

# Unconventional Attack against Voting Machines Enlarging the Scope of Cybersecurity Risk Analysis

Eric Filiol<sup>1,2</sup> 

<sup>1</sup>ENSIBS, Lab-STICC/IRIS, Vannes, France

<sup>2</sup>Higher School of Economics, Moscow, Russia

**Keywords:** Social Terrorism, Precautionary Principle, Standards, State Regulation, Security Policies, Security Models.

**Abstract:** Most modern democracies and states have adopted a large number of standards and norms to promote and harmonize international trade. 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, institutional security and stability and now cybersecurity has become heavily dependent on these new forms of regulation. In this article we will show how this regulation arsenal could be exploited by cybercriminals. It is indeed possible through a broader vision of the notion of cyber attack to turn these norms and standards and this precautionary principle precisely against those they are supposed to protect. Among many possible scenarios, we consider a specific one for illustration with respect to the attack of voting machines. The main conclusion is that any (cyber)security risk analysis should now extend the mostly favoured technical view to a more operational vision in which non technical aspects also be included.

## 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 in case of wrong decisions. On the other side, citizens have strong 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, freedom and civil rights, (cyber)security... Recent cases throughout Europe and the USA 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, (too) drastic limits are taken. The problem with this principle is twofold:


- On a first hand, there is nothing to prove/confirm 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 might be sometimes worse than the disease.

In this article we discuss and 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 and Wang, 1999; Filiol, 2009).

We identified several instances of malicious exploitation of the precautionary principle, norms and standards that can be very effective in an enlarged view of what a cyber attack is or could be. 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. This scenario lies on a detailed analysis of specific and real cases (a few being rather recent ones) from which our study and operational approach is based in which reasonable doubt and equally reason-

<sup>a</sup>  <https://orcid.org/0000-0001-5101-8073>

able suspicion cannot be completely ruled out. Reasonable doubt is in a way the other side of the precautionary principle.

If this particular case-study can be solved easily by suitable policy choices (forbidding the use of voting machine), for many others it is unfortunately not possible unless important changes are made in society, in critical or industrial infrastructures, large scale processes, large IT systems or whatsoever similar. Additionally, decision-makers are even more reluctant to adopt strong measures without challenging huge financial interests.

As far as the security experts are concerned, this shed a new light on the cybersecurity evaluation process and (cyber)security risk analysis which can no longer consider technical aspects only. Any attacker may consider a broader view and environment to build and drive his attack. In this respect turning the precautionary principle against the target can not only weaken its security but also hinder its defence, reaction and protection ability.

The paper is organized as follows. Section 2 first presents the definition of standards/norms and of the precautionary principle. We focus on their intrinsic differences. Section 3 then addresses the particular case of cell telephony and voting machines, on a technical basis. Section 4 then explains how an attacker could exploit the norms in the field of cell telephony and the application of the precautionary principle of voting machines. We then illustrate how to mix those two (seemingly) different and uncorrelated aspects with our scenario, 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

First a technical standard is an established norm or requirement about technical systems (Wikipedia, 2020c): *“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 know how they work, think and develop,
- to determine 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 so does recently Apple or Google (Jennings R., 2020). This is the reason why most of the attacks are targeting Windows systems. 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 only, does not hold since it relies on a widely used system. The Stuxnet attack is likely to be a specific instance of a larger series of attacks. 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, 2020a): *“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 (European Commission, 2000). Figure 1 illustrates the complex decision diagram used to enforce the precautionary principle. 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.

### Precautionary Principle

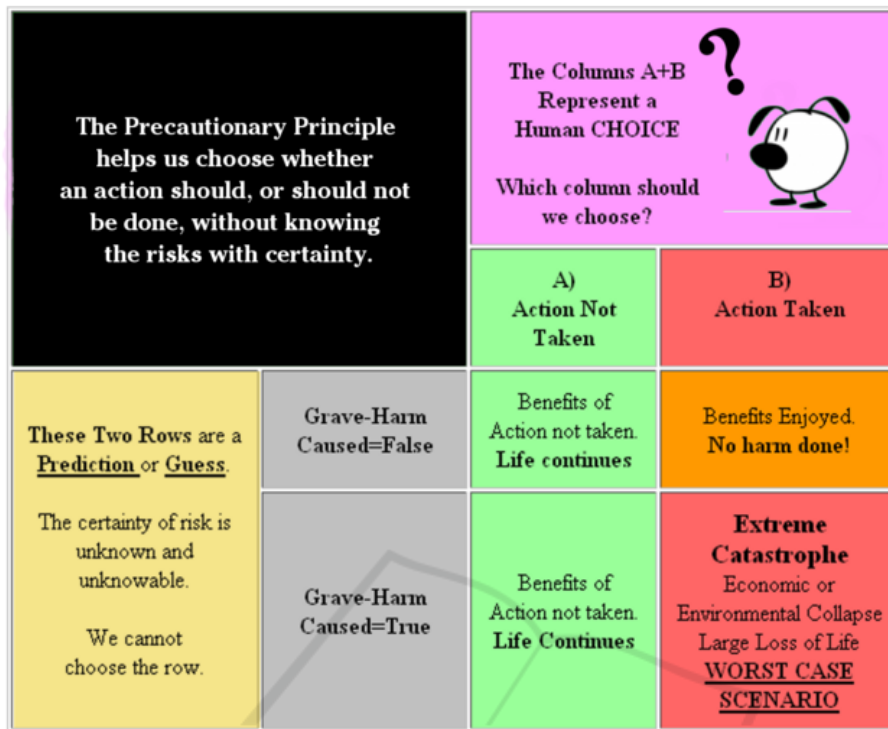


Figure 1: Decision diagram of the Precautionary principle (source <https://www.sourcewatch.org/index.php/Precautionary-principle>).

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 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 (Feynman et al., 2010):

$$E = E_1 + E_2 + E_3 \dots$$

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.

In fact, to be more precise, the fields do not add up arithmetically. The resulting field  $E_{\text{res}}$  is equal to the square root of the sum of the squares of the different components, i.e.:

$$E_{\text{res}} = \sqrt{E_1^2 + E_2^2 + \dots}$$

There are continuous fields (AC fields) and alternating fields (AF field or E-Field). DC fields have a fixed direction and a constant (or nearly constant) intensity over time (fields produced by a permanent magnet or the earth's magnetic field). Conversely, the strength of an alternating field varies over time (fields produced by the electrical grid or radio communication antennas for instance). Generally, variations in field intensity are repetitive with cycles of constant duration; frequency (expressed in Hz) is the number of times a cycle occurs in a second. The frequency of the fields produced the GSM 900 and DCS 1800 mobile telephone networks is 900 and 1800 MHz respectively (Pirard W., 2003).

### 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 1,800 MHz (GSM) and 2100MHz (UMTS) without forgetting the 2,400 MHz 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! As for newer 4G (LTE) and 5G, they respectively work at 2-8 GHz and 3-300 GHz.

Low frequencies such as 900 MHz 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 1,800 than 900 MHz. The current of UMTS 2,100 MHz is rather fragile (we realize this by observing the bars, especially indoors). The 2,400 MHz 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).

The 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)).

As for the 4G (LTE), a number of studies have established that the risk seems to be lower than for 2G and 3G phones (M. Hietanen and V. Sibakov, 2007; P. M. Mariappan and D. R. Raghavan and S.H.E. Abdel Aleem and A. F. Zobaa, 2016). According to (Persia et al., 2018), the EMF risk with respect to 5G seems possible. However there are still not enough studies on the risk of interferences to assess the actual level of risk.

### 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 the French law) of meth-



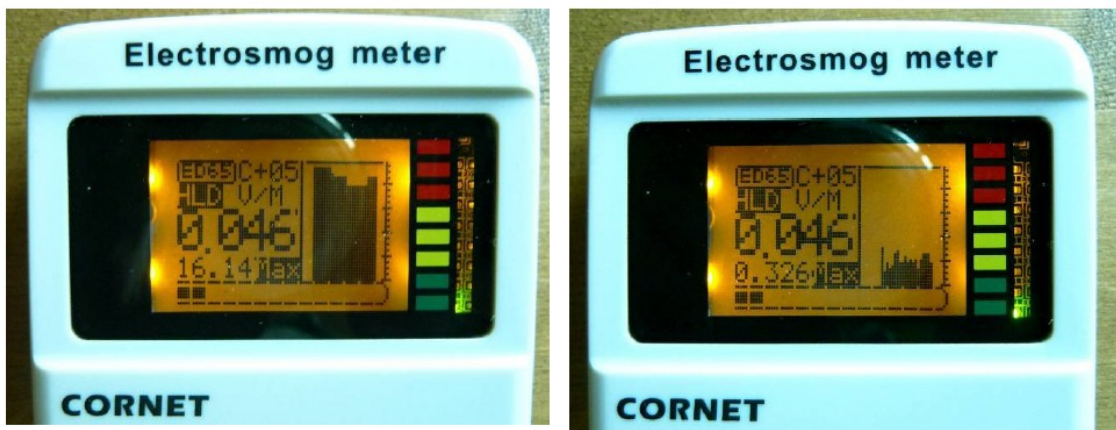


Figure 2: Example of measurements with a probe ED65 Cornet: two photos taken during a test with a 2G/3G mobile, 30cm probe, short network connection (consulting of the talking clock) successively in GSM (left) and UMTS (right). The reception level is between 1 and 2  $\mu W/m^2$ ). There is a maximum 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 (source (Electrosmog.info, 2010)).

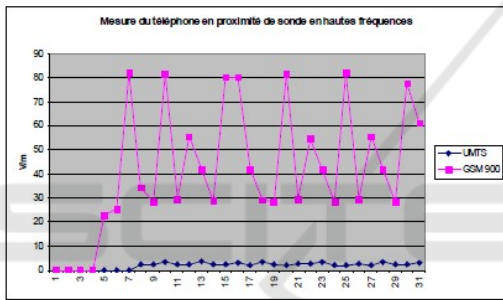


Figure 3: Electric field values for GSM and UMTS emissions (source (Electrosmog.info, 2010)).

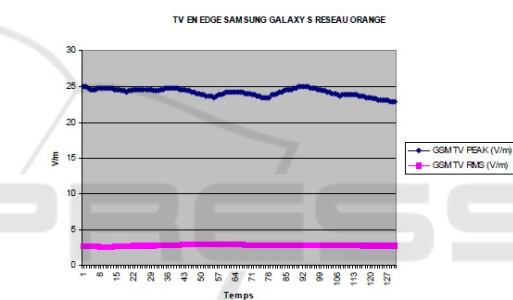


Figure 5: Electric field emitted by a Samsung Galaxy S (TV on edge mode) (source (Electrosmog.info, 2010)).

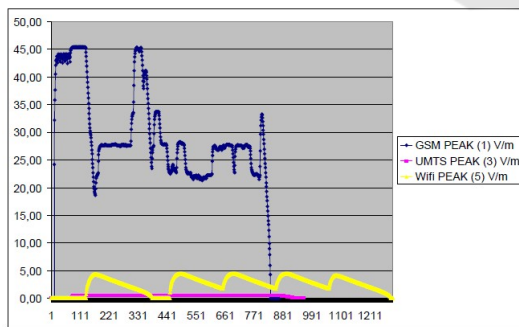


Figure 4: Electric field (HF) in peak mode (smartphone) (source (Electrosmog.info, 2010)).

ods 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 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 (Zdnet, 2007) more than 3,500 people could reach 5% of the electorate (1.4 million voters), and thus play a significant role in the choice of France's president. The main supplier of voting machines is the Dutch company Nedap (Gonggrijp, R. and Hengeveld, W.-J., 2007; OSCE, 2007; France Elections, 2020; Wikipedia, 2020b). 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. More recently, the US President 2020 elections have confirmed the ever-growing use of voting machines with a significant number of suspected security issues (for instance the case of Georgia (Gerstein J., 2020)).

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 or other Court (in the USA (Gerstein J., 2020)) may be filed to cancel the election. Several cases are known in which local results have been cancelled or voting machines have been forbidden (Reuters Staff, 2017; EDRi, 2007).

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 (US Election Assistance Commission, 2018, page 31, requirement 4.1.2.10), (Wyle Laboratories, 2007, page 9, section 6.2.4), (US Election Assistance Commission, 2015, Section 4.1.2.10). In all equipments, the precise requirement is *"Vote scanning and counting equipment for paper-based systems, and all DRE equipment, shall be able to withstand an electromagnetic field of 10 V/m modulated by a 1 kHz 80% AM modulation over the frequency range of 80 MHz to 1000 MHz, without disruption of normal operation or loss of data"*.

It is worth stressing on the fact that these technical limitations and requirements are nearly the same for medical equipments or critical equipments (European Commission, 2014, section E.1.1 p. 156) or (Zradzieski P. and Karpowicz J. and Gryz, K. and Leszko, Z., 2018, page 798). It is even more important to mention that a number of critical incidents have been reported over the years with respect to electromagnetic interferences on critical equipments (J. Ely, 2005; A. Boyer, 2018; R. D. Leach and M. B. Alexander and G. C., 995 ; The Independent, 2007). This is the reason why a number of political instances have enforced the precautionary principles to mitigate these risks as much as possible.

As a consequence, beyond these limits, votes could be considered as non reliable because of electromagnetic pollution or intentional generation of electromagnetic/electrostatic fields in the close environment of voting machines in use.

## 4 ATTACK SCENARIO: CAUSING A NATIONAL POLITICAL SECURITY CRISIS

Now that the technical context is set up we will see how an attacker can exploit this, through a fictitious but realistic attack scenario (inspired by real cases-studies).

### 4.1 The Tactical 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 rumours, 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 GREEN country. Fundamentalist extremists in this latter country accuse the WHITE country has to have voting laws that go against the commandments of their religious faith. The WHITE country has adopted voting machines in many cities, which affects approximately 6% of voters.

### 4.2 The Course of Events

On May 6<sup>th</sup>, 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<sup>th</sup>, the Constitutional Council decided to cancel the votes of the seven cities. The reason is that suspected 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 The Course of Events Analysis

Facts in fact very simple are based on a legal but malicious manipulation of the precautionary principle. Many groups of GREEN country supporters were instructed to spend the whole day in polling centers equipped with voting machines. They were also instructed to bring their 2G/3G smartphones and actively communicate with them.

At the same time, WHITE 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 cancelling 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 pre-eminent role of the technology and the market over the minds and over citizens. It is not only a technology issue but also a problem of political will.

This case above all shows that evaluating the security must go far beyond the pure technical aspects.

Any security risk analysis method should take non-technical attacks into account. Manipulating minds (as Psyops techniques usually do) may be as efficient as pure technical approach. Only the final result matters.

Finally, 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.

## REFERENCES

- A. Boyer (2018). Qualité Sécurité Environnement Risques électromagnétiques. <http://www.alexandre-boyer.fr/alex/enseignement/Boyer%20-%20QSE%202017-18%20-%20Risques%20EM%20-%20AE.pdf>.
- EDRi (2007). Electronic voting machines eliminated in the Netherlands. <https://edri.org/our-work/edriagramnumber5-20e-voting-machines-netherlands/>.
- Electrosmog.info (2010). Mobiles et Champs Electromagnetiques. <http://www.electrosmog.info/IMG/pdf/Telephones-Mobiles.pdf>.
- European Commission (2000). Communication From the Commission on the Precautionary Principle. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_00\\_96](https://ec.europa.eu/commission/presscorner/detail/en/IP_00_96).
- European Commission (2014). Electromagnetic Fields Vol. 1: Practical Guide - Directive. <https://osha.europa.eu/fr/legislation/guidelines/non-binding-guide-good-practice-implementing-directive-201335eu>.
- Feynman, R. P., Leighton, R. B., and Sands, M. (2010). *The Feynman lectures on physics; New millennium ed., Vol II*. Basic Books, New York, NY.
- Filiol, E. (2009). Operational aspects of cyberwarfare or cyber-terrorist attacks: what a truly devastating attack could do. In *ECIW'2009, 8th European Conference on Information Warfare and Security*, pages 71–79. ACPI.
- France Elections (2020). Machine à voter. <http://www.france-election.fr/machine.php>.
- Gerstein J. (2020). Judge freezes voting machines in 3 Georgia counties. <https://www.politico.com/news/2020/11/30/judge-freezes-voting-machines-georgia-counties-441342>.
- Gonggrijp, R. and Hengeveld, W.-J. (2007). Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective. pages 1–1.
- J. Ely (2005). Electromagnetic Interference to Flight Navigation and Communication Systems: New Strategies in the Age of Wireless.

- Jennings R. (2020). Google, Apple, Mozilla enforce 1-year max certificate expiration. <https://techbeacon.com/security/google-apple-mozilla-enforce-1-year-max-security-certifications>.
- M. Hietanen and V. Sibakov (2007). Electromagnetic interference from GSM and TETRA phones with life-support medical devices. *Annali dell'Istituto superiore di sanita*, 43:204–7.
- OSCE (2007). France - Presidential Election 22 April and 6 May 2007. <http://aceproject.org/ero-en/regions/europe/FR/france-election-assessment-mission-report/at.download/file>.
- P. M. Mariappan and D. R. Raghavan and S.H.E. Abdel Aleem and A. F. Zobaa (2016). Effects of electromagnetic interference on the functional usage of medical equipment by 2G/3G/4G cellular phones: A review. *Journal of Advanced Research*, 7(5):727 – 738.
- Persia, S., Carciofi, C., Barbiroli, M., Volta, C., Bontempelli, D., and Anania, G. (2018). Radio frequency electromagnetic field exposure assessment for future 5g networks. In *2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 1203–1207.
- Pirard W. (2003). Champs électromagnétiques et téléphonie mobile. <https://www.issep.be/wp-content/uploads/cem-et-telephonie-mobile.pdf>.
- Qiao, L. and Wang, X. (1999). *Unrestricted Warfare*. People Liberation Army. Litterature and Arts Publishing House, Beijing.
- R. D. Leach and M. B. Alexander and G. C. (1995 ). *Electronic systems failures and anomalies attributed to electromagnetic interference*. National Aeronautics and Space Administration, Marshall Space Flight Center ; National Technical Information Service, distributor MSFB, Ala. : [Springfield, Va .
- Reuters Staff (2017). France drops electronic voting for citizens abroad over cybersecurity fears. <https://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233>.
- 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>.
- US Election Assistance Commission (2015). Voluntary Voting System Guidelines - Volume I. <https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines>.
- US Election Assistance Commission (2018). Implementation Statement (D-Suite 5.5-A) Amended 2018-12-13. [https://www.eac.gov/sites/default/files/voting\\_system/files/Attachment\\_A\\_-\\_Dominion\\_D-Suite\\_5.5-A\\_Implementation\\_Statement.pdf](https://www.eac.gov/sites/default/files/voting_system/files/Attachment_A_-_Dominion_D-Suite_5.5-A_Implementation_Statement.pdf).
- Wikipedia (2020a). Precautionary principle. [http://en.wikipedia.org/wiki/Precautionary\\_principle](http://en.wikipedia.org/wiki/Precautionary_principle).
- Wikipedia (2020b). ESF1. <https://fr.wikipedia.org/wiki/ESF1>.
- Wikipedia (2020c). Technical standard. [http://en.wikipedia.org/wiki/Technical\\_standard](http://en.wikipedia.org/wiki/Technical_standard).
- Wyle Laboratories (2007). Hardware Qualification Testing of the Sequoia AVC Advantage D-10 DRE Voting Machine (Firware Version 10.3.11). <https://www.state.nj.us/state/elections/assets/pdf/voter-criteria/vvpr-hearing-reports-06-07-08/wyle-sequoia-avc-advantage-d-10.pdf>.
- Zdnet (2007). La liste des 82 communes équipées de machines à voter. <https://www.zdnet.fr/actualites/la-liste-des-82-communes-equipees-de-machines-a-voter-39368609.htm>.
- Zradzieski P. and Karpowicz J. and Gryz, K. and Leszko, Z. (2018). Evaluation of the safety of users of active implantable medical devices (AIMD) in the working environment in terms of exposure to electromagnetic fields - Practical approach to the requirements of European Directive 2013/35/EU. *International Journal of Occupational Medicine and Environmental Health*, 31:795–808.