sustainability

MDPI

Article

Digital Threat and Vulnerability Management: The SVIDT Method

Roland W. Scholz [1,2,3]

[1] Department of Knowledge Management and Communication, Faculty of Business and Globalization, Danube University, 3500 Krems, Austria; roland.scholz@donau-uni.ac.at or roland.scholz@emeritus.ethz.ch; Tel.: +43-0-2732-2893-2330

[2] Department of Environmental Systems Science, ETH Zurich, 8092 Zurich, Switzerland

[3] Department of Psychology, University of Zurich, 8050 Zurich, Switzerland

Academic Editor: Marc A. Rosen

Received: 28 January 2017; Accepted: 30 March 2017; Published: 5 April 2017

Abstract: The Digital Revolution is inducing major threats to many types of human systems. We present the SVIDT method (a Strengths, Vulnerability, and Intervention Assessment related to Digital Threats) for managing the vulnerabilities of human systems with respect to digital threats and changes. The method first performs a multilevel system–actor analysis for assessing vulnerabilities and strengths with respect to digital threats. Then, the method identifies threat scenarios that may become real. By constructing, evaluating, and launching interventions against all identified digital threats and their critical negative outcomes, the resilience of a specific human system can be improved. The evaluation of interventions is done when strengthening the adaptive capacity, i.e., a system's capability to cope with negative outcomes that may take place in the future. The SVIDT method is embedded in the framework of coupled human–environment systems, the theory of risk and vulnerability assessment, types of adaptation (assimilation vs. accommodation), and a comprehensive sustainability evaluation. The SVIDT method is exemplarily applied to an enterprise (i.e., a Swiss casino) for which online gaming has become an essential digital-business field. The discussion reflects on the specifics of digital threats and discusses both the potential benefits and limitations of the SVIDT method.

Keywords: digital revolution; vulnerability analysis; resilience management; sustainability evaluation; strategic planning

1. Vulnerability Management as a Means of Successfully Using and Adapting to Digital Environments

1.1. Objectives

The development of the proposed method has been motivated by the issue that the *Digital Revolution* is causing various *threats* and changes that have the potential to endanger the viability or future existence of individuals, companies, industries, and other *human systems* (H). Experts in computer technology claim that technological threats induce a dramatic transformation of our economy and societal institutions with unknown benefits and damages [1]. Thus, a challenge for many human systems is to assess which new demands, types of activities, rules of communication, opportunities, etc. call for action, and what actions they call for.

We are dealing with situations where a *specific human system* H^* is exposed to evident or potential *digital threats*. The paper introduces a *comprehensive method* for *reducing the vulnerability* of H^* and for *increasing the resilience* in regard to these threats for a *specific* human system H^*, which could be an individual deliberating how to maintain his/her employment, a company whose supply chain is undergoing a rapid technological transition, a branch of an industry whose products are being replaced by digital services, or a region of a city whose industrial production and services are susceptible to being replaced by digital technologies.

Here, the challenges are to *identify digital threats* and to *assess the strengths and vulnerabilities* of H^*, as well as to think about what adaptions by which *appropriate actions* (interventions) are meaningful. We call these actions *intervention scenarios*. In practice, the challenge is to identify those threats that demand rapid interventions, in addition to other threats that may require major actions in the future. In the frame of strategic planning, this may require *increasing adaptive capacity*. Thus, the vulnerability assessment goes beyond risk assessment and takes a different perspective. Instead of providing an a priori analysis and an evaluation of the loss potential for a human system, H, when exposed to a threat (i.e., risk), it identifies and evaluates the action strategies H may take if a threat has become real [2], which is the adaptive capacity.

The proposed method includes the *identification of the main actors* whose behaviors, demands, services, etc. are likewise changing due to the rapid spread of technologies. This is done by looking for win–win strategies among related actors, e.g., partners of the supply-chain network [3]. The identification of main actors or stakeholders (including governmental framing agents) is accomplished by *multilevel coupled-systems analysis*. This is done as we relate to a *hierarchical conception of human systems* (including individuals, groups, and organizations such as companies or NGOs, institutions, societies, supra-societal levels, and the human species). This (level of) hierarchical order facilitates a better conceptualization and modeling of the rationales and goals of human systems when referring to different social sciences (see Supplementary Materials S1 and S2). It includes top-down and bottom-up processes. When structuring the complexity, we further suggest looking at *coupled systems*. We focus on how H^* interacts with the main actors H (as important elements of the social environment) and how H^* and other actors cope and adapt to rapidly changing *digital environments* (E_D). Thus, we deal with complex, coupled human–environment (HES) systems that are becoming an increasingly important aspect of sustainability research [4–6].

1.2. The Specifics of Digital Threats

We define the digital environments of human systems simply as all technologies and (human-made) information that is based on digital data. We may state that the digital age began in 2002, the first year in which digital storage capacity become larger than analog capacity [7].

Scholz [8] argues that digital technology heralds a new, historically unknown stage of the appropriation of nature. He stresses that large-scale and potentially unintended and unwanted side effects or secondary feedback loops (also called rebound effects) of the use of digital technology should become the focus of research programs. One example of this is the manipulation of DNA, which is mostly conceived as a genuine digital construct (if the folding of the DNA, which usually is conceived to be analog, is ignored). Digital technology allows for *directed evolution* (e.g., the genetic manipulation of seeds) that may result in unwanted side effects and feedback loops (for references and an explanation, see [8]). The same holds true for the ongoing development toward the integration of living cells in computers. Computers take on organismic characteristics and become biocomputers, whose understanding may call for new forms of logic as the functioning of cells may differ from that of relays.

Moreover, the *human individual* (in general) is also facing potential digital threats. There are theoretical arguments (see [8]) that excessive exposure to information and stimuli from digital media may have *epigenetic effects* or may have the potential to alter *brain structure* in certain users. The putative reason for this potential involves the intense exposure to new types and (as yet unknown) speeds and informational content (which may also induce Internet addiction [9,10]). Further, from the perspective of Western common-law rights, the human individual's right to privacy may be undermined, diminished, or redefined by Big Data [11,12].

From a societal perspective, the rapid and fundamental change of *economic* and *social structures* calls for *resilience management*. Solid research and modeling, for instance, reveal that 47% of the current jobs in the US are at risk of being eliminated [13,14]. Here, the US may be considered as a specific *H*, and the loss of jobs considered the digital threat to which the proposed method may be applied. The automatization of society by globally networking, interactive systems is rapidly changing and calls for new forms of managing global techno-socio-economic-environmental systems on all scales [15,16].

We want to note that the proposed method may be applied not only to digital threats but also to other factors such as disaster management and risks related to, for example, the societal impacts of migration. However, it has been shaped specifically for environmental threats. When we think about the specifics of the Digital Revolution or Transition, we can see that the new type of knowledge representation (digital vs. analog), and the speed, volume, and ubiquity of information storage, retrieval, processing, and transmission form the essence that changes technology and communication. We think that this rapid spread of digital technology challenges companies, institutions, and other H with more than just a soft, *assimilation-like* adaptation. In many cases, there will be a need to develop new behavioral, cognitive, organizational, material (including technological), and operative structures in order to cope with environmental demands and to maintain viability. This thorough type of adaptation is called *accommodation* [17]. Digital threats, therefore, represent a particular variant of the *innovator's dilemma* [18] and can cause discontinuities on the level of organizations and industries [19,20], as *H* will often be challenged for disruptive innovation.

1.3. Methodological Background

The presented method on the resilience management of H in order to confront digital threats refers to three methodologies and related (sub)disciplinary methodologies. The *first* are *problem-structuring methods* (PSM, systemic structuring) as a part of *operations research* (OR). Problem-structuring methods acknowledge the subjective and contextual sides of modeling a perceived problematic situation and the demand by users to not only describe but also manage a system [21]. This stream includes *Strategic Choice* [22], *Soft Systems Methodology* [23], the *Viable System Model* [24], and, in particular, *Strategic Options Management* [25] as the proposed method that will provide intervention scenarios.

The *second* is *transdisciplinarity* as an important methodology of the emerging discipline of sustainability science [26–28]. Transdisciplinarity is considered to be a methodology that integrates knowledge from science and from practice in the sustainable transitioning of ill-defined, complex, societally relevant, real-world problems. The development of methods for this endeavor began in the 1990s, when tools for structuring sustainable transitions were demanded [29,30]. Here, Robert Yin's idea of embedded case studies has offered important input. The term "embedded" indicates that a complex, real-world situation of interest is considered within a conceptual grid (which acknowledges the complexity of the case). Based on this embedding, we may develop methods of problem representation, problem formation, and problem transitioning (including evaluation). A recent paper discusses the challenges of structuring (more than forty large-scale) transdisciplinary processes [31].

The third methodology for coping with threats, hazards, etc. is known as *risk and decision sciences*, which represent an important reference stream. From a methodological perspective, risk and decision sciences overlap the previously described streams, but both have their own scientific communities and journals. Risk research has strong economic [32], psychological [33], and human health [34] foundations among others. Given the character of digital threats (in particular, their complexity, the incompleteness of information, and the potential costs of failing to act), we suggest extending the risk concept by the property of *adaptive capacity* (see Section 2.1, [2]), which assesses a system's capability to cope with threats from a posterior perspective if they have become real. Experimental research has shown that adaptive capacity is cognized as a specific component of technological threats [35]. Finally, we want to mention that the proposed method, SVIDT, utilizes a specific form of *evaluation*, i.e., it integrates ideas from potential *bio-ecological potential assessment* (BEPA; [30]) into *multicriteria evaluation* [36,37].

The presented Strengths, Vulnerability, and Intervention Analysis against Digital Threats (SVIDT) method may be perceived as a method of strategic management. It is a semi-quantitative method and thus avoids quantified modeling (if the data or uncertainty does not allow for it), focus a structured, data-based systemic strategy formation [38]. In some respects, the SVIDT analysis resembles the SWOT analysis ([39], which will be included as a substep). Both approaches support the management process of innovation. In other respects, the two methods differ. The SVIDT method is conceptually and methodologically a hybrid method that includes formative scenario analysis, multilevel analysis, vulnerability assessment, multi-attribute utility assessment, and other methods for certain steps.

The presented method is not designed for desktop studies only. Characteristics of PSM knowledge from key agents (from practice) must be involved, as this method is achieved through problem-structuring processes [40–43] or in (Mode 2) transdisciplinary processes, in which integrated processes from practice and science are launched [26,28,44–46].

1.4. What Will Be Found in the Following Sections?

Section 2 first introduces the concepts of vulnerability and resilience, and then specifies the conception of coupled systems on which the multilevel analysis is based. The section also discusses a systemic sustainability function that will be used to assess and prioritize interventions. Section 3 presents the scaffolding for the SVIDT. Section 4 illustrates the SVIDT method using the case of Swiss gambling casinos and their adaptation to online gambling. The discussion and conclusion (Sections 4 and 5) stress how commercial enterprises can benefit from SVIDT analysis and how to cope with practical and theoretical challenges related to the proposed methodology.

2. Theoretical and Conceptual Foundations of Vulnerability Management

2.1. Vulnerability and Resilience in the Frame of Sustainability

The concept of *vulnerability* became an important concept in the Third Assessment Report of the International Panel of Climate Change: "Vulnerability is conceived as the degree to which a system is susceptible to, or unable to cope with, adverse effects ... including ... variability and extremes. Vulnerability is a function of the character, magnitude, and rate of ... [external] variation to which a system is exposed, its sensitivity, and its adaptive capacity" [6,47]. Thus, Scholz et al. [2] formally define vulnerability as a function of exposure toward a threat, (uncertain) sensitivity with respect to the impacts of a threat, and the adaptive capacity to cope with these impacts (if they have become real). This we may (semiformally) write as

$$vul = f(exposure, sensitivity, adaptive\ capacity) \tag{1}$$

The *SVIDT method* should ensure that *human systems (For simplicity, both the singular and plural forms of human system are abbreviated as H.)*, *H*, *reduce their vulnerability* against threats that emerge from the ubiquitous spread of digital technologies. As vulnerability is the complement of resilience (see below or [2,48–52]), applying the SVIDT method involves resilience management. *Resilience management is a key component of sustainability management.* This holds true, at least, if we refer to the following *definition of sustainability* as:

(I) an ongoing inquiry for
(II) system-limit management (i.e., avoiding system collapse)
(III) in the frame of intra-generational and
(IV) intergenerational justice [53,54].

Resilience—and thus vulnerability—refers to (II) system-limit management. We argue that vulnerability management against digital threats is a challenge for avoiding (human systems') "hard landings".

2.2. The Relationship between Risk and Vulnerability

Risk can be defined as a function of *exposure* toward an uncertain threat (i.e., an event with negative outcomes) and the *sensitivity* of a system toward the impacts of this threat, i.e.,

$$risk = g(exposure, sensitivity) \tag{2}$$

The presented definition has been used predominantly in toxicology [55]. A decision theoretic definition relates exposure to the choice among different alternatives, of which one is linked to an uncertain negative outcome [56]. Exposure is operationalized by the intensity at which a human system, H, is exposed to an environmental pollutant or another type of *environmental threat* (which we may define as E_{threat}). *Sensitivity* is recognized as the set of negative impacts in the (material) biophysical layer of a human system (called H_m) or the socio-epistemic layer (called H_s, which, in the case of a human individual, can be considered as the psychological layer). Figure 1 presents this relationship in graphical form. The upper part of the two boxes on the right in Figure 1 denotes the abiotic environment E_{abio}; the lower part denotes the biotic environment E_{abio}. An *environmental threat* can be induced by the digital environment.

For instance, the (blue) radiation of (certain) computer screens [57] may cause melatonin deficiency (in H_m of young students) and, thereby, the potential for developing a sleeping problem and/or a mental disorder (on the level H_s) [58]. An individual may adapt by looking at the screen less, wearing special glasses, or choosing screens that emit less "critical blue light". All three of these actions *reduce exposure*. Moreover, if the individual were to ingest supplementary melatonin in pill form, this would result in *reducing sensitivity* for him or her. In the face of digital threats, a desired capability of a system is:

(1) To diagnose, anticipate, and evaluate critical negative impacts; and
(2) To have the sufficient resources (e.g., financial means) to change the behavioral setting in order to

  (2a) Reduce exposure,
  (2b) Reduce sensitivity (and increase robustness), and
  (2c) Cope with any negative impacts that have taken place.

The latter (2c) we call *adaptive capacity*.

We denote the perception or assessment of (pure) risk by a human system as risk function. The risk function can be considered an *evaluation of the loss potential* linked to a situation (or—in decision theoretic terms—of a decision alternative). *Risk management* is linked to (1) and (2) above. In principle, risk management is rather *reactive* by nature. *Vulnerability assessment* evaluates the means that can be taken to reduce risk and includes an evaluation of what can be done when the negative events have already taken place. Improving the adaptive capacity means to empower the repertoire of cognitive, behavioral, organizational, operative, financial, etc. capabilities in an anticipatory manner that is needed when a negative event becomes real. Increasing the adaptive capacity is *proactive* by nature.

We should note that the above-mentioned also holds true if we switch to *speculative risk* [59], which includes the evaluation of potential losses in relation to potential gains/benefits. Cognitively, risk is a subjective and idiosyncratic evaluation of an individual or a specific assessment of a human system. The expected value or expectancy value can serve as a risk function, but there are many others such as the highest potential loss or the probability of critical losses [56,60]. The presented vulnerability concept was developed by ecologists. The idea of vulnerability and adaptation describes aspects of evolution and counters conceptions of staticness and equilibria [61,62], as organismic systems are supposed to collapse, reorganize, and evolutionarily develop.

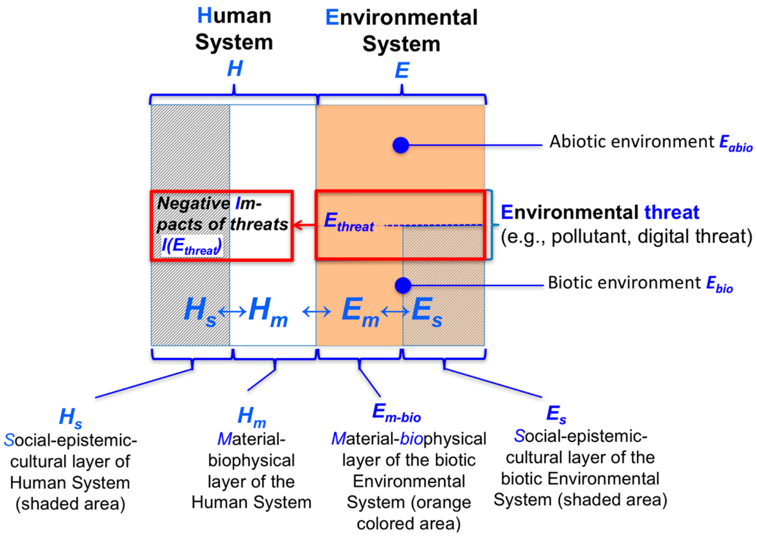

Human System
H
Environmental System
E
Abiotic environment E_{abio}
Negative Impacts of threats
$I(E_{threat})$
E_{threat}
Environmental threat
(e.g., pollutant, digital threat)
Biotic environment E_{bio}
$H_s \leftrightarrow H_m \leftrightarrow E_m \leftrightarrow E_s$
H_s
Social-epistemic-cultural layer of Human System (shaded area)
H_m
Material-biophysical layer of the Human System
$E_{m\text{-}bio}$
Material-biophysical layer of the biotic Environmental System (orange colored area)
E_s
Social-epistemic-cultural layer of the biotic Environmental System (shaded area)

Figure 1. Environmental threats from a coupled-system perspective.

2.3. *Vulnerability from a Multilevel Coupled Human–Environment Systems Perspective*

We suggest that vulnerability assessment calls for considering the coupling of human systems H with the digital environment E_D, particularly if we want to assess the vulnerabilities with respect to the *key performance* of interest. Let us exemplarily consider a specific company H^* that wants to remain a key actor in the market. Whether this is feasible depends on the rationales of other human systems H, particularly those that are affecting the key performance.

For instance, for a company of interest, the *supply–demand chain* [63] includes the key human systems and human systems' actions, the material and human resources used by these actors (including E_D), and the (digital and non-digital) information involved in: (a) the (upstream) supply chain by suppliers; (b) the (downstream) demand side by customers; (c) the company itself; and (d) framing agents that may affect the functioning of the whole supply–demand chain. Please note that other human systems involved in the supply–demand chain may call for different definitions. For instance, for the human individual as customer, we may refer to models such as the *customer journey* [64].

For structuring the complexity, we refer to the Human Environment Systems (HES) framework [6,65]. This framework (see Supplementary S1) includes postulates on structuring HES. The first is the *Complementary Postulate P1*. This is visualized in Figure 1 and in the above-presented complementarity between the *material–biophysical* layer H_m and a *socio-epistemic cultural* layer of human systems H_s (Scholz, 2016 or Scholz, 2011, Chapter 16). We argue that, since the Benenson automaton [66], computers are on the cusp of becoming (semi-)organismic beings, and, thus, they also have a "socio-epistemic" layer, which we call H_s. Additionally, biocomputers that include cells are considered to have a mind. This is represented by part of the shaded area in the lower-right, framed middle rectangular section of Figure 1 (and might be denoted as $E_{S\ bio}$). We do not examine this point in depth here, but we argue that human systems may reflect on adaptive capacity in response to threats to the biotic and abiotic environment.

The HES framework takes a *hierarchy perspective* (see Supplementary S2, Postulate 2). It is interesting that, for each level of human systems, one finds a scientific discipline (at least one) that is specialized to describe the drivers and rationales of the human system. For instance, cell biology for cells, psychology for the human individual, business science for companies, or anthropology and philosophy for the human species (see above; Table S2 in Supplementary S2). An essential issue in the HES framework is that human systems on different hierarchy levels have different goals, drivers, and rationales. This induces interferences (Supplementary S1, Postulate 3) and conflicting goals.

Individuals want to protect their privacy. Governments, which represent societies' interests, have to protect social interests. An example is the case of the US White House vs. Apple in regard to unlocking the code of a smartphone owned by Syed Rizwan Farook, who was judged to be a terrorist after killing 14 people with a firearm at a County Department of Public Health meeting after his female partner pledged allegiance to the leader of the Islamic State and the Levant [67]. We may well imagine that Barack Obama might have different preferences as a private person (level of the individual) and as President of the United States (level of society). We can learn from this that stakeholder analysis is a multilevel issue. Theoretical frameworks such as the HES framework may be considered as tools for structuring goals and rationales with respect to the vulnerability of actors (human systems). The hierarchy postulate is a meaningful tool in applications for structuring complexity. A main task of a vulnerability analysis of digital threats is to identify (delayed) *rebound effects* that might affect various human systems on different levels, *critical trade-offs*, and change rates that may overburden the adaptation of human systems or launch *tipping points* (this is the subject of HES Postulate 4; see Supplementary S1). From a societal perspective, the *breaking of privacy* by digital technologies may have strong rebound effects on the principles of democracy [68,69].

Two of the HES frameworks refer strongly to basic postulates of decision research that are applied in multilevel analysis. One is that any organismic being or human system, from the cell to the human species, pursues goals and thus has preference functions. Human systems, when confronted with environmental challenges such as fulfilling a certain need or adapting to digital environments, may show different degrees of environmental awareness. They may be: (a) self-centered, encapsulated in their common behavioral, cognitive, etc. routines, and believe that the environment will continue to provide services in the same way as in the past; (b) aware of their impacts on the environment and thus notice that, by utilizing specific digital tools, performance is decreasing or increasing; and (c) for the highest level of environmental awareness, capable of anticipating which secondary feedback loops are affecting the environment and the human system itself if they take a certain action that may be linked to the introduction of new digital technologies.

However, a rapid digital revolution may endanger many human systems, H, by overburdening them. *Change rates may be too rapid to allow for adaptation* for valuable enterprises, social rules, or systems of storing and reproducing knowledge. The digital systems may cause unintended side effects and destroy the foundations necessary for building sustainable social rules, or they themselves may lack *robustness*, e.g., in storing fundamental data. Not only librarians but also lawyers talk about the threat of the "digital time bomb" [70,71]. Cybersecurity will increase in importance, and living with cybercrime [72] will continue to be a threat for the next several centuries. We stated that the Digital Revolution changes social and economic structures. Digital technologies have the potential to support large freelance businesses such as in the case of UBER, which may establish new rules of economic reproduction.

2.4. Assimilation and Accommodation as Two Levels of Adaptation

If (human) systems are facing transitions within their environments, they have to adapt. A critical question is whether they possess *sufficient adaptive capacity* [2,35,50]. In order to better differentiate forms or depths of adaptation, we introduced (see above) Piaget's [73] distinction between assimilation and accommodation. *Assimilation* means to slightly modify *already available behavioral patterns or structures* or to apply them to new problems or environmental challenges. A company, for example, may introduce new software or technology with the same staff, type of hardware, buildings, administration, and communication tools. *Accommodation*, in contrast, calls for the acquisition of new and not-yet-available structures. This may induce a long-lasting, painful, and erroneous process of adaptation. In the case of a company, the digital, globalized business may demand new computerized forms of production and management. These, in turn, may call for new knowledge and, thus, new or modified staff, or they may require the reorganization of a company. In addition, using English as the global working language may be seen as adaptation.

Let us thus consider this distinction with *two examples*. Piaget developed his *theory of ontogenetic cognitive development* and showed that a child is continually developing qualitatively new types of cognitive operations in order to cope with more complex situations. For instance, when deciding which of two ratios, a_2/b_2, is bigger, a child at the preoperative level is cognitively operating with visual images (of real-world entities) related to the nominator and denominator. Thus, the child may decide that 6/9 is bigger than 5/9 (as he or she can imagine the relationship by visualizing physical comparisons). However, when comparing ratios such as 6/9 and 5/8, the child is overburdened and needs the new cognitive capability of arithmetic (e.g., knowing that "6/9 to 5/8" is equivalent to "6×8 to 5×9" and mastering multiplication). This example shows that new, previously unavailable cognitive rules and algorithms are needed [74] for the comparison of certain fractions (which can be applied to all fractions).

The difficulties of adaptation to new situations may be well illustrated by, *second, turning the global economy into a digital economy.* Digitalized products and services can be produced in all places. Market leaders are multinational companies that look intelligently for options to save *taxes* through suitable transnational inner-company transactions. This has become possible as intangible operations and assets became more important (and often more valuable) than physical transactions. The costs of storing and transporting digital products are almost zero. Furthermore, digital products can be replicated at almost no cost, and numerous firms "outsource many corporate functions to territories with lower costs" [75] if tangible products do not allow for smart solutions. Neither should we exclude the possibility that the ownership of cloud technology, 3D printing, and the Internet of Things (IoT) may disappear among the boundaries of the 193 countries of the United Nations. A critical question is what the tax system in a digital economy might look like. Several countries and some states of the US, for instance, try to *assimilate* and rely on general laws to govern the taxation of digital goods. Others, such as Kentucky, have enacted new laws that specifically address the taxation of digital goods [76]. As it is difficult to tax such products reliably, one idea would be to shift all taxation to the consumer. This could be viewed as *accommodation*. Digital economics demonstrates a new type of mobility. The national taxation laws are inhomogeneous and certain mini states may offer special opportunities. Thus, one may seek a new global taxation in a kind of supra-national setting, as exemplarily demonstrated by the European Union for environmental regulations and other issues (but not, as yet, for taxation).

2.5. Vulnerability as a Component of Sustainability Evaluation

Interventionary studies involving animals or humans and other studies that require ethical approval must list the authority that provided approval and the corresponding ethical approval code.

Resilience is the complementarity of vulnerability and thus means essentially the same. If vulnerability is assessed quantitatively (by real numbers on a scale between 0 and 1), we may write

$$rel(H^*) = 1 - vul(H^*) \tag{3}$$

As shown above, *resilience* (see Section 2.3 can be considered the operationalization of (II) "system-limit management" in the above-mentioned definition of sustainability. However, sustainability is always related to core *functions of a system's performance*, the vulnerability of which should be secured. What exactly is or should be the function of a system and what degree of resilience is targeted are usually not well defined but rather subjects of ongoing inquiry.

If we want to embed a vulnerability assessment in a comprehensive *sustainability evaluation*, we may include it as an indicator in a comprehensive set of indicators [77–82]. For digital threats, we suggest a different approach, i.e., a semiquantitative, system theoretic evaluation that takes an evolutionary perspective, i.e., the *Bio-Ecological Potential Analysis* (BEPA, [30]). The evaluation includes three main aspects (see Table 1): (1) the *function*; (2) *vulnerability*; and (3) the *normative aspect of justice*.

The above mentioned BEPA (and an extended model of evaluation called *Sustainable Potential Analysis (SPA)* [83,84] identifies several system properties that affect the vulnerability of a system. These are the overly fast growth or decline of a system (i.e., change rates, see, Table 1), the question of whether a system may be considered as *well-structured* (and whether the *dependence on the inputs of other systems* (see Section 2.3) is overly critical. The latter resembles cluster risks in economics.

The proposed sustainability evaluation includes (3) *intra- and intergenerational justice*. In the context of the Digital Revolution, this aspect, for instance, refers—if we consider the human species *H* as a human system—to the question of in what way(s) digital technologies increase economic and social inequality. What this may mean for other systems (e.g., individuals or companies) has to be considered case-wise, and we deal with this partly in Section 5.

Table 1. Aspects of a systemic sustainability evaluation (see [30], Chapter 19 Bio-Ecological Potential Analysis).

No.	Labels from BEPA and SPA	Essential Properties
(1)	Function/system productivity and performance	The functions a human system may provide
(2)	Vulnerability (ability to accommodate)	***Components of vulnerability***
		(2a) Exposure to threats (probability)
		(2b) Sensitivity to threats (magnitude of harm), also considered a complement of robustness (which includes buffer capacity)
		(2c) Adaptive capacities
	Properties affecting vulnerability	
	(2.1) Change rates	Sensitivity increases in times of overly fast decline or growth of a system.
	(2.2) Well-structuredness	Does the system show an inefficient connectivity, edginess, network structure, or other patterns?
	(2.3) (In-)Dependence on other systems	Can the system survive if other systems are in a critical state?
(3)	Societal justice, normative aspects, intra- and intergenerational justice	Does the distribution of wealth enter a stage that the poor will resist? Will future generations (or the system at later points in time) suffer because of the consumption/environmental impacts of today's generation?

3. The SVIDT Method

This section introduces the major steps of the SVIDT method. Certain steps will be illustrated in some depth in the presented case of the transition of conventional Swiss gambling casinos to (also offering) online gambling (see Section 4). The "*Hitchhiker's Guide*" to SVIDT (see Appendix A) shows how the different theoretical components may be used for realizing a comprehensive sustainability evaluation of the relationship between human systems and digital environments (see Figure A1). The formation of an SVIDT team of scientists (consultants) and members of the specific system of interest may be seen as an important separate step preceding the study [85,86]. The steps of the procedure are numbered in Figure 2.

Step 1: Goal formation. The scientific team, preferably together with a main representative of the investigated human system *H** formulates a goal that specifies the scope (i.e., the guiding question) and depth of the vulnerability assessment for the vulnerability management of a specific human system *H** against digital threats. This is best achieved by a *guiding question* that defines the system boundaries. If possible, one or a few sufficient target variables should be identified that represent the coupled system's performance. A typical *guiding question* may read: *What digital equipment, knowledge, and practices are needed for reducing energy and raw-material use and for increasing the return* *of investment/profitability of a certain company H^**. Here, naturally, the digital technology is part of the environment and affects the human systems (primarily) by the return of investment as a key function.

Step 2: Coupled system analysis. The analysis starts with the construction of a system model of the environment of the main actor H^*. This environment includes the identification of the *main actors* H^1, H^2 . . . and of all *framing agents*. The specific digital environment, i.e., the key digital technologies that are used to attain the key functions (as described in the guiding question), is part of this step. By framing agents, we denote those actors, usually of higher levels of human systems such as institutions or societies, that do not directly interact with H^* but whose action strongly affects the main performance of H^*.

Step 3: System analysis of main actors. This step includes an actor analysis [46] and a *rough* system analysis of a (sub)set of identified *main actors* H^1, H^2, whose actions are expected to affect the *performance of* H^* depending on the use of digital technologies. This analysis should include an assessment of the drivers and rationales of the human systems. The digital environment is also seen as an interface between H^* and the other actors.

Step 4: Multilevel system analysis. This step refers to a kind of multi-agent modeling. In a first step, the main actors are assigned to the specific hierarchy levels (i.e., individual, group, organization, institution, society, supranational systems, human species). Then, interferences (or synergies) among the hierarchy levels are assessed. If we are faced with a pre-competitive situation or if there is a strong partnership with stakeholders [87], we may think about a transdisciplinary process [46] that can be launched (i.e., including other stakeholders and scientists) to develop improved strategies for H^1, H^2, . . . to collaborate with H^* in jointly designed digital environments.

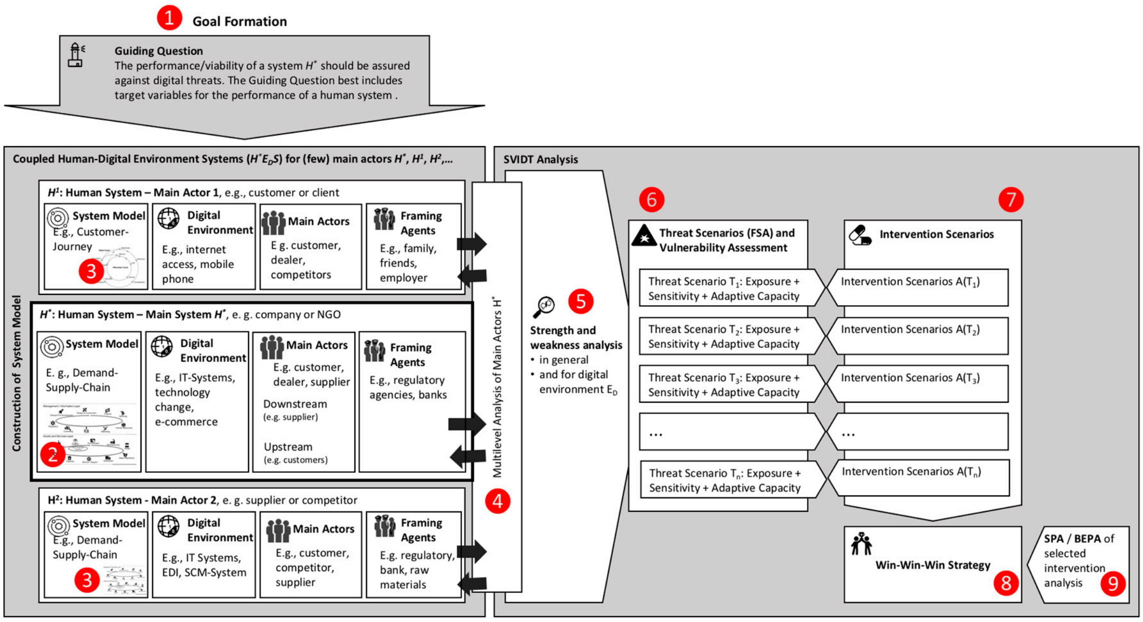

1
Goal Formation
Guiding Question
The performance/viability of a system H^* should be assured against digital threats. The Guiding Question best includes target variables for the performance of a human system .
Coupled Human-Digital Environment Systems (H^*E_DS) for (few) main actors H^*, H^1, H^2,...
Construction of System Model
H^1: Human System – Main Actor 1, e.g., customer or client
System Model
E.g., Customer-Journey
3
Digital Environment
E.g., internet access, mobile phone
Main Actors
E g. customer, dealer, competitors
Framing Agents
E.g., family, friends, employer
H^*: Human System – Main System H^*, e. g. company or NGO
System Model
E. g., Demand-Supply-Chain
2
Digital Environment
E.g., IT-Systems, technology change, e-commerce
Main Actors
E.g. customer, dealer, supplier
Downstream
(e.g. supplier)
Upstream
(e.g. customers)
Framing Agents
E.g., regulatory agencies, banks
H^2: Human System - Main Actor 2, e. g. supplier or competitor
System Model
E.g., Demand-Supply-Chain
3
Digital Environment
E.g., IT Systems, EDI, SCM-System
Main Actors
E.g., customer, competitor, supplier
Framing Agents
E.g. regulatory, bank, raw materials
Multilevel Analysis of Main Actors H^*
4
SVIDT Analysis
5
Strength and weakness analysis
• in general
• and for digital environment E_D
6
Threat Scenarios (FSA) and Vulnerability Assessment
Threat Scenario T_1: Exposure + Sensitivity + Adaptive Capacity
Threat Scenario T_2: Exposure + Sensitivity + Adaptive Capacity
Threat Scenario T_3: Exposure + Sensitivity + Adaptive Capacity
...
Threat Scenario T_n: Exposure + Sensitivity + Adaptive Capacity
7
Intervention Scenarios
Intervention Scenarios $A(T_1)$
Intervention Scenarios $A(T_2)$
Intervention Scenarios $A(T_3)$
...
Intervention Scenarios $A(T_n)$
Win-Win-Win Strategy
8
SPA / BEPA of selected intervention analysis
9

Figure 2. The SVIDT method from a coupled multilevel HE_DS perspective (for an enlarged version Supplementary S2, Figure S1).

Step 5: Strengths and weaknesses of H^*. The research team, most advantageously in collaboration with agents from, deliberate and identify digital threats for H^*, its coupling to digital environments, its subsystems, different fields of action, dependencies on other systems, products, services, etc. Usually, in this step, a *transformational view* is taken. This means that a point in the (foreseeable) future (i.e., in a time range of five years) may be taken as a reference when certain activities have become digitally governed. This step should already include an identification and sampling of (single) threats (see Figure 3).

Step 6: Threat scenarios. The most important, comprehensive, and critical steps are (see Figure 2):

(6.1) the identification of digital threats,

(6.2) the construction of *threat scenarios,* and

(6.3) the assessment of the *deliberation of vulnerability* (among a research team or in a dialogue between scientists/method experts and representatives of *H**) with the three main components: exposure, sensitivity, and adaptive capacity.

Step 6 includes a complex process of differentiating the system model (of Step 2) and specifying what the main digital threats are, how threats may jointly appear (i.e., the construction of threat scenarios; see Figures 3 and 4), and what negative outcomes can result (that call for interventions related to improving digital technologies and knowledge). This induces a deliberation of initially vague and intuitive (holistic and gut-feeling-based) rough ideas about threats and the three components of vulnerability, i.e.,

- the degree of exposure;
- the likelihood of negative effects given a certain exposure, i.e., sensitivity; and
- adaptive capacity that evaluates what countermeasures can be taken against threat scenarios to avoid a "hard landing" of *H**.

The process of *identifying threats* can be accomplished by brainstorming with the help of the repertory grid method (e.g., when comparing threats on different domains or subsystems [88,89]) or other methods such as cognitive maps. For instance, we may apply Causal Chain Analysis (CCA) to identify *digital threats* (as an impact of general changes) *related to:* (a) *direct utilization/non-utilization of digital technologies;* or (b) through the *use (or non-use) of digital technologies by others* that may result in *one or more* negative effects for *H**, either *directly* or *indirectly*.

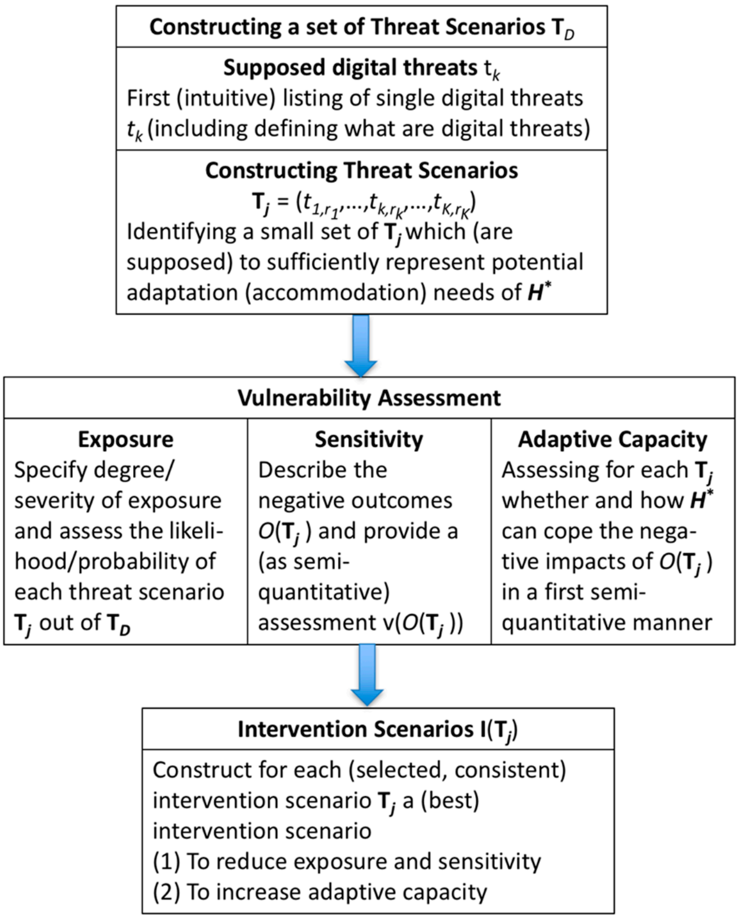

Constructing a set of Threat Scenarios $\mathbf{T}_D$
Supposed digital threats t_k
First (intuitive) listing of single digital threats t_k (including defining what are digital threats)
Constructing Threat Scenarios
$\mathbf{T}_j = (t_{1,r_1},\ldots,t_{k,r_k},\ldots,t_{K,r_K})$
Identifying a small set of $\mathbf{T}_j$ which (are supposed) to sufficiently represent potential adaptation (accommodation) needs of $\boldsymbol{H}^*$
Vulnerability Assessment
Exposure
Specify degree/severity of exposure and assess the likelihood/probability of each threat scenario $\mathbf{T}_j$ out of $\mathbf{T}_D$
Sensitivity
Describe the negative outcomes $O(\mathbf{T}_j)$ and provide a (as semi-quantitative) assessment $v(O(\mathbf{T}_j))$
Adaptive Capacity
Assessing for each $\mathbf{T}_j$ whether and how $\boldsymbol{H}^*$ can cope the negative impacts of $O(\mathbf{T}_j)$ in a first semi-quantitative manner
Intervention Scenarios $\mathbf{I}(\mathbf{T}_j)$
Construct for each (selected, consistent) intervention scenario $\mathbf{T}_j$ a (best) intervention scenario
(1) To reduce exposure and sensitivity
(2) To increase adaptive capacity

Figure 3. Main steps of the SVIDT assessment.

These causal models of internal and external digital threats can be seen as cognitive models about cause-and-effect relationships [90]. Usually, a threat analysis is carried out when incorporating people from the human system H^* or experts concerning this system. This can be done in a transdisciplinary venture. We want to note that the construction of causal chains for digital threats also provides insight into the general, non-digital resilience of H^* itself and thus is overly appreciated. This is similar to the general ISO 14000 certification. The SVIDT method takes a specific "digital" perspective, but it can be meaningfully applied only if the whole system H^* is sufficiently understood and acknowledged. After the single threats are listed separately (including the positioning in the system model and the actors/actions causing them), we may start with the construction of threat scenarios. We suggest applying a modified *Formative Scenario Analysis* [30]. Each threat may be considered an impact factor that has two levels, i.e., "taking place" and "not taking place". An important step for reducing the scenarios is consistency analysis. This analysis sorts out combinations of the occurrence and non-occurrence of threats that do not fit together. Then, a small set of 5 +/− 2 threat scenarios (with high consistency) should be selected that represent different clusters (or types) of scenarios. There are software programs that support this step [91]. We should also note that ideas from Stafford Beer's [24] *viable system theory*, such as identifying threats that must be blocked at any cost, may be utilized here.

Figure 4 sketches major actions of Steps 6 and 7 for the case presented in Section 3. In a differentiated analysis, for each of the selected threat scenarios, an *exposure assessment* and a *sensitivity* analysis may follow. The *degree/strengths* and the *likelihood* of exposure to a threat scenario T_i can be assessed in a semiquantitative manner or in a quantitative manner when assigning negative numerical values/utilities (as outputs) and probabilities for each negative outcome $\mathrm{O}_k(T_i)$. For running a quantitative analysis, the reader may refer to Scholz et al. [2]. For a *semiquantitative* assessment, the likelihood of a (well-defined) critical degree of negative impact or outcome can be rated or assessed by a binary (yes/no) or ordinal Likert-type scale (e.g., with 1 being a very low and 10 a very high rating). In addition, likelihoods may be attributed on an ordinal scale. For this step, it is often meaningful to specify the time range (e.g., within the short term vs. the long term). This serves not only to identify short-term threats but also unintended rebound effects (see Postulate 3 of the HES framework, S2) and critical tipping points that can result from overburdening the system due to delayed utilization/over-utilization by digital technologies.

Step 7: Intervention scenarios. If the exposure against critical digital threats has been assessed, a rating of *sensitivity* against the different negative outcomes may follow. This is conceptually challenging and the most important step of the SVIDT method. *The goal is to construct a sufficient set of three to seven threat scenarios that may induce critical, negative outcomes for which we want to construct intervention scenarios.* We suggest that the intervention scenarios be constructed by means of Formative Scenario Analysis in a participatory process with the main actors [92]. The intervention scenarios should then serve to *improve the adaptive capacity* in a short-, mid-, and long-term time frame. The term *formative,* i.e., giving form, indicates that the process of constructing scenarios is itself an important process for capacity building of the system H^*. One important part of this step is to classify interventions as being the *assimilation or accommodation* type.

Please acknowledge that the above steps not only extend risk management but also change the perspective as *we shift from* a priori *risk/threat assessment to a posteriori crisis management* (see Figure 4). The idea is to develop coupled digital threat × intervention scenarios and to assess how costly the (accommodative and assimilative) actions taken are. Naturally, a detailed elaboration and implementation of the interventions goes beyond the presented semiformal analysis. However, as presented in Figure 4, the vulnerability analysis can also be performed in a semiquantitative manner.

Step 8: Checking of win–win strategies: If there is an opportunity to include other actors, we may consider constructing action/intervention scenarios for the main partners and attaining synergies by constructing win–win (or triple-win or even quadruple-win) strategies. This may be the case with suppliers and customers, but competitors might also build an alliance, for instance, a group of neighboring wine growers could join together in an online marketing venture.

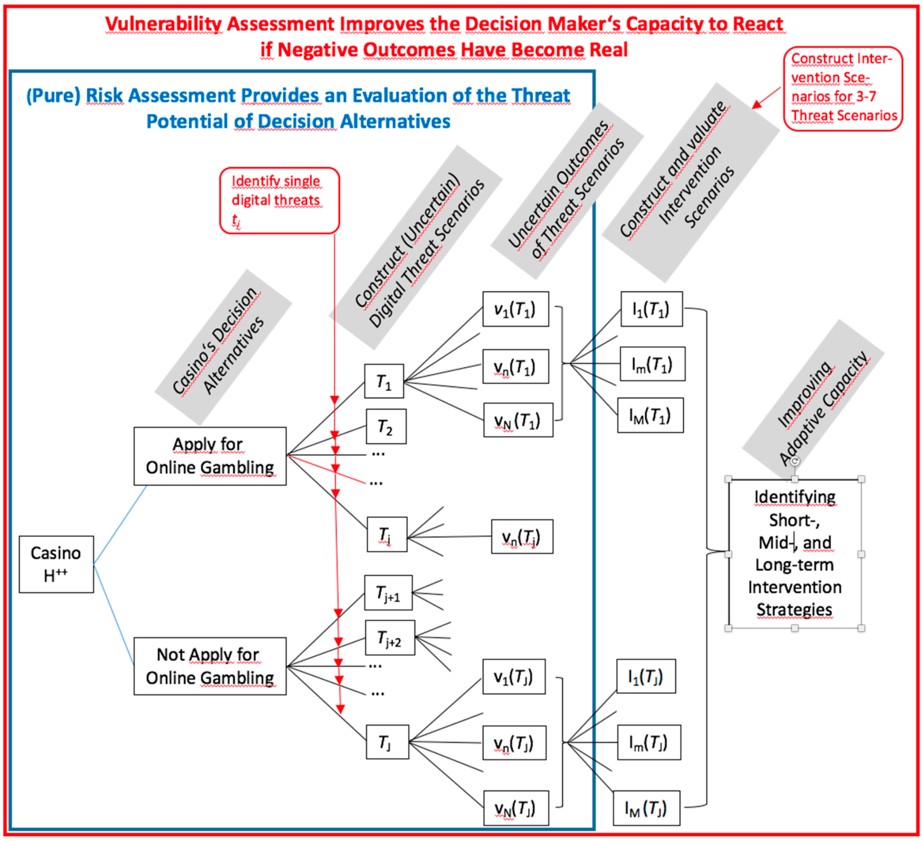

Vulnerability Assessment Improves the Decision Maker's Capacity to React if Negative Outcomes Have Become Real
(Pure) Risk Assessment Provides an Evaluation of the Threat Potential of Decision Alternatives
Construct Inter-vention Sce-narios for 3-7 Threat Scenarios
Identify single digital threats t_i
Casino's Decision Alternatives
Construct (Uncertain) Digital Threat Scenarios
Uncertain Outcomes of Threat Scenarios
Construct and valuate Intervention Scenarios
Improving Adaptive Capacity
Casino H^{++}
Apply for Online Gambling
Not Apply for Online Gambling
T_1
T_2
...
...
T_j
T_{j+1}
T_{j+2}
...
...
T_J
$v_1(T_1)$
$v_n(T_1)$
$v_N(T_1)$
$v_n(T_j)$
$v_1(T_J)$
$v_n(T_J)$
$v_N(T_J)$
$I_1(T_1)$
$I_m(T_1)$
$I_M(T_1)$
$I_1(T_J)$
$I_m(T_J)$
$I_M(T_J)$
Identifying Short-, Mid-, and Long-term Intervention Strategies

Figure 4. Key steps of vulnerability and sensitivity analysis (in a simplified manner; all variables are explained in detail in Section 4.4).

Step 9: Sustainability assessment. Interventions may require fundamental changes (i.e., a change in business strategy, new products, and/or other forms of adaptation) that seem to be too costly and may appear unattractive. Other interventions might seem more attractive economically, but there may be some doubt about whether they are sufficient. Therefore, we suggest finalizing the vulnerability assessment with an SPA evaluation (see Table 1). This should start *first* with a benchmarking of the current performance to the (supposed) ideal (potential) performance/function(ing) $v_{sust}(H^*)$. The *second* step is the system and vulnerability/resilience assessment of each of the systems both without (i.e., $vul(H^*)$) and with interventions (i.e., $vul(H^*(I(T_i))$ or $vul(H^*(I(T_D))$. The *third* aspect is whether the interventions contribute to or harm intra- and intergenerational justice. The overall SPA judgment may be provided quantitatively or qualitatively. For a more thorough analysis, see Binder et al. [82] or Scholz and Tietje [93].

4. Applying the SVIDT Method

4.1. System Analysis for a Swiss Casino Facing a Transition to Online Gambling

We apply the SVIDT method to legalizing online gambling using the case of *one* of the 21 publicly licensed *Swiss casinos*, which we will call H^{++}. This case is of societal and theoretical interest. As the subject matter, theoretical background, and methodology may be overly complex, the reader may first wish to read *The Hitchhiker's Guide to SVIDT* (see Appendix A Figure A1).

We refer to the challenge of Swiss casinos using one we call casino H^{++}. A first challenge is to understand the problem and to perform a system analysis (Steps 1–4 of SVIDT). The transition of H^{++} to online gambling is framed by a draft of a new Swiss Law of Real Money Games (German: Geldspielgesetz) [94]. This law has passed the consultation step in the Swiss Parliament including. Currently, in a final step, the operationalizing of Internet censorship of foreign online gambling providers is discussed [95]. The case is related to major digital threats such as Internet addiction [8,96]. From the perspective of digital threats, protecting gamblers from the addictive and putative epigenetic impacts linked to Internet gaming is a key issue in this complex legislative draft.

In 2014, legal casinos (which do not include lotteries and sports betting) provided a revenue of 710 million CHF (given 8.2 million inhabitants), resulting in federal taxes of 336 million CHF [97]. We should note that there is an estimated loss of 300 million CHF among Swiss gamblers abroad, due in part to an increasing amount of (foreign) online gambling. From 2008 to 2014, revenue decreased by 30.4% due to foreign gamblers' visits to casinos close to Swiss borders, banning gambling based on social responsibility, i.e., enforced addiction control, and other reasons (e.g., forbidding smoking); during the same period, online gambling increased [97]. The latter is not allowed by Swiss providers. Thus, Swiss casinos—and perhaps also the Swiss government and taxpayers—are facing a digital threat that is compelling this industry to adapt to an e-business model. All three main subcategories of games, e.g., the roulette-like and poker-/blackjack-like table games and the most profitable, slot-machine gambling (which comprises 82% of the revenue), should be offered online.

Online gambling is not yet permitted by Swiss law, but, according to the new draft law on money games, the licensing of some terrestrial Swiss casinos will be extended to online gambling (Art. 5 and 9; see FDJP 2016a). In order to stay in business, casino H^{++} has to compete with other Swiss casinos for an online license. One important decision criterion (besides a solid business plan) is for the casino to develop a *social concept* (Art. 74). The (terrestrial and licensed) casinos have to develop a *new business model for online gambling*. The realization of the social concept for online gambling will be a main challenge and criterion for being granted a license by the Swiss Federal Gaming Board (FGB). Since allowing casino gambling in 2001, Switzerland has developed extensive means, i.e., as a social concept, for protecting gamblers who participate in conventional gambling. This is unique in the world. *Switzerland is, as far as we know, the world's leader* among countries with legalized money gaming in regard to protecting people against over-gambling and financial ruin due to addiction or other reasons. A key objective for the framing agent, the FGB (see Figure 4), is to maintain the standards for terrestrial gambling and apply them to online gambling. We should note that Art. 84 of the draft law intends to block access to foreign *online gambling providers* [95,98,99], such as the viewing of child pornography.

Let us briefly look at the extensive regulations Swiss *casinos* must follow for non-online gambling. Slot machines are controlled and have to guarantee a certain payout ratio. Players must register by passport. (High) Player's pools have to be observed, and disclosures of income and bank balances are required if critical observations (e.g., big stakes/pools) are made. A critical question is what these procedures, including information acquisition from banks, might look like in an online gambling context. This is part of a *social concept for online banking* (Art. 8.2, [94]). In the future, casino H^{++} has to present a convincing concept about how to inform online gamblers about risks with the same efficacy. Early-recognition tools for identifying endangered players, means of inducing self-control, limited playing rules, and banning endangered players from casinos in a timely manner should function with the same efficacy as they do in off-line gambling. This is also of significant importance for the casino itself. Recently, a Swiss casino was penalized by the Federal Supreme Court with a fine of about 1.5 million CHF (coming down from a first instance sentence with about five million) due to an accusation of the FGB. The gambler had not been banned, although the casino must have had clear evidence that the (expected) losses would be above the (known and extraordinarily high) income that the player had to reveal to the casino according to the social concept [100].

For a *multilevel analysis* (see Figures 3 and 4), we first focus on three levels of actors (see Figure 5b), i.e., gamblers H^{+}, the casino H^{++}, and the framing agents H^{+++}. We consider the gambler-protection association SOS (e.g., Spielen ohne Sucht Switzerland, in English, Gambling without Addiction) as an important stakeholder. SOS is not a traditional NGO but a joint initiative between an NGO-like organization (i.e., Sucht Schweiz, in English, Addiction Switzerland, a private foundation with some minor public involvement in 16 Swiss cantons) and a community-based family service of one Swiss canton (Perspektive Thurgau). In Figure 4, we placed SOS as a stakeholder on the level of an organization, although it is in some places closely linked to gamblers and their family members (hierarchy level of the group). In 2012, about 70.6% of all Swiss adults had gambling experience, and 46.4% gambled for money [101]. The estimates of the number of people demonstrate that critical or pathological gambling behavior in Switzerland varies between 76,000 [101] and 120,000 [102]. About 43,000 (corresponding to approximately more than 1 of every 150 adult residents of the nation) were banned by Swiss casinos in 2014 [103]. The *hidden social costs* of gambling, including lotteries, amount to 551 to 648 million CHF annually [104,105]. The Swiss Association of Casinos judges the contribution of the gambling industry to the GDP to amount to five billion CHF. Thus, *Swiss society* is facing a delicate trade-off between the *costs* of gambling (which include personal bankruptcy, suicide, and risks to health, family, and work as well as procurement crimes) and benefits by income, employment, etc. One *societal threat* is that online gambling does not allow for the similar protection of gamblers that terrestrial gambling does. A threat for the (competing) casino H^{++} is to develop a convincing strategy for the social concept that convinces the regulating authority FGB (H^{+++} in Figure 4) that the individual gambler H^{+} is sufficiently protected and that all loopholes (an addicted player may take advantage of) are closed.

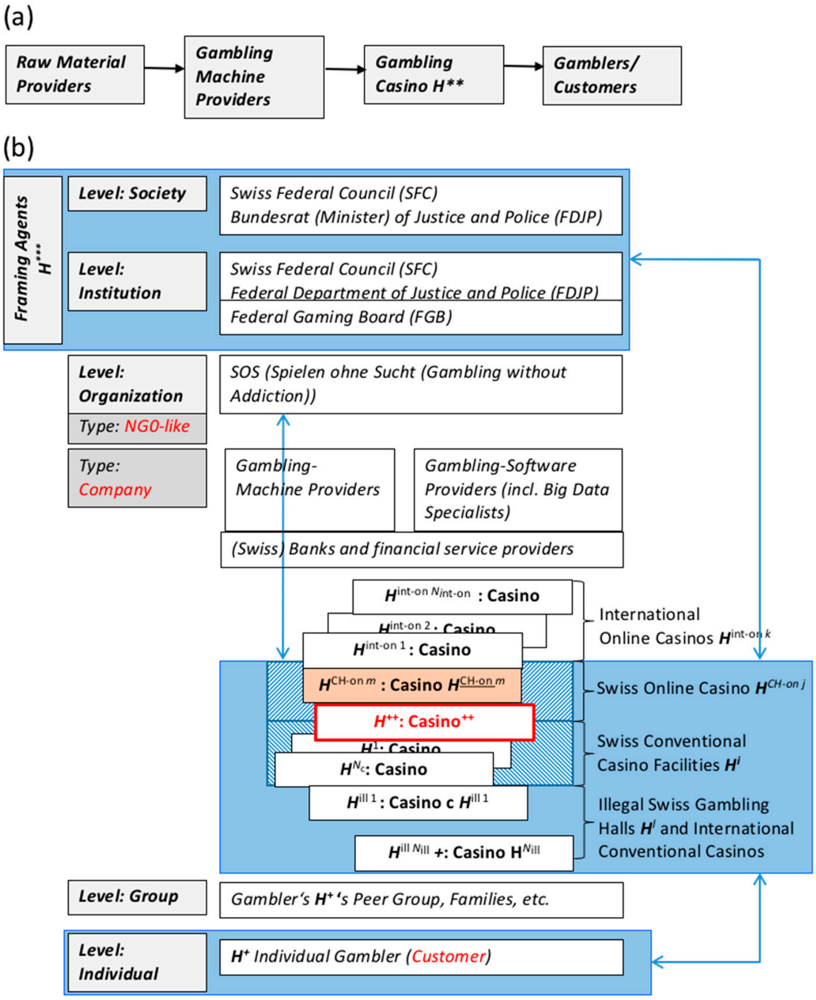

(a)
Raw Material Providers
Gambling Machine Providers
Gambling Casino H**
Gamblers/ Customers
(b)
Framing Agents H***
Level: Society
Swiss Federal Council (SFC)
Bundesrat (Minister) of Justice and Police (FDJP)
Level: Institution
Swiss Federal Council (SFC)
Federal Department of Justice and Police (FDJP)
Federal Gaming Board (FGB)
Level: Organization
Type: NGO-like
SOS (Spielen ohne Sucht (Gambling without Addiction))
Type: Company
Gambling-Machine Providers
Gambling-Software Providers (incl. Big Data Specialists)
(Swiss) Banks and financial service providers
$H^{\text{int-on } N_{\text{int-on}}}$: Casino
$H^{\text{int-on } 2}$: Casino
$H^{\text{int-on } 1}$: Casino
International Online Casinos $H^{\text{int-on } k}$
$H^{\text{CH-on } m}$: Casino $H^{\underline{\text{CH-on}}\, m}$
Swiss Online Casino $H^{CH\text{-}on\ j}$
H^{++}: Casino^{++}
H^{1}: Casino
H^{N_c}: Casino
Swiss Conventional Casino Facilities H^{i}
$H^{\text{ill } 1}$: Casino c $H^{\text{ill } 1}$
$H^{\text{ill } N_{\text{ill}}}$ +: Casino $H^{N_{\text{ill}}}$
Illegal Swiss Gambling Halls H^{l} and International Conventional Casinos
Level: Group
Gambler's H^{+}'s Peer Group, Families, etc.
Level: Individual
H^{+} Individual Gambler (Customer)

Figure 5. (**a**) Simplified supply chain of a Swiss gambling casino H^{++}. (**b**) Multilevel human-systems analysis (actor analysis). The light-blue boxes represent actors of the presented systems included in the three levels, i.e., the individual gambler H^{+}, the casino H^{++}, and the framing agents H^{+++}.

4.2. Goal Formation

The starting point for an SVIDT analysis is goal formation. Casino H^{++} has to develop new technologies, control mechanisms, staff competences, etc. for socially responsible online gambling that meets the high standards of the social concept. This requires H^{++} to engage in drastic accommodations in regard to organization, knowledge, financial planning, etc. The challenge is to develop a business plan for *responsible and sustainable online gambling* that provides a high profit (which in is the interest of the owners, mostly communities). The application of an SVIDT analysis should help determine whether the casino should apply for the license and what next step or steps to take if (a) it does not apply, (b1) it applies but does *not receive* a license, and (b2) it applies and is granted a concession.

The *supply chain* consists of "all parties involved, directly or indirectly, in fulfilling a customer request" [106]. The supply chain of *conventional casinos* is simple (Figure 5a). The main upstream party is the mechanical, electromechanical, and electronic gambling-machine providers (see Figure 4a,b). Slot machines have to fulfill certain criteria of the FGB (e.g., reliably meeting a payout ratio). The simulation of reliable (i.e., fair) and transparent probabilities for payout rates (which calls for proper control mechanisms that allow regulatory bodies as well as players to recognize that the proclaimed probabilities are fulfilled) is an important aspect. One may speculate whether *gambling software* including the survey of Big Data (e.g., about the characteristics of poker gamblers, payoff rates of machines) will become a new business sector and part of the supply chain (see Figure 4b).

4.3. Multilevel SVIDT Analysis Applied to Online Transitioning of the SWISS CASINO H^{++}

Figure 5b presents Casino H^{++} in the middle box. H^{++} is a company. Other casinos are the main actors on the daily market. Only current terrestrial casinos are allowed to apply for licenses to provide online gambling. Therefore, there will be few future Swiss online providers $H^{\text{int}-\text{on}\ m}$ $(0 \leq m \leq N_{CH} = 21)$ and a large number of (already existing) European and international online casinos $(1 \leq j \leq N_{int-on})$, which are currently illegal), illegal Swiss gambling joints $(0 \leq l \leq N_{ill})$, and H^{++} foreign casinos (close to the border) among the competitors. Naturally, there are some international players, such as the Court of Justice and Policy of the European Union and the committees of the European Union on social regulations and online gambling, that may react to planned action (e.g., the [100] restriction of online access). We do not address these players here.

The most important challenges (and digital threats) for H^{++} are to present a convincing, comparably strong *social concept for online gambling* and to prepare (i.e., to develop adaptive capacity) for the event that certain processes do not work well (i.e., the above-mentioned banning of Internet access to foreign Internet providers) or that gamblers find *digital loopholes* and play abroad; or other digital threats.

4.4. From Strengths and Weaknesses to Threat and Intervention Scenarios

After Steps 3 and 4 (see Figure 3), casino H^{++} has to check its human resources, financial power, competiveness, etc. related to digital threats. Typical questions here are as follows:

- How is the organizational structure to be changed?
- Do staff possess sufficient knowledge to be prepared to run an online business, including management of Big Data?
- What (international) online-gaming software providers may economically implement a Swiss, social-concept-tailored Internet platform for managing and monitoring gaming?
- What human resources are needed to design procedures for a social concept? Should NGOs or organizations such as SOS or other experts/researchers be included?
- Do we have the right connections with competitors or stakeholders to balance precompetitive joint lobbying (e.g., for collaborating with banks) and competition for getting an online license?

In the course of answering these questions, H^{++} may *determine digital threats* (see Step 6 of the SVIDT method). This is done exemplarily in Table 2. All single threats t_k $(k = 1, \ldots, K)$, such as the further reduction of hall gambling after legalization and the situation of online gambling (t_1) and the functioning of banning international online gambling (t_2, see Table 2, have to be identified first. As some banks are currently under public control because of profitability (due to the reduction of hall gambling), H^{++} has to determine whether it can afford to apply (given the risk of the proposal being declined, $t_{3,}$). Finally, the quality of the *social concept* for online gambling will be "*the*" critical selection criterion. The casino has to decide whether it has the competence and adequate financial means to prepare the application (t_4), whether it can afford to apply in the event that its proposal is denied (t_5), etc.

We do not go into all the technical details of constructing and selecting consistent threat scenarios here (see Scholz and Tietje, 2002, Chapter 5). However, for facilitating applications, we present consistent formal definitions and describe a template for the application. The reader should refer to Figure 3 when reading the subsequent text. A threat scenario T_j (see column "Constructing threat scenarios") is characterized by a complete combination of levels of all K impact factors. For defining the levels of impact factors (e.g., "1" means low threat, "2" means high threat), we assume that the levels are numbered by an index r = 1, 2, 3, ... , R. Then, for a threat scenario T_j each (single) threat t_k shows a specific (intensity) level $r_{k,j}$. Thus, the threat scenario T_j may formally read $T_j = \left(t_{1,r_{1,j}} \ \ldots, t_{\mathrm{i},r_{k,j}}, \ldots, t_{\mathrm{K},r_{K,j}}\right)$.

Table 2. (a) Digital threats t_k for a Swiss casino H^{++} (b) in the transition to online gambling. For nomenclature, see text.

Label	Threat for a Swiss Casino H^{++}	Levels (r = 1, 2)	Key Questions for Identifying Interventions
t_1	Critical decline of pre-tax profit after legalizing Swiss online gambling.	$r = 1$: <x% $r = 2$: $\geq x$%	How does a business plan look with reduced demand for terrestrial gambling if no online concession is received (a, b1) or if a concession is received (b2)?
t_2	How does the banning of foreign Internet access function?	$r = 1$: well-functioning $r = 2$: not functioning	What levels of reduction can be met with what means? By what promotion might we get what share of gamblers and what gaming sum?
t_3	Investment for successfully introducing online gambling is beyond the possibility/capacity of the casino.	$r = 1$: yes $r = 2$: no	If one's own capacity is too small, who might become a business partner?
t_4	Costs and conceptualizing an application for an online license (including a social license), given (*) a decline of the proposal by FGB, are too high.	$r = 1$: too high to survive; $r = 2$: feasible	If 1, who is a potential partner for a joint application?
t_5	Costs for practicing/running a social concept for online monitoring.	$r = 1$: feasible; $r = 2$: too high to survive	Can you build an alliance with other casinos?
...			
t_k	...		
t_{k+1}	(Swiss) Banks do not cooperate in the monitoring of endangered gamblers.	+/−	What alliances/laws/decrees are needed?
...			
t_K	...		...

Each threat scenario T_j may provide different relevant outcomes $O_n,\ n = 1, \ldots, N$ whose valuation we call $v_n(T_j)$. Depending on the likelihood of the threat scenario (i.e., exposure) and the profile of valued outcomes (i.e., sensitivity), which are mostly negative, a small set of 3–7 threat scenarios $\mathrm{T}_{Intervention} = \{T_{I_1}, T_{I_2}, \ldots, T_{I_1}\}$ for which intervention scenarios should be constructed have to be selected.

The construction of intervention scenarios $I_m(T_j),\ m = 1, \ldots, M$ formally resembles the construction of threat scenarios. In a first step, facing the selected threat scenarios, possible single interventions are identified. Then, these are composed as "threat scenarios". Here, the art is to construct a small, reliable set of consistent scenarios that sufficiently represent the frame of possible actions. This is a common challenge of scenario construction that can be supported by computer programs [91]. The interventions and the intervention scenarios should be valuated (roughly) for costs and benefits.

The final step is to classify and prioritize the intervention scenarios (see Figure 4) and to identify short-, mid-, and long-term intervention scenarios that reduce risk (exposure and sensitivity) and increase adaptive capacity.

5. Discussion: Vulnerability Assessment as Part of Sustainability Assessment

5.1. The Problem/Challenge

Machines promise faster and cheaper ways of performing what human beings do. Digital technologies transform how we work and live. They provide new business worlds and health care systems, and they augment human sensory systems. The Internet of Things (IoT) allows these to take place on all scales, from sensors on microprocesses (e.g., about physiological functions) to cloud-based Big Data structures that may be used to describe global processes. From a biological perspective, we encounter visions of the 3D printing of human bones and tissues that are, seemingly, overly optimistic and naïve. In addition, there are new forms and qualities of machine-to-machine and other innovations [107]. These examples strongly suggest that humankind's creation of digital environments has the potential to result in new forms of human environment interactions and of human life.

Human systems today, and those of tomorrow, can interact with digital environments in a form that is evolutionarily unknown. This takes place on all levels of human systems, from the cell whose processes can be diagnosed and manipulated up to the human species, which becomes a networked real-time mind. Digital environments allow for the tremendous augmentation of human senses such as visualizing nanoparticles or virtually visiting other planets. However, as innovation includes creative destruction [108], we have to acknowledge that any innovation is Janus-faced. This is also why this paper presents a method for how the potential vulnerabilities of human systems can be approached and managed in order to prevent unnecessary and unwanted "hard landings".

From a *history of knowledge and science* perspective (see [8]), there are few key inventions of the mind (such as the place value of numbers, Boolean algebra, and simulation by smart algorithms) or breakthroughs in technological developments (such as the mastery of the electron that launched the creation of E_D) that may store, process, retrieve, and network seemingly unlimited amounts of digital information with tremendous speed that may be used independently of any geographic constraints. From an *evolutionary* perspective, the mastery of cell processes by digital technology (including genetically modified organisms and biocomputers), the tremendous amount of storage (including retrieval and processing), and real-time global networking herald a new level of evolution. Key challenges of digital threat management include the complexity, the multilayeredness, and horizontal and vertical Internetting; the speed of change and dissemination; the incomplete knowledge of human systems; and the tremendous potential for disruption. Problems like these call for soft-systems methodology such as procedure and capacity building for strong adaptation (accommodation). The presented SVIDT method relies on this method and on more than two decades of experience with transdisciplinary transitioning. It is genuinely designed for the digital-threat management of companies, but it can also be applied to other levels of H and non-digital threats of similar ontology.

5.2. The Conceptual Framework

We show (see Table 1) that *vulnerability* is complementary to *resilience* and thus a key part of *sustainability*. Vulnerability includes adaptive capacity as a main component [2,50] and extends risk assessment in multiple ways. *Adaptive capacity* changes the decision makers' perspectives *from pre to post* with respect to the occurrence of negative impacts of threats. The method suggests thinking ahead about what has to be done if the potential negative impacts of digital threats become real. Thus, the presented method can be considered a blueprint for assessing and managing the digital threats to a human system H^* in order to sustain viability. This is accomplished from the perspective that intervention strategies for coping with negative impacts are developed for a small set of threat scenarios. We have mentioned that this selection of scenarios is a key concept of SVIDT. The challenge here is to select a set of threat and intervention scenarios that are sufficiently large and diverse that a specific human system H^* knows what to do to maintain viability. Here, concepts such as the *satisficing principle* [109] and Brunswik's *vicarious mediation* [110] are important. The sets of scenarios must be sufficiently large to identify all relevant interventions and selected in such a way that if a single threat or intervention is missing, the other (selected one) is sufficient for successful adaptation.

The SVIDT method has been described in the text and in figures with various degrees of abstraction. One important idea is to utilize both for threats and interventions, the ideas of *Formative Scenario Analysis* [30] in which a scenario is perceived as a complete combination of levels of impact factors that, in their simplest form, have two levels: "taking place" and "not taking place". We may note that, in addition, ideas from Beer's [24] viable system theory, such as identifying threats that must be blocked at any cost, may be utilized here.

The *vulnerability concept* is embedded in an evaluation concept that has been transferred from an ecological system analysis (BEPA) by including the aspect of *intra- and intergenerational justice* [54]. There is much evidence [111–113] that the Digital Revolution induces a digital divide rather than equity in regard to knowledge and income. Here, a critical question is what ownership, control, access, and knowledge a human system H has about the environmental system E_D.

The HES framework (see Supplementary S1) is conceived as a basic conceptual tool that helps to reduce the complexity of coupled HES. It does not only allow for a concise definition of different types of environments (e.g., abiotic vs. biotic; biophysical vs. sociocultural epistemic) for properly describing the effects of E_D on different types and layers of H and vice versa. Rather, the postulates of the framework (e.g., the conception of the level hierarchy postulates P2 and P3) or the decision theoretic (P4 and P5) provide a common language and thus allow for the traceability and the replicability of the presented SVIDT method.

If we reflect on the weaknesses of the presented framework, one may argue that the agency of digital structures or networks has not been sufficiently acknowledged. This is due to the decision theoretic perspective and the focus on human interventions. The presented framework includes digital systems as an important component of the environment, but it postulates that these systems can only be properly utilized based on human systems' decisions and behaviors.

5.3. Strengths and Limits of the Proposed SVIDT Method

The proposed method links a (coupled) HES system analysis and a vulnerability assessment including the construction and evaluation of intervention strategies. The method has multiple methodological roots such as formative scenario analysis, integrated risk assessment, and utility function-based evaluation of strategies, among others. The application of the methods in the frame of SVIDT is usually semiquantitative in nature and not based on real numbers. Thus, the proposed framework should rather be considered as scaffolding that directs different steps of semiquantitative assessments that help analysts acquire insights into the necessary assimilations (i.e., soft adaptations) and the more thorough accommodations. This is in line with other soft-operational research techniques; the problem structuring and the support of decisions are main objectives [22,42,114–117].

We have stressed in various places that SVIDT can be best applied when collaborating with actors from the specific system *H** that becomes the subject of analysis. The incorporation of stakeholders (who are incorporated in the multilevel analysis) can also be achieved effectively in transdisciplinary processes whose products are the development of socially robust solutions for a "sustainable and resilient relationship with E_D" [31,46].

The specific ontology of digital threats (see Section 5.1) refers not only to uncertainty (in knowledge) but also to ignorance. This is well reflected in the distinction between *specified* and *general resilience*. Whereas specified resilience refers to known threats, general resilience means an ability to cope with the unknown. We may question whether, by applying the proposed SVIDT method, we improve the analyst's and the specific human system *H**'s capacity to cope with unknown digital threats. There are two arguments here. First, by increasing the adaptive capacity, etc., of a system *H**, the system itself becomes less vulnerable to some of the unknown threats. Second, the capacity of analysts and members of *H** to cope with presently unknown risks is improved by working with SVIDT and being able to apply it. Thus, the SVIDT method is a tool that successfully strengthens the capacity of human systems to meaningfully utilize the opportunities of the digital world.

6. Conclusions

The proposed SVIDT method supports strategy formation for constructing intervention scenarios that increase the resilience of coupled human–digital environment systems. SVIDT goes beyond conventional risk management. It focuses not only on the magnitude and likelihood of exposure and sensitivity but also on the system's ability to increase the adaptive capacity of a specific system *H** of interest. The application of SVIDT should help to identify disruptive transitions and to prepare human systems for hard, accommodation-like adaptations that call for new material, behavioral, cognitive, organizational, and operative structures.

The method is designed to deal with the ambiguity due to uncertainty and the unknown about future digital settings. Given the vast amount of social, natural, and engineering knowledge that is needed to gain insights into societal and technological changes, we suggest that SVIDT works best when the practitioners, i.e., representatives of *H**, participate in the process of applying the method, that is, in a transdisciplinary process.

There is a vast set of digital threats related to the rapid, ubiquitous, and economically obvious and overly beneficial spread of digital technologies that may intelligently support the fulfillment of human needs on all levels and activities of human systems. A challenge is that all E_D rapidly induce evolutionary new forms of augmented communication among human systems and their abiotic environments (including smart conventional digital systems), human systems, and presumably enhanced biotic environments (such as digitally equipped beings and systems or biocomputers), and new forms of interaction among smart machines with other smart machines. The presented method may help to better cope with disruptions in the forthcoming ontogenetic and phylogenetic development.

Supplementary Materials: The following are available online at www.mdpi.com/2071-1050/9/4/554/s1.

Acknowledgments: I want to thank Reiner Czichos, Bernhard Geissler, Christian E. Scholz, and Gerald Steiner for their valuable inputs and reviews and Elaine Ambrose for the English editing. The section on the transition of the transition of the Swiss casinos to online gambling received feedback from Jean Marie Jordan (Swiss Federal Gaming Board), Sylvia Steiner (Sucht Schweiz), and Marcel Tobler (Grand Casino Baden).

Author Contributions: This paper is a single-author paper. The author conducted all of the research himself.

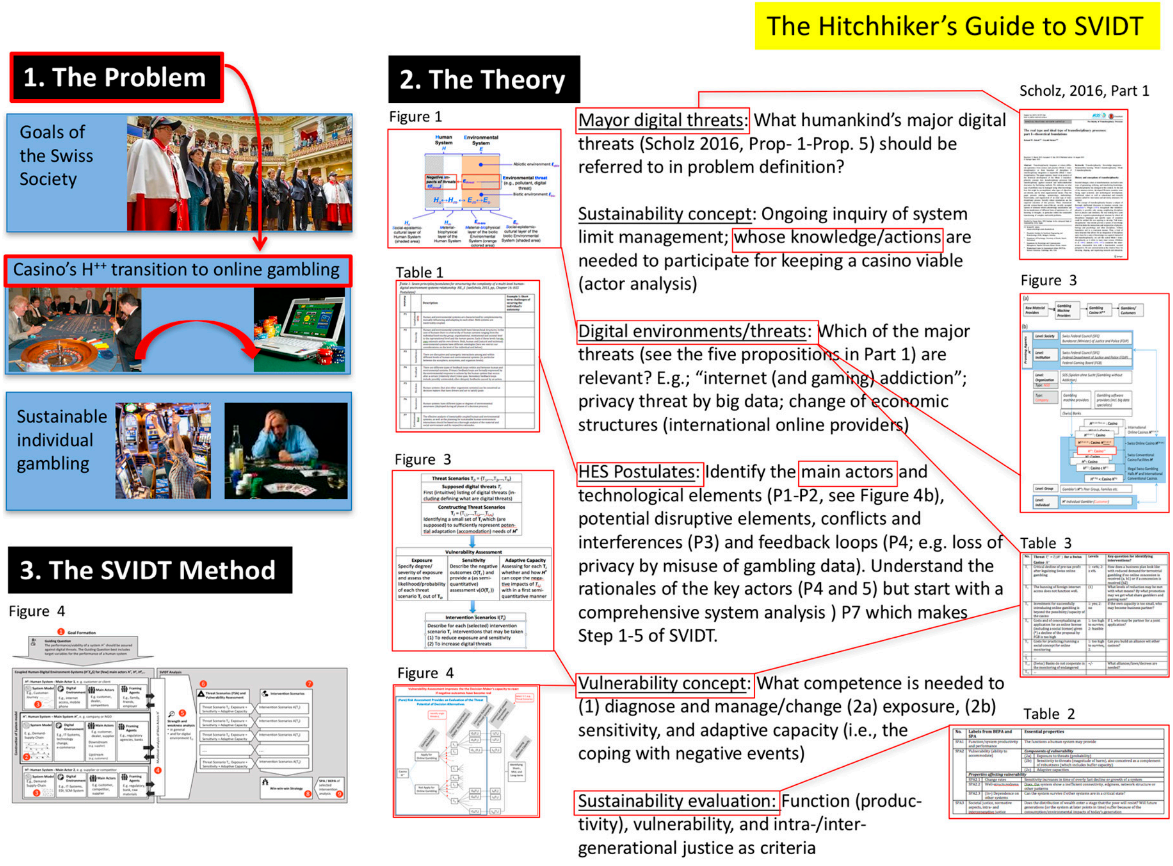
Conflicts of Interest: The authors declares no conflict of interest.

Appendix A

When applying the nine steps of the SVIDT method or when reading through the Swiss casino case, the reader may have difficulties understanding how the many theoretical concepts presented in Section 1 of Part 2 and the Propositions of Scholz (2016) [8] can be meaningfully used. This holds particularly true for readers who are not literate in the HES framework (see Scholz, 2011) [65], vulnerability analysis (Scholz et al., 2015) [2], or methods of complex case study such as BEPA (see Scholz and Tietje, 2002 [30]; Scholz and Steiner, 2015, a, b [31,46]).

In this case, the reader might benefit from using "The Hitchhiker's Guide to SVIDT". This is not a work of science fiction comedy such as Douglas Adams's books, which involved looking for a cyberspace bypass. We just want to look ahead for a specific human system. Here, we take one of the Swiss gambling casinos that want to engage in an online-gambling enterprise. The casino is challenged by the exceptional goals of the Swiss government to establish socially responsible and sustainable gambling (see the upper left part of the guide). The social concept for players (which is promoted by some NGOs; see Part 4) has to become subject to the world of future legal Swiss gambling.

The right column ("the theory") shows where the proposed theoretical milestones of analyzing, designing, and developing sustainable digital environments can be utilized in the different steps of SVIDT. Thus, the hitchhiker's guide links the real-world problem with the theory of a sustainable digital environment and the SVIDT method, which may be considered a tool for establishing a resilient partnership with digital technologies, i.e., sustainable HE_DS.


The Hitchhiker's Guide to SVIDT
1. The Problem
Goals of the Swiss Society
Casino's H⁺⁺ transition to online gambling
Sustainable individual gambling
3. The SVIDT Method
Figure 4
2. The Theory
Figure 1
Table 1
Figure 3
Figure 4
Scholz, 2016, Part 1
Figure 3
Table 3
Table 2

Mayor digital threats: What humankind's major digital threats (Scholz 2016, Prop- 1-Prop. 5) should be referred to in problem definition?

Sustainability concept: Ongoing inquiry of system limit management; whose knowledge/actions are needed to participate for keeping a casino viable (actor analysis)

Digital environments/threats: Which of the major threats (see the five propositions in Part 1) are relevant? E.g.; "internet (and gaming) addiction"; privacy threat by big data; change of economic structures (international online providers)

HES Postulates: Identify the main actors and technological elements (P1-P2, see Figure 4b), potential disruptive elements, conflicts and interferences (P3) and feedback loops (P4; e.g. loss of privacy by misuse of gambling data). Understand the rationales of the key actors (P4 and 5) but start with a comprehensive system analysis) P7 which makes Step 1-5 of SVIDT.

Vulnerability concept: What competence is needed to (1) diagnose and manage/change (2a) exposure, (2b) sensitivity, and adaptive capacity (i.e., the coping with negative events)

Sustainability evaluation: Function (productivity), vulnerability, and intra-/inter-generational justice as criteria

Figure A1. The Hitchhiker's Guide to SVIDT.

References

1. Helbing, D. *Thinking Ahead-Essays on Big Data, Digital Revolution, and Participatory Market Society*; Springer: Cham, Switzerland, 2015.
2. Scholz, R.W.; Blumer, Y.B.; Brand, F.S. Risk, vulnerability, robustness, and resilience from a decision-theoretic perspective. *J. Risk Res.* **2012**, *15*, 313–330. [CrossRef]
3. Klibi, W.; Martel, A.; Guitouni, A. The design of robust value-creating supply chain networks: A critical review. *Eur. J. Oper. Res.* **2010**, *203*, 283–293. [CrossRef]
4. Bauch, C.T.; Sigdel, R.; Pharaon, J.; Anand, M. Early warning signals of regime shifts in coupled human-environment systems. *Proc. Natl. Acad. Sci. USA* **2016**, *113*, 14560–14567. [CrossRef] [PubMed]
5. Galvani, A.P.; Bauch, C.T.; Anand, M.; Singer, B.H.; Levin, S.A. *Human–Environment Interactions in Population and Ecosystem Health*; National Academy of Sciences: Washington, DC, USA, 2016.
6. Scholz, R.W.; Binder, C.R. Principles of human-environment systems (HES) research. In *Complexity and Integrated Resources Management Transactions of the 2nd Biennial Meeting of the International Environmental Modelling and Software Society*; Pahl-Wostl, C., Schmidt, S., Rizzoli, A.E., Jakeman, A.J., Eds.; Zentrum für Umweltkommunikation (ZUK): Osnabrück, Germany, 2004; pp. 791–796.
7. Hilbert, M.; López, P. The world's technological capacity to store, communicate, and compute information. *Science* **2011**, *332*, 60–65. [CrossRef] [PubMed]
8. Scholz, R.W. Sustainable Digital Environments: What Major Challenges Is Humankind Facing? *Sustainability* **2016**, *8*, 726. [CrossRef]
9. Block, J.J. Issues for DSM-V: Internet addiction. *Am. J. Psychiatry* **2008**, *165*, 306–307. [CrossRef] [PubMed]
10. Petry, N.M.; Rehbein, F.; Gentile, D.A.; Lemmens, J.S.; Rumpf, H.J.; Mößle, T.; Bischof, G.; Tao, R.; Fung, D.S.; Borges, G.; et al. An international consensus for assessing internet gaming disorder using the new DSM-5 approach. *Addiction* **2014**, *109*, 1399–1406. [CrossRef] [PubMed]
11. Helbing, D. Big Data, privacy, and trusted web: What need to be done. In *Thinking Ahead-Essays on Big Data, Digital Revolution, and Participatory Market Society*; Helbing, D., Ed.; Springer: Cham, Switzerland, 2015.
12. Shum, S.B.; Aberer, K.; Schmidt, A.; Bishop, S.; Lukowicz, P.; Anderson, S.; Charalabidis, Y.; Domingue, J.; de Freitas, S.; et al. Towards a global participatory platform Democratising open data, complexity science and collective intelligence. *Eur. Phys. J. Spec. Top.* **2012**, *214*, 109–152. [CrossRef]
13. Frey, C.B.; Osborne, M. *The Future of Employment. How Susceptible Are Jobs to Computerisation*; University of Oxford: Oxford, UK, 2013.
14. Frey, C.B. *How Susceptible Are Countries Worldwide? Jobs at Risk of Automatation*; Oxford University, Oxford Martin School: Oxford, UK, 2016; pp. 11–19.
15. Helbing, D. *The Automatization of Society Is Next*; Amazon: Berkshire, UK, 2015.
16. Bertelsmann Stiftung. *"To the Man with a Hammer...". Augmenting the Policymaker's Toolbox for a Complex World*; Verlag Bertelsmann Stiftung: Gütersloh, Germany, 2016.
17. Piaget, J. *The Development of Thought*; Viking: New York, NY, USA, 1977.
18. Christensen, C. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*; Harvard Business Review Press: Cambridge MA, USA, 2013.
19. Tushman, M.L.; Anderson, P. Technological discontinuities and organizational environments. *Adm. Sci. Q.* **1986**, *31*, 439–465. [CrossRef]
20. Carlo, J.L.; Lyytinen, K.; Rose, G.M. Internet computing as a disruptive information technology innovation: The role of strong order effects. *Inf. Syst. J.* **2011**, *21*, 91–122. [CrossRef]
21. Ackermann, F. Problem structuring methods 'in the Dock': Arguing the case for Soft OR. *Eur. J. Oper. Res.* **2012**, *219*, 652–658. [CrossRef]
22. Friend, J.; Hickling, J. *Planning under Pressure. The Strategic Choice Approach*; Elsevier: Amsterdam, The Netherlands, 2005.
23. Checkland, P.; Poulter, J. Soft systems methodology. In *Systems Approaches to Managing Change: A Practical Guide*; Reynolds, M., Holwell, S., Eds.; Springer: London, UK, 2010; pp. 191–242.
24. Beer, S. The Viable System Model: Its provenance, development, methodology and pathology. *J. Oper. Res. Soc.* **1984**, *35*, 7–25. [CrossRef]
25. Eden, C.; Ackermann, F. SODA—The principles. In *Rational Analysis for a Problematic World Revisited*; Rosenhead, J., Mingers, J., Eds.; Wiley: Chichester, UK, 2001; pp. 21–41.

26. Klein, J.T.; Grossenbacher-Mansuy, W.; Häberli, R.; Bill, A.; Scholz, R.W.; Welti, M. (Eds.) *Transdisciplinarity: Joint Problem Solving among Science, Technology, and Society. An Effective Way for Managing Complexity*; Birkhäuser: Basel, Switzerland, 2001.
27. Scholz, R.W.; Steiner, G. Transdisciplinarity at the crossroads. *Sustain. Sci.* **2015**, *10*, 521–526. [CrossRef]
28. Jantsch, E. Inter- and transdisciplinary university: A systems approach to education and innovation. *Policy Sci.* **1970**, *1*, 403–428. [CrossRef]
29. Scholz, R.W.; Marks, D. Learning about transdisciplinarity: Where are we? Where have we been? Where should we go? In *Transdisciplinarity: Joint Problem Solving among Science, Technology, and Society*; Klein, J.T., Grossenbacher-Mansuy, W., Häberli, R., Bill, A., Scholz, R.W., Welti, M., Eds.; Birkhäuser Verlag AG: Basel, Switzerland, 2001; pp. 236–252.
30. Scholz, R.W.; Tietje, O. *Embedded Case Study Methods: Integrating Quantitative and Qualitative Knowledge*; Sage: Thousand Oaks, CA, USA, 2002.
31. Scholz, R.W.; Steiner, G. The real type and the ideal type of transdisciplinary processes. Part II—What constraints and obstacles do we meet in practice? *Sustain. Sci.* **2015**, *10*, 653–671.
32. Harsanyi, J.C. Cardinal utility in welfare economics and in the theory of risk-taking. *J. Political Econ.* **1953**, *61*, 434–435. [CrossRef]
33. Slovic, P. Assessment of risk-taking behavior. *Psychol. Bull.* **1964**, *61*, 220–233. [CrossRef] [PubMed]
34. Paustenbach, D.J. (Ed.) *The Risk Assessment of Environmental and Human Health Hazards: A Textbook of Case Studies*; Wiley & Sons, Inc.: New York, NY, USA, 1989.
35. Moser, C.; Stauffacher, M.; Blumer, Y.B.; Scholz, R.W. From risk to vulnerability: The role of perceived adaptive capacity for the acceptance of contested infrastructure. *J. Risk Res.* **2015**, *18*, 622–636. [CrossRef]
36. Keeney, R.L.; Raiffa, H. *Decisions with Multiple Objectives: Preferences and Value Trade-Offs*; Wiley: New York, NY, USA, 1976.
37. Saaty, T.L. *The Analytic Hierarchy Process*, 2nd ed.; RWS Publications: Pittburgh, PA, USA, 1990; Volume 287.
38. Mintzberg, H. The fall and rise of strategic planning. *Harv. Bus. Rev.* **1994**, *72*, 107–114.
39. Helms, M.M.; Nixon, J. Exploring SWOT analysis—Where are we now? A review of academic research from the last decade. *J. Strategy Manag.* **2010**, *3*, 215–251. [CrossRef]
40. Checkland, P.; Scholes, J. *Soft Systems Methodology in Action*; Wiley: Chichester, UK, 1990.
41. Midgley, G.; Cavana, R.Y.; Brocklesby, J.; Foote, J.L.; Wood, D.R.R.; Ahuriri-Driscoll, A. Towards a new framework for evaluating systemic problem structuring methods. *Eur. J. Oper. Res.* **2013**, *229*, 143–154. [CrossRef]
42. Rosenhead, J.; Mingers, L. (Eds.) *Rational Analysis for a Problematic World Revisited*; Wiley: Chichester, UK, 2001.
43. Midgley, G. *Systems Thinking*; Sage: London, UK, 2003; Volumes I–IV.
44. Gibbons, M.; Limoges, C.; Nowotny, H.; Schwartzman, S.; Scott, P.; Trow, M. *The New Production of Knowledge*; Sage: London, UK, 1994.
45. Scholz, R.W.; Lang, D.J.; Wiek, A.; Walter, A.L.; Stauffacher, M. Transdisciplinary case studies as a means of sustainability learning: Historical framework and theory. *Int. J. Sustain. Higher Educ.* **2006**, *7*, 226–251. [CrossRef]
46. Scholz, R.W.; Steiner, G. The real type and the ideal type of transdisciplinary processes. Part I—Theoretical foundations. *Sustain. Sci.* **2015**, *10*, 527–544. [CrossRef]
47. McCarthy, J.; Canziani, O.F.; Leary, N.A.; Dokken, D.J.; White, K.S. *Climate Change 2001: Impacts, Adaptation and Vulnerability*; Contribution of Working Group II to the Third Assessment Report of the IPPC; Cambridge University Press: Cambridge, UK, 2001.
48. Holling, C.S.; Gunderson, L.H. Resilience and adaptive cycles. In *Panarchy: Understanding Transformation in Human and Natural Systems*; Gunderson, L.H., Holling, C.S., Eds.; Island Press: Washington, DC, USA, 2002; pp. 25–63.
49. Folke, C.; Carpenter, S.; Walker, B.; Scheffer, M.; Elmqvist, T.; Gunderson, L.; Holling, C.S. Regime shifts, resilience, and biodiversity in ecosystem management. *Annu. Rev. Ecol. Evol. Syst.* **2004**, *35*, 557–581. [CrossRef]
50. Adger, W.N. Vulnerability. *Glob. Environ. Chang.* **2006**, *16*, 268–281. [CrossRef]

51. Turner, B.L.; Kasperson, R.E.; Matson, P.A.; McCarthy, J.J.; Corell, R.W.; Christensen, L.; Eckley, N.; Kasperson, J.X.; Luers, A.; Martello, M.L.; et al. A framework for vulnerability analysis in sustainability science. *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 8074–8079. [CrossRef] [PubMed]
52. Turner, B.L.; Matson, P.A.; McCarthy, J.J.; Corell, R.W.; Christensen, L.; Eckley, N.; Hovelsrud-Broda, G.K.; Kasperson, J.X.; Kasperson, R.E.; Luers, A.; et al. Illustrating the coupled human-environment system for vulnerability analysis: Three case studies. *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 8080–8085. [CrossRef] [PubMed]
53. Laws, D.; Scholz, R.W.; Shiroyama, H.; Susskind, L.; Suzuki, T.; Weber, O. Expert views on sustainability and technology implementation. *Int. J. Sustain. Dev. World Ecol.* **2004**, *11*, 247–261. [CrossRef]
54. World Commission on Environment and Development. Our common future. In *UN Documents*; United Nations: New York, NY, USA, 1987.
55. Paustenbach, D.J. (Ed.) *Human and Ecological Risk Assessment. Theory and Practice*; Wiley: New York, NY, USA, 2002.
56. Vlek, C.A.J.; Stallen, P.-J. Judging risks and benefits in the small and in the large. *Organ. Behav. Hum. Perform.* **1981**, *28*, 235–271. [CrossRef]
57. Oh, J.H.; Yang, S.J.; Do, Y.R. Healthy, natural, efficient and tunable lighting: Four-package white LEDs for optimizing the circadian effect, color quality and vision performance. *Light Sci. Appl.* **2014**, *3*, e141. [CrossRef]
58. Figueiro, M.G.; Wood, B.; Plitnick, B.; Rea, M.S. The impact of light from computer monitors on melatonin levels in college students. *Neuroendocrinol. Lett.* **2011**, *32*, 158–163. [PubMed]
59. Brachinger, H.W.; Weber, M. Risk as a primitive: A survey of measures of perceived risk. *Oper. Res. Spectr.* **1997**, *19*, 235–294. [CrossRef]
60. Aven, T. Risk assessment and risk management: Review of recent advances on their foundation. *Eur. J. Oper. Res.* **2016**, *253*, 1–13. [CrossRef]
61. Holling, C.S. Resilience and stability of ecological systems. *Annu. Rev. Ecol. Syst.* **1973**, *4*, 1–23. [CrossRef]
62. Gunderson, L.H.; Holling, C.S. (Eds.) *Panarchy: Understanding Transformation in Human and Natural Systems*; Island Press: Washington, DC, USA, 2002.
63. Cohen, M.A.; Lee, H.L. Strategic analysis of integrated production-distribution systems—Models and methods. *Oper. Res.* **1988**, *36*, 216–228. [CrossRef]
64. Tax, S.S.; McCutcheon, D.; Wilkinson, I.F. The Service Delivery Network (SDN): A Customer-Centric Perspective of the Customer Journey. *J. Serv. Res.* **2013**, *16*, 454–470. [CrossRef]
65. Scholz, R.W. *Environmental Literacy in Science and Society: From Knowledge to Decisions*; Cambridge University Press: Cambridge, UK, 2011.
66. Soloveichik, D.; Winfree, E. The computational power of Benenson automata. *Theor. Comput. Sci.* **2005**, *344*, 279–297. [CrossRef]
67. Ryan, M.; Goldman, A. Officials: San Bernardino Shooters Pledged Allegiance to the Islamic State, in Chicago Tribune. Available online: http://www.chicagotribune.com/news/nationworld/ct-san-bernardino-shooting-20151208-story.html (accessed on 1 April 2017).
68. Schwartz, P.M. Privacy and democracy in cyberspace. *Vanderbilt Law Rev.* **1999**, *52*, 1607. [CrossRef]
69. Sklansky, D.A. Too much information: How not to think about privacy and the Fourth Amendment. *Calif. Law Rev.* **2014**, *102*, 1069–1121.
70. Hedstrom, M. Digital preservation: A time bomb for digital libraries. *Comput. Humanit.* **1997**, *31*, 189–202. [CrossRef]
71. Morency, K. Cybersecurity finally takes centers stage in the US. *J. High Technol. Law* **2014**, *15*, 192–229.
72. Yar, M. *Cybercrime and Society*; Sage: Thousand Oaks, CA, USA, 2013.
73. Piaget, J. *Genetic Epistemology*; Columbia University Press: New York, NY, USA, 1968.
74. Scholz, R.W. Begriffslernen als Regelerwerb: Die Entwicklung des Proportionsbegriffs aus der Sicht des Informationsverarbeitungsansatzes. [The acquisition of the concept of proportions from a rule assessment approach]. *Math. Didact.* **1989**, *12*, 63–87.
75. *Commission Expert Group on Taxation of the Digital Economy, Report*; European Commision: Brussels, Bulgium, 2014.
76. Justitia US Law. *2014 Kentucky Revised Statutes, Chapter 139—Sales and Use Taxes*; Justitia: Mountain View, CA, USA, 2014.

77. Bell, S.; Morse, S. *Sustainability Indicators: Measuring the Immeasurable?* Earthscan: London, UK, 2008.
78. Bell, S.; Morse, S. *Measuring Sustainability: Learning from Doing*; Routledge: London, UK, 2013.
79. Parris, T.M.; Kates, R.W. Characterizing and measuring sustainable development. *Annu. Rev. Environ. Resour.* **2003**, *28*, 559–586. [CrossRef]
80. Evans, A.; Strezov, V.; Evans, T.J. Assessment of sustainability indicators for renewable energy technologies. *Renew. Sustain. Energy Rev.* **2009**, *13*, 1082–1088. [CrossRef]
81. Singh, R.K.; Muty, H.R.; Gupta, S.K.; Dikshit, A.K. An overview of sustainability assessment methodologies. *Ecol. Indic.* **2009**, *9*, 189–212. [CrossRef]
82. Binder, C.R.; Feola, G.; Steinberger, J.K. Considering the normative, systemic and procedural dimensions in indicator-based sustainability assessments in agriculture. *Environ. Impact Assess. Rev.* **2010**, *30*, 71–81. [CrossRef]
83. Lang, D.J.; Binder, C.R.; Scholz, R.W.; Wiek, A.; Stäublib, B.; Sieber, C. Sustainability Potential Analysis (SPA) of landfills—A systemic approach: Initial application towards a legal landfill assessment. *J. Clean. Prod.* **2007**, *15*, 1654–1661. [CrossRef]
84. Lang, D.J.; Scholz, R.W.; Binder, C.R.; Wiek, A.; Stäublib, B. Sustainability Potential Analysis (SPA) of landfills—A systemic approach: Theoretical considerations a systemic. *J. Clean. Prod.* **2007**, *15*, 1628–1638. [CrossRef]
85. Hermans, L.M.; Thissen, W.A.H. Actor analysis methods and their use for public policy analysts. *Eur. J. Oper. Res.* **2009**, *196*, 808–818. [CrossRef]
86. Bryson, J.M. What to do when stakeholders matter. Stakeholder identification and analysis techniques. *Public Manag. Rev.* **2004**, *6*, 21–53. [CrossRef]
87. Steiner, G. Supporting sustainable innovation through stakeholder management: A systems view. *Int. J. Innov. Learn.* **2008**, *5*, 595–616. [CrossRef]
88. Kelly, G.A. *The Psychology of Personal Constructs*; Norton: New York, NY, USA, 1955.
89. Fransella, F.; Bell, R.; Bannister, D. *A Manual for Repertory Grid Technique*; John Wiley: New York, NY, USA, 2004.
90. Eden, C. Analyzing cognitive maps to help structure issues or problems. *Eur. J. Oper. Res.* **2004**, *159*, 673–686. [CrossRef]
91. Tietje, O. Identification of a small reliable and efficient set of consistent scenarios. *Eur. J. Oper. Res.* **2005**, *162*, 418–432. [CrossRef]
92. Von Wirth, T.; Hayek, U.K.; Kunze, A.; Neuenschwander, N.; Stauffacher, M.; Scholz, R.Z. Identifying urban transformation dynamics: Functional use of scenario techniques to integrate knowledge from science and practice. *Technol. Forecast. Soc. Chang.* **2014**, *89*, 115–130. [CrossRef]
93. Tietje, O.; Scholz, R.W.; Hesske, S.; Grasmück, D.; Sell, J.; Weber, O. Integrale Bewertung von Sanierungsalternativen: Potentiale, Komponenten und Grenzen eines transdisziplinären Prozesses. *TerraTech* **2002**, *2*, 44–48.
94. FDJP. Bundesgesetz über Geldspiele (Geldspielgesetz, BGS) [935.51] (Entwurf)—Federal Law on Real Money Gabling [935.51] (Proposal). 2016. Available online: https://www.admin.ch/opc/de/classified-compilation/20151500/index.html (accessed on 7 April 2016).
95. Renz, F.; de Carli, L. Schweiz bricht Tabu und sperrt Website. *TagesAnzeiger*, 2 March 2017; p. 1.
96. Grusser, S.M.; Thalemann, R.; Griffiths, M.D. Excessive computer game playing: Evidence for addiction and aggression? *Cyberpsychol. Behav.* **2007**, *10*, 290–292. [CrossRef] [PubMed]
97. SCV. *Jahresbericht SCV*; Schweizer Casino Verband: Bern, Switzerland, 2014.
98. Glarner, A.; Valloni, N. The Principal Objections to the Swiss Draft Gambling Law. Available online: http://www.cecileparkmedia.com/online-gambling-lawyer/article_template.asp?Contents=Yes&from=woglr&ID=2098 (accessed on 1 April 2017).
99. FDJP. Neues Gesetz für alle Geldspiele: Bundesrat Verabschiedet Botschaft. 2015. Available online: http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2015/2015-10-21.html (accessed on 21 October 2015).
100. Swiss Supreme Court. *Swiss Supreme Court, BGer 2C_776/2013 vom 27.05.2014*; University of Bern: Bern, Switzerland, 2014; Available online: http://www.servat.unibe.ch/dfr/bger/140527_2C_776-2013.html (accessed on 1 April 2017).
101. Eichenberger, Y.; Rihs-Middel, M. *Glücksspiel: Verhalten und Problematik in der Schweiz. Schlussbericht, 7 August 2016*; Ferarihs: Villars-sur-Glâne, Switzerland, 2014.

102. Bondolfi, G.; Jermann, F.; Ferrero, F.; Zullino, D.; Osiek, C. Prevalence of pathological gambling in Switzerland after the opening of casinos and the introduction of new preventive legislation. *Acta Psychiatr. Scand.* **2008**, *117*, 236–239. [CrossRef] [PubMed]
103. Abderhalden, I. *Schweizer Suchtpanorama 2016, Mediendossier, 8 February 2016*; Sucht Schweiz: Lausanne, Switzerland, 2016.
104. Jeanrenaud, C.; Gay, M.; Kohler, D.; Besson, J.; Simon, O. *Le Coût Social du jeu Excessif en Suisse*; Institut de Recherches Économiques de l'Université de Neuchâtel et Centre du jeu Excessif: Neuchatel, Switzerland, 2012.
105. Sucht Schweiz. *Stellungnahme von Sucht Schweiz zum neuen Geldspielgesetz (BGS) vom 18.8.2014*; Sucht Schweiz: Lausanne, Switzerland, 2014.
106. Chopra, S.; Meindl, P. *Supply Chain Management. Strategy, Planning & Operation*; Prentice Hall: New York, NY, USA, 2012.
107. Bojanova, I. *The Digital Revolution: What's on the Horizon?* IEEE: Piscataway, NJ, USA, 2014; pp. 8–12.
108. Schumpeter, J.A. The process of creative destruction. In *Capitalism, Socialism and Democracy*; Schumpeter, J.A., Ed.; Allen and Unwin: London, UK, 1950.
109. Simon, H.A. A behavioral model of rational choice. *Q. J. Econ.* **1955**, *69*, 99–118. [CrossRef]
110. Brunswik, E. *The Conceptual Framework of Psychology*; University of Chicago Press: Chicago, IL, USA, 1952.
111. Ragnedda, M.; Muschert, G.W. (Eds.) *The Digital Divide. The Internet and Social Inequality in International Perspective*; Routledge: London, UK, 2013.
112. Van Dijk, J.; Hacker, K. The digital divide as a complex and dynamic phenomenon. *Inf. Soc.* **2003**, *19*, 315–326. [CrossRef]
113. Wessels, B. *The Reproduction and Reconfiguration of Inequality: Differentiation and Class, Status and Power in the Dynamics of Digital Divides in The Digital Divide. The Internet and Social Inequality in International Perspective*; Ragnedda, M., Muschert, G.W., Eds.; Routledge: London, UK, 2013; pp. 17–29.
114. Seagriff, T.; Lord, S. Soft operational research techniques : Current and future uses. *YoungOR* **2009**, *17*, 40–53.
115. Mingers, J.; Rosenhead, J. Introduction to the special issue: Teaching soft OR, problem structuring methods, and multimethodology. *INFORMS Trans. Educ.* **2011**, *12*, 1–3. [CrossRef]
116. Gregory, R.; Failing, L.; Harstone, M.; Long, G.; McDaniels, T.; Ohlson, D. *Structured Decision Making. A Practical Guide to Environmental Management Choices*; Wiley: Chicester, UK, 2012.
117. Wang, W.; Liu, S.W.; Mingers, J. A systemic method for organisational stakeholder identification and analysis using Soft Systems Methodology (SSM). *Eur. J. Oper. Res.* **2015**, *264*, 562–574. [CrossRef]