

MODERN ELECTROMAGNETIC SPECTRUM BATTLEFIELD

From EMS global supremacy to local superiority...

By

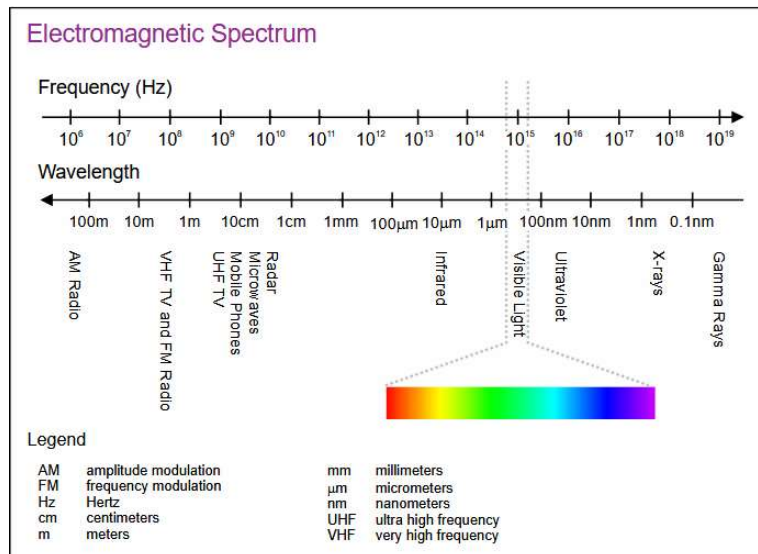
Major (Army) Stéphane RICCIARDI

Major (Armament Corps) Cédric SOUQUE

The views expressed are those of the authors and do not necessarily reflect the official policy or position of the French Ministry of Armed Forces or the French Government.

INTRODUCTION

As defined in the Joint Doctrine Note 3-16, the electromagnetic spectrum (EMS) is “the range of all frequencies of electromagnetic radiation. The electromagnetic radiation consists of oscillating electric and magnetic fields characterized by frequency and wavelength”¹. This radiation has particularly interesting properties: it can be visible or invisible, move at speeds approaching that of light, cross certain obstacles or, on the contrary, bounce off them (thus indicating their presence), transport energy or data.



Electromagnetic Spectrum (Joint Doctrine Note 3-16)

Considered nowadays as a strategic domain in its own right, EMS is at the heart of modern military operations and is the essential link between the land, air, naval, space and even cyber domains. At the base of all operational functions (remote sensing telecommunications, navigation), it also enables the delivery of offensive or defensive effects through electronic warfare (EW) or signal intelligence (SIGINT).

Since the end of the Cold War, the Western Armed Forces, exploiting a comfortable technological lead, had managed to achieve almost total electromagnetic supremacy. In other words, they have been able to use all their electromagnetic transmission and/or reception means without major constraint. They had real freedom of action in the field of frequencies during the whole duration and over all the geographical zone of the operation. This undisputed domination was notably decisive in the success of military operations in the Persian Gulf, the former Yugoslavia, Afghanistan, Libya and Mali.

Unfortunately, the increasing complexity and congestion of the electromagnetic environment (EME), as well as the emergence or return of competitors who have made a great effort regarding EMS capabilities, seem today to call into question the Western domination in this area.

Indeed, civilian applications are multiplying and the commercial stakes around EMS, such as 5G networks and internet of things (IoT), are constantly growing. In the military domain, hyper-connectivity and increasing digitization have also led to an exponential growth in frequency requirements.

Moreover, during the two last decades, many competitors have caught up technologically and developed means of contesting EMS. This evolution concerns both near-peer competitors², such as Russia or China, and intermediate powers, such as Iran. Even non-state actors (insurgents and terrorist groups) have benefited from the democratization of "low cost" EW equipment, most often based on dual-use technology.

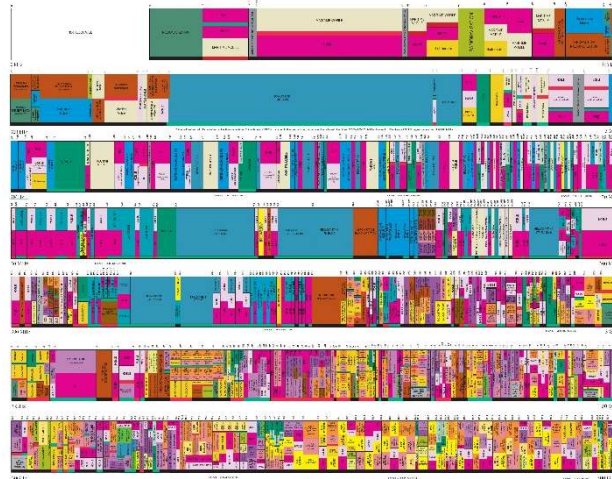
Given this increasingly congested and contested EMS, it seems appropriate to ask what strategy the Western Forces should adopt in order to maintain their freedom of action. Is it still reasonable to seek to regain global supremacy in EMS through a headlong technological rush?

The answer is no, because while R&D and funding will of course be essential to develop disruptive technology over the long term, they will not be sufficient in the short and medium term to regain initiative.

A more pragmatic and affordable approach must therefore be considered. It must be based on a more agile and intelligent management of the spectrum, but mostly on the concentration of effects and the subsidiarity at the tactical level in order to regain electromagnetic local superiority. In other words, it will be a question of establishing an EMS domination limited to the space-time framework of the current operational maneuver and strictly necessary for its achievement.

Electromagnetic spectrum: a complex and congested environment

"The spectrum has become increasingly complex. More players are accessing and leveraging sections of bandwidth, making it congested." Air Force Maj. Gen. Lance Landrum, 2020³



US Frequency Allocations - 2016 (U.S. Department of Commerce NTIA)

The multiplication of civil and military systems using the electromagnetic spectrum (EMS) leads to an increasingly congested environment and is the source of unintentional disturbances and a reduction of the operational margins of maneuver in the field of the EMS operations (EMSO).

Competition and interferences with civilian and commercial use

One of the main sources of congestion in EMS is due to its widescale use for commercial and non-commercial civilian applications. This general interest in the exploitation of EMS has led to an increased densification of transmitting systems, particularly in the frequency bands between 500MHz and 10GHz. Some bands, such as the 2 to 4GHz band, are particularly congested with the development of technologies such as Bluetooth, Wifi, WiMax, 4G networks and tomorrow's 5G.

This situation leads to many problems that affect military systems: competition between private companies and state agencies, inter-system interference and increasingly complex management of this resource. Moreover, faced with the economic and social stakes of these civilian needs, the political authorities are increasingly asking the military authorities to accept compromises (reduction or abandonment of frequency bands) or to find technical solutions to enable these developments for the public.

Among all civilian applications using EMS, the advent of the 5th generation networks (5G) will have the greatest impact on military systems in the coming years. The civil applications are quite numerous: high-speed communications, internet of things (IoT) and machine-to-machine (M2M) communications⁴ including autonomous vehicles. These developments and the use of new frequency bands (e.g. around 3.5GHz and 26GHz) will inevitably be a source of disturbance for military systems. That will affect many operational functions, such as:

- Tactical Radio communications. 5G characteristics (higher data rate, higher number of connected objects and higher number of frequency bands) will induce an overall increase in the level of electromagnetic radiation. This will inevitably lead to problems of electromagnetic compatibility (EMC) and interference on military radio systems;
- Satellite communications. The use by the 5G of the 26GHz band (24.25-27.5GHz) could disturb many Ka-band (27-31GHz) satellite telecommunications systems and cause degradations of the associated military capabilities.
- Weather forecasts. The use of the 26GHz band could also disrupt space weather systems operating between 23.6 and 24GHz. Specialists estimate that this could degrade by approximately 30% the reliability of weather forecasts⁵ that are critical to military operations.
- Radar and SIGINT systems. 5G technologies will make increasing use of the 3.5 GHz band, which is also used by many S-band (2 to 4 GHz) radars⁶. This could affect the detection capabilities of air traffic control and air defense radars in these bands. Signals intelligence systems could also be impacted in their detection and discrimination capabilities;
- GPS systems. Initiatives by companies such as Ligado Networks⁷ in the United States to deploy a low-power national 5G network in close proximity to the GPS frequency band could lead to interference with this critical positioning system for multiple military systems.

This issue will be much more complex than the frequency allocation as 5G applications is not exactly the same in all countries. Indeed, the standard identifies different frequency bands that can be used. Then, each country chooses which one will be used, taking into account its own constraints. For example, in France or the USA, 5G is deployed in the 3.5 GHz band while in China it is also deployed in the immediate vicinity of 5 GHz. In the future, these differences in frequency allocations could be an additional source of interference for the military EMS capabilities.

Of course, the interference related to 5G could increase and be even more complex to manage, since military capabilities should also exploit this technology in many fields of application⁸ such as command & control (C2), intelligence, surveillance, and reconnaissance (ISR) areas. Beyond the risk of interference, 5G-based military systems may be more vulnerable to cyber-attacks and espionage⁹. So far, most 5G equipment comes from China and it is difficult to control its security level¹⁰. Specific measures¹¹ will have to be taken to mitigate this risk, such as giving preference to Western suppliers or imposing stricter security rules on Chinese equipment¹².

Finally, in addition to the problems related to civil transmitting systems, other very specific sources of disturbance can unintentionally constrain EMSO. These include, for example, the topography (mountain, forest), urban buildings, climatic and meteorological conditions and some industrial activities such as wind turbine farms that have a negative impact on radar systems¹³.

Risk of interference with all deployed systems

However, civilian systems are not the only sources of the EMS congestion. Indeed, modern military operations, such as those conducted by Western Armed Forces, require increased capabilities using electromagnetic energy¹⁴: communication systems (for coordinating, navigation and C2 systems), active (radars and LASERs) and passive detection systems (electromagnetic and

optical sensors) and electronic attack systems (including directed effect weapons and jammers). These systems are distributed over the entire EMS¹⁵.

Consequently, frequency bands and data rate requirements¹⁶ have never been more important for military applications. At the same time, the increasing number and complexity of military transmitters on land, naval and air platforms create significant electromagnetic radiation that multiplies the risk of intra-system interference (auto-jamming, and even damage on front-end electronic components).

While the level of emission from each weapons system is already a big electromagnetic compatibility (EMC) issue, it becomes much more important in the case of a military force deployment. The multiplication of weapons systems in a small area increases the risk of disturbances. This will be the case in all domains; for example, in a naval deployment with aircraft carrier, destroyers and fighter aircraft or within a deployed battle group with many different types of ground vehicles and helicopters. As an indication, in 2015, the U.S. Armed Forces were a victim of more than 261 satellite communications jamming events. According to General John Hyten,¹⁷ Head of Air Force Space Command in 2015, the majority, indeed perhaps all, were caused by self-jamming.

And what about the risk of interference in a coalition operation or exercise? The majority of Western Armed Forces have chosen to improve their connectivity and resilience in EMS, and most have highly radiant communications and weapons systems, not to mention their own EW capabilities. As the different actors do not use the same types of equipment or even the same standards, the constraints on the EME worsen because of significant emissions in conflicting frequency bands.

How to deal with this environment without adapted EMS management tools?

As previously demonstrated, the increased use of EMS by civilians and the military is likely to disrupt many operational functions, such as tactical communications or connected C2. Even ISR systems and navigation capabilities could see their effectiveness reduced due to the blinding generated by this congested EMS. These disturbances, if they do not irremediably call into question the capacity for action in the spectrum, are nevertheless likely to degrade and constrain it from time to time.

Most of this interference could be reduced or even avoided if Western forces had agile and interoperable electromagnetic battle management (EMBM) tools¹⁸. Unfortunately, current tools are not adapted to this congested and complex environment because they were developed before the advent of 5G and the rise of military connectivity. This limitation will be all the more significant as the majority of the transmitting and receiving systems used by Western forces do not have the flexibility to adapt to this environment. Their ability to change frequency bands or waveforms to face interferences brought on by other civilian or military systems remains too weak.

In the short term, these limitations will require more and more circumvention measures, such as prohibiting the use of certain frequency bands, limiting the power of emissions or taking into account minimum distances between systems. If nothing is done, the accumulation of these measures will tend to reduce the maneuver margins of Armed Forces. However, some actions can be envisaged to mitigate this growing risk:

- Improving collaboration with civil and political actors to defend military interests directly within the decision-making board in charge of frequency band allocation and management;
- Adapting the existing EMS military systems by implementing waveforms that allow coexistence with civilian systems using the same frequency bands;
- Fostering the development of future capabilities increasingly flexible in terms of frequency band and waveform;
- Reviewing the EMBM tools¹⁹ to ensure compatibility with this modern environment. This will require better interoperability between systems.

Pending the implementation of these solutions, Western forces will continue to be constrained by this modern EME. While it will be difficult enough to deal with this complex and saturated spectrum, the main challenge ahead in this area for Western forces will most likely be the EMS contestation coming from their competitors.

Electromagnetic spectrum: a contested battlefield

*“The next war will be won by the side that best exploits the electromagnetic spectrum.”
Soviet Admiral Sergei G. Gorshkov, Commander of the Soviet Navy, 1973*



Russian Krasukha-4 EW system (Picture: mil.ru)



PLA EW capabilities (Picture: Global Times)

Recent strategic and technological developments have resulted in an increase in contestation in the electromagnetic field²⁰. Indeed, the threat has developed on three levels: leading actors in the EMS field who would like to acquire total domination; the probable rise in range of regional powers wishing to increase their capacity to deny access; but also the entry into the race of non-state actors relying most often on dual-use technology.

Strengthening EW capabilities of our near-peer competitors

Whether as an enabler of operational functions, for SIGINT or more directly for EW, EMS quickly emerged as a means of compensating for conventional power asymmetry in military confrontations. Russia was first to realize the advantage this could provide and throughout the twentieth century made the Red Army a reference in this field.

With the fall of the USSR, the young Russian Republic was unable to capitalize on its expertise and gradually lost its lead in EMS. However, Russia, but also China and other intermediate powers, took advantage of this turning point in history to pose as observers during the 1990s and 2000s and learn from the Western camp. Thus, the Gulf War, NATO's involvement in the Balkans but also, more recently, in Afghanistan, gave them the opportunity to monitor and analyze Western C2, ISR and EW systems and, moreover, build a tailored capability response to counter them.

In parallel with this technical and operational monitoring conducted in Western theaters of operations, China and Russia have also faced challenges in their own spheres of interest that have made them aware of the relative advantage they could gain from mastering EMS.

Russia

During the Georgian conflict of 2008, the first post-Soviet symmetrical conflict, the Russian army became suddenly aware of its lack of preparedness, even its downgrading, in the field of EW. This "electroshock" was one of the triggers of the Serdioukov reform of 2008²¹, which notably aimed

at a complete overhaul of the EW Russian model to make it the cornerstone of the Soviet defense system.

Above all, this reform involved a structural reorganization aimed at restoring general consistency to EW capabilities by integrating all resources under a single command²². Land forces today have five independent brigades to conduct EMS actions at the operational or strategic level, and each combat brigade has its own EW company. Naval forces have five centers dedicated to EW, two of which are exclusively for the Pacific fleet. Finally, the Air Force has five battalions directly integrated into the air defense divisions, 14 helicopter detachments, and one specifically dedicated to combat aircraft.

However, beyond a simple reorganization, the Russian electromagnetic reform has above all brought about a doctrinal rupture. Whereas the traditional Russian approach was essentially based on escort jamming, the new policy aims to be much more offensive and to move from the blockade of electronic information to the usurpation and destruction of opposing systems.

Moreover, it seems that this new, more agile doctrine was not devised in isolation but, on the contrary, to deliver its full potential within a more comprehensive strategy, that of hybrid warfare. Mastery of EMS can indeed be a particularly decisive asset to blind, deceive, or demoralize an adversary in a context of unclear engagement, where actions are difficult to attribute and remain permanently below the threshold of a declared war. The Ukrainian Donbass conflict of 2014-2015 demonstrated this effectiveness²³.

Regarding the capability aspect, without going into exhaustive detail, it is interesting to take a quick overview of the most disruptive equipment²⁴.

Within the Army, the heaviest investments have been made in jammers and SIGINT capabilities. Deployed in Syria and Ukraine, these systems have proved particularly effective in gaining full control of GSM networks²⁵, giving the lowest tactical level an offensive jamming and self-protection capability, but also in countering the ground-to-air threat by distorting aircraft location data, even when encrypted.

The Russian Navy also has a wide range of modern means dedicated to self-protection, jamming and decoying. Its most modern frigates are equipped with electro-optical countermeasure systems using low frequencies to disorient and blind enemy pilots. The Air Force, already at the forefront in the field, has supplemented its capabilities, especially via the development of new electronic countermeasure systems aiming to break through NATO's interdiction bubbles.

Finally, in addition to the modernization of its conventional electromagnetic capabilities, the Russian Armed Forces seem to have reinvested, in recent years, in research on directed energy weapons (A60 aircraft and the Peresvet gun project), as well as in weapons and ammunition using high-power microwaves to remotely neutralize the hardware of enemy aircraft up to 40km away.

China

Following in the footsteps of its Russian model, China quickly came to understand that EW will be a tool to be developed as a priority in order to deny its main competitors access to and control of the Western Pacific. This realization led to an accelerated modernization of its organization, doctrine and equipment which began with the concept of Integrated Network Electronic Warfare in the early 2000s²⁶.

This integrative logic has led organizationally to the creation of a Strategic Support Force (SSF) that controls all information warfare units, including cyber, space and EW.

In parallel with this structural reorganization, the People's Liberation Army (PLA) has also evolved its doctrine to ensure dominance over the entire EMS. This new strategy focuses more particularly on removing, degrading, disrupting or deceiving enemy electronic equipment.

Regarding its capabilities, it is particularly difficult to obtain precise information on the PLA's level of EW equipment. However, the latest annual report to the US Congress on the Military and Security Developments Involving the People's Republic of China²⁷ suggests that the PRC has a fairly complete spectrum of capabilities.

The Air Force, for example, might have a large fleet of SIGINT aircrafts and a special effort seems to be made regarding space capabilities: jamming of Western satellites' data and SATCOM using rendezvous and proximity operations (RPO)²⁸.

Finally, there is now no doubt that in the context of a major conflict the Chinese government is also preparing to use high altitude electromagnetic pulse weapons²⁹ (HEMP). By producing a powerful electromagnetic pulse, these weapons have an immediate, irreversible and devastating effect on electrical facilities, computer equipment and, more generally, on all communication systems within a certain perimeter.

For the Chinese government, HEMP could therefore be the ultimate building block in the so-called total information war. In a 2016 article by the Chinese National Security Policy Committee, HEMP is presented as a disruptive technology capable of recalibrating the balance of power. Embedded in hypersonic missiles or, even worse, in satellites, it could constitute a formidable "strategic surprise". Some experts now talk about a potential 21st century Pearl Harbor.

Democratization and proliferation of EMS among intermediate powers and non-state actors

While the last 20 years have seen strong resurgence of China and Russia in the race for dominance of EMS, there has been a parallel proliferation and democratization of EW means among both poorly equipped regional powers and non-state actors.

Indeed, the market for electromagnetic equipment has been largely restructured and diversified in recent years, favoring a drop in prices³⁰ and allowing intermediate powers to gain access to an "off-

the-shelf" range of equipment. In the Soviet market, for instance, a streamlining effort has been undertaken. Of the 120 companies listed in 2010, only 13 have survived and the two largest groups, KRET and Sozvezdie, share most of the domestic market as well as the export market.

Finally, in parallel with the development on offer, the market for EW equipment has also been boosted by an increase in demand. The proliferation of ISR and anti-access area denial (A2AD) means, particularly in Asia and the Middle East, is likely the main factor.

Thus, this concomitant increase in supply and demand has contributed to the proliferation of EW equipment among regional powers, whether they are allies or potential competitors.

For instance, in the Middle East's so called "arc of crisis", Israel is undoubtedly the regional power with the most comprehensive EW capabilities. Its ground forces have a full range of capabilities in signals intelligence, influence and communications jamming, as well as explosive device disposal³¹. Other neighboring nations such as Iran, although less advanced in the field, might still have GSM, SATCOM and GNSS jamming capabilities, as well as integrated EW systems, probably purchased from Russian companies.

The widening of the circle of states equipped with EW means is therefore a reality that will have to be dealt with in the years to come. However, while the threat from the main competitors will inevitably be the most serious, it will not be the only one in the field. Indeed, many non-state actors (insurgent movements, pirates, terrorist organizations or even proto-States) favoring asymmetrical confrontation can today more easily gain access to equipment that can disrupt the use of EMS in a more or less significant way. The latter, by using dual-use equipment or more simply by hijacking the use of purely civilian systems, will probably be able to bypass international arms trade legislation.

While their presence has not yet been officially observed, it is highly likely that we will soon find some of the following equipment or capabilities deployed in theaters of operation:

- Software Defined Radio (SDR), which leverages the intrusion capabilities into GSM, Wifi and Tetra networks³²;
- The jamming or even spoofing of unprotected GNSS equipment³³.

Impact on the Western armies' freedom of action

The strengthening of contestation in EMS and the spread of threats are not without consequences for the freedom of action of Western armies. Indeed, these may challenge their ability to carry out both offensive and defensive actions by depriving them of an enabler, which has become essential.

First, at the strategic level, this vulnerability might concern satellite telecommunications, which are today the keystone of an info-centric operations model (SATCOM, data transmission, GNSS).

Secondly, at the operational level, the democratization of A2AD equipment incorporating new-generation, barely detectable radars could directly threaten the ability of Western Armed Forces

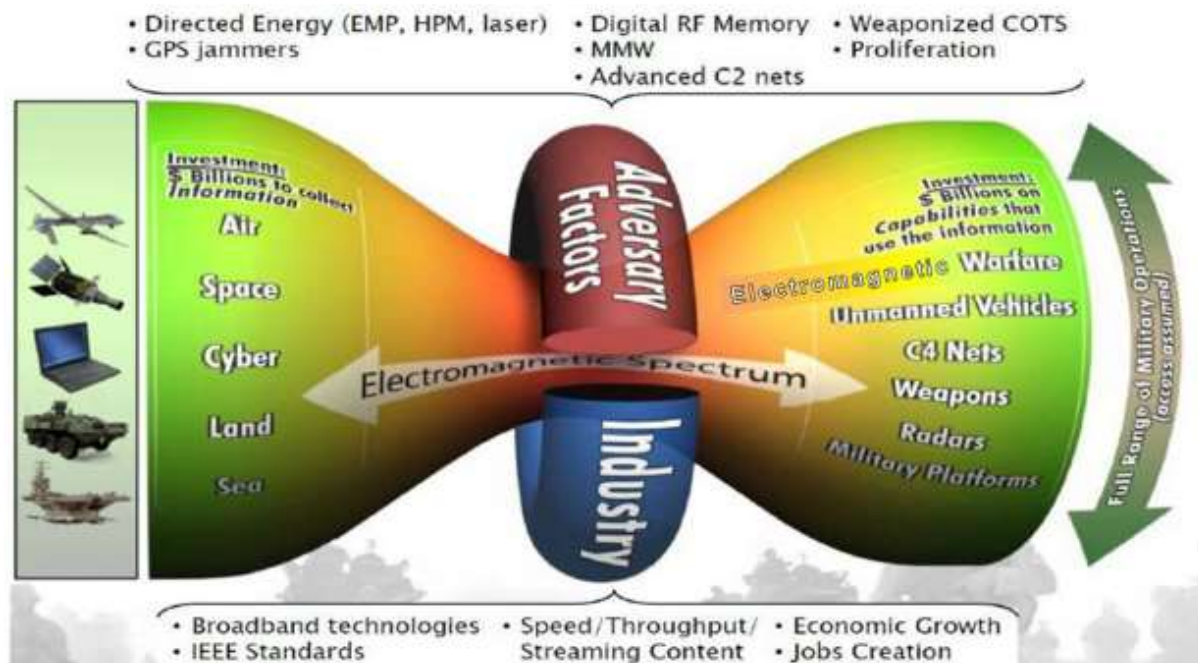
to get in first. And with regard to the defensive aspect, the threat might result in the use of low-technological means that, if used in significant quantities, could saturate even the most sophisticated defense systems.

Furthermore, it is perhaps at the tactical level that the loss of control of EMS could have the most critical consequences. Actions on GNSS services, for example, in addition to the effects on positioning and navigation, might hamper the use of Blue Force Tracking (BFT) or even lead to friendly fire in case of signal spoofing.

In the end, it seems that in parallel with the ever-increasing congestion of EMS we are also witnessing an insidious and widespread increase in the threat level in this strategic domain. Based on this observation, an effective strategy to deal with this has yet to be defined.

The utopian notion of regaining EMS supremacy

“We have lost the electromagnetic spectrum.” Alan Shaffer, Pentagon’s research and engineering chief, 2014³⁴



Challenges of regaining a congested and contested EME (US Air Force AFDP 3-51)

Taking into account this increasing congestion and contestation of EMS, the first option for Western countries could naturally be to try to regain global supremacy in this environment. To assess whether such a reconquest is possible, it is necessary for Western countries to ask themselves three key questions. The first one is about the current state of EMS and EW capabilities of the Western armed forces, i.e. the starting point. The second concerns the new technologies needed to regain this supremacy and their level of maturity, i.e. the means to achieve it. The last question is the ability of Western countries to win this future arms race, i.e. the credibility of this approach.

What is the current situation of Western EMS and EW capabilities?

After the end of the Cold War, Western Forces (especially American, French and English) intervened mainly in theaters where the electromagnetic field was barely contested. Thus, during operations in Afghanistan or the Sahel, EMS supremacy was acquired from the outset, and during the Iraqi, Balkan and Libyan campaigns, it was won relatively quickly thanks to kinetic and EW means outperforming the opposing forces.

However, from the early 2000s, insurgents from Afghanistan, Iraq or the Sahel region began to challenge this supremacy by conducting operations in EMS: RC-IED attacks, coordination in the context of ambushes, communication jamming or even GPS jamming, and more recently attacks using mini-drones or even interception of tactical data links. Unfortunately, as shown, these weak

signals were only the tip of the iceberg constituted by the massive rearming of intermediate and upper-spectrum powers in EW. The Western Forces failed to take the measure of this evolving conflict, which was a form of strategic myopia³⁵.

Since the low power opponents did not fundamentally succeed in challenging the freedom of maneuver of Allied Forces in these theaters of operation, Western countries did not seek to pursue their efforts to innovate in the field of EMS³⁶, particularly in the area of EW. On the contrary, Western countries have concentrated their investments in the acquisition of existing systems and in the adaptation of these means to threats or local specificities (RC-IED threat or resistance to GPS jamming), without taking into account the developments underway in other countries.

As the Western countries have not invested, at least not sufficiently, in new EW technologies and in new concepts of EMSO, the delay suffered by their armed forces in this area is significant today.

What are the new technologies needed and their maturity level?

Considering the current state of the EMS capabilities, regaining global supremacy in this area will require the development of new and innovative systems. The goal is to be able to deal with multi-domain strategies and systems (cyber, EW, A2AD) developed to reduce our capacity of action. Several orientations are being studied to find long-term solutions:

- Low Probability of Interception and Detection (LPI/ LPD) communication systems³⁷ that minimize the emission level and "dilute" the signal in order to complicate its detection for intelligence or jamming purposes;
- Cognitive EW systems³⁸ and other intelligent systems³⁹ with deep-learning capabilities;
- Quantum-based systems⁴⁰ such as quantum sensors⁴¹ (for enhanced radar or navigation systems), quantum communications (allowing high secure exchange against SIGINT systems), quantum computing (to speed up certain calculations such as EW data processing).

These solutions will rely on disruptive technologies (quantum or artificial intelligence) whose level of maturity must be developed before any operational deployment. These advances should make it possible to maintain an eventual supremacy regained over time by reversing the technological value chain and making it more complex for future adversaries to implement effective countermeasures.

Unfortunately, the development of these new technologies will require significant financial commitment, likely several billion euros over the coming decade. Beyond that, it is above all the quantity and diversity of weapons systems to be realized that will complicate this choice. In a particularly constrained economic context due to the consequences of the COVID-19 crisis, the sustainability of such a financial commitment is not guaranteed in the short term. It will require prioritization and trade-offs with other capabilities and will raise the inevitable question of abandoning other operational means.

Another fundamental issue is the time required to develop these new technologies. Thus, regardless of cost, it would likely take more than a decade⁴² to bring them to maturity and to develop and produce all the necessary weapon systems. Moreover, it is necessary to consider the additional time allowing for the operational ramp-up (recruitment and training of experts) in the use and maintenance of these new technologies.

In conclusion, the time and money needed to regain this global supremacy would leave Western Armed Forces vulnerable to threats in EMS in the short and medium term.

Could the Western camp win this new arms race?

The previous considerations do not take into account the likely reactions of the Western Forces' competitors. It is illusory to think they will passively wait for us to surpass them again. They will more likely continue their investments (until at least 2025 for Russia⁴³) and adapt their systems and strategies accordingly. Meanwhile, the intermediate powers will continue their reinforcement in EW.

The choice to invest massively in new technologies for EW, telecommunications or guidance and navigation in order to regain supremacy over EMS will inevitably lead to a new arms race. In fact, the race seems to have already begun, judging by how Beijing communicates frequently on their new military EMS technologies⁴⁴: anti-satellite weapons, directed effect weapons, artificial intelligence or quantum technologies. This competition would be profoundly different from the one that took place during the Cold War. Indeed, Western Allies will not have just one major competitor to contain but two, Russia and China, not to mention intermediate powers. This situation will make the management of this arms race much more complex and its outcome uncertain.

Another major issue is that the China of the 2020s is not comparable to the Cold War USSR. Indeed, the current economic power of China⁴⁵ alone is greater than that of the former USSR. Whereas the USSR's GDP never reached 50% of the USA GDP⁴⁶ during the Cold War, China's GDP has never stopped growing and today represents more than 66% of that of the US. Moreover, with an annual growth rate more than twice as high⁴⁷, China's economy could surpass that of the US by the end of the decade⁴⁸. On the other hand, although the Russian economy is more fragile⁴⁹, this country has abundant energy resources and a positive trade balance with a public debt lower than that of the Western powers. They should therefore be able to continue their efforts in the EMS field so as to be a credible competitor in this arms race.

The situation could be misleading regarding military spending. While the US remains largely in the lead in this area, it is necessary to pay attention to the underlying trends. Therefore, the gap that existed with China and Russia at the end of the Cold War has never stopped narrowing. This can be explained by a greater increase in military spending in both countries in recent decades. By comparing the average level of military spending during the 2000s with the 2010s⁵⁰, it appears that US military spending increased by 14% while it increased by more than 150% in China and 85% in Russia.

Moreover, this gap can also be qualified by the way the different competitors have invested. As demonstrated, Western countries have spread their investments over all capability sectors while Russia and China have focused their financial efforts specifically on EMS, which they consider the main axis of vulnerability of Western Armed Forces.

This economic and military context makes the situation less favorable for Westerners striving to regain EMS supremacy. With their favorable economic indicators, a reorganized military industry, a large labor force and unparalleled political freedom of action, China and Russia have significant advantages in this future arms race. Moreover, it is not necessary for them to conquer this supremacy: they need only maintain their ability to challenge it. Therefore, the technological and financial effort they will have to make will be less than that of the Western powers.

In conclusion, the success of such a purely technological and capability-based approach seems utopian in the short and medium term. This should force Western Forces to consider another choice, more progressive and based on adapted investments and new doctrines: regaining a localized superiority, in time and space, one sufficient enough to carry out each future operation.

Local EMS superiority instead of global supremacy



Whereas the restoration of global supremacy in EMS no longer seems attainable in the short and medium term for Western countries, this does not mean that they must completely change their concept of operations, which is primarily based on the mastery of information from the tactical to the strategic level.

However, preserving freedom of action in future conflicts will require an adaptation of this model via a more agile and intelligent management of the frequential resource but, above all, by concentrating the electronic effects in a well-defined space-time framework.

Local superiority, or the art of concentrating effects and means

As is already the case in other fields, the principle of concentration of effort, applied to EMS, would make it possible to compensate for the loss of global supremacy. The principle of concentration of effort is one of the three principles of war attributed to Marshal Foch and which have since constituted the fundamental basis of Western doctrinal thought. Conceptually, it is a matter of concentrating in the same place and at a particular time all the power vectors in order to tilt or re-establish a favorable balance of power. Thus, in a situation where the overall domination of the adversary would not be attainable by qualitative or quantitative outclassing, the partition of the enemy by the maneuver can allow for their sequential defeat.

Yet in EMS, what could this local superiority correspond to? As we have seen previously, it now seems to be illusory to want to dispose of the entire EMS at will and, at the same time, deny the enemy access to it for their own use. The conquest of electromagnetic superiority limited in time and space would aim at providing the strictly necessary and sufficient EMS resources to carry out a given mission within a well-defined space-time context. In other words, it would be a matter of concentrating EMS efforts on a particular point of application and during a chosen time period in order to guarantee the use of an effector deemed essential to the accomplishment of the mission, or conversely, to deprive the enemy of a key capability.

For instance, it could be a question of preventing the enemy from local use of its communications and its EW means by massive and indiscriminate jamming, accepting, if necessary, and as a counterpart, the deprivation of one's own EMS means. This could also result in increasing the use of decoy and deception in making the adversary doubt the effectiveness of their EW and A2AD systems.

Strictly necessary and sufficient capabilities to open a window into enemy defenses (available and cost-effective technologies)

The preference for local EMS superiority rather than global supremacy is justified in part by a rejection of a new, potentially ruinous and uncertain arms race. However, this does not imply the complete banishment of technology from future orientations but rather integrating into weapons systems technology that already exists, potentially dual-use and available in sufficient quantities. Such technology would notably allow for greater agility and resilience while also being cost-effective. Indeed, the conquest of local electromagnetic superiority will require strong autonomy of the most advanced units and consequent adaptability of their systems using EMS. In particular, the aim would be to deploy offensive EW systems down to the lowest tactical level, offering jamming, interception and electromagnetic deception capabilities.

In addition, a transition to increasingly software-defined types of equipment will also bring more physical agility and better system survivability by transitioning from heavy systems to potentially lighter (with equivalent capacities) and redundant ones.

Moreover, in order to confer local EMS superiority, it is essential that these future systems be saturating owing to their “mass effect”, and inexpensive with regard to their efficiency. Therefore, in addition to the above-mentioned directions it will also be necessary to have low-cost, low-tech equipment, capable of deceiving or momentarily saturating the enemy's sensors owing to weapons or EW payloads.

For example, in the air environment, this approach could be based on the use of swarms of air-launched mini-UAVs, or decoy systems with a reasonable cost (lower than that of a cruise missile), equivalent to the U.S. ADM-160 MALDs⁵¹. Inert, or equipped with adapted decoy capabilities, or even powerful jammers, these effectors could locally and temporarily incapacitate the most sophisticated enemy defense systems by saturating their sensors and information processing capabilities and depleting their ammunition stocks. Moreover, they could also be highly effective in conducting deception operations, by stunning enemy C4ISR systems.

During their various deployments in the Syrian, Libyan and more recently in the Nagorno-Karabakh regions, the Turkish Armed Forces have demonstrated the effectiveness of this strategy. With the massive use of UAVs equipped with destruction capabilities and EW payloads, they have succeeded in saturating their enemy's defenses and inflicting significant losses at a relatively limited cost⁵².

This strategy can also be applied to land operations, and many projects are underway to provide local saturation capabilities in EMS. In particular, the United States is reportedly developing a concept called the Modular Electromagnetic Spectrum Deception Suite (MEDS)⁵³. This system should eventually enable electromagnetic deception operations by reproducing the electromagnetic signatures of friendly units, but also creating electromagnetic noise capable of saturating enemy detection and command systems.

Finally, one of the keys to regaining local electromagnetic superiority could lie in integrating into EW, at the tactical level, the cyber component. Indeed, due to an ever-increasing part of the logical and application layers in all systems using EMS, it seems that the boundary between EW and cyber warfare is tending to disappear, such that it is now appropriate to refer to it as cyber-electronic⁵⁴ warfare. The perspective of local electromagnetic dominance would thus imply the emergence of some degree of autonomy in cyber combat down to the tactical level.

This evolution will largely rely on the development of individual human skills but will also require an increasing integration of artificial intelligence to overcome the technical barriers between the cyber and EMS fields. In particular, it will make it possible to place cyber actions in the tighter tempo of EW actions by automating the phases of acquisition and analysis of cyber intelligence, as well as the development of ad hoc malware to attack enemy systems.

Accepting to fight in a degraded EME by developing decision-making autonomy down to the lowest level of command

While the conquest of local EMS superiority will not be possible without the help of technological tools, it will also call for a doctrinal paradigm shift in order to promote decision-making autonomy down to the lowest level of command. This change will concern tactical and operational means of action, command systems and procedures, but also the collective and individual ability to fight in a contested and congested EME.

The undisputed dominance of EMS over the last twenty years in expansionary conflicts has gradually led Western Armed Forces to have an increasingly centralized command and control system for their operations. Indeed, the ability to access information relatively consistently and instantaneously down to the lowest level of command has contributed to an overwhelming of decision-making levels and created a strong dependence of our command architectures on information and communication systems.

Therefore, conducting operations in a contested EME will inevitably imply getting used to intermittently losing the link with the most forward units, giving more space for subsidiarity. Actually, it would mean adapting the concept of the "conducted battle", where the subordinate iteratively performs a series of tasks (or sub-missions) in order to achieve an overall objective, in favor of the concept of "mission command". The latter cedes more initiative to the subordinate to choose the course of action best suited to the success of the mission.

In addition to a potential loss of connectivity to the rear, a highly contested EME could disrupt or even disable the overall consistency of the most advanced weapons systems, whose strength relies heavily on the hyper-connectivity of their various components. Therefore, on the one hand Western Armed Forces will need to ensure that these new systems are as resilient as possible to the threat (in particular by using highly directional beams, such as FH, which are difficult to jam and intercept) but also, on the other hand, must prepare for the worst-case scenario by considering the eventuality of temporarily operating in degraded mode.

Moreover, beyond the doctrinal and technological evolution, the ability to win in a contested EME will depend on how well troops have prepared for it through training and drilling.

Nowadays, it must be noted that Western Armed Forces, excepting perhaps the Americans, no longer train or do very much in these degraded electromagnetic conditions and, above all, no longer have the capabilities and structures that would allow them to do so. It might be appropriate, for example, to develop a larger center in Europe allowing for the use of longer-range weapons and using more modern ground-to-air threat simulation systems.

With regard to land forces, a small joint mobile Red Team-type unit could be created to systematically test the cyber vulnerabilities and capabilities of the units. This type of approach has, for example, been undertaken by the US Army, which is testing its new network architecture thanks to its Network Integrated Evaluation (NIE). In addition, it is essential that specific training be provided within each operational unit. In particular, it is important to re-educate tactical operators on electromagnetic discretion: whether for communications or data transmission, each soldier must learn how to choose the most suitable means of transmission and, above all, its transmission power, according to this factor.

Finally, it seems obvious that the ability to fight and gain superiority in a contested EME will also require a change of mindset and education within the armed forces, to instill an EMS "culture".

This change of outlook will aim in particular to minimize the weaknesses caused by the fighter's individual behavior and, on the contrary, exploit those of the enemy. As an illustration, local Wi-Fi networks deployed on forward bases in theaters of operation are potentially vulnerable to short-range adversary attacks.

Moreover, these networks constitute a further vulnerability since they are also used for the soldiers' well-being and personal communications. By simply monitoring social networks, but also by conducting influence actions through them, the enemy could weaken the morale and cohesion of the force or, worse still, compromise the execution of ongoing operations.

In addition, fighters' personal devices also constitute a vulnerability due to their technical characteristics. Smartphones are now ubiquitous in operations, and it is increasingly rare for soldiers to consent to part with them, even when engaged on the front line. However, beyond the source of information they represent, these devices are first and foremost transmitters that can betray the nature, volume and, above all, position of a unit through their electromagnetic signature.

In 2014, during the Donbass conflict, a Ukrainian artillery battalion was decimated within fifteen minutes by Russian counter-battery fire after its position was betrayed by an application installed on the personal smartphones of the unit's soldiers⁵⁵. Protection against electromagnetic attacks is therefore not just a matter for specialists. It concerns each soldier and requires individual awareness and discipline to reduce collective vulnerabilities.

CONCLUSION

Finally, it seems that an increasingly congested and contested EMS is a problem serious enough to challenge the dominance of Western Armed Forces in this field. More broadly, this loss of supremacy could jeopardize their freedom of action and their ability to conduct operations in an operating environment where information mastery has become a key issue.

This new situation calls for an immediate response, or a strategic downgrading will be unavoidable. First of all, it seems obvious that a financial and capability effort must be made; in the long term, only R&D will provide equipment disruptive enough to bridge the accumulated gap in the electromagnetic field and restore a favorable balance of power. However, this strategy will not be sufficient; indeed, it may not prove successful for several decades and could lead to a new, potentially ruinous technology race. Other options must therefore be considered in the short and medium term to maintain the initiative.

First, congestion of the spectrum might be overcome by a more agile and smart management of the frequency resource. This will be possible in the future through better coordination with civilian organizations, but above all by the development of new tools allowing for a dynamic control of EMS. Regarding the EMS contestation, a more pragmatic approach must be envisioned, one favoring the conquest of local electromagnetic superiority. The objective would be to regain the necessary and sufficient freedom of action to carry out any mission in a reduced space-time framework. The creation of this "window" in the enemy defense would require the development of saturating and decoying cost-effective capabilities, more agility and more decision-making autonomy, but also learning to fight in a now degraded EME.

Beyond a simple organizational and capability overhaul in EMS, it will surely be necessary to adopt an even broader approach in the longer term. Indeed, the limits between the different domains related to information management are becoming increasingly thin. Communication, influence, cyber and electromagnetic actions all tend today to form a technological and operational continuum, and it would be a mistake to keep considering them separately.

NOTES

- ¹ “Joint Doctrine Note 3-16 - Joint Electromagnetic Spectrum Operations,” Joint Doctrine (Joint Chief of Staff, October 20, 2016), I-2, https://fas.org/irp/doddir/dod/jdn3_16.pdf.
- ² “Strategic Update 2021” (French Ministry for the Armed Forces, 2021), 16, <https://www.defense.gouv.fr/content/download/605304/10175711/file/Strategie%20update%202021.pdf>.
- ³ C. Todd Lopez, “As in Other Domains, U.S. Use of Electromagnetic Spectrum Is Contested,” May 20, 2020, <https://www.defense.gov/Explore/News/Article/Article/2193532/as-in-other-domains-us-use-of-electromagnetic-spectrum-is-contested/>.
- ⁴ “Vodafone M2M Barometer Report: Internet of Things,” July 2015, <https://www.vodafone.com/business/news-and-insights/press-release/vodafone-m2m-barometer-report-reveals-rapid-growth-in-internet-of-things>.
- ⁵ Jason Samenow, “Head of NOAA Says 5G Deployment Could Set Weather Forecasts Back 40 Years. The Wireless Industry Denies It. - The Washington Post,” March 23, 2019, <https://www.washingtonpost.com/weather/2019/05/23/head-noaa-says-g-deployment-could-set-weather-forecasts-back-years-wireless-industry-denies-it/>.
- ⁶ Hugh Griffiths et al., “Radar Spectrum Engineering and Management: Technical and Regulatory Issues,” *Proceedings of the IEEE* 103, no. 1 (January 2015): 85–102, <https://doi.org/10.1109/JPROC.2014.2365517>.
- ⁷ Jill C Gallagher, Alyssa K King, and Clare Y Cho, “Spectrum Interference Issues: Ligado, the L-Band, and GPS” (Congressional Research Service, May 8, 2020).
- ⁸ John R Hoehn, Jill C Gallagher, and Kelley M Sayler, “Overview of Department of Defense Use of the Electromagnetic Spectrum” (Congressional Research Service, October 8, 2020).
- ⁹ John R Hoehn and Kelley M Sayler, “National Security Implications of Fifth Generation (5G) Mobile Technologies” (Congressional Research Service, October 8, 2020).
- ¹⁰ Andrea Gilli and Francesco Bechis, “NATO and the 5G Challenge,” *NATO Review*, September 30, 2020, <https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html>.
- ¹¹ 5G Working Group - INSA Cyber Council, “The National Security Challenges of Fifth Generation (5G) Wireless Communications - Winning the Race to 5G, Securely” (Intelligence and National Security Alliance (INSA), June 2019), https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf.
- ¹² Andy Purdy et al., “Don’t Trust Anyone - The ABCs of Building Resilient Telecommunications Networks,” *PRISM* 9, no. 1 (October 2020): 115–29.
- ¹³ ANFr, “Perturbations du fonctionnement des radars fixes de l’aviation civile et de la défense par les éoliennes,” May 2, 2006, <https://www.anfr.fr/fileadmin/mediatheque/documents/etudes/Rapport%20perturbations%20fonctionnement%20radars%20fixes%20Aviation%20Civile%20et%20Defense%20par%20eoliennes.pdf>. which covered the question of static Civil aviation and Defence radars (static air monitoring radars)
- ¹⁴ US Joint Chiefs of Staff, “Joint Publication 3-85 - Joint Electromagnetic Spectrum Operations,” Joint Publication, May 22, 2020, https://fas.org/irp/doddir/dod/jp3_85.pdf.
- ¹⁵ Department of Defense, “DoD Strategic Spectrum Plan” (US DoD, February 2008), https://www.ntia.doc.gov/files/ntia/publications/dod_strategic_spectrum_plan_nov2007.pdf.
- ¹⁶ “Electromagnetic Spectrum Superiority Strategy” (US DoD, October 2020), <https://archive.defense.gov/news/dodspectrumstrategy.pdf>.
- ¹⁷ Sydney J. Freedberg Jr., “US Jammed Own Satellites 261 Times; What If Enemy Did?” *Breaking Defense*, December 2, 2015, <https://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-an-enemy-tried/>.
- ¹⁸ Curtis E. Lemay Center, “AFDP 3-51 Electromagnetic Warfare and Electromagnetic Spectrum Operation,” Air Force Doctrine Publication 3-51 (US Air Force, July 30, 2019), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-51/3-51-Annex-EW-EMSO.pdf.
- ¹⁹ “Electromagnetic Spectrum Superiority Strategy” (USA Department of Defense, 10/20), https://media.defense.gov/2020/Oct/29/2002525927/-1/-/1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF.
- ²⁰ Olivier Letertre et al., “Regards croisés sur la guerre électronique,” *Etudes de l’Ifri* Focus stratégique, no. 90 (July 2019): 54.
- ²¹ Roger N McDermott, “Russia’s Electronic Warfare Capabilities to 2025” (International Center For Defense And Security (ICDS), September 2017).
- ²² Jean-Jacques Mercier, “L’organisation de La Guerre Électronique Russe,” *DSI*, no. 143 (October 2019).
- ²³ Aurélien Duchêne, “Guerre Électronique : Comment Les Capacités Russes Pourraient Fragiliser Les Forces Occidentales,” Aurélien Duchêne, September 2020, <https://aurelien-duchene.fr/guerre-electronique-russie/>.
- ²⁴ Yannick Genty-Boudry, “Guerre Électronique, Le Multiplicateur de Force Russe,” *DSI*, September 2019.

-
- ²⁵ Unknown, "In Syria Spotted New Russian RB-341V «Leer-3» Electronic Warfare System," *Defense News* (blog), 3, accessed January 14, 2021, http://defensenews-alert.blogspot.com/2016/03/in-syria-spotted-new-russian-rb-341v_14.html.
- ²⁶ Roger Cliff, "Anti-Access Measures in Chinese Defense Strategy" (RAND CORPORATION, 2011).
- ²⁷ Office of the Secretary of Defense, "Military and Security Developments Involving the People's Republic of China, Annual Report to Congress," 2020.
- ²⁸ Prepared Statment of Mr David Chen, Independent Analyst, "China's Advanced Weapons" (U.S.-China Economic and Security Review Commission, February 2017).
- ²⁹ Peter Vincent Dr. Pry, "CHINA EMP THREAT - The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack" (EMP Task Force on National and Homeland Security, June 10, 2020), <https://securethegrid.com/wp-content/uploads/2020/06/CHINAempTHREAT2020logo.pdf>.
- ³⁰ Brendan I. Koerner, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *WIRED*, February 18, 2014, <https://www.wired.com/2014/02/spectrum-warfare/>.
- ³¹ "IDF's Electronic Warfare Battalion: The Enemy's Headache," iHLS Israel Homeland Security, 2014, <https://i-hls.tumblr.com/post/106593530750/idfs-electronic-warfare-battalion-the-enemys>.
- ³² Simon Ballantyne, "Wireless Communication Security: Software Defined Radio-Based Threat Assessment," 2016, 72.
- ³³ Philippe Gros, "Les Opérations En Environnement Électromagnétique Dégradé" (IFRI, Observatoire des conflits futurs, May 2018), 10.
- ³⁴ Sydney J. Freedberg, "US Has Lost 'Dominance In Electromagnetic Spectrum,'" *Breaking Defense*, September 3, 2014, <https://breakingdefense.com/2014/09/us-has-lost-dominance-in-electromagnetic-spectrum-shaffer/>.
- ³⁵ Brendan I. KOERNER, "Inside the New Arms Race to Control Bandwidth on the Battlefield," *WIRED*, n.d., <file:///C:/Users/steph/Zotero/storage/36IQQGWH/spectrum-warfare.html>.
- ³⁶ Bryan Clarck, Whitney Morgan Mc Namara, and Timothy A. Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum" (Center for Strategic and Budgetary Assesments (CSBA), 2019), 3, https://csbaonline.org/uploads/documents/Winning_the_Invisible_War_WEB.pdf.
- ³⁷ Clarck, Mc Namara, and Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum," 2019, 25.
- ³⁸ John G. Casey, "Cognitive Electronic Warfare: A Move Towards EMS Maneuver Warfare," *Over The Horizon (OTH)*, July 3, 2020, <https://othjournal.com/2020/07/03/cognitive-electronic-warfare-a-move-towards-ems-maneuver-warfare/>.
- ³⁹ Matthew J Florenzen, "Unmasking the Spectrum with Artificial Intelligence," *JFQ Quaterly* 95 (October 2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-95/jfq-95_116-123_Florenzen-Skulkitas-Bair.pdf?ver=2019-11-22-151711-083.
- ⁴⁰ Rajesh Uppal, "With China Rapidly Militarizing Quantum Technologies, U.S. Army Funding Assessment of Military Potential of Quantum/Electronic Warfare (EW) Based Threats | International Defense Security & Technology Inc.," May 29, 2019, <https://idstch.com/threats/china-rapidly-militarizing-quantum-technologies-u-s-army-funding-assessment-military-potential-quantumelectronic-warfare-ew-based-threats/>.
- ⁴¹ Patrick Tucker, "Army Creates Quantum Sensor That Detects Entire Radio-Frequency Spectrum," *Defense one*, February 8, 2021, <https://www.defenseone.com/technology/2021/02/army-creates-quantum-sensor-detects-entire-radio-frequency-spectrum/171939/>.
- ⁴² Clarck, Mc Namara, and Walton, "Winning the Invisible War - Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum," 2019, 39.
- ⁴³ Roger N McDermott, "Russia's Electronic Warfare Capabilities to 2025" (International Center for Defence and Security - Republic of Estonia Ministry of Defence, September 2017), https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.
- ⁴⁴ Dr. Pry, "CHINA EMP THREAT - The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack."
- ⁴⁵ World Bank, "World Development Indicators," n.d., <https://datatopics.worldbank.org/world-development-indicators/>.
- ⁴⁶ Angus Maddison, *The World Economy: Historical Statistics*, OECD Publications, 2003, https://www.oecd-ilibrary.org/development/the-world-economy_9789264104143-en.
- ⁴⁷ World Bank, "World Development Indicators."
- ⁴⁸ CEBR, "World Economic League Table 2021," December 2020, 231, <https://cebr.com/wp-content/uploads/2020/12/WELT-2021-final-23.12.pdf>.
- ⁴⁹ Maddison, *The World Economy: Historical Statistics*.
- ⁵⁰ SIPRI, "Military Expenditure Database," 2020, <https://www.sipri.org/databases/milex>.
- ⁵¹ "MALD Decoy | Raytheon Missiles & Defense," www.raytheonmissilesanddefense.com, accessed January 16, 2021, <https://www.raytheonmissilesanddefense.com/capabilities/products/mald-decoy>.

⁵² Scott Ritter, “‘Like Horse-Mounted Cavalry against Tanks’: Turkey Has Perfected New, Deadly Way to Wage War, Using Militarized ‘Drone Swarms’ — RT Op-Ed,” [www.rt.com](https://www.rt.com/op-ed/508000-turkey-drone-swarms-war/), November 2020, <https://www.rt.com/op-ed/508000-turkey-drone-swarms-war/>.

⁵³ Mark Pomerleau, “US Army Working on New Electromagnetic Deception Tool,” C4ISRNET, November 23, 2020, <https://www.c4isrnet.com/electronic-warfare/2020/11/23/us-army-working-on-new-electromagnetic-deception-tool/>.

⁵⁴ Aymeric Bonnemaïson and Stéphane Dossé, *Attention : Cyber ! Vers le combat cyber-électronique*, 1re édition (Paris: Economica, 2014).

⁵⁵ Laurent Lagneau, “Les positions de l’artillerie ukrainienne trahies par une application pour téléphone mobile,” www.opex360.com, *Zone Militaire* (blog), December 23, 2016, <http://www.opex360.com/2016/12/23/les-positions-de-lartillerie-ukrainienne-trahies-par-application-pour-telephone-mobile/>.