Risk Analysis of Intentional Electromagnetic Interference on Critical Infrastructures

Benjamin Donald Oakes

Licentiate Thesis in Risk and Safety
KTH Royal Institute of Technology
Stockholm, Sweden 2017

Risk Analysis of Intentional Electromagnetic Interference on Critical Infrastructures

IBSN 978-91-7729-321-7
ISSN 1654-627X

KTH Royal Institute of Technology
School of architecture and the Built Environment
Department of Transport Science
Division of System Analysis and Economics
Center for Safety Research
SE-100 44 Stockholm, Sweden

Main Supervisor:
Professor Sven Ove Hansson, KTH Architecture and the Built Environment, Department of Philosphy and History, Division of Philosophy

Supervisors:
Assistant Professor Per Näsman, KTH Architecture and the Built Environment, Department of Transport Science, Center for Safety Research
Adjunct Professor Mats Bäckström, KTH School of Electrical Engineering, Department of Electromagnetic Engineering and SAAB Aeronautics

Mentor:
Professor Emeritus Lars-Göran Mattsson, KTH Architecture and the Built Environment, Department of Transport Science, Division of Transport Planning, Economics and Engineering

Akademisk avhandling som med tillstånd av Kungliga Tekniska Högskolan framlägges till offentlig granskning för avläggande av teknologie licentiatexamen i planering och beslutsanalys fredagen den 7 April 2017 klockan 10:00 i sal D3, Kungliga Tekniska Högskolan, Lindstedtsvägen 5, Stockholm

Print: Universitetsservice US-AB

Abstract

Our modern society depends on the functioning and interplay of a wealth of infrastructures. Practically all of these infrastructures are in some form or another, dependent on electrical and electronic systems. The majority of modern infrastructure is dependent on electric power and controlled by Supervisory Control and Data Acquisition (SCADA) systems. Electronic systems are sensitive to electromagnetic interference and at the same time, sources of electromagnetic interference are becoming more readily available on the market.

This means that certain important electronic infrastructure could be exposed to the risk of intentional electromagnetic interference (IEMI). Therefore, and also due to the complex nature of electronic infrastructure, a comprehensive risk assessment methodology is needed. A game-theoretic approach for quantitative risk assessment of the recently recognised threat of intentional electromagnetic interference on critical infrastructures is presented. The thesis bridges the gap between the fields of IEMI and risk analysis and lays a foundation for further development within this multidisciplinary field.

In paper I, the probability distribution function of the electric field strength from a continuous wave source is estimated in complex building structures. Probability distribution functions are combined for small and large scale fluctuations.

In paper II, a structured risk assessment framework is presented for identifying and quantifying the risk of IEMI on a distribution network infrastructure. The dimensions and components of risk are dissected and a suitable definition of risk is formulated.

In paper III, an operational model is formulated to optimise the operation of a wireless network under the course of a coordinated jamming attack. The model captures the time dimension and illustrates how the network operator must dynamically control the network so as to reduce the total network operational cost.

Sammanfattning

Det moderna samhället är starkt beroende av funktionaliteten och samspelet mellan en mängd olika infrastrukturer. Alla dessa infrastrukturer beror på ett eller annat sätt på elektriska och elektroniska system. Majoriteten av modern infrastruktur är beroende av elkraft och styrs av så kallade Supervisory Control and Data Aquisition (SCADA) system. Elektronik är känslig mot elektromagnetiska störningar och samtidigt har elektromagnetiska störsändare blivit alltmer lättillgängligt för allmänheten på marknaden.

Således kan viss kritisk teknisk infrastruktur vara utsatt för risk av avsiktliga elektromagnetiska störningar. Denna sårbarhet och komplexiteten hos elektronisk infrastruktur kräver en utförlig metod för riskanalys. Här presenteras en spelteoretisk metod för kvantitativ riskanalys av det relativt nyligen identifierade hotet avsiktlig elektromagnetisk störning av samhällsviktig teknisk infrastruktur. Avhandlingen knyter ihop ämnesområdena IEMI och riskanalys och lägger en grund för vidare utveckling inom samverkansområdet.

I papper I beräknas sannolikhetsfördelningen hos elektriska fältstyrkan från en kontinuerlig vågkälla i komplexa byggnadsstrukturer. Sannolikhetsfördelningar kombineras för små och storskaliga fluktuationer.

I papper II presenteras ett strukturerat ramverk för riskanalys som identifierar och kvantifierar risken för IEMI hos en infrastruktur i form av ett distributionsnätverk. Dimensionerna och komponenterna av risk identifieras och riskbegreppet definieras specifikt för IEMI.

I papper III formuleras en “operational model” som optimerar underhållningen av ett trådlöst nätverk under ett koordinerat jamming attack. Modellen tar hänsyn till tidsdimensionen och illustrerar hur nätverksoperatorn måste dynamiskt styra om nätverket så att totala underhållningskostnaden minimeras.

Acknowledgements

I would like to thank my main supervisor Professor Sven Ove Hansson, my supervisors Per Näsman and Mats Bäckström and mentor Lars-Göran Mattsson who made this research possible and especially Per Näsman and Lars-Göran Mattsson for their many hours of meeting time and quick and quality feedback. They have been relentlessly patient and persistent and taught me a lesson or two.

I would also like to thank the funders of this work, the Swedish Civil Contingencies Agency (MSB), the Swedish Fortifications Agency (Fortifikationsverket), the Swedish Post and Telecom Authority (PTS) and the National Food Agency, Sweden (Livsmedelsverket).

Finally, of course, I thank my loving family and best friends Alex, Jessica, Niklas and Pierre for their indispensable support to the very end. Thank you father for your inspirational discussions about science and how to solve the worlds problems. An unending amount of gratitude goes to my mother and grandmother who have been so close despite living on the other side of the planet and have always provided unconditional support. It would not have been possible without you either. Last but certainly not least, a special thanks to Viktoria who was kept awake every night by the sound of mouse clicking and keyboard typing.

Table of contents

List of papers

I. Andrés Alayon Glazunov, Mats Bäckström, Benjamin Donald Oakes.
Probability Distribution Function of the Electric Field Strength from a CW IEMI source.
IEEE Transactions on Electromagnetic Compatibility, pp. 1550 – 1558, 2014.

II. Benjamin Donald Oakes, Lars-Göran Mattsson, Per Näsman, Andrés Alayon Glazunov.
A Systems-Based Risk Assessment Framework for Intentional Electromagnetic Interference (IEMI) on Critical Infrastructures.
Final version submitted to Risk Analysis, 2017.

III. Benjamin Donald Oakes, Lars-Göran Mattsson, Per Näsman, Mats Bäckström.
A Dynamic Operational Model for Improving the Resilience of Wireless Networks Against Jamming.
Submitted to Reliability Engineering and System Safety, 2017.

Declaration of contributions

I. In paper I, B. D. Oakes collaborated as a co-author with main author Andrés Alayon Glazunov and co-author Mats Bäckström. Glazunov contributed to all the central concepts of the paper and was the main author. B. D. Oakes contributed to writing part of the text and refining some mathematical and statistical formulations. All authors have read and approved the final version of the manuscript.

II. In paper II, all authors made substantial contributions to the paper and all authors took part in the interpretation of the results. B. D. Oakes drafted the manuscript and finalised the manuscript after it had been reviewed and edited by all authors. Most of the original ideas were developed by B. D. Oakes who is also responsible for writing the manuscript. The concepts presented in the manuscript have been developed by B. D. Oakes, P. Näsman and L-G. Mattsson. All authors have read and approved the final version of the manuscript.

III. In paper III, all authors made substantial contributions to the paper and all authors took part in the interpretation of the results. B. D. Oakes drafted the manuscript and finalised the manuscript after it had been reviewed and edited by all authors. Most of the original ideas were developed by B. D. Oakes who is also responsible for writing the manuscript. The concepts presented in the manuscript have been developed by B. D. Oakes, P. Näsman, L-G. Mattsson and M. Bäckström. All authors have read and approved the final version of the manuscript.

1. Introduction

1.1 Background

Society today depends on the functioning and interplay of a wealth of infrastructures. They are interdependent, and failure of one can lead to a cascade of failures, resulting in disorder within the society [1]. An example of this is provided by the US commission report [2]:

"the telecommunications infrastructure requires power that is delivered by the power infrastructure. If power delivery is disrupted by disturbances in the power grid, telecommunication substations will run for a while on reserve battery power but would then need to switch to reserve backup generators (if they have them). The generator's operation would rely on fuel, first from on-site storage and then conveyed to a central distribution point by the energy distribution infrastructure and delivered to the telecommunications substation by the transportation infrastructure and paid for by the components of the financial infrastructure. The technicians who show up, through the transportation infrastructure, to make repairs would not do so unless they have been sustained by the food and water delivery infrastructures, and so forth. In turn, a functioning telecommunications system provides critical situational awareness and control to a power infrastructure that must keep its power generation in balance with its load in a dynamic control process over a very large geographical area. Telecommunications also plays a critical role in controlling the transportation system and is the basis of data exchange within the financial infrastructure."

Certain critical infrastructures as listed in the United States Executive Order [3] are described as "so vital that their incapacity or destruction would have a debilitating impact on society". They are the following:

- Water supply systems,
- Transportation,
- Electric power,
- Telecommunications,
- Banking and finance,
- Gas and oil storage and transportation,
- Emergency services (including medical, police, fire, and rescue),
- Continuity of government.

Extreme events – natural, accidental and intentional resulting in the failure of critical infrastructure can lead to heavy costs on society, e.g. 9/11 and the recent hurricanes Katrina and Rita [2]. After 9/11, and subsequent anthrax attacks in the United States, the interest in methods to assess the vulnerability of critical infrastructures to extreme events and in particular intentional attacks, has dramatically increased [4].

In the recent years, increased attention has come to the fact that almost all modern infrastructures are in some form reliant on electrical and/or electronic systems. An example of such systems are the Supervisory Control And Data Acquisition (SCADA) systems which were originally applied in telemetry systems used by the railroad and aviation industries, but currently are used for data acquisition and control over large and geographically distributed infrastructure systems. SCADA systems are important for the quality and the distribution of many vital commodities such as electric power, gas and oil and clean drinking water [5]. SCADA system architecture is often not dissimilar to that of a personal computer.

Electronic components and systems are by nature vulnerable to electrical overstress (EOS). The typical cause of permanent damage in semiconductors induced by EOS is the junction burnout [6], resulting from insufficient heat dissipation upon an instantaneous high surge of current across the junction. EOS can cause electromigration across semiconductor junctions, distorting the physical structure of the junction crystal lattice. This sets a maximum limit on the amount of energy absorbed by the junction which is proportional to the time integral of the electric field strength squared of a radiated field. A high total signal energy and peak signal power can cause overheating and thermal runaway in resistive loads. The amplitude (time domain peak) of the transient can directly be sufficient to cause an electric breakdown and arc-over effects and can result in resistive load termination [7]. Arc-over effects and breakdown in inductive and capacitive loads are caused by excessive peak time rates of change and peak time integrals of the pulse, respectively.

Electromagnetic interference (EMI) caused by natural phenomena has lead to the disruption of critical infrastructures in the past. One such disaster caused by lightning was the New York Blackout in 1977 [8] several consecutive lightning bolts struck several transformer tanks and circuit breakers, melting the windings causing the tanks to burn up. Geomagnetic storms have also destroyed transformers by inducing high currents in the windings [9], e.g. the Hydro Quebec or Carrington Event [10]. Another solar storm that impacted society was the so-called “Great storm” or the “New York Railroad Storm” that burned down a telegraph station in Karlstad, Sweden in 1921 [11]. The failure was caused by stray magnetic flux impinging on the transformer core.

A recently increasing concern is that EMI can also be created by man-made technology. Prior to the world’s first atomic test TRINITY in 1945, Nobel laureate physicist Enrico Fermi made the first attempt to predict the electromagnetic fields that would be produced from the nuclear explosion. This can be considered as the birth of the study of HPEM [12]. High altitude Electromagnetic Pulse (HEMP). The act of deliberately disturbing electronic devices using such technology is called Intentional Electromagnetic Interference (IEMI) and is, as stated by Giri [13], defined as the following:

> *“Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes.”*

The different means of IEMI can be categorised into the following major groups [14]:

- High Altitude Electromagnetic Pulse (HEMP);
- High Power Electromagnetic (HPEM) environments, e.g. High Power Microwave (HPM) and current injection;
- “Low-level” interference;

The different categories are ranked after their supposed relative likelihood. The least uncommon of the categories is low-level interference, which includes *front-door* interference, commonly referred to as jamming, where energy is coupled through antennas distorting the received (desired) signal, and *back-door* interference [15], i.e. interference in electronic circuits caused by coupling of electromagnetic energy to cables and leads. The remaining categories have higher power levels and can cause permanent damage of electronic components. They are often used in military applications and typically require a greater level of skill and precision to acquire than low-level jamming devices. It is worthwhile mentioning that the term "IEMI" originally referred to the use of HPEM sources for terrorist or criminal purposes. However, it now generally represents all the above categories, including jamming and HEMP.

Real and anecdotal evidence of IEMI has appeared during the first decade of the 21st century. The nature and intentions of IEMI attacks have the potential of being highly diverse. To illustrate this, some historical, real-world instances of IEMI are listed in the following [16]:

- In Japan, criminals used an EM disruptor to interfere with the computer of a gaming machine and falsely triggered a win.

- In St. Petersburg, a criminal used an EM disruptor to disable a security system of a jeweler store. The reports mentioned that building the EM disruptor posed a technological challenge similar to assemble a home microwave oven.

- In Kizlyar, Dagestan, Russia, Chechen rebel command disabled police radio communication using RF jammers during a raid.

- In multiple European cities (e.g. Berlin) criminals used GSM-Jammers to disable the security system of limousines.

- In Russia, Chechen rebels used an EM disruptor to defeat a security system and gain access to a controlled area.

- In London, UK, a city bank was the target of a blackmail attempt whereby the use of EM disruptors was threatened to be used against the banks IT-system.

- In the Netherlands an individual disrupted a local bank IT network because he was refused loan. He constructed a briefcase-size EM disruptor, which he learned how to build from the Internet. Bank officials did not realise that they had been attacked or what had caused the disruption until the assailant was caught.

- In Moscow, the normal work of one automatic telephone exchange station has been stopped as a result of remote injection of a voltage in to a telephone line. As a result two hundred thousand people had no phone connection for one day.

1.2 Motivation and research objectives

Since the late 1990's, awareness of the potential threat of IEMI on critical infrastructures had increased [17]. The threat is one to be taken seriously for a number of reasons, which can be summarised as follows [18, 19]:

- Increased complexity and interdependence of infrastructures,

- Terror threats are increasing worldwide, whereby covert operation outside physical barriers is attractive,

- The majority of critical infrastructures are reliant on automated electronic systems,
- The proliferation of IEMI sources is increasing,
- Technological advances have produced higher-energy RF sources and more efficient antennas,
- Electromagnetic susceptibility of new high-intensity IT systems working at higher frequencies and lower voltages is increasing.

In 2011, the Swedish Electrical Safety Board (Elsäkerhetsverket) conducted a preliminary study on the vulnerability of critical infrastructure to IEMI. The incentive for this was that the authority had in the previous year conducted a preliminary risk and vulnerability analysis and identified intentional generation of electromagnetic interference as a potential threat to societally critical infrastructure. The preliminary study reveals that for approximately 15 years the military has been aware that sources of electromagnetic interference (IEMI sources) can be harnessed by antagonists or criminals to disturb or destroy societally critical systems such as SCADA systems. The study also states that jamming devices designed to disturb GSM, GPS, wireless cameras, WLAN and Bluetooth can be bought on the Internet at affordable prices.

As a continuation of this initiation, a project was started in 2012 driven by the Swedish Fortifications Agency (Fortifikationsverket) called "protection against electromagnetic risks, intentional electromagnetic threats". The project was funded by the Swedish Fortifications Agency (Fortifikationsverket), the Swedish Civil Contingencies Agency (MSB), the Swedish Post and Telecom Authority (Post och Telestyrelsen (PTS)) and the National Food Agency, Sweden (Livsmedelsverket). In late 2013, B. D. Oakes was employed at KTH Royal Institute of Technology in Stockholm to work on the project. The overall objectives of the project were the following:

- Acquire new knowledge within the responsibility area for operators of societally critical infrastructure,
- Distribute the new knowledge to operators of societally critical infrastructure within Samverkansområdet Teknisk Infrastruktur (SOTI),
- Assess the vulnerability of societally critical infrastructure with regards to IEMI,
- Recommend and verify protection solutions.

The contribution of this thesis is to address the third and to some extent the first and second point above by formulating a method for assessing the vulnerability of societally critical infrastructure with regards to IEMI. Specific objectives include the following:

- To define and dissect the dimensions of risk in the context of IEMI,
- Establish a structured risk analysis technique to identify the risk of IEMI on an infrastructure,
- Produce a decision support model for identifying suitable and cost effective protection measures to mitigate the IEMI risks,
- Provide a stochastic vulnerability assessment approach for electronic equipment inside complex building structures.

1.3 Brief review of risk assessment techniques and models

Existing definitions of risk

There is today no universally established quantitative definition of “risk”. The precise definition of risk depends on the context of what one is studying. What is known today as the most universal standard of risk management is the ISO 31000, defines risk as the “effect of uncertainty on objectives” [20], where an “effect” is a positive or negative deviation from what is expected. There is always a chance that things will not go according to plan when trying to achieve an objective. Uncertainty is defined as the lack of certainty in knowing the current or future state of something, e.g. the weather tomorrow and is present due to incomplete or inadequate information. Before the twenties, there was no established distinction between risk and uncertainty. In 1921, Frank Knight distinguished the notions of risk and uncertainty, where he describes risk as a measurable, quantifiable uncertainty, or knowable amount of uncertainty [21]. Uncertainty which is present but cannot be quantified is not surprisingly called Knightian uncertainty.

Before the 17th century, uncertainty was considered impossible to measure and that no man could predict the future. Chance was considered mythical, or the will of the gods. Out of his passion for gambling however, and desire to “beat nature”, the founder of decision theory Blaise Pascal in the mid 1600s formulated probability theory and solved the problem of points [22, 23]. Having established expected utility maximisation, he could calculate how to divide the stakes fairly in an interrupted game of chance.

The father of modern risk assessment is Norman Rasmussen who adopted Pascal’s concept of expected utility to define risk. He argued that it is safer to build and operate a nuclear power plant than to drive your car to the minimart. The Rasmussen report of 1975 [24] established Probabilistic Risk Assessment (PRA) where risk of the failure is defined as the expected loss, or the probability of the failure times the consequence of the failure:

$$\text{Risk}(\text{Failure}) = \text{Probability}(\text{Failure}) \times \text{Consequence}(\text{Failure}), \tag{1.1}$$

PRA was initially used to assess random, unintentional events but has also been applied to assess the risk of antagonistic threats [25]. An adapted version of the PRA definition of risk above which is commonly applied in the context of antagonistic threats, is the Department of Homeland Security’s risk assessment method (DHS risk equation), or the Threat, Vulnerability, Consequence (TVC) method [26]:

$$\text{Risk}(\text{Failure}) = \text{Threat}(\text{Failure}) \times \text{Vulnerability}(\text{Failure}) \times \text{Consequence}(\text{Failure}), \tag{1.2}$$

where consequence is the asset at risk, vulnerability is the probability of the asset being lost given an attack occurs and threat is the probability of the initiation of an attack. The TVC method however, assumes that threat, vulnerability and consequence are independent, which is clearly not the case. As pointed out by Cox [27, 28], these models can mislead analysts, rendering nonsensical advice. One reason for this is that probabilities T and V are correlated, since a weak target is more likely to be attacked than a well-protected one [4], i.e. the probability of a target being attacked is greater if the probability of succeeding with the attack is higher. Furthermore, V and C depend on the allocation of effort by both the attacker and defender and therefore are also correlated. Kaplan and Garrick realised in the eighties that probability and consequence cannot be regarded as independent inputs and proposed what is perhaps the most officially established definition of risk today which is that risk is a set of triplets [29]:

$$\text{Risk} = \{\langle \text{Scenario}_i, \text{Probability}_i, \text{Consequence}_i \rangle\}, \quad i = 1, 2, ..., I, \tag{1.3}$$

where each triplet is the risk contribution of a scenario, i.e. what can go wrong, the probability of that scenario and the severity or consequence of that scenario.

A “vulnerability-based” definition of risk tailored for IEMI, or “the risk cube” was proposed by Månsson et al. [30], where risk is a triplet of consequence, susceptibility and accessibility. Susceptibility is the sensitivity of an electronic device to EMI and accessibility refers to the minimum distance an attacker can position an IEMI source to a target. This definition poses a reasonable starting point, and the concepts of susceptibility and accessibility are utilised in the proposed risk assessment method in chapter 3. However, like most definitions of risk, it is by no means complete. For instance, it lacks the “threat” dimension, an issue which is addressed in this thesis.

Universal risk assessment frameworks

A decade ago, the International Standards Organization (ISO) reviewed existing standards from Australia, New Zealand and Canada among others and created a new architecture and agreed upon updated terminology [31]. The first international standard on the practice of risk management was published in 2009 as ISO 31000, which was by 2015, adopted by 57 countries as their national standard for the management of risk. ISO 31000 is broadly accepted by public and private companies, governments, nonprofits and charitable organizations.

Here, we briefly review the risk management process of the ISO 31000 and a brief description of some of the terminology used in the standard in order to later be able to place the proposed risk assessment framework in relation to the global standard and provide the reader with some risk vocabulary as it is defined in the standard. *Risk management* is the process of coordinated activities to direct and control an organization with regard to risk. The risk management framework of ISO 31000 is presented in Figure 1.1.

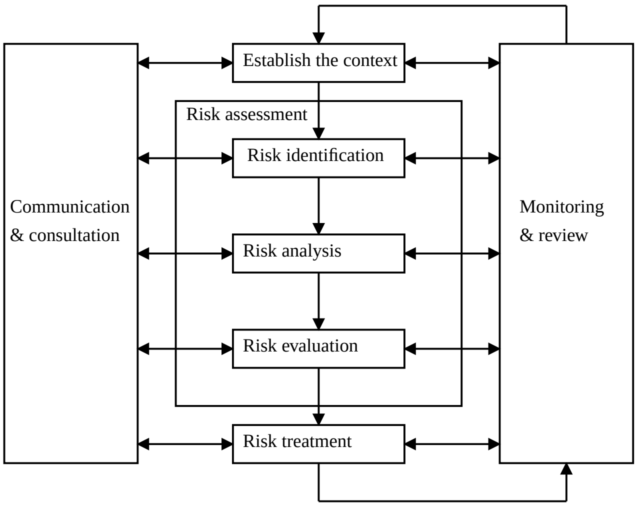

Figure 1.1: Risk management process of the ISO 31000:2009 standard, adopted from [20].

Establishing the context is defining the external and internal parameters to be taken into account when managing risk, and setting the scope and *risk criteria*, i.e. the terms of reference against which the significance of a risk is evaluated. *Risk assessment* includes risk identification, risk analysis and risk evaluation. *Risk identification* is the process of finding, recognising and describing risks. *Risk analysis* is the process of comprehending the nature of risk and determining the level or magnitude of risk. *Risk evaluation* is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Finally, *risk treatment* is the process of modifying the risk. For more on risk terminology, consult [32].

1.4 Challenges

A significant challenge in the risk assessment of IEMI is that IEMI attacks are rare events and historical data on such events is scarce. This makes the probabilities of IEMI attacks difficult to accurately estimate. The consequences could potentially be severe if the wrong equipment fails. For these reasons, IEMI attack may be considered as a Black Swan; i.e. a low probability, high impact event [33]. How can one quantify the risk of a Black Swan?

Even the consequences of an IEMI attack may be difficult to accurately estimate due to the complex nature of electronic infrastructure and the electromagnetic propagation from the IEMI source to targeted electronic equipment. Theoretical models are only practically applicable if coarse simplifications are made on modelling the complex geometries of reality, e.g. assume free-space propagation, predict antenna gains, attenuation, etc.

Evidently, the process of risk assessment of IEMI is not a simple one. There are many parts to this puzzle and arriving at a rational level of risk is a complex task. Each step of the risk assessment, e.g. risk identification is a complex task alone. Hence the need for a structured risk assessment process.

2. Approach and concepts

In this chapter, we address the scope, fundamental assumptions and terminology used in this thesis.

2.1 An adversarial game between an attacker and an operator

Due to the absence of historical data and limited information on potentially existing adversaries and their plans to conduct attacks, accurately knowing the probability that a successful IEMI attack occurs is practically impossible. Moreover, the probability, i.e. a number between one and zero of a successful attack is not a fixed value, it will change over time with the development of new technologies and the emergence new potential adversarial figures. The National Research Council (NRC) has criticised the use of probabilities to model the behavior of an intelligent, goal-oriented terrorist [34]. Moreover, Brown and Cox [35] explain how probabilistic assessment of terrorism risk can be misleading. Therefore, we resort to a game theoretical approach to our risk analysis, similar to the proposal by Alderson et al. [36], which does not necessarily require probabilities.

We begin by defining the stakeholders of the game and presume the existence of an *infrastructure*, *consumers*, an *operator* and an *attacker*. The infrastructure is a network comprised of *nodes* and capacitated *links* and could be e.g. a water supply system, an electric power grid or a telecommunications system and serves to provide consumers (people using the service) with a *commodity*, e.g. water, electricity or a telephone connection. The operation of the infrastructure is funded by the operator, i.e. the cost of transporting the commodity across links, or the *transit costs*. Upon consumer unmet demand, the operator is issued a hefty penalty cost (increasing with the amount of unmet demand), which is typically many times greater than the transit costs. The operator's objective is to minimise the operational cost. She does this by routing the commodity flows in the network in the cheapest possible manner to avoid the penalty costs of unmet demand. In the event of a disruption on a link, i.e. the link capacity is degraded, the operator will try to "bypass" the blocked flow on that link by rerouting the link flows in the network so as to meet as much consumer demand as possible, and preferably avoid consumer unmet demand entirely. Due to the high penalty costs, she is strongly motivated to go to lengthy efforts to meet consumer demand. She will also assign resources to remove the cause of reduced link capacity, in the context of IEMI, she will send resources to locate and remove an IEMI source which is somehow degrading the link capacity.

The attacker is a malicious individual or organisation of individuals who aspires to create as much havoc for the operator as he possibly can. His objective is to maximise the operator's operational cost using a limited amount of *resources*. He achieves his goal by attacking electronic devices or systems which maintain the link capacity and/or the continuous link functionality. These electronic systems shall henceforth be called the *targets*, since they are natural targets for an attacker using IEMI to achieve his objectives. Each target has a number of possible failure modes or *failure states*. The vector containing all target failure states forms the *system operational state F*. The link capacities and transit costs are functions of the system operational state, whose form will depend on the domain-specifics of the infrastructure under study. In turn, the failure state of a target depends on the electromagnetic environment the target is exposed to which is created by the attacker's IEMI sources. In order for a target to acquire a certain functionality state, the electromagnetic environment which it is exposed to must meet certain criteria. A simplistic type of criteria which is often applied in IEMI literature is that of susceptibility levels [37, 38, 39]. For radiated environments, a susceptibility level is commonly a critical level of electric field strength. The instant the target is exposed to an electric field strength at this level or higher, it will acquire another functionality state. Analogously, for conducted environments, susceptibility levels are often critical voltage or current levels. In the case of radiated sources, the electric field strength (the far field) at the target depends on the distance between the source and the target, decreasing linearly with distance [13]:

$$E = \frac{V}{r} \tag{2.1}$$

where V is the far voltage of the source and r is the distance from the source. To achieve a more devastating target functionality state, the attacker will try to place his source as close to the target as possible. The distance the attacker can position his source from the target depends on how easily he can access a point that distance away from the target with the source. Targets can be located inside buildings or large complexes with vast perimeter defences such as fences or walls or other barriers. These barriers we call *intrusion barriers* and the areas they circumscribe the *intrusion areas* or simply *zones*. The concept of intrusion areas has been applied in many security assessments [40, 41]. To be able to infiltrate a zone with a certain type of IEMI source, the attacker must posses a minimum amount of resources. The attacker's specific objective is to choose the zones in which to deploy each of his sources so as to achieve the worst-case system operational state for the operator, i.e. the one which yields the highest operational cost.

2.2 Assumptions and limitations

Due to the operator's limited knowledge about the attacker, she assumes the attacker has perfect information about her. She can only imagine different types of attackers and therefore conceptualises different categories of attackers with specific capabilities. Given an attacker with a specified amount of resources, the operator assumes the attacker will try to succeed with the worst-case scenario for the operator allowed by his resources. More precisely, we assume that the attacker's objective is to maximise the operational cost for the operator similarly to a zero-sum game in that the operator's loss is equal to the attacker's gain. (reference). Therefore, the operator "imagines" the attacker and prepares for the worst attack that attacker is capable of. This type of adversarial game where the defender (in our case, the operator) follows the attacker and is often referred to as a Stackelberg game [42].

Another core assumption is that the attacker is confined to using IEMI sources as means to disturb the functionality of the infrastructure, however may use other types of resources to prepare the attack, e.g. for intrusion into unauthorised areas and transporting or deploying the IEMI sources.

Moreover, we assume the attacker is *static* and the operator is *dynamic*. By this we mean that the attacker does not change the position of his sources throughout the entire attack but we allow the operator to reroute flows to consumers and allocate resources to reduce the increased operational cost resulting from the attack. Since the nature of IEMI attacks is renown for being covert in literature [43], we assume a scenario where the attacker deploys his sources in a hidden location or one which is not noticeable and leaves them there throughout the entire attack. Moreover, we assume that the attacker deploys and activates his sources simultaneously. If the operator does not intervene with the operation of a source, it will remain activated for a finite period of $\bar{\tau}_s$ which is an upper limit on operational time, e.g. battery time or the time of the pulse width if the source only produces a single pulse to permanently damage targets.

3. Risk assessment framework

3.1 Defining risk in the context of IEMI

We adopt a similar definition of risk as the most established one by Kaplan and Garrick in Equation (1.3), however, we do not apply the notion of probability to define risk due to reasons explained earlier. Probability is "replaced" by *resources* and *plausibility*, and we arrive at the following definition of risk being a set of quadruplets:

$$\text{Risk} = \{\langle \text{Scenario}_i, \text{Resources}_i, \text{Plausibility}_i, \text{Consequence}_i \rangle\}, \quad i = 1, 2, ..., I, \tag{3.1}$$

where I is the total number of possible scenarios conceived by the operator. The respective risk factors *scenario*, *resources*, *plausibility* and *consequence* are defined below.

Scenario – each quadruplet represents the risk contribution from a certain possible *scenario*. A scenario is a set of attacks $\langle t, s, z \rangle$, where an attack is defined as the deployment of source s inside zone z to attack target t.

Resources – a set of vectors that contain the minimum quantities of different types of equipment required to carry out the scenario. A resource vector ρ is not a minimum resource vector if there exists another resource vector ρ' such that $\rho_j \geq \rho'_j$ for all j.

Plausibility – is the least objective of the risk factors, where plausibility$_i$ represents the operator's level of uncertainty that scenario$_i$ will occur. Since it is the most speculative of the risk factors, it is also the last of the factors to be evaluated. The operator conceptualises (or imagines) a number of different types of real-world attackers who are believed to have the motivation to degrade the performance of the network by means of IEMI and assigns a resource vector to each type of attacker representing the resources they are thought to possess. The plausibility of a scenario is the level of belief that there is an attacker whom possesses the motivation, at least one of the necessary resource vectors allowing that scenario and the knowledge required to carry out that scenario. Plausibility may be a qualitative variable with e.g. two levels "implausible" or "not implausible". The former level implies that the scenario is completely unrealistic, while the latter means that there is a level of perceived uncertainty by the operator that this might occur. Notice that the latter level is called "not implausible" rather than "plausible" since the threat of IEMI is after all hardly a plausible threat. Hence, "not implausible" implies the existence of uncertainty and the belief that there is a "possibility" of the scenario occurring. It should be noted that plausibility is the least important of the risk factors, since we in our case know little if anything about potential attackers, and should generally be regarded as an additional indicator of the magnitude of the risk. Note that plausibility may seem to resemble "threat" in Equation (1.2). However, unlike "threat", it is not a probability and its value does not necessarily impact the operator's perceived level of risk in a proportional manner. While the value of risk directly hinges upon the value of "threat" in Equation (1.2) and allows risk to be compared to e.g. a monetary cost, plausibility may be conceptualised as an additional risk indicator to be considered if the operator deems the consequence of an attack to be unacceptable and the necessary resources reasonably low.

Consequence – is defined as the operator's monetary loss as a result of the scenario. This includes the penalty costs of consumer unmet demand and the additional network operational costs induced by the attack, e.g. rerouting flows along other links to "bypass" congested links.

3.2 Risk assessment process

In section 1.3, we revised the global standard of the overall risk management process. Here, we detail core contributions of this thesis which are the process of risk identification and risk analysis within the risk assessment process. We also briefly go over the process of establishing the context.

Below there follows a list of concise descriptions of the first stages of the risk management process including establishing the context, risk identification and risk analysis and their substeps as a contribution of this thesis. After this, the details of each step are described.

1. Establish the context
2. Risk identification
   - 2.1. Identify targets, system functionality states and associated operational costs per unit time
   - 2.2. Identify possible scenarios
   - 2.3. Identify minimum resource vectors for each scenario
3. Risk analysis
   - 3.1. Estimate resilience loss (consequence) for each scenario
   - 3.2. Assess plausibility of scenarios
   - 3.3. Formulate the risk

1. Establish the context – Much of this has is covered in chapter 2, where we set the scope of the risk analysis, define the stakeholders, etc. The specific infrastructure under study should be chosen here, the consumers and the type of commodity the infrastructure supplies, e.g. water, power, data transmission.

2.1. Identify targets, system functionality states and associated operational costs per unit time – Begin by drawing a graph of the network illustrating nodes and links. Then, identify the major systems which are critical for maintaining and regulating the flows on the links, and in turn, on a lower system level, identify the electronic devices which play a critical role in maintaining these systems. These critical electronic devices are rendered the targets. When subjected to EMI, a device might remain fully functional, completely lose its functionality or only partially lose it functionality. Targets have various possible failure modes or *functionality states* which are commonly in literature:

1. Immunity,
2. Interference,
3. Crash, self recovery,

4. Crash, operator intervention,

5. Permanent damage.

During an attack, the targets may take on different functionality states. We call the set of all target functionality states the *system operational state*. The system operational state will have a bearing on the link capacities and thereby the operator's ability to deliver flow to consumers. Upon unmet demand, the operator is issued a penalty cost by her consumers. Given a system operational state, the operator will try to reduce consumer unmet demand so as to reduce her operational cost as must as possible. She does this by rerouting flows in the network so as to "bypass" restricted links and also by locating and neutralising jammers. The operator's objective function is of the following form:

$$C(F) = \min_{Y_{ij},X_n} \sum_{(i,j)\in\mathscr{L}} c_{ij}(F)Y_{ij} + \sum_{n\in\mathscr{N}} p_n X_n, \tag{3.2}$$

where $C(F)$ is the operational cost per unit of time depending on the system operational state vector F, Y_{ij} is the flow on link (i,j), X_n is the unmet demand at node n, c_{ij} is the transit cost per unit of time and p_n is the per unit penalty cost per unit of time at node n.

By the end of this step we have obtained all possible system operational states and the operational cost per unit of time for each possible operational state when the operator optimises flows in the network and tries to locate and neutralise jammers in an optimal order.

2.2. Identify possible scenarios – Select some categories of IEMI sources which pose a legible threat to the identified targets. Target susceptibility levels for each of the selected source categories are identified and the zones (of relevant zone type) surrounding the targets are identified. Then the worst-case functionality state which is possible to inflict using a source in a zone is evaluated for all source-zone combinations or attacks $\langle t,s,z\rangle$. Finally, the operational cost per unit of time is evaluated for each scenario, i.e. combination of attacks.

2.3. Identify minimum resource vectors which allow each scenario – We here begin by identifying each possible means of breaching each barrier with each IEMI source category and the respective resources, e.g. vehicles and other equipment. By identifying the resources needed to transport the source within each zone and breach each barrier, each combination of resources which can be used to access zone z with source category s is represented as a vector where each entry is a positive integer representing the quantity of a certain type of resource. The *minimum resource vectors* for attack $\langle t,s,z\rangle$, are the resources vectors that allow attack $\langle t,s,z\rangle$ and are not strictly greater than any other resource vector of the resource vectors which allow attack $\langle t,s,z\rangle$. From this, we establish the set of minimum resource vectors which allow each scenario.

3.1. Estimate resilience loss (consequence) for each scenario – The consequence can be measured as the resilience loss resulting from the attack. This corresponds to the time integral of the difference of operational cost per unit of time in Equation (3.2) and the operational cost per unit of time when the network is not under attack (represented by $\hat{C}^K$ in Figure 3.1). The operational cost per unit of time may change as the IEMI source batteries run out, if the operator locates and neutralises a source or repairs a damaged target.

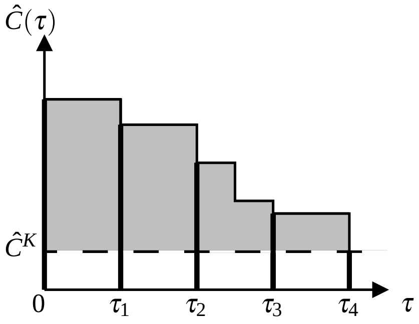

Figure 3.1: Example of the operational cost per unit of time as a function of time when the operator is able to reroute edge traffic flows, regulate unmet demand and search for jammers at the decision times indicated by bold vertical lines $(K = 4)$. The grey area represents the increase in operational cost, or resilience loss. Notice that between decision times τ_2 and τ_3 one of the jammer batteries goes flat and the cost per unit time drops.

3.2. Assess plausibility of scenarios – As a final step in the risk assessment, we assess the scenario plausibility by gathering expert opinion on if the scenario is remotely likely (e.g. there is suggestive evidence or partially suggestive evidence of potential attackers who possess the necessary knowledge, motivation and resources allowing a scenario) (and if it is an acceptable scenario).

3.3. Formulate the risk – A list of scenarios and their respective consequence, resources and plausibility is taken forward.

4. Discussion and Conclusions

4.1 Contributions

This thesis presents a definition of risk for intentional electromagnetic interference on infrastructures and a risk assessment framework to assess the risk of IEMI on distribution network infrastructures taking the efforts of the infrastructure operator to reduce the consequence of an ongoing, coordinated IEMI attack. The thesis bridges the gap between risk analysis and IEMI, integrating the two fields and provides a foundation for further development within the topic of risk analysis of IEMI on critical infrastructures. In addition, a stochastic method for evaluating the probability distribution function of the electric field strength inside complex building structures is presented.

4.2 Limitations

A characterising limitation of this study is that it assumes that a "plausible" attacker with IEMI resources is perfectly rational and will carry out the worst-case attack possible allowed by his resources. However, would a perfectly rational attacker carry out an IEMI attack? This issue may be partly addressed in the plausibility assessment. If a scenario is not plausible, there is no fear of any "rational" attackers who would be inclined to carry out such an attack. However, there is much missing information about the attacker and one must have a point of departure for a risk analysis.

The primary focus of this thesis is risk assessment and primarily risk identification of IEMI risks on distribution network infrastructures and minimising the consequence of an ongoing attack by rerouting flow in the network and attempting to disable the attackers IEMI sources and repair damaged targets. We have not included risk evaluation and risk treatment methods for deciding which countermeasures to take to prepare for a conceived attack, e.g. hardening targets or changing the network topology to increase redundancy. This could be a possible continuation of the project, however, without probability it is difficult to value different countermeasure alternatives. In the risk evaluation process, one could compare the risk to a risk criteria decided upon by the operator. For instance, the operator might render a scenario unacceptable which comprises less than a specified number of attacks, is allowed by a minimum resource vector which is lower than a specified resource vector, has a consequence above a critical level and is considered "not implausible". In the risk treatment process, the risk is reduced as cost-effectively as possible by e.g. installing protection solutions so as to increase the required resources and reducing the risk. It is worthwhile mentioning that some infrastructures or functionalities are simply "too important to fail" [44], i.e. a failure is absolutely unacceptable and cannot be weighted against the monetary costs of protection solutions. If the infrastructure maintains a critical societal function which is "too important to fail", perhaps this alone should be enough to justify investing in reducing the risk and one should not be all too cautious of "overspending" on defensive mitigation measures. The "risk" produced by following the methodology outlined here is intended to provide an operator as much information about the true level of risk as possible, but cannot provide perfect information, mainly due to the high level of uncertainty about the attacker. Though the proposed risk assessment method should be used as an informative decision tool rather than a minor indicator, it is up to the operator to decide how much she is willing to spend on countermeasures given (1) the proposed risk assessment framework, (2) her risk perception or perceived level of risk and (3) the cost of reducing the risk.

The objective function used in this thesis is exemplary. The cost of rerouting flows in a network is typically much smaller than the penalty cost. For simplification, it may suffice to only include penalty cost. Other variations of objective functions are possible. Moreover, we do not go into the details on algorithms for efficiently solving the proposed optimisation problem, e.g. greedy algorithms which are commonly applied to activity selection problems [45]. This goes beyond the scope of this thesis.

In this thesis, we assume that the consequence of a scenario depends on where the attacker deploys his sources, i.e. the scenario and the impact of the IEMI on the operational cost of the network alone. Another expansion would be to allow the consequence to also depend on the resources used for a scenario (it may be possible to carry out a scenario using one of several different minimum resource vectors). The attacker might cause damage to a facility when deploying an IEMI source depending on which resource vector is used. The analysis here however is delimited to focus on the costs of network operation and the penalties involved of not meeting consumer demand as a direct result of the IEMI attack rather than the cost of damaged property resulting from the preparation of an attack, e.g. replacing damaged locks from break-ins by the attacker to deploy sources. These costs however can be considered to be covered by insurance and not by the operator herself and are therefore, and for the sake of simplicity not covered in this stage of the analysis. Moreover, as stated in section 2.2, the context of this risk analysis is IEMI with the core assumption that the objective of the attacker is to maximise the operator's cost of operating the network by using IEMI and is not interested in causing other damage by use of other means than IEMI. However, more damage might be consider a bonus for an attacker, which is not covered in this analysis.

Note that we make the simplification that the operator does not schedule the order of searching for the IEMI sources or repairing damaged targets at each decision time. The myopic nature of the operator could lead to an operational cost which is not optimal in the long term. An argument in favor of this assumption however is that the operator has no way of knowing how the electromagnetic environments at the targets will change in the future and the best she can do is to optimise the operational cost per unit time at the present time. However, if the operator assumes that electromagnetic environments at the targets will remain constant throughout the entire attack (and accurately estimates the search and repair times), a scheduled approach to managing the search for targets could be an option.

4.3 Implications and further development

This thesis provides a basis within the field of risk assessment of IEMI on critical infrastructures and is intended to be the beginning a proliferation of further research. Infrastructure operators and decision makers can use the methodology presented in this thesis as a point of departure for risk assessments on their specific infrastructures and tailor the more general framework presented here to suit their specific type of infrastructure.

As mentioned in the previous section, the contributions of this thesis are rather methods of risk assessment and to an extent, risk management, i.e. a process leading to the reduction of risk. Risk management is addressed here in that the operator can try to track down IEMI sources and neutralise them, thereby working to reduce the consequence under an ongoing attack, and ultimately, reduce the risk. We also presume that the operator repairs her damaged equipment after a certain amount of fixed time, which limits the consequence. A next step would be to infer a comprehensive risk management procedure after the risk assessment as proposed in section 3.2. Varying repair times and limited repair budgets can be introduced in a future model. So far, we have only described limiting the consequences during an attack, however consequences can also be reduced by e.g. building new links and altering the network topology such as establishing parallel connections instead of series connections. Risk can also be reduced by increasing the minimum resource vectors allowing the scenarios. This can be done by adding protection to targets, e.g. reinforcing barriers or building new barriers. A risk management model which reduces risk by optimising the reduction of consequence and increasing the minimum resource vectors, as well as the cost of implementing the "hardening" strategy could be a reasonable continuation.

4.4 Ethical aspects of the research

How safe is it to openly publish the information in this thesis to the common public? Who should have access to information produced by this type of research? Should research on every type of infrastructure be publicly available? Should the public even be made aware of this threat? These are some ethical issues which we attempt to address in the following. The information provided in this thesis is derived from commercial sources only, meaning that all the details presented on IEMI sources and infrastructures can be found on the Internet or in publicly accessible literature. Moreover, the susceptibility levels provided here are merely hypothetical and by no means represents true levels. The purpose of this work is not to provide such information but rather to offer infrastructure operators the tools they need for conducting a proper IEMI risk assessment, in order to ultimately, make their infrastructures safer and more reliable. The operator can use her own measured susceptibility levels and other values which apply to her specific infrastructure. What information given in this thesis provides to potential adversaries is similar to that of the media. Criminal offenses are broadcasted on the media but not detailed descriptions of precisely how the attacker succeeded with the attack. Unfortunately however, copycat behaviour has been known to emerge as an aftermath of crime on the open media [46].

Despite the fact that only hypothetical examples are provided in this thesis on some types of infrastructure, even hypothetical risk assessment examples on certain types of infrastructure which are not mentioned here for obvious reasons, should only be available to the relevant infrastructure operators.

5. Summary of papers

5.1 Paper I: Probability Distribution Function of the Electric Field Strength from a CW IEMI Source

In this paper, a stochastic propagation model is formulated to calculate the probability distribution of the electric field strength originating from a continuous wave IEMI source at a given point inside a complex building structure. This is a more realistic estimate of the electric field strength estimated by Friis simplistic propagation model as in Equation (2.1) and can be applied when identifying scenarios in step 2.2 of the risk assessment framework in section 3.2. Combining probability density functions of small- and large-scale fluctuations of the electric field strength results in a Suzuki distributed electric field strength impinging at the equipment. Specifying the susceptibility level or the critical electric field strength of the target, the vulnerability of a target is evaluated as a function of the distance between source and target, taking into account losses from in and outside the building. Vulnerability isocontours defined as lines of constant probability of exceeding the susceptibility level are presented for a generic, continuous wave power source in a scenario emulating a dense urban microcell propagation environment. A comparison of the vulnerabilities predicted based on the Suzuki and the Lognormal distributions are also been provided for the same scenario. The proposed method provides estimates of critical distances of radiated IEMI attacks and may have use when deciding on the perimeter defense of a facility.

5.2 Paper II: A Systems-Based Risk Assessment Framework for Intentional Electromagnetic Interference (IEMI) on Critical Infrastructures

In this paper, we formulate the proposed definition of risk in section 3.1 and detail the steps of risk identification 2.1, 2.2, 2.3 and risk analysis 3.2 and 3.3 of the risk assessment framework in section 3.2. Risk evaluation is also briefly addressed where only “important” scenarios are included in risk which are scenarios that are considered high risk by the operator.

We introduce the specific terminology used for this risk assessment such as targets, susceptibility levels and intrusion areas. and classify electromagnetic source technology according to key attributes.

An example of the proposed risk assessment framework is provided on a hypothetical water distribution network. Worst-case scenarios are identified for different quantities of attacker resources and the most plausible and consequential of these are deemed the most important scenarios and should provide useful decision support in a countermeasures effort.

5.3 Paper III: A Dynamic Operational Model for Improving the Resilience of Wireless Networks Against Jamming

This paper features the importance of the time dimension in evaluating the consequence of an attack. The details of step 3.1 of the risk analysis framework in section 3.2. are presented. The time dimension is particularly relevant for jamming attacks where jammers can be left on for longer periods of time and the operator must try to find and deactivate them. We present a dynamic operational model for improving operational resilience of wireless networks which use dynamic routing against jamming attacks. The model serves to optimise the operation of a wireless network so as to minimise the total operational cost, or resilience loss, when the network is subjected to a combined jamming attack. The model first minimises the total amount of blocked data traffic using dynamic routing, i.e. routing the traffic depending on the signal to noise ratios at the wireless access points. Assuming the operator is able to discern and sound out jamming signals, the jammers are located and neutralised by search teams starting with the jammers that contribute to the highest operational cost. The searches for the jammers have finite time durations, which is captured in the model. Results are presented for a hypothetical Wireless Local Area Network (WLAN) attacked at two locations by jammers.

6. References

[1] Cats O, Jenelius E. Planning for the Unexpected: The Value for Reserve Capacity for Public Transport Network Robustness. Transportation Research Part A: Policy and Practice, 2015.

[2] Critical National Infrastructures. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Congressional EMP Commission, 2008.

[3] Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.

[4] Bier V. Game Theoretic and Reliability Methods in Counterterrorism and Security. Modern Statistical and Mathematical Methods in Reliability, Vol. 10, series on Quality, Reliability and Engineering Statistics, 17–38, 2005.

[5] Myndigheten för Samhällsberedskap (MSB). Kartläggning av SCADAsäkerhet inom svensk dricksvattenförsörjning. 2010.

[6] Metzger, F. Failure Modes of Electronics. The English Press, 2011.

[7] Taylor CD, Giri DV. High-Power Microwave Systems and Effects. Taylor & Francis, 1994.

[8] Systems Control Inc. Impact Assessment of the 1977 New York Blackout. Energy Systems Division, 1978.

[9] Kappenman J. Geomagnetic Storms and Their Impacts on the U.S. Power Grid. Metatech, 2010.

[10] Royal Academy of Engineering, Extreme space weather: impacts on engineered systems and infrastructure, February 2013.

[11] Lundstedt H, Persson T, Andersson V. The extreme solar storm of May 1921: observations and a complex topological model. Annales Geophysicae, 33, 109–116, 2015.

[12] Baum CE. Reminiscences of High-Power Electromagnetics. IEEE Transactions on Electromagnetic Compatibility, Vol. 49, No. 2, May 2007.

[13] Giri DV, Tesche FM. Classification of Intentional Electromagnetic Environments (IEME). Electromagnetic Compatibility, IEEE Transactions on, vol. 46, no 3, pp. 322-328.

[14] International Electrotechnical Commission, IEC. Electromagnetic compatibility (EMC) – Part 2–13: Environment - Highpower electromagnetic (HPEM) environments – radiated and conducted, 2003.

[15] Bäckström MG, Lövstrand KG. Susceptibility of Electronic Systems to High-Power Microwaves: Summary of Test Experience. IEEE Transactions on Electromagnetic Compatibility, August 2004; 46(3):396–403.

[16] Sabath F. What can be learned from documented Intentional Electromagnetic Interference (IEMI) Attacks? URSI General Assembly and Scientific Symposium, 2011.

[17] Radasky W, Bäckström M. Brief Historical Review and Bibliography of Intentional Electromagnetic Interference (IEMI). Beijing, China: URSI General Assembly, 16-23 August 2014.

[18] Calvano CN, John P. Systems engineering in an age of complexity. Systems Engineering, 2004; 7(1):25-34.

[19] Radasky WA, Baum CE, Wik MW. Introduction to the Special Issue on High-Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI). IEEE Transactions on Electromagnetic Compatibility, Vol. 46, No. 3, August 2004.

[20] International Organization for Standardization. ISO 31000:2009, Risk management — Principles and guidelines. 2009.

[21] Knight, FH. Risk, Uncertainty, and Profit. Boston: Hart, Schaffner & Marx, 1921.

[22] Ore O. Pascal and the Invention of Probability Theory. The American Mathematical Monthly, Vol. 67, No. 5, 1960, pp. 409-419.

[23] F. N. David. Games, Gods, and Gambling. Griffin Press, 1962.

[24] United States Nuclear Regulatory Commission. Reactor Safety Study. An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants. Main report. WASH-1400, 1975.

[25] Genender E, Sabath F, Garbe H. Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level. IEEE Transactions on Electromagnetic Compatibility, February 2014; 56(1):200–207.

[26] Masse T, O'Neil S, Rollins J. The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress. CRS Report for Congress, February 2007.

[27] Brown G, Cox A. How probabilistic risk assessment can mislead terrorism risk analysis. Risk Analysis, 2011; 31:196–204.

[28] Cox A. Some limitations of risk = threat × vulnerability × consequence for risk analysis of terrorist attacks. Risk Analysis, 2008; 28:1749–1761.

[29] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis, Vol. 1, No. 1, 1981.

[30] Månsson D, Thottappillil R, Bäckström M. Methodology for Classifying Facilities with Respect to Intentional EMI. IEEE Transactions on Electromagnetic Compatibility, Vol. 51, No. 1, February 2009.

[31] Knight KW. Risk Management, a Journey not a Destination. Presentation to the RusRisk/-Marsh "ISO 31000 Risk management standard: principle and implementation trends", Seminar, Moscow on 15th December 2010.

[32] International Organization for Standardization. ISO Guide 73:2009, Risk management — Vocabulary. 2009.

[33] Taleb NN. The Black Swan: The Impact of the Highly Improbable. Random House, 2007.

[34] National Research Council (NRC). Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis. Department of Homeland Security Bioterrorist Risk Assessment: A Call for Change. Washington, DC: National Academies Press, 2008.

[35] Brown G, Cox A. How probabilistic risk assessment can mislead terrorism risk analysis. Risk Analysis, 2011; 31:196–204.

[36] Alderson DL, Brown GG, Carlyle WM. Operational Models of Infrastructure Resilience. Risk Analysis, 2015; 34(4):562–586.

[37] Hoad R, Carter NJ, Herke D, Watkins SP. Trends in EM Susceptibility of IT Equipment. IEEE Transactions on Electromagnetic Compatibility, August 2004; 46(3):390-395.

[38] Bäckström M, Nordström B, Lövstrand KG. Is HPM a Threat Against The Civil Society? Proceedings of the 27th General Assembly of the URSI, Maastricht, Netherlands, August 2002.

[39] Nitsch D, Sabath F, Schmidt H, Braun C. Comparison of the HPM and UWB Susceptibility of Modern Microprocessor Boards. Proceedings of the EMC Symposium Zurich 2003, Zurich, Switzerland, February, 2003; 121–126.

[40] ITU. High-power electromagnetic immunity guide for telecommunication systems. ITU-T, K.81, 2015.

[41] Shafieezadeh A, Cha EJ, Ellingwood BR. A Decision Framework for Managing the Risk to Airports from Terrorist Attack. Risk Analysis, February 2015; 35(2):292–306.

[42] von Stackelberg HV. Grundlagen einer reinen Kostentheorie. Vienna: Verlag von Julius Springer, 1932.

[43] Heddebaut M, Deniau V, Rioult J, Copin G. Method for detecting jamming signals superimposed on a radio communication, Application to the surveillance of railway environments. IEEE International Symposium on Electromagnetic Compatibility (EMC), 2015.

[44] Kappenman JG, Radasky WA. Too Important to Fail: The Looming Threats of Large Geomagnetic Storms and Other High-Altitude Disturbances with Modern Electric Power Grids May Produce Significant Damage to Critical Infrastructure. Space Weather Journal, May 2005.

[45] Kolisch R, Hartmann S. Heuristic Algorithms for the Resource-Constrained Project Scheduling Problem: Classification and Computational Analysis. Volume 14 of the series International Series in Operations Research & Management Science pp 147-178, 1999.

[46] Jewkes Y. Media & Crime, 3rd Edition. SAGE Publications, 2015.