Colonel Boyer also insists on the adaptability and plasticity of strategies, which should draw on skills in sociology, psychology, behavioral economics and emerging technologies *(artificial intelligence tools, massive data processing)* to exploit adversaries' vulnerabilities.

« Opinions are forged on networks and spread through their intermediaries. »

Digital operations should therefore enable an *« equal arms«* engagement, offering tactical opportunities to regain the upper hand against irregular actors, while integrating these dynamics into a structured and effective digital counterinsurgency doctrine

Unlike conventional and traditional warfare, where physical resources play a dominant role, warfare in cyberspace relies on a combination of technical skills and the ability to influence human behavior.

Colonel Boyer explains that digital *conflicts* often exploit human weaknesses, often relying on the exploitation of cognitive heuristics *(mental shortcuts of thought)* : associative, availability, memory, judgment, or even phenomena such as *credulity* or *inattention*.

Phishing attacks, for example, succeed not because of complex technical flaws, but by playing on the psychology of users, who don't pay attention to the accuracy of an Internet link or download *url : typosquatting (changing url)*, *cybersquatting (parasitizing Internet traffic normally destined for another site)*, *Punycode* attack *(changing character encoding)*.

In this new form of warfare, training and awareness-raising are essential defensive weapons.

b. Guerrilla warfare 2.0 : a digital extension of historical insurgencies

« With two thousand years of examples behind us, we have no excuse, when we fight, if we fight badly. », Thomas Edward Lawrence

In his book, Colonel Boyer introduces the concept of *guerrilla warfare 2.0* as an evolution of traditional insurgencies. He begins with a review of the notion of *ADversaire IrRégulier (ADIR)* in the French armed forces.

The irregular adversary in French doctrine is defined through a distinction between rebellion and insurrection, based on the degree of involvement of the population in the conflict.

The irregular adversary in French doctrine

Whereas rebellion presupposes a neutral or passive population, insurrection marks a generalized shift against the authority in place. These notions, inherited from the experiences of decolonization and coalition warfare, are part of a doctrinal approach that associates the fight against these irregular actors with political, ideological or religious issues

French doctrine analyzes insurrection as a structured mode of action designed to bring about political change by violent or subversive means, exploiting social and institutional vulnerabilities. It also distinguishes between different types of actors : predatory *(motivated by profit)*, vindictive *(seeking local power)* and subversive *(idealistic or revolutionary)*.

Digital guerrilla warfare as historical continuity

However, these categories tend to blur in the context of hybrid and digital conflicts, where *guerrilla warfare 2.0* fuses traditional tactics and technological tools to destabilize states.

In the face of this evolution, connected insurgency is becoming a global phenomenon, exploiting digital networks to recruit, mobilize and disseminate ideological narratives. It challenges conventional definitions of asymmetrical conflict, and calls for a strategic adaptation that integrates both the historical legacy of small-scale warfare and the new realities of digital globalization. Colonel Boyer underlines the need for a modernized approach, combining traditional military doctrines and technological innovations, to counter these diffuse and connected threats.

The contribution of small wars to digital combat 2.0

The contribution of small-scale warfare to guerrilla warfare is based on the use of irregular tactics and light troops, whose effectiveness has been demonstrated since Antiquity and confirmed over the centuries, notably during the European wars of the 18st century.

Although long marginalized in classical strategic thinking, this approach has proved its relevance against more powerful enemies, thanks to methods such as ambushes, cunning and raids.

The history of small-scale warfare reveals that these tactics emphasize surprise and adaptability, while mobilizing limited resources. Figures such as *Clausewitz* and Count *Von Gneisenau* theorized this model, emphasizing its potential for innovation and its ability to compensate for asymmetric forces through popular mobilization. This principle was illustrated in the Spanish guerrillas against *Napoleon*, where irregular groups managed to paralyze far superior regular armies.

Today, these lessons are echoed in *guerrilla warfare 2.0*, which transposes the principles of small-scale warfare to cyberspace. Like historical sieges, where resources were cut off, modern cyberattacks exploit the flaws in digital systems to paralyze the adversary. The use of malware or social engineering techniques is the contemporary equivalent of the ambushes and stratagems of yesteryear.

Colonel Boyer therefore calls for the modernization of these practices through the creation of specialized digital warfare units, capable of combining technological innovation and tactical flexibility. He

also stresses the importance of mobilizing digital reserves in the form of hacker communities *(via bug bounty programs, for example)* to strengthen response capacity in the face of hybrid threats.

Guerrilla *warfare 2.0* takes up the fundamental principles of small-scale warfare - *mobility, adaptability and asymmetry* - to establish itself as a strategic mode of action in a world where conflict now extends to the digital domain

In a world saturated with data, information manipulation is becoming a formidable weapon. Colonel Boyer explains how the mastery of *narratives* and the fight against information manipulation have become central issues, at a time when *fake news (false information or « infox » in French) is* making its presence felt not only in the words of re-elected US President Donald Trump, but also in many *mainstream* media, and when *WikiLeaks* is setting itself up as the censor of weakened democracies.

In order to frame this analysis, the book also proposes a classification of informational action processes on the *semantic (or psycho-cognitive)* layer of cyberspace, arranged in four main categories : *communication, mystification, alienation,* and *protection*.

- *Communication* is based on *information*, *argumentation*, *suggestion* and *persuasion* to influence perceptions and behaviors.
- *Mystification* uses strategies such as *stratagem*, *deception*, *intoxication* and *disinformation* to deceive the opponent.
- *Alienation* aims to manipulate in depth through *propaganda*, *indoctrination*, *subversion* and even *terrorism*, to destabilize and control.
- In contrast, *protection* includes defensive mechanisms such as *counter-information, counter-propaganda* and *de-persuasion* to preserve the integrity of information systems and counter enemy attacks.

These processes, although powerful, require rigorous and ethical application in the context of their uses within the armed forces, because abusive use can compromise credibility and cause adverse effects. Their effectiveness depends on careful strategic planning and controlled execution.

Guerrilla warfare 2.0 : a form of conflictuality adapted to the immaterial world

More than a simple implementation of the cyber domain in confrontation methods, it's more a question of an asymmetrical struggle amplified by technology. This new form of guerrilla warfare is based on several operational invariants :

- *Insurgent adaptability :* Irregular actors, such as *terrorist groups* or *hacktivists*, use digital tools to circumvent power asymmetries. These tools enable them to act effectively against states or institutions that are far better equipped technologically and materially.

- *Classic guerrilla tactics* : historical guerrilla strategies - *surprise, subversion, territorial control* - are adaptable to the digital environment.

    1. *Digital ambush :* Targeted attacks on critical infrastructures, such as hospitals, energy infrastructures or banks.

    2. *Controlling digital zones :* dominate online spaces, such as forums or social platforms, to spread effective propaganda messages.

    3. *Offensive use of subversion :* Using social networks to manipulate perceptions, recruit supporters, or discredit competitors and opponents.

- *Accessible technologies :* With the emergence of open-source software and easy-to-use tools, individuals or small groups can orchestrate large-scale actions. This lowers the barrier to entry for irregular warfare.

By way of example, Colonel Boyer analyzes the case of the Islamic State terrorist group *(Daesh)*, which has been able to exploit social networks to recruit fighters, disseminate propaganda messages and organize terrorist attacks, while remaining relatively elusive thanks to inexpensive encryption tools, anonymization *(online forums)* and a practice of encrypting exchanges, combined with the use of closed networks *(i.e. for which entry rights are required : Telegram, WhatsApp, Signal…)*

c. The invariants of warfare and their adaptation to the digital age

Although cyberspace is changing the nature of confrontation, Colonel Boyer insists on the continuity of the fundamental principles of warfare. Here are just a few of these tactical and strategic invariants :

- *Surprise and decentralization :* These tactics, which were essential for traditional guerrilla warfare, are just as relevant in cyberspace. For example, sudden attacks such as ransomware cripple institutions without warning *(cyberattack on the Université Paris-Saclay, claimed on Wednesday October 9 by a ransomware group)*.

- *The need to rally :* Every conflict, whether *physical* or *digital*, requires a support base. In cyberspace, this translates into mobilizing an online community to amplify a message or coordinate actions.

- *The importance of narrative :* Winning the *war of narratives* has become as important as winning physical battles. Influence campaigns aimed at delegitimizing the adversary while reinforcing internal cohesion are thus at the heart of *guerrilla warfare 2.0*.

Ultimately, *guerrilla warfare 2.0* doesn't reinvent warfare ; it adapts it to a new terrain, exploiting the opportunities offered by technology while relying on tried-and-tested tactics.

IV. Food for thought

One of the major avenues explored by Boyer is strengthening *national resilience* to cyber threats. In his view, it is not enough to develop offensive or defensive capabilities to be effective in cyberspace. One of Colonel Boyer's central theses in this book is that cyberspace offers unprecedented leverage for weak actors to exert disproportionate pressure on more powerful targets.

The speed, stealth and reach of digital actions are profoundly changing the rules of the game.

Nations also need to invest in robust infrastructures capable of withstanding prolonged attacks, and in educational programs to make citizens aware of digital dangers. Let's take a look at some of his ideas.

a. The need for national resilience and the integration of a digital counter-guerrilla strategy

Like the guerrillas of the 20th century, digital attacks aim to destabilize established powers by exploiting systemic vulnerabilities. Colonel Boyer refers in particular to the creation of *« resilient networks »*, where each element of a critical infrastructure is capable of functioning in isolation in the event of an attack on the overall system. This approach, inspired by biology and decentralized systems, aims to minimize the impact of massive cyberattacks *(the image of a digital Blitzkrieg)*, even when they succeed in compromising part of the network.

To meet the new challenges of *guerrilla warfare 2.0*, Boyer proposes a *proactive* strategy based on :

- *Surveillance and data analysis :* Armies and governments must use digital tools to identify emerging threats, monitor adversary narratives, anticipate malicious actions, and detect weak signals.
- *The role of partnerships :* Collaborating with the private sector, *NGOs (non-governmental organizations)* and civilian actors is essential to pool resources and ensure a coordinated response to hybrid threats.
- *Information warfare :* one of the objectives of *L2I* in the French armed forces is to strengthen strategic communications in response to disinformation campaigns and build a positive narrative capable of mobilizing the population *(see above)*.

In this context, organized cyber armies need to be created and organized, made up of a variety of players: *volunteers, mercenaries, regular military units and private organizations*.

These forces need to deploy a variety of techniques, ranging from strategic communication campaigns to convince and persuade, to more offensive actions, such as *disinformation*, *deception* or even *the intoxication of* opposing decision-makers.

However, Colonel Boyer underlines the limits and risks of these practices, particularly for democracies, which must preserve their credibility and legitimacy while avoiding ethical excesses. Modern armies, now dependent on information, expose themselves to disruption and manipulation, which calls for strict rules to govern these *digital counter-guerrilla* operations.

The emergence of *cognitive warfare* is forcing us to rethink traditional methods of disseminating information. From now on, content must be adapted to each platform and exploit the technical specificities of social networks. In this new environment, the manipulation of perceptions becomes as important as the manipulation of facts, requiring a more flexible and reactive approach to managing the unpredictability of adversary reactions.

Finally, information warfare in cyberspace relies on the ability to saturate the environment with contradictory narratives, creating confusion that limits the capacity for critical analysis.

This mode of action seeks not only to make people believe, but above all to make them act, by steering the adversary's decisions in a direction favorable to strategic objectives.

However, Colonel Boyer once again warns against the unpredictable and sometimes counterproductive effects of these maneuvers, insisting on the need for meticulous planning and rigorous control to avoid any slip-ups.

b. Modernizing legal and organizational frameworks as a key to national security

In a field as interconnected as cyberspace, Colonel Boyer stresses the importance of international cooperation to establish a legal framework for responding to irregular threats in cyberspace. As cyber-attacks respect no borders, it is essential for states to work together to share intelligence, coordinate their responses and establish common standards, over and above traditional cooperation frameworks *(bilateral agreements, the North Atlantic Treaty Organization, exchanges between intelligence services)*.

However, Colonel Boyer recognizes the challenges inherent in this cooperation. Cultural differences, geopolitical rivalries and lack of mutual trust often complicate collective efforts. To overcome these obstacles, he points to regional initiatives and public-private partnerships, which can serve as models for broader agreements on a global scale. It also highlights the need to strengthen partnerships between governments, technology companies and citizens.

Indeed, cyberspace is also a civilian arena, and defense must be collective. He stresses the need to adapt structures and regulations to deal with digital threats through various medias :

- *Regulating cyber operations :* Develop international conventions to regulate conflicts in cyberspace and prevent uncontrolled escalation.

- *Clarification of responsibilities :* Define precisely the roles of the various entities - *armed forces, governments, companies* - in defending against and taking responsibility for cyberthreats.

- *Organizational and operational flexibility :* Rigid structures cannot keep pace with rapidly evolving digital threats. It seems imperative to adapt our institutions as networked organizations, capable of adapting and reacting in real time.

c. Investing in education, innovation and shaping tomorrow's military doctrines in the age of cyberspace

For Colonel Boyer, the key to effective defense lies in the development of :

- *Training the armed forces :* Cyber-fighting soldiers need to be trained in the specifics of digital combat, from gathering open-source information - OSINT *(Open-Source Intelligence)* - to conducting psychological operations.

- *Technological innovation :* States need to invest in emerging technologies *(artificial intelligence tools, cybersecurity)* to stay one step ahead of their competitors and irregular adversaries.

- *Raising public awareness :* Educating citizens about the dangers and risks of online information manipulation remains essential to strengthening national resilience in the face of hybrid threats.

Another major avenue for reflection concerns the integration of cyberspace into national military doctrines. This book criticizes traditional approaches that treat cyberspace as a separate domain, often relegated to technical experts. Cyberspace should be seen as an intrinsic dimension of all military operations, on a par with land, air, sea and space.

To this end, he calls for widespread training of military personnel in the fundamentals of cyberspace, so that they can integrate these considerations into their overall strategies. He also stresses the importance of realistic simulations, enabling armed forces to test their ability to operate in an informational, cultural, linguistic, sociological and physical environment where cyber-attacks and disinformation are omnipresent.

Conclusion

Bertrand Boyer's book *Guerrilla 2.0 : irregular warfare in cyberspace* is an essential analysis of the strategic challenges posed by digital conflict. Exploring the technical, psychological and geopolitical dimensions of cyberspace, Colonel Boyer offers a comprehensive vision of this new era of irregular warfare.

His book highlights the importance of a multidimensional approach to tackling these complex threats. It's not just a question of developing more advanced technologies, but of rethinking our institutions, our military doctrines and our international cooperation.

Finally, Boyer calls for a *collective awareness* : in a world where cyberspace has become a battlefield, every individual, organization and nation has a role to play in ensuring security and stability

Faced with the rise of digital irregular warfare, this holistic book invites us to rethink our approaches to security and defense. Far from being a mere technical field, cyberspace is a terrain where political, psychological and social battles are played out, requiring a multidimensional and proactive response

References

[1] Lentz, T. (2001). Napoleon reinvented the art of war . *Idées reçues*, 83-86, [online], December 31, 2024.

[2] Mhalla, A. (2024). Technopolitics : how technology is turning us into soldiers . Seuil, [online], December 31, 2024.

[3] Ministry of the Armed Forces, November 2018. The Joint Environmental Action Center , [online], December 31, 2024.

[4] M82 Project website, Presentation of the M82_Project , [online], December 31, 2024.

[5] Boyer, B. (2012). Cyberstratégie : l'art de la guerre numérique. Éditions Nuvis, [online], December 31, 2024.

[6] Boyer, B. (2014). Cybertactics : leading the digital war. Éditions Nuvis. [online], December 31, 2024.

[7] Boyer, B. (2015). Dictionary of cybersecurity and networks . Éditions Nuvis, [online], December 31, 2024.

[8] Journal Officiel de la République Française website. Appointments to the Journal Officiel de la République Française in the name of Bertrand Boyer, [online], December 31, 2024.

[9] General Valery Gerasimov, The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, Voyenno-Promyshlennyy Kurier, (Feb. 26, 2013), Original version in Russian , Military Review (Jan.-Feb. 2016) Version traduite en anglais

[10] Gray, C. S. (2006). Irregular Enemies and the Essence of Strategy : Can the American Way of War Adapt? . Strategic Studies Institute, US Army War College, [online], December 31, 2024.

[11] Hammes, T. X. (2006). The sling and the stone : on war in the 21st century. Zenith Press, [online], December 31, 2024.

[12] Claverie, B. (2014). From cybernetics to NBIC : information and machines towards human surpassing. *Hermès*, (1), 95-101, [online], December 31, 2024.

[13] Metz, S. (2003). Asymmetric warfare and the future of the West . *Politique étrangère*, 25-40, [online], December 31, 2024.

[14] Centre Interarmées de Doctrines et d'Expérimentations, joint concept CIA-0.1.1_M2MC (2021), *Multimilieux et multichamps (M2MC), la vision française interarmées* , [online], December 31, 2024.

[15] Statista, *Internet penetration worldwide in July 2024, by region* , [online], December 31, 2024.

[16] Kushner, D. (2013). *The real story of stuxnet.* *ieee Spectrum*, *50*(3), 48-53, [online], December 31, 2024.

[17] Sami, A. (2019). *SCADA (Supervisory Control and Data Acquisition)* , [online], 31 December 2024.

[18] Vilmer, J. B. J. (2015). *Crimée : les contradictions du discours russe* . *Politique étrangère*, (1), 159-172, [online], December 31, 2024.

[19] Isaak, J., & Hanna, M. J. (2018). *User data privacy : Facebook, Cambridge Analytica, and privacy protection.* *Computer*, *51*(8), 56-59, [online], December 31, 2024.

[20] Le Monde, (2024). *« En raison de l'influence de TikTok, les juges roumains annulent la présidentielle »* , [online], December 31, 2024.

[21] Tangredi, S. J. (2013). *Anti-access warfare : countering A2/AD strategies* . Naval Institute Press, [online], December 31, 2024.

[22] Limonier, K., & Gérard, C. (2017). *Russian hybrid warfare in cyberspace* . *Herodotus*, *166167*(3), 145-163, [online], December 31, 2024.

[23] Orinx, K., & de Swielande, T. S. (2021). *Cognitive warfare-Why the West might lose to China.* . *Cognitive Warfare, La guerre cognitique*, 8-1, [online], December 31, 2024.

[24] Taillat, S. (2016). *A dissymmetric mode of hybrid warfare? Le cyberspace.* ***Stratégique*****, 89-106, [online], December 31, 2024.**

[25] Liang Q., Xiangsui W., (1999). *« Unrestricted warfare«* **, Beijing: PLA Literature and Arts Publishing House Arts, [online], December 31, 2024.**

[26] Sidaway, J. D., & Woon, C. Y. (2017). *Chinese narratives on « One Belt, One Road« (一带一路) in geopolitical and imperial contexts.* ***The Professional Geographer****,* ***69*****(4), 591-603, [online], December 31, 2024.**

[27] Mackiewicz D., (2018). « Cognitive warfare: Hamas & Hezbollah and their insidious efforts » **, Conference: INSS-Summer Institute 2018, Tel Aviv, Israel, [online], December 31, 2024.**

[28] Coelho,O. (2023). *Geopolitics of Digital Imperialism by leaps and bounds.* **. [online], December 31, 2024.**

[29] Pariser, E. (2011). *The Filter Bubble: What the Internet is Hiding from You* **. Penguin Press, [online], December 31, 2024.**

[30] Laban, T. A. (2024). *The Role of TikTok in Disseminating the Palestinian Narrative during the War on Gaza from the Perspective of Palestinian University Students.* ***Advances in Journalism and Communication****,* ***12*****(3), 394-408.**

[31] CNE Pascal MARTIN (Unité Nationale Cyber), (2024). *Note N° 109 - Le renouveau des « mesures actives« soviétiques avec le numérique et la « russianisation » des opérations de manipulation de l'information* **, Centre de Recherche de la Gendarmerie nationale (CRGN), [online], December 31, 2024.**

[32] Rémy Hémez, (June 2018). *« Deception operations. Rethinking Guile in the 21st Century »* **, Strategic Focus, n° 81, Ifri, [online], December 31, 2024.**

[33] Hung T. C, Hung T. W, (2022). *« How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars »***, Journal of Global Security Studies, vol.7, n° 4, [online], December 31, 2024.**

[34] Nye, J. S. (2019). *Protecting democracy in an era of cyber information war* **. Belfer Center for Science and International Affairs.**

[35] Hung T. C, Hung T. W, (2022). *« How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars »* **, Journal of Global Security Studies, vol.7, n° 4, [online], December 31, 2024.**

[36] Julien Debidour Lazzarini, (2024). *Au-delà des champs de bataille de la guerre régulière : modes d'actions et cibles des opérations de guerre cognitive* **, PANTHÉON-SORBONNE SÉCURITÉ-DÉFENSE, [online], December 31, 2024.**

[37] Bleakley, P. (2023). ***Panic, pizza and mainstreaming the alt-right : A social media analysis of Pizzagate and the rise of the QAnon conspiracy.*** ***Current sociology*****,** ***71*****(3), 509-525.**

[38] Le Monde, (2024). ***L'Europe face à l'ingérence russe*** **, [online], December 31, 2024.**

[39] Institut Français d'Enseignement Stratégique et Opératif website, ***Éléments de compréhension de l'art opératif*** **, [online], December 31, 2024.**

[40] Kaspersky website, ***What are bots? Definition and explanation*** **, [online], December 31, 2024.**

[41] Remarks by Colonel Bansept, researcher at Ifri's Center for Security Studies and member of the Defense Research Laboratory. In : ***Action in the « gray zone« will be the future focus of French Special Forces*** **, Zone Militaire** ***(www.Opex360.com)*****, [online], December 31, 2024.**

[42] ***Éléments publics de doctrine militaire de lutte informatique d'influence (L2I)*** **, Ministère des Armées, COMCYBER, (2021), [online], December 31, 2024.**

[43] Laurent Figneau, (2024). ***A submarine cable linking Finland to Germany has been cut by an « outside force«*** **, Zone Militaire** ***(www.Opex360.com)*****, [online], December 31, 2024.**

[44] Le Monde, (2024). ***Baltic submarine cable failure : suspect tanker from Russia boarded*** **, [online], December 31, 2024.**

[45] Le Monde, (2024). ***Nord Stream : plus d'un an après le sabotage des gazoducs, l'enquête en Suède se terminée sans aucune poursuite*** **, [online], December 31, 2024.**

[46] Bertrand, M. (2024). ***Hybrid war in the Red Sea-Houthis versus Western coalition*** **.** ***Global Security*****, (1), 25-28, [online], December 31, 2024.**