Rogue exploitation of standard/norms and of the precautionary principle: how terrorism could exploit and pervert them

LCL Eric Filiol (ret)
ESIEA - Operational virology and cryptology laboratory
38 rue des Dr Calmette et Guérin 53000 Laval, France
filiol@esiea.fr, https://sites.google.com/site/ericfiliol/

Abstract: Most modern democracies and states have adopted a large number of standards and norms to promote and harmonize international trade. More recently, the precautionary principle has come to complete this regulatory arsenal especially in the field of security of states and citizens, their health, their private life ... The aim is also to protect government agencies against wrong decisions, especially when uncertain, immature technologies are concerned. Social, political and institutional security and stability has become heavily dependent on these new forms of regulation.
In this article we will show how this regulation arsenal could be exploited by actors whose purpose is to undermine seriously the States and their citizens. It is indeed possible to cause political, economic and social problems and then provoke severe disruption in the State activities and citizens' life. These attacks are likely to question the stability of these states by exploiting the protections designed specifically to protect them. We will consider one specific scenario for illustration. This scenario lies on a detailed analysis of specific and real cases from which our study and operational approach is based.
As a consequence we stress on the fact that an excess of regulation is likely to hinder the security and stability of nation states. In this context, it is not possible to have security/stability and freedom at the same time. The only solution seems to come back to fewer regulations, to replace the human component at the centre of a number of critical activities/domains and to limit the power and invasion of technology in them.

Keywords: Social terrorism – Precautionary principle – Standards – State regulation – Terrorism.

1 Introduction

Citizens in modern countries want to be protected against almost any kind of risks. On the other side, decision-makers who want to be re-elected or who fear the permanent risk of being prosecuted if they make wrong decisions as well take citizens' demands for a life increasingly safer and more secure.

This is particularly true when considering the technology issues. Science and technical world make too quick progress to take the time of questioning this progress and its consequences on society and citizens' life, health... Recent cases throughout Europe have made headlines.

As it is inconceivable to restrain and slow technological progress, the precautionary principle has been adopted as a routine safeguard: when in doubt we shall not be fixed and drastic limits are taken. The problem with this principle is twofold:

- Firstly there is nothing to prove that these limits are sufficient. They are often set by experts who have direct links with industry and with commercial interests.
- On the other hand, these limitations and their existence can be exploited by malicious people to conduct attacks. In other words, measures taken to protect the State and/or its citizens can backfire. The cure is worse than the disease.

In this short article we will show through a simple scenario how the precautionary principle and the norms/standards can be exploited and misused. It is important to keep in mind that the term "attack" must be taken in the broadest sense: it is any action whose outcome is likely to disturb public order, the stability of a state, the health and/or the safety and security of citizens ... (Qiao & Wang, 1999; Filiol, 2008).

We identified several instances of malicious exploitation of the precautionary principle, norms and standards that can be very effective. In order not to give ideas that could be used for bad purposes, we present only one scenario in this paper to illustrate our idea. If the latter can be avoided by suitable policy choices, for many others it is unfortunately not possible unless important changes are made in society or/and unless challenging huge financial interests.

The paper is organized as follows. Section 2 will first present the definition of standards/norms and of the precautionary principle. We will focus on their intrinsic differences. Section 3 will then address the particular case of cell telephony and voting machines, on a technical basis. Section 4 will then explain how an attacker could exploit the norms in the field of cell telephony and the application of the precautionary principle of voting machines. We will then show with our scenario how to mix those two (seemingly) different and uncorrelated aspects to cause a major, political crisis in a Western country. We will then conclude by addressing the protection issues against that particular risk.

2 Standards, norms and the precautionary principle

Let us recall a few terms in order to make things clear in the reader's mind.

First a **technical standard** is an established norm or requirement about technical systems (Wikipedia, 2010a): ``*It is usually a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. In contrast, a custom, convention, company product, corporate standard, etc. which becomes generally accepted and dominant is often called a de facto standard […] The standardization process may be by edict or may involve the formal consensus of technical experts*.'' So norms and standards do not imply security or safety issues but are just way to make industry speak the same voice. But since all people are working on the same (technical) basis, it is then possible to

- To know how they work, think and develop.
- What they use (on the customer's side)
- To design a powerful attack that has the maximum impact.

The most widely known case relates to operating systems. Microsoft Windows has de facto become some sort of norms. This is the reason why most of the attacks are targeting Windows systems. More recently the analysis of the Stuxnet worm has shown that the wide use of Siemens' Programmable Logic Controllers (PLC) in industry may have facilitated an attack against a large number of industrial systems (and not only against Iranian nuclear facilities as claimed by a large number of ``experts''). The hypothesis according to which Stuxnet attack was a targeted one precisely does not hold since it relies on a widely used system. The rogue exploitation of standards/norms has been treated extensively in the literature so we will not address this case.

As for the precautionary principle is concerned, we will use the following definition (Wikipedia, 2010b): ``*The **precautionary principle** states that if an action or policy has a suspected risk of causing harm to the public or to the environment, in the absence of scientific consensus that the action or policy is harmful, the burden of proof that it is not harmful falls on those taking the action […]*

This principle allows policy makers to make discretionary decisions in situations where there is the possibility of harm from taking a particular course or making a certain decision when extensive scientific knowledge on the matter is lacking. The principle implies that there is a social responsibility to protect the public from exposure to harm, when scientific investigation has found a plausible risk. These protections can be relaxed only if further scientific findings emerge that provide sound evidence that no harm will result.''

In some legal systems, as in the law of the European Union, the application of the precautionary principle has been made a statutory requirement.

Figure 1 illustrates the complex decision diagram used to enforce the precautionary principle.

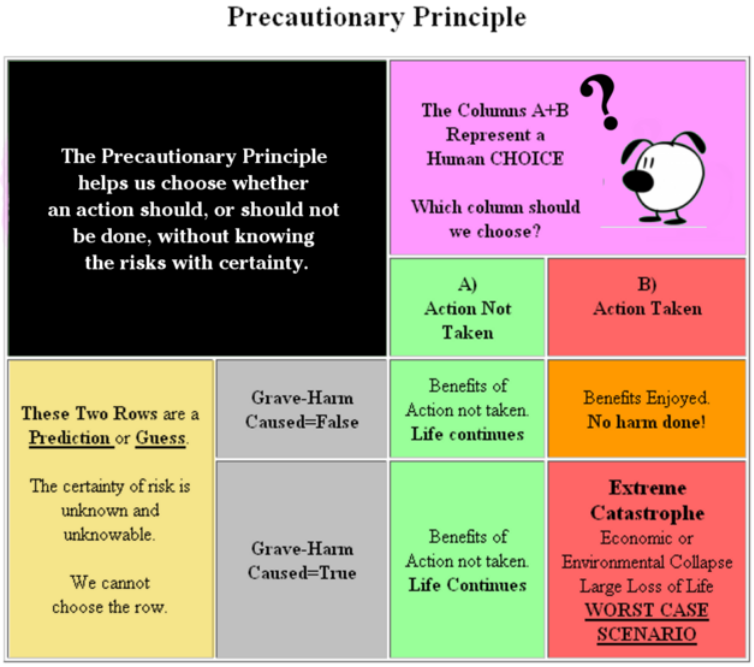

Figure 1. - Decision diagram of the Precautionary principle (source: Wikipedia, 2010b)

This diagram shows clearly that the aim, this time, is to find a balance between risks and benefits in an uncertain technological environment. The precautionary principle is in fact the principle of minimum risk, in a context of partial information due to the limits of the scientific knowledge.

There are a lot of examples in which this principle is applied. One of the best example relate to the effect of cell phone on users' health. Consequently to prevent any possible risk, a large number of limits have been imposed: cell phone power emission, antennas installation authorization, age of cell phone users... Public health is also another field where this principle has been widely applied.

Surprisingly we observed that the limits imposed because of the precautionary principle are different according to the field considered. This reflects the multiplicity of actors involved, the interests involved and the complexity of the context in which actors of different nationalities can intervene (national actors, supra-national actors...). This leads to inconsistencies that an attacker can exploit as we shall see in the scenario of Section 4.

3 Laws of Physics, Cell telephony and Voting machines

Before presenting our attack scenario, we need to recall a few technical facts in order to understand what is at stake.

3.1 A (very) few basics regarding the physics of electric fields

In physics, electric field denotes a field created by electrically charged particles. This field is used to determine at any point in space the electric force exerted by these remote electric charges. In the case of fixed charges in our study, the electric field is called the electrostatic field. More generally any device powered by electricity also produces an electric field denoted E. This is a vector field that at

any point in space combines a direction, a direction and a magnitude (amplitude). The norm of this vector is expressed in volts per meter (V/m). The scope of the electric field is theoretically infinite, their values at any point depending on the charge distribution or the nature of the material filling the space. According to the law of superposition if we have n charges q_i located at points P_i, producing an electric field E_i, the total electric field is additive (Durand, 1953):

$$E = E_1 + E_2 + E_3 + ...$$

Two charges (or devices) exert on the other an electric field which describes the interaction force between charges (or devices) point. Two charges repel each other while two charges of opposite signs attract each other proportionally to the product of their charges and inversely proportional to the square of their distance, the forces are of equal values and opposite directions, according to the principle of action and reaction.

3.2 Cell phone electric Fields

In the field of mobile telephony, most of the norms and standards were chosen so to satisfy (more or less explicitly) one or more principles of precaution, mainly to face to the controversy about the adverse effects on human health.

Mobile phones are radio transmitters/receivers that communicate with antennas. The frequencies currently used are within the range of 900 or 1800MHz (GSM) and 2100MHz (UMTS) without forgetting the 2400MHz range corresponding to Wi-Fi and Bluetooth for wireless access to terminals or using accessories communicating with mobile Bluetooth. Specifically, a GSM mobile always transmits with high power while the transmission power of a real 3G is usually much lower than that of GSM. Note that power is often not (or poorly) controlled via Wi-Fi and Bluetooth. It was therefore more likely to be exposed during an internet connection via Wi-Fi than 3G. Knowing that the frequency of Wi-Fi (2.4 GHz) has a reputation for being particularly harmful it is strongly advised to avoid this type of connection!

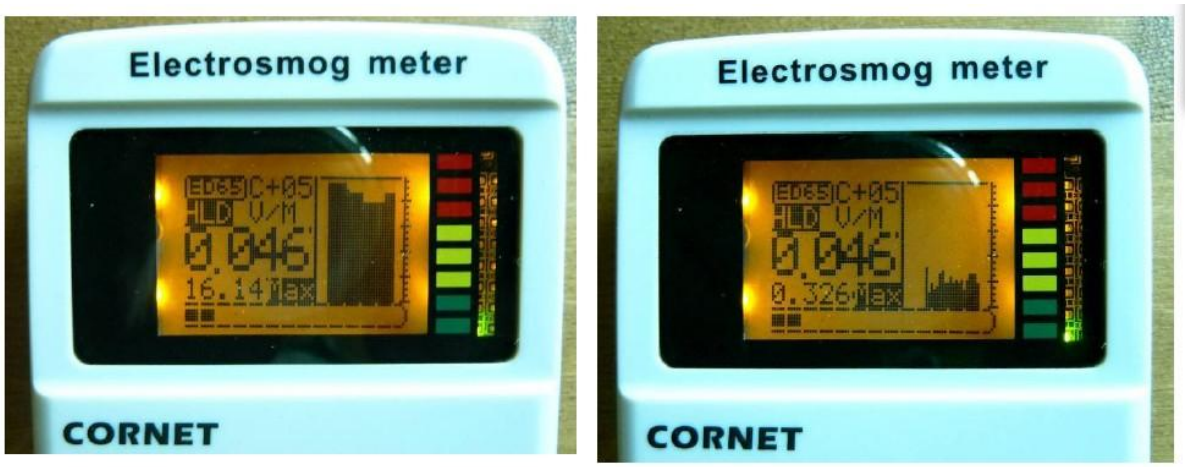

Figure 2.- Example of measurements with a probe ED65 Cornet: two photos taken during a test with a 2G/3G mobile, 30cm probe, short network connection (consulting of the talking clock) successively in GSM (left) and UMTS (right). The reception level is between 1 and 2 µW/m^2). There is a maximum level in GSM high (16V/m) and an ineffective regulation. As for 3G, the maximum level is much lower (0.3 V/m) and the control more responsive, without issuing full-power.

Low frequencies such as 900MHz are stronger than the higher frequencies. They are more penetrating (pass more easily through walls) and are therefore less absorbed by the body through. The high frequencies are less penetrating and therefore are more absorbed by the body exposed. They generate more energy. We must therefore reduce the power, which explains that GSM is issued 2 times weaker in 1800 than 900MHz. The current of UMTS 2100MHz is rather fragile (we realize this

by observing the bars, especially indoors). The 2400MHz used for Wi-Fi is the frequency used by microwave (high absorption)! Using a probe to measure the electric field produced by an HF phone allows an assessment of actual exposure in real time (this varies widely) by measuring the electric field mode ridge preferably, within different situations and mobile-probe distances.

GSM generate tens of V/m (sometimes more than 100V/m) in contact with the mobile and several V/m in an area close (few meters). The level depends on the mobile and the power regulation, but is still high in GSM. Levels generated by the 3G (UMTS) are much more variable depending on conditions (see Figure 2).

Measurements of electric fields emitted by smart or cell phones can, according to the use, reach several tens of m/V. Figures 3, 4 and 5 show this very clearly (source (electrosmog.info, 2010)).

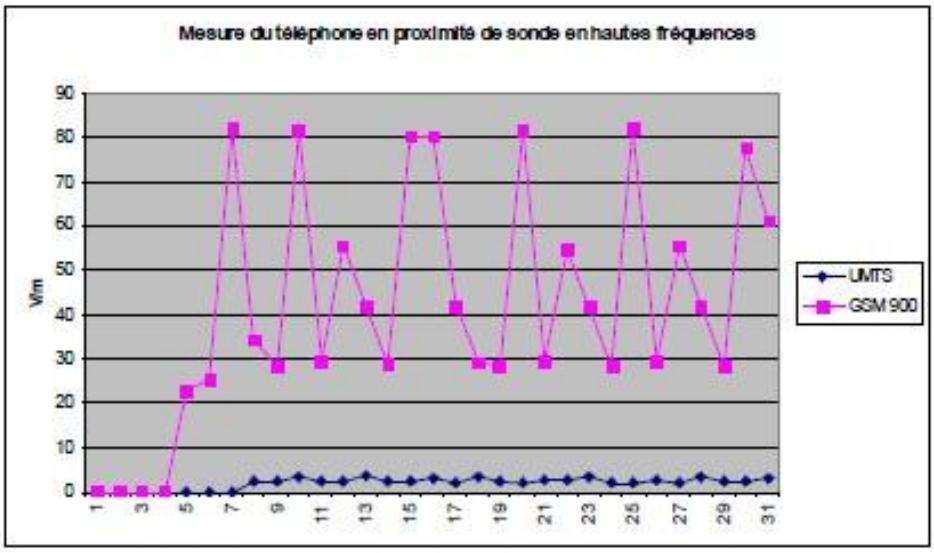

Figure 3.- Electric field values for GSM and UMTS emissions

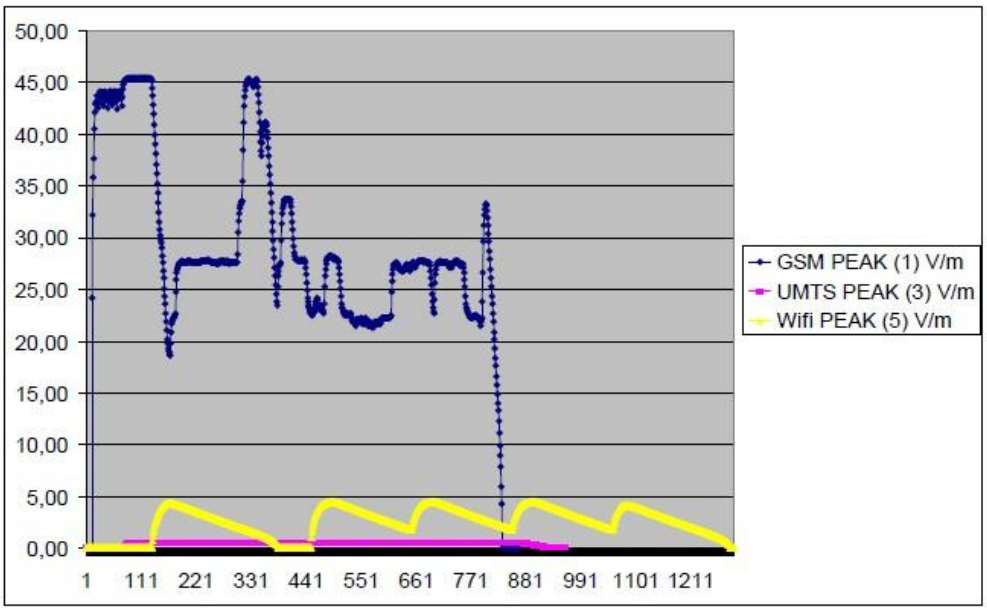

Figure 4.- Eletric field (HF) in peak mode (smartphone)

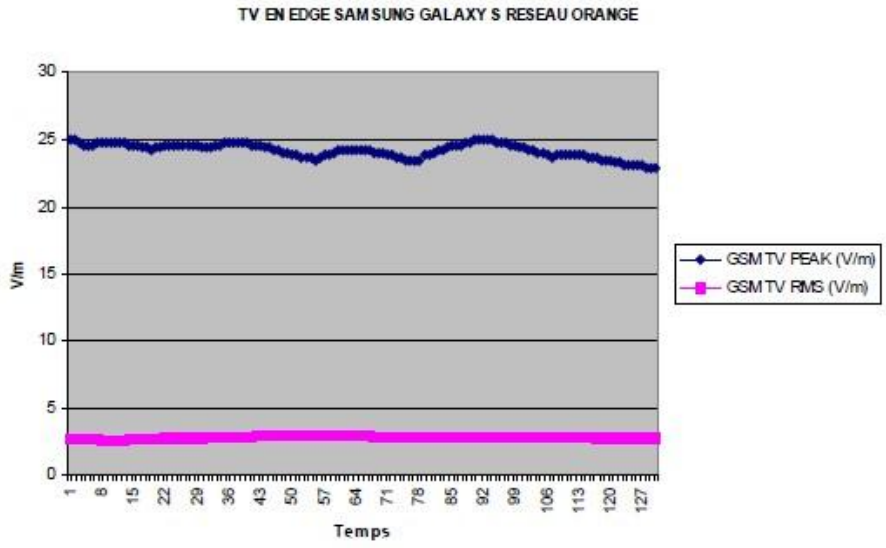

Figure 5.- Electric field emitted by a Samsung Galaxy S (TV on edge mode)

3.3 Voting machine and electromagnetic security

Electronic voting is a system of automated voting using computer systems. Electronic voting means the integration through the "electronic ballot box"(also called "voting machine" in French law) of methods to involve private companies in the voting system. The main selling point used to promote these products based on the idea of accelerating the process of the votes cast.

Despite a lot of discussions and passionate debates about the security of such machines voting machines are little by little invading the Western countries. As an example, in France, more than 750 polling stations have been equipped in 2005. Among the clients there were 45 cities cities including Le Havre, Brest, Lorient, Mulhouse, Bourges, Nevers.... A number of these cities are medium in size and represent, therefore, a significant percentage of voters. Thus, in France, the use of voting machines in 82 cities[1] more than 3500 people could reach 5% of the electorate (1.4 million voters), and thus play a significant role in the choice of France's president[2]. The main supplier of voting machines is the Dutch company Nedap. Nedap machines represent 80% of the installed base in France to cover 1.4 million voters. A number of other Western countries are also using electronic vote more and more.

We will not discuss the security issues regarding the vote itself. We will just mention the fact that a number of standards/norms have been fixed, most of them being chosen primarily to enforce the precautionary principle and stop critics against voting machines. To summarize, as soon as those limits and constraints are not fulfilled, an appeal to the Constitutional Council may be filed to cancel the election. Several cases are known in which local results have been cancelled.

We will consider one of these limits. Whatever the precautions taken, an electronic machine is susceptible to electromagnetic field (EMC) and the immunity levels of these machines is 10V/m[3]. Beyond this limit, votes cannot be considered reliable because of Electromagnetic Pollution or intentional generation of electromagnetic fields, if proof of compliance with the level of 10V/m can be provided by automatic recording level electromagnetic fields of each voting machine from the boot up count.

---

[1] http://www.zdnet.fr/actualites/informatique/0,39040745,39368609,00.htm?xtor=RSS-1

[2] http://www.marianne2007.info/Inquietantes-machines-a-voter-plus-d-1,4-million-d-electeurs-concernes_a935.html

[3] http://fr.wikipedia.org/wiki/Vote_%C3%A9lectronique

4 Scenario I: causing a national political security crisis

Now that the technical context is set up we will see how an attacker can exploit this.

4.1 The tactic theme

The WHITE country is on the eve of electing its president. According to surveys, the second round of elections will be very tight: the candidate of the ruling party is credited with 49% while that of the opposition can expect 51%. The WHITE country – which belongs to the Group of Eight G8 - is facing an economic and political crisis for several months. Its leadership in the world is threatened. International rating agencies, according to recurrent rumors, are thinking for several months to lower WHITE country's rating from AAA to AA +, AA or even AA-. If this were the case, it would cause major instability mainland and undermine the global financial balances worldwide.

The white country is involved in the war in BouKistan. Fundamentalist extremists accuse the WHITE country has to have voting laws that go against the commandments of Boukistanese religion.

The WHITE country has adopted voting machines in many cities, which affects approximately 6% of voters.

4.2 The course of events

On 6 May 2012, the second round of elections takes place. Participation is massive. Polling stations are full. After the election, the opposition candidate was elected with 50.8% of the vote. Within hours, the opposition appealed to the Constitutional Council to overturn the vote in 7 cities. This potentially affects 1.3% of the voters. The opposition claims of political manipulation and fear an attempted constitutional uprising. It follows a political crisis that will last a week. Many riots and street demonstrations as well large strikes are held across the country. The WHITE country is suspended to the decision of the Constitutional Council to validate or invalidate the results of these cities.

On May 15, 2012, the Constitutional Council decided to cancel the votes of the seven cities. The reason is that attempts to sabotage on voting machines make these votes invalid. New elections must be held. The opposition is convinced that it is an attempt at political manipulation. The crisis becomes more serious, the country is blocked strikes, violent riots. Supporters of the opposition leader try to occupy the National Assembly and block the presidential palace to protest against this cancellation.

International rating agencies lower the WHITE country's rating to AA. A major crisis has begun.

4.3 Course of events analysis

Facts are in fact very simple are based on a legal but malicious manipulation of the precautionary principle. Many groups of Boukistanese supporters were instructed to spend the whole day in polling centers equipped with voting machines. They were also instructed to bring their smartphones and watch TV on these smartphones.

At the same time, opposition leaders have been warned anonymously that the opposition was seeking to distort the functioning of voting machines and it would be nice to make measurements of electric field by a sworn person (bailiff) during the day. In a climate of political tension and of distrust with respect to voting machines, bailiffs equipped with sensors have detected an average electric field 4 times higher than the standard allowed to validate the electronic ballot.

The Constitutional Council had no other choice, once entered, to proceed to the cancellation of the vote concerned.

From a technical point of view, the continuous and additive emission of a significant number of electric field result in a global electric field interaction that exceed the limits imposed by the precautionary principle.

5 Conclusion

This simple scenario may appear somehow artificial not to say extravagant. In fact it is not. First it is inspired by real facts both related to voting machines and to other fields where the precautionary principle is (sometimes abusively) applied. Second, in this kind of attacks the problem is not to determine whether it had an actual effect requiring canceling indeed the vote. It just suffices to pour the doubt into the decision-makers and into the public opinion. Then this poison makes its effect. This is precisely where the insidious side of the precautionary principles.

The solution is not easy to take. It implies to change our views on the preeminent role of the technology and the market over the minds and over citizens. It is not a technologic issue but a problem of political will.

References

Col. Qiao, L. and Wang X. (1999) "*Unrestricted Warfare"*. People Liberation Army. Litterature and Arts Publishing House, Beijing. [online] http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf

Filiol E. (2009). *Operational aspects of cyberwarfare or cyber-terrorist attacks: what a truly devastating attack could do*. Proceedings of the 8th European Conference on Information Warfare and Security (ECIW 2009), Lisbon, Portugal, pp. 71—79.

Wikipedia (retrieved December 2010). Technical standard
http://en.wikipedia.org/wiki/Technical_standard

Wikipedia (retrieved December 2010) Precautionary principle
http://en.wikipedia.org/wiki/Precautionary_principle

The Independent (2007). *Public health: The hidden menace of mobile phones.*
http://www.independent.co.uk/life-style/health-and-families/health-news/public-health-the-hidden-menace-of-mobile-phones-396225.html

Émile Durand (1953). *Électrostatique*, Masson Ed. France. (1953). Seminal reference monography in three volumes : (Vol 1*: Distributions*, Vol 2*: Problèmes généraux & conducteurs*, Vol 3*: Méthodes de calcul).*

Electrosmog.info (2010). *Téléphones Mobiles et Champs Électromagnétiques.*
http://www.electrosmog.info/IMG/pdf/Telephones-Mobiles.pdf