

The problematic of cyber Warfare: conceptual challenges and polemology.

Par Pr Joseph Vincent NTUDA EBODE

Dans **REVUE AFRICAINE DE PROSPECTIVE STRATÉGIQUE (RAPS)**, volume spécial, N°3, « Retour de la guerre », 2026

Joseph Vincent NTUDA EBODE (Dir)

Éditions **CENTRE DE RECHERCHE D'ÉTUDES POLITIQUES ET STRATÉGIQUES / UNIVERSITÉ DE YAOUNDÉ II**, Page 5 à 8

ISBN : 978-9956-0-2264-9

Article disponible en ligne à l'adresse
<https://www.creps.com>



Distribution électronique

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur au Cameroun. Il est précisé que son stockage dans une base de données est également interdit.

THE PROBLEMATIC OF CYBER WARFARE: CONCEPTUAL CHALLENGES AND POLEMOLOGY¹

Pr Joseph Vincent NTUDA EBODE

Professeur Titulaire des Universités Hors Échelles

Directeur du Centre de Recherche d'Études Politiques et Stratégiques

Université de Yaoundé II

For many experts in cyber war, the year 2012 has been an important date in the history of cyberspace. While the year 2011 was marked by a significant increase in information risk on the internet, in 2012, States that were previously observers of the anarchic development of globalized computer systems, for the most part, adopted internet security policies. This observation is based on what can be qualify as the recent emergence of a Cyber Cold War. Indeed, it can be argued that since 2012 the atmosphere among the five members of the Security Council can best be described as one of electronic Cold War. The United States, the United Kingdom and France, whose sensitive infrastructures (ministries, research centers, strategic companies), are increasingly targeted, and on the other hand, Russia and China, known for the bulk of cyber threats from criminal gangs and state intelligence services. This new dynamic, though still discreet, is evidenced by acts of large-scale cyber attacks. What is now commonly referred to as Operation Shady RAT, is a good example of such attacks. Unveiled in early 2011, this operation will have provided a typical example of the new geostrategic reality of what cyberspace has become. By encouraging military measures in the United States, Britain and France, Operation Shady RAT has managed to get cyber war out of its purely virtual dimension, into a tangible reality. This essay is structured into two main parts: the first part is a clarification of the concept of cyberwar (I), the second part will be concerned with the polemology of the cyber warfare (II).

THE CONCEPT OF CYBER WAR

The world of the twenty-first century seems to be one of information. The control of its means of production, processing and transport has become crucial and we cannot ignore the role played by the growth of the Internet. Information today and probably tomorrow will remain a major issue around which future conflicts will polarize. It is to these upheavals that policymakers, researchers and the military responded, thereby creating a major debate both on security and defense, and the new security challenges of the international community. Of these debates, it appears overall that though

¹ Cet article a initialement été publié dans le *Bulletin du CREPS*, n°002-003 de mars 2013

Internet opens up possibilities previously unimaginable for communication and information sharing, it is also the source of new threats.

In fact, the use of the network for civilian and military communication or data exchange... presents a multitude of threats that affect the very essence of war. The French specialist in security issues Jean Guinsel, discusses this perspective in his book *Wars in Cyberspace*, highlighting the changes that have and will affect the doctrines, concepts and modes of action in this new information environment. This is what was qualified in the early 1990s in the United States of America as, a revolution in military affairs (RMA).

Along with abundant literature dealing with the consequences of these new developments and future challenges, first in the U.S.A and then in Europe, many neologisms emerged to describe different situations, concepts and techniques... Phrases such as; information warfare, cyber warfare, cyber threats, cyber terrorism and cyber attack, dealing with relatively different phenomena such as economic espionage, revolution in military affairs, hacker attacks... separately or all together, became increasingly used.

If the study of cyber warfare is proving a tricky business, because of different classifications from one author to another, attempts to conceptualize these new forms of confrontation, however, were developed since 1992 under the general term Information Warfare. Martin Libiki of the RAND Corporation offers seven techniques of warfare including cyber warfare; the latter being for him a hodgepodge of techniques. More recently, his colleagues at the same Corporation, John Arquill and David Ronfeldt, in their book *Athena's Camp: Preparing for Conflict in the Information Age*, highlighted the two concepts of cybernetic war and war of networks. Cybernetic war is described as a technique of warfare to deal with future conflicts, while the war of networks is analyzed as a civil war part of this cyber warfare.

Through this informational perspective, the definition of war advanced by Sun Tzu in the fifth century Before Christ: «To subdue the enemy without fighting»; seems to be the essence of the information war; the aim being to gain control of the battlefield or even the neutralization of the opponent without physical fight. Ultimately, therefore, cybernetic war means this new form of confrontation in cyberspace opposing entities of different species such as states, corporations, opinion groups and individuals; for the control of information. It depicts actors who, through advanced techniques, dispute the information literacy and involve the civil and military information security.

In purely military terms, it is an operation in which computer technology replaces conventional weapons. The goals are multiple: to break the enemy computer defenses, steal information contained on opponent hard disk drives; jam enemy communications, destroying crucial information, spread propaganda... or do it all at once.

It proceeds through several methods:

- Vandalism that is materialized through attacks to alter or deface Web pages, or denial of service attacks. This type is easy to fight and usually causes little damage;

- Propaganda and disinformation: these are political messages (or of other types) likely to «shell» anyone on the internet;
- Data collection (using Trojans and spyware): here, confidential information that is not properly secured can be intercepted and modified, making espionage across the world possible;
- Stoppage or sabotage of equipment: in this case, military activities that implement computers and satellites to coordinate defense particularly targeted by attacks. Orders and communications can then be intercepted or altered, endangering the troops.
- Attacks on critical infrastructure: power plants, waterworks, petroleum tanks and pipelines, transportation and communication networks are vulnerable to such attacks. Cyber warfare encompasses all these forms, and can be considered as the use of computers and the Internet to wage war in cyberspace. That is why some experts describe it as a Fourth Generation War.

POLEMOLOGY OF CYBER WARFARE

From a polemological perspective, cyber warfare has seen two developments. Initially, in 1989, U.S. strategists gathered around W.S. Lind construed it as a Fourth Generation War (abbreviated as 4GW); understood as a total war that shows the limits of military power of the strong, rich and powerful.

According to these strategists, the First Generation of war based on the human mass, arranged in rows and columns on the battlefield, spanned from the era of the musket to WW I. The second based on the firepower of the gun and the airplane; mobilized upstream entire industrial machine to power opposite fronts such as the trenches. As for the Third Generation, it implied the ability to maneuver, as the Blitzkrieg of WW II. The victor in this case is the party that scatters and destroys enemy troops. The main determinants of power in this case are technology and speed. The Fourth Generation War (4GW), finally, is the product of information revolution and involves entire populations in an antagonism that spreads to all domains: political, economic, social and cultural. The target is the mental and organizational system of the opponent.

This fourth form, that is completely asymmetric, opposes two actors having nothing in common. On one side, there are high tech powers, supposedly favored by the Revolution in Military Affairs (real-time information, accurate and smart weapons, and remote command by digital networks). On the other, are scattered transnational or sub-national actors, religious, ethnic or interest groups, that attack markets, symbols of power and communications indiscriminately. The latter obey logic of disruption.

In a nutshell, if it is difficult to distinguish the idea of 4GW from related concepts such as asymmetric, non-state, low intensity conflicts, Net war or network warfare, it seems there is some unanimity in recognizing that given its characteristics, this new form of

war strikes at the heart of the enemy and deploys its resources in search for a media and psychological impact.

Ultimately it is the separation between war and peace that seems to be affected by this change. The basic question is what is the purpose of a war, where the strongest wins battle after battle only to lose all peace? This paradox has consequently led other scholars to talk about Fourth Generation War. Indeed, after the third, called the Cold War, the war waged by the United States today against terrorism and Islamism is like a new generation of war in which the superpower, unable to eliminate her enemies, rather multiplies them. Unable to submit her enemies to her will as in a conventional war, rather strengthens their hatred and resentment and, by affirming the existence of a unique and absolute enemy, opens new sources of hostility. As Gary Wilson quite appropriately asked, how do we fight and can we defeat an enemy without shape? How do you know that you won? What is gained and when do we know we won?