Towards Cognitive Tools: Systems Engineering Aspects for Public Safety and Security

Wolfgang Koch
Fraunhofer FKIE, Wachtberg, Germany

Living safely and securely is a basic human desire with many facets. Its satisfaction has psychological and societal, but also technical, legal, and economic implications. Moreover, rapid progress in networking sensors producing an ever increasing diversity of information has profoundly transformed the notion of public security. This technological revolution is driven by algorithms for extracting high-value information from sensor data streams – an enabling technology rooting in the Aerospace and Electronic Systems community. Besides discussing general design principles of security assistance systems, it is a serious concern to pinpoint also societally relevant challenges that are pressing and to be solved in an interdisciplinary approach.

SAFETY AND SECURITY—DESIRABLE GOODS AT ALL?

Perhaps it is not as obvious as we may be used to think that safety and security are desirable goods at all.

The influential philosopher Friedrich Nietzsche (1844–1900) at least, whom not so few people call the first of truly post-modern men [1], is by no means recommending us to satisfy our desire for safety and security: "For believe me: the secret for harvesting from existence the greatest fruitfulness and the greatest enjoyment is – *to live dangerously*. Build your cities on the slopes of Vesuvius! Send your ships into uncharted seas! Live at war with your peers and yourselves!"[2].

In a "dangerous" world, however, safety and security have become fundamental requirements, first of all, for mental liberality and cultural achievements. Ludwig van Beethoven (1770–1827), whose Chorus in his Ninth Symphony has become Europe's anthem, quite openly confesses: "It must be the aspiration and the aim of each true artist to acquire a position, where he can devote himself totally to the composition of larger works and is not prevented from this by a lack of safety and security" [3]. It is perhaps worthwhile to note that German as other European languages does not distinguish between "safety" and "security," but covers both notions with a single term: *Sicherheit*.

Moreover, safety and security are basic for calculable economic and societal processes, providing services of public interest, or achieving proper social balancing. In addition, modern industrialized societies fundamentally depend on inherently risky technologies. Corresponding safety and security technologies are thus enabling stability and prosperity.

Not unexpectedly, the fundamental human desire for safety and security, taken as an individual and societal phenomenon, has been an object of philosophical, psychological, and historical speculation for a long time. "But let our maxim be: for being safe and secure, sacrifice to the evil demons!" recommends the philosopher Arthur Schopenhauer (1788–1860). "The clearest example of this rule is the insurance premium. . . . It is a sacrifice publicly offered up" [4]. Akin to Nietzsche, Sigmund Freud (1856–1939), the founder of psychoanalysis, seems to see the desire for safety and security rather skeptically: "Civilized man has exchanged some part of his chances of happiness for a measure of safety and security [5]," while the Austrian historian and novelist Stefan Zweig (1881–1942) also sees a link to insurance: "The century of safety and security became the golden age of insurance industry. . . . Only who expected the future unworried, could enjoy the present time with happy sentiments" [6].

APPROACH AND PHILOSOPHICAL PRELIMINARIES

Since safety and security are basic human desires [7], their satisfaction is expected to be a major political, societal, legal, and psychological factor of governmental and private agency that is creating a corresponding safety and security industry. How can safety and security be improved by morally and legally conformable, societally acceptable, as well as economically affordable "products" or "services" to be offered on appropriate markets? Needless to say, the "Edward Snowden effect" not only in Europe has made a wide public aware of these issues.

To provide possible contributions for answering these difficult questions from a systems engineering point of view, this article basically follows three lines of thought:

1. In a sociopolitical perspective, we consider the desire for safety and security as a fundamental function of responsibility of government introducing the problem of reconciling the values of greater safety and security with the values of

Author's current address: W. Koch, Fraunhofer FKIE, Fraunhoferstrasse 20, Wachtberg, D53343, Germany, E-mail: Wolfgang.Koch@fkie.fraunhofer.de.
SYSAES-2013-0213r was received December 19, 2013, revised March 24, 2014, and ready for publication April 21, 2014.
DOI. No. 10.1109/MAES.2014.130213.
Review handled by P. Willett.
0885/8985/14/ $26.00 © 2014 IEEE

the liberality, freedom, personal dignity, or privacy that an individual foregoes.

2. In a systems engineering and architectural perspective, we discuss principles that allow the design of effective safety and security systems that are scalable and adaptable, and may facilitate the assessment of the value of the additional safety and security against the liberty, freedom, and privacy lost.
3. Guided by the spirit of concept development and experimentation [8], we consider a modular, prototypical realization as a "concrete example" that is addressing the problem of hazardous material localization in public infrastructures along with the concepts and principles previously discussed.

Since any systems engineering approach to public safety and security is at least implicitly embedded in a philosophical framework, the views underlying our considerations should be made explicit at least to a certain degree. We hope these views have a potential of being widely acceptable.

Besides being capable of "insight," human beings, and partly even other living creatures, are often said to be characterized by their ability of using tools for interacting with their environment and of communicating with other creatures or reflecting on themselves that may provide additional "insight." This very general observation seems to be visible in the polarity of Western civilization with its technology-driven and language-encoded strands of thought. The "tools" for improving safety and security seem to be the emerging sociotechnical infrastructures that massively gather data and transform them into information, the basis for decision making and governmental as well as private agency. Quite obviously, such technological systems have normative impacts and are intimately related to legal systems seen as a language-encoded "repository of knowledge, a formal accumulation of practical judgments. The law embodies the core insights about the way the world works and how we evaluate it" [9]. In other words, the issues of safety and security enforce a joint effort of the two polar strands of Western civilization.

Of crucial importance is the relation between the emerging safety and security technology and the notion of an individual human subject born with free will, capable of and accountable for deliberate intentional action, and entitled to "inalienable fundamental rights to which a person is inherently entitled simply because she or he is a human being" [10]. This very hallmark of Western democracy and the basic assumption of Western legal systems is the guiding principle also in our approach, where we consider liberality, freedom, personal dignity, privacy, etc., as "inalienable fundamental rights."

The notion of inalienable natural law and human rights as a consequence of it are fundamental to Western civilization [11]. When visiting the German Parliament in 2011, Pope Benedict XVI briefly sketched the legal heritage of the Western world: "In the first half of the second century B.C., the social natural law developed by the Stoic philosophers came into contact with leading teachers of Roman Law. Through this encounter, the juridical culture of the West was born, which was and is of key significance for the juridical culture of mankind. This pre-Christian marriage between law and philosophy opened up the path that led via the Christian Middle Ages and the juridical developments of the Age of Enlightenment all the way to the Declaration of Human Rights and to our German Basic Law of 1949, with which our nation committed itself to 'inviolable and inalienable human rights as the foundation of every human community, and of peace and justice in the world.'" [12]

Rooted in ancient Roman and medieval juridical thinking, but from a different philosophical perspective, political thinkers such as Thomas Hobbes (1588–1679), Samuel von Pufendorf (1632–1694), and John Locke (1632–1704) have in modern times made the notion of "inalienable rights" a key element in the United States Declaration of Independence and the Constitution of the United States as well. Especially von Pufendorf's political concepts have become part of the cultural background of the American Revolution. In view of these considerations, medieval and modern European and U.S.-American legal traditions at least in certain, but essential, points coincide.

INSURANCE, LAW, AND INFORMATION FUSION

Some historical reflections and a look at the parallels between insurance industry and emerging safety and security technologies provide a starting point and initial insight.

Insurance companies improve safety and security for individuals or legal entities by providing financial compensation of contingent, uncertain losses. This is made possible by collecting relatively small monetary contributions from a large number of insurees. Consequently, the methodological basis of this business model is mathematical statistics for calculating appropriate premiums, while its modern enabling technology

is provided by information engineering due to its nature as a mass business. Already in the 1950s, insurance industry began to introduce computers [13], invented in the 1940s by Konrad Zuse (1910–1995) [14] and others in the United States and the United Kingdom. Needless to say, insurance industry is of high economic importance for modern societies.

Statistics and informatics, however, are also the backbones of the emerging and rapidly evolving safety and security technologies for reducing risks caused by contingent, uncertain threats. In contrast to insured events, where *post-loss compensation* is contracted, *loss prevention* is in the focus here. By analyzing uncertain, incomplete, imperfect, and massively collected sensor and context data, safety and security threats are to be recognized *before* injuries and damages have occurred or at least mitigated in their effects. Along with technological progress, a specialized industry is marketing safety and security products or services with an ever increasing economic impact. A recent study of the German Federal Ministry of Economics and Technology anticipates for the German safety and security market in 2015 a value of more than 30 billion Euros [15], already the sixth part of the total German premium income in 2012 [16]. Moreover, in analogy to insurance law, legal structures for supervising safety and security technologies are currently framed [17].

Perhaps rather surprisingly, the notion of "subjective probabilities" and their "fusion" by "uncertain reasoning" have been developed in medieval rabbinic jurisdiction, where even a first idea of the *Bayesian formalism* has been developed [18]. Analysis of evidence, methodical questioning, calculation of risks, and evaluation of uncertain data, reports, and particular circumstances—all these tasks to be solved wherever human beings form a society—in one way or other involve accumulation of individual probabilities. According to modern terminology, this reasoning is called "information fusion" and enables the design of assistance systems for computer-aided reasoning and decision making [19]. In analogy to mechanical tools facilitating human labor and enhancing human physical strengths, informational assistance systems serve as "cognitive tools" that enhance our mental capabilities to deal with uncertain data that may massively be streaming in by providing "situation pictures" of possibly dynamically evolving phenomena.

First philosophical reflections along these lines have already been made in medieval scholasticism, culminating in the work of the logician, philosopher, theologian, and poet Raymundus Lullus (c. 1232–1315), one of the early ancestors of modern computer science [20]. His *Ars generalis ultima*, published in 1305, is considered as the first idea of a general purpose computer. It influenced the thinking of the Jesuit Athanasius Kircher [21] (1602–1680) and Gottfried Wilhelm Leibniz (1646–1716), who contributed to the intellectual foundations of modern computer science. Interestingly enough, Leibniz is also among the founders of modern actuarial science [22].

A pioneer of modern sensor data and information fusion is Thorvald Nicolai Thiele (1838–1910), an outstanding Danish astronomer, actuarian, and mathematician, who is perhaps not adequately remembered. In his famous textbook *Statistical Methods* (1932), the mathematician Ronald A. Fisher (1890–1962) provides a list of the main contributors to statistics containing only six names: Bayes, Laplace, Gauß, K. Pearson, Student (Gosset), and Thiele [23]. While Fisher's *information matrix* is a fundamental notion in information fusion as well, Thiele's extensive paper "The General Theory of Observations: Calculus of Probability and the Method of Least Squares" (1889) contains many ideas shaping modern sensor data and information fusion, e.g., a complete version of the *Kalman filter and smoother*, a clear and distinct expression of the idea of *likelihood,* and an instance of what is now called the *Expectation-Maximization* algorithm that is useful, e.g., for solving data association problems in fusion applications [24]. Among his many other activities, Thiele was founder and mathematical director of the *Hafnia* insurance company, Copenhagen, which existed until 1992. Also a large portion of Harald Cramér's (1893–1985) work, whose famous *Cramér-Rao-Lower-Bound* using Fisher's information matrix is a key tool in current fusion research, concerned the field of mathematical risk theory, actuarial science, and insurance mathematics [25]. Obviously, insurance and information fusion are the two major ways to do business with statistics, where fusion still has an enormous potential of development, scientifically and economically.

THE NOTION OF PUBLIC SAFETY AND SECURITY

Before any further considerations on safety and security technology evolving from these roots, a look at the concise definition of public safety and security in juridical handbooks might provide some clarity: "The notion of public safety and security covers the integrity of the . . . fundamental institutions . . . of the state as well as the integrity of health, honor, freedom, property, and related objects of legal protection of its citizens. Defense against endangerment of public safety and security is the task of public safety and security authorities." [26]

Considering a familiar example, "integrity of health and property of citizens" is certainly affected by automotive traffic, for in the European Union alone more than 26,000 traffic deaths have been reported in 2013 [27], while globally 1.2 million persons have lost their lives due to traffic accidents. According to the previous definition, public safety and security authorities should actually forbid private transport in view of these facts. Nevertheless, individual mobility is a desirable good of high public and economic interest.

According to these considerations, there is a need for properly pursuing the apparently competing goods of public safety and security and individual mobility in a way that is harmonized to correspond to the common good. For reaching this goal, a triple strategy, based on the three pillars of technology, law, and insurance, has been developed over decades:

1. Primarily, injuries and damages are prevented or mitigated in their effects by a hierarchy of technological measures, such as vehicle inspections, robust vehicle bodies, passenger belts, airbags, or by the most recent advance, *multiple sensor driver assistance systems*.

2. This engineering work is accompanied by developing appropriate legal structures comprising road traffic law, including mandatory seat belt wearing or banning of mobile phone use by drivers, etc. In addition, proper police authorities enforce such regulations.
3. Since the financial loss by traffic accidents may easily exceed individual fortunes, the monetary aspects of affecting "integrity of health and property of citizens" is covered by a specialized traffic insurance industry, which has a large economic impact itself.

In this more general systemic approach, technology is put in context with complementary, nontechnological elements. Obviously, this approach is practically proven and effective. From its maximum of more than 20,000 traffic deaths on German roads in the early 1970s, this number dropped down to 3,340 in 2013, while the number of registered vehicles has grown from 14 million in 1970 to 52 million [28]. As these numbers show, individual mobility, taken as a private individual good, can rather successfully be pursued in a means that corresponds to the common good, i.e., assisted by technology, law, and insurance.

A quite analogous triple strategy based on technological, legal, and actuarial measures, has been developed for other risky technologies as well, such as air traffic control, off-shore or chemical industry, and even nuclear industry, while in the latter case this strategy certainly reaches its limitations because of the sheer size of potential harm.

The discussion of the individual mobility example also illustrates that individuals often appear to take a comparatively simple utilitarian view placing a subjective value upon the benefit and cost-loss considerations, which can lead to a substantially different stance when compared to government surveillance. Internet platforms such as Google and Facebook or smartphone tracking provides examples where even technically well-informed individuals appear to be perfectly content to surrender substantial privacy in exchange for a "no-cost service" that provides benefits they value. This rather puzzling psychological phenomenon should be analyzed in greater detail.

In the 9/11 attacks, 2,976 citizens died. The attacks in Madrid on March 11, 2004, and in London, July 7, 2005, cost 191 and 56 lives of citizens, respectively. According to the previous definition, defense against endangerments of public security by such attacks is the task of public authorities. Even more than mobility as in the previous example, liberality, privacy, informational self-determination, civil rights, preservation of respectful treatment, and personal dignity are (highly!) desirable goods, even natural rights.

Why shouldn't we react in a similarly unexcited manner to resolve this dilemma? Why shouldn't we be following the well-proven triple strategy with its three pillars, i.e., a combination of preventive or mitigating measures of risk management (technologically and legally based), which is complemented by financial residual risk compensation, i.e., by insurance? As the individual mobility example shows, this approach may increase the value that both society and an individual can derive from a risky activity that involves a large number of organizations and individuals whilst simultaneously bounding cost and risk. The "point of balance," however, is not necessarily static over time: the perceived level of terrorist risk/activity, for example, may cause it to move.

Figure 1.
A public infrastructure with security personnel (© by IK's World Trip under CC-by-2.0).

One might argue that terrorist events are essentially deliberate acts in contrast to merely "accidental" traffic accidents. Since this systemic approach is undoubtedly effective also in case of other deliberate acts, such as speeding or drunk driving, and even in crime prevention, e.g., housebreaking, we expect *The Three Pillars of Public Safety and Security* to be an effective strategy even in case of terrorist crimes and other safety and security applications.

SECURITY ASSISTANCE: GENERAL PRINCIPLES

In the domain of public security, multiple sensor security assistance systems are expected to play a role comparable to existing car driver assistance systems, i.e., contributing to the first, the technological pillar of a triple strategy.

Considering a concrete example, let us focus on detecting and preventing harm caused by hazardous materials in public infrastructures, e.g., by explosives or radioactive substances. The related events are contingent, uncertain, and rare, when happening, however, resulting in serious injuries of the "integrity of health, honor, and property" of a large number of citizens. Such events may even threaten "fundamental institutions of the state." Typically, security contractors, a new and highly specialized profession, are responsible for countering such threats, thereby acting on behalf of public authorities. Let us consider a departure hall such as shown in Figure 1. Obviously, the security forces need support to fulfill their duty in such scenarios. Desirable are informational assistance systems that pinpoint potential threats, such shown in Figure 2, where a person is labeled as a potential threat, e.g., as carrying homemade explosives similar to the London attacks in 2005.

More generally speaking, automated recognition of security relevant features in public scenarios is a key functionality of

security assistance systems. It has to fulfill several overall requirements that need to cover a broader range of issues than conventional engineering standards such as:

1. Unburden from routine and mass tasks to gain room for human expertise and insight.
2. Focus human attention to potential threats, hazards, or anomalies as a key functionality.
3. Preserve dignity and informational self-determination by collecting threat-relevant data only.
4. Operate permanently without interfering with or annoying everyday public life.
5. Exploit sensors enabling apprehension beyond natural senses for threat recognition.
6. Indicate properly the possibly limited quality of inferences from inaccurate and incomplete data.
7. Profit from technology trends (sensors, communications, databases, processors).
8. Fuse multiple sensor data and context information to the extent that is allowed.
9. Guarantee constant and standardized quality levels for any module used in public security applications.
10. Design scalable architectures to be adapted to large diverse networks of sensors and data bases.
11. Enable the utility-cost-privacy balance of each module be understood and its impact assessed.
12. Provide intuitive interfaces to human decision makers, adapted to their specific needs.

Essentially, multiple sensor security assistance systems that are designed along these lines combine the strengths of automated and human data exploitation by:

Figure 2.
Potential terrorist such as in the London tube attack 2005 (labeled red, © by drp under CC BY-NC-ND 2.0)

- real-time analysis of large streams of multiple sensor data and context databases,
- while enabling high decision competence in individual situations by expert knowledge.

Security assistance systems may thus be considered as "cognitive tool." They provide providing awareness of threats that enhance our natural mental capabilities of dealing with large amounts of security relevant sensor and context data in an analogous way as mechanical tools enhance our physical capabilities. Their development should be accompanied by considering technology-driven legal aspects and covering residual risks by properly designed insurance products. Moreover, by identifying fundamental technological limitations of preventive measures and quantitative performance analysis of modular and standardized security assistance systems, the residual risks and therefore even corresponding insurance premiums may become calculable, which would otherwise hardly be possible.

ON HAZARDOUS MATERIAL LOCALIZATION

Returning to the London terrorist example shown in Figure 2—what makes the labeled person suspicious? Is there a chance to sense the threat connected to him, to single him out in a crowd of nonsuspects?

There is certainly little chance of threat recognition by video analytics alone. Probably, the suspect has not shown any type of individual behavior not being shared with many other persons. What makes him different, however, is the very fact of carrying a significant amount of explosives, homemade explosives that to a certain extent "smell," not to human noses, but to dogs' noses, for example, and olfactory chemical sensors. While in the biosphere "noses" are among the oldest of senses, their technical equivalents are still subject to a rapid technological development. Only recently, they have reached a level of maturity that makes their use an option for a growing number of hazardous materials. See Figure 3 for experimental examples. Chemical sensors detecting even traces of popular explosives in open systems, however, are still in a prototypical state and not yet available as stable products. In 3–5 years, however, this situation is expected to have changed completely. System design considerations taking these new sensing options into account should thus start right now.

The design principle of a potentially inexpensive class of chemical sensors with enormous market potential, so-called quartz microbalances, is quite intuitive [29]. Basically, they consist of an oscillating quartz crystal coated with a macromolecular receptor substance that selectively absorbs particular substances to be detected. Even a few absorbed molecules cause an increase of mass attached to the oscillating crystal, which is sufficient for inducing a tiny, but measurable frequency shift. Quartz microbalances can thus be highly *sensitive*. By considering crystal arrays with different coatings, a significant *selectivity* can be reached as well. With this principle, even sensors for detecting biological agents are within reach, where enzymatic coatings are reversibly reacting with particular proteins, viruses, or even bacteria.

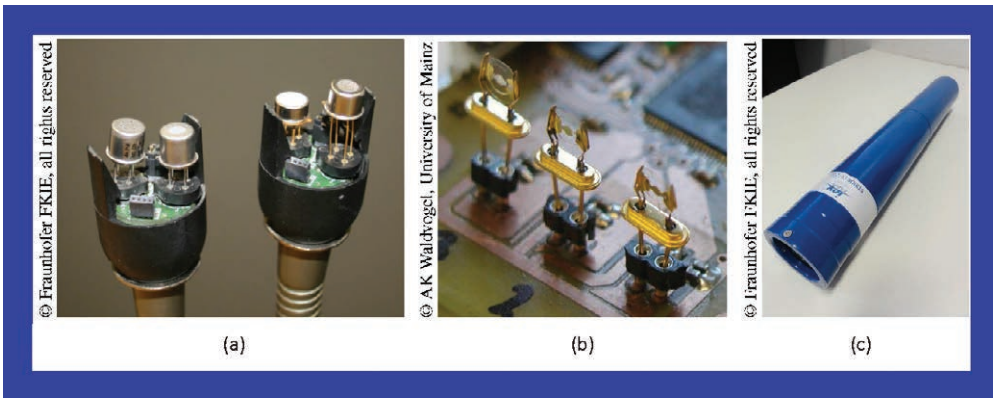

Figure 3.
Detection of gases and radiation in open systems. (a) The semiconductor sensors (pictured at left) absorb molecules on a metal-oxide (MOx) coating. (b) The sensor uses coated quartz micro balances (QMB). (c) The scintillation counter counts gamma quanta from radioactive sources, potentially indicating "dirty" bombs.

Apart from all physiological or chemical differences in olfactory senses or sensors, a fundamental commonality of all attribute sensors of this type can be identified, i.e., their inherently *limited space-time resolution capability*. While attribute sensors are able to detect the presence of a particular substance or classes of substances among a variety of alternatives, they on principle are unable to provide useful information on their location. They neither enable any association of the sensed signature to a particular carrier, nor any tracking of its position over time if the substance is carried on. The same observation is valid for wider classes of attribute sensors such as radioactive sensors.

Obviously, the situation in Figure 1 is by far too complex to provide any reasonable technological aid, at least in the foreseeable future. To enter public places like this, however, persons often have to pass well-defined access areas, skywalks, or escalators such as shown in Figure 2, where the complexity of the surveillance task is much reduced. Tunnel-type areas, where persons enter, stroll along, and finally leave, enable a space-time approach for tracking-aided hazardous material localization. We may span a temporal basis to collect data over time and exploit space by spatially distributing attribute sensors along the walls. The temporal dimension is used by video cameras or laser scanners for tracking each person. By fusing measurements of each chemical sensor over time with the tracking data of all potential carriers of hazardous materials, we get a chance to overcome the limited space-time resolution capability of attribute sensors. More abstractly speaking, we wish to learn from uncertain data, which time-varying object can be classified as suspect or nonsuspect [30].

HAMLET: AN EXPERIMENTAL EXAMPLE

To illustrate tracking-aided multiple object, multiple sensor classification for informational security assistance systems, we discuss an experimental set-up called HAMLeT (Hazardous Material Localization and Person Tracking) [31]. A prototypical demonstration system like HAMLeT may serve as an example of how taking sensors plus associated system components, including a walkway, for example, creates a safety and security assistance module that conforms to the design principles identified earlier.

Firstly, relevant object properties are to be identified and modeled, e.g., by random vectors their kinematical characteristics, by random matrices their shape, by discrete random variables the class they belong to, such as "nonsuspect" or "suspect" along with the potential type of threat. The collection of such quantities referring to a particular object at a given time defines the *object state* at this very time. For dealing with uncertain knowledge on objects states, appropriate functions of them are considered, mainly probability density functions, but also proper generalizations of this notion, such as probability hypothesis densities [32] or intensity functions [33]. Spiky functions of this type indicate precise information on the states, while multimodal or "broad" functions represent ambiguous or imprecise knowledge. Data-driven "learning" of object properties is essentially an iterative updating of such functions. For doing so, the relationships between sensor data and objects states are to be modeled, as well as possible errors and uncertainties attached to them. Formally, this is described by functions of the object states, measurements, and sensor parameters, called likelihood functions, which reflect the physical characteristics of the sensor data to be processed in the updating procedure. For initiating or terminating this learning iteration, statistical decision making is required.

A key problem in hazardous material localization is uncertainty on which position and attribute measurements are to be associated to which individual object. Among several solutions, Expectation-Maximization methods prove to be of particular value providing a unified and actually very beautiful framework. According to this methodology, each measurement is associated to all persons of interest with appropriate weighting factors. Ideally, measurements actually originating from a particular person have weight one; all other measurements zero weight. Expectation-Maximization serves as a method to estimate the weighting factors from the measured data iteratively.

Figure 4.
Views of the HAMLeT system. In the upper row, (a) and (b) show the system plan and a photo of the system assembly. The middle row is dedicated to the sensors that are integrated with the system. In particular, (e) sketches the air stream which blows molecules towards the chemical sensors hooked into the tubes. The lower row shows people walking through the system corridor. (© by Fraunhofer FKIE).

In other words, joint estimation of objects states and data association weights is considered [34].

Chemical sensors are influenced by numerous external factors not easily modeled. Of strong impact on the data quality and time delays involved are the distances between potential carriers, their velocities, temperature, humidity and other environmental parameters such as the degree of turbulence, etc. For designing overall system parameters and quantitative performance predictions, experimental investigations are therefore inevitable. Figure 4 shows the experimental system HAMLeT, where in a corridor persons are entering and leaving. Three laser range scanners, four chemical sensors, and three miniaturized gamma spectrometers are collecting data. For a detailed description of the methodology used and experimental results obtained see [35]. Figure 5 provides an impression of the system's operation.

Of growing concern for public safety and security are so-called dirty bombs, a threat that came to global awareness by the 2014 Nuclear Security Summit [36]. In such devices, radioactive materials, readily available for medical or commercial use, are combined with conventional explosives to be used for dispersion in public infrastructures [37]. Their damage potential is high in view of contamination, health damage, and the psychological and societal impact in general. The HAMLeT approach might be use-

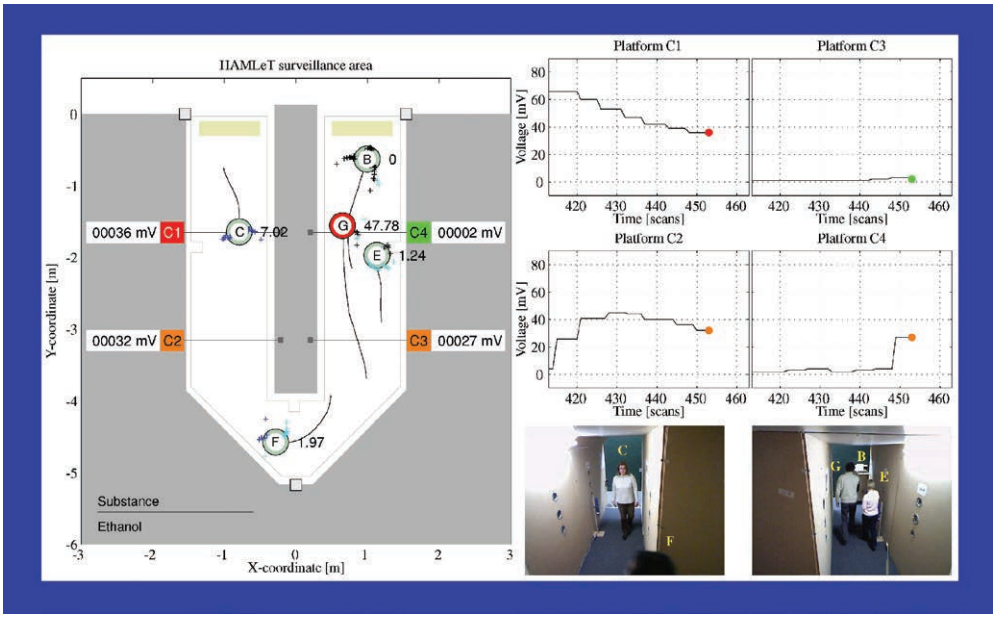

Figure 5.
Persons walking arbitrarily, one of them with chemicals (snapshot 2). The left plot shows the surveillance corridor, the sensor placement, the signals of the chemical sensor platforms, and the person tracks with their carrier potential. The four plots on the right visualize the development of the voltage signals over time. The video snapshots show the current person constellation. (© by Fraunhofer FKIE).

ful in this context as well (see Figure 3c) [38]. There is also an ever increasing need for localizing radioactive materials in logistic chains or when deconstructing nuclear plants, where millions of tons of radioactively contaminated concrete and other debris have to be transported safely. A mobile version of the HAMLeT tunnel may be helpful even in case of catastrophes where incidents at chemical or nuclear plants are involved.

To sum up: by quantitatively analyzing the performance characteristics of an experimental system such as HAMLeT, it is in particular possible to assess the utility-cost-privacy balance, to define information needs and information outputs, to define the usual engineering interfaces and standards, and to define contractual interfaces. It also provides a means to measure or assess the marginal impact upon utility/cost/privacy of providing access to additional background, context, or historical information, or of providing additional output information. Systems like HAMLeT thus provide a means to test emerging architectures for security assistance systems.

LAW COMPLIANCE BY DESIGN?

Besides its use for system design considerations and quantitative performance prediction and evaluation, HAMLeT may also serve as a concrete example to raise societally relevant aspects of security assistance systems and to discuss "The Three Pillars of Public Safety and Security" on a more systemic level, i.e., the interrelations of their technological, legal, and actuarial elements.

First of all and on principle, systems like HAMLeT do not collect any biometrically relevant parameters and therefore preserve the anonymity of the observed individuals by their very technical design. Only positional data in the corridor are collected for tracking-aided association of chemical or radioactive signatures to a distinct carrier. At least in the foreseeable future, chemical sensors are not capable to sense olfactory signatures characteristic of individuals. HAMLeT is thus "blind for normal people," i.e., for the vast majority of persons not carrying hazardous materials. Even though false alarms and manual inspection of a few remaining persons cannot be avoided, such systems may enable "normal" public life without extensive security checks at an ever increasing number of occasions that consider everybody as a suspect. Moreover, multiple sensor security assistance systems may seamlessly be embedded in public infrastructures making them essentially invisible. Since the airflow in public infrastructures, for example, can often be modeled fairly well, chemical sensors could be part of the air conditioning system of a public building.

There are, however, numerous procedurally and societally relevant questions in the context of security assistance systems that still have to be answered:

1. *How to act when a threat is recognized?* This task is by no means easy in cases as shown in Figure 2, where any open police action is likely to trigger an explosion. This question raises the problem of automated or semi-automated actions involving possibly even lethal effects and serious legal problems [39].
2. *Which domains of life will be safe and secure?* Security assistance systems are opening a security umbrella wherever the necessary investments are made. Will countering security threats remain the task of public authorities? Will living safely and securely remain an affordable public good?

3. *How to certify security assistance systems?* As demonstrated by systems such as HAMLeT, certain aspects of law-compliance are "in-built" technical features. Is this to be formalized to cover more features for wider classes of assistance systems? Are there procedures for certification and verification?
4. *How to standardize security assistance systems?* Calculation of residual risks and design of more intelligent legal measures for event prevention and actuarial residual risk compensation seem to become possible by standardized quality measures and quantitative performance evaluation for such systems.
5. *What is the legal role of security contractors?* New treat recognition technologies are likely to change traditional roles, since specialized technical understanding and training are required. In which way do security contractors participate in public authority? Who is controlling and limiting them in their actions?
6. *How to check system integrity?* Security assistance systems cannot exist in hermetic environments and thus need a sort of immune system, since they are predictably targets in cyber-attacks or subject to varying and unpredictable conditions or malfunctions and must be capable to reconfigure themselves.

At any rate, such questions among others have a significant societal and political impact, they involve even psycho-emotional and cultural apprehension, interpretation, and reaction patterns, and should therefore be discussed publicly. Interestingly enough, these topics are already present in early science fiction novels [40] and recent movies.

It seems worth mentioning that the technical term *information fusion* was coined in George Orwell's very year 1984 in the domain of *Aerospace and Electronic Systems*, when the first attempt to scientifically systematize this emerging technology was made [41]. Orwell's warning "Don't let it happen!" may call us to think of potential threats to human society that may be related to this technology having reached a fairly mature level in the meantime. Attempts to identify and to counter undesirable developments will have to comprise interdisciplinary efforts by engineers, computer scientists, philosophers, sociologists, and, last but not least, by lawyers and actuaries, "the engineers of ethics" that frame robust legal systems from more theoretical ethical insights and calculate residual risks based on statistical considerations.

TRENDS IN HUMAN ASSISTANCE SYSTEMS

Selected overall characteristics of multiple sensor assistance systems and their potential benefits have been described. They essentially provide "cognitive tools" enhancing our mental capabilities to deal with large data streams from heterogeneous sources beyond the sensing or memory capabilities "naturally" accessible to human beings. Kenneth R. Boff, a well-respected and influential scientist in human factors engineering [42], puts the notion of informational assistance systems for enhancing human capabilities in the much wider perspective of human enhancement engineering and its further development. Already in 2006, he identified four generations of human factors and ergonomics [43]:

1. *Physical fit:* Adapt equipment, workplace, and tasks to human capabilities and limits, which is realized on a rather mature level.
2. *Cognitive fit:* Harmoniously integrate humans, technology, and work to enable effective systems (on a growing level of technical realization).
3. *Neural fit:* Amplify human physical and cognitive capabilities to perform work through symbiotic coupling with technology (emerging technology level).
4. *Biological fit:* Biologically modify physical and/or cognitive capabilities to maximize human effectiveness (embryonic level).

According to Boff's taxonomy, research and development towards multiple sensor security assistance systems as previously discussed aim at the second generation of human factors engineering. It is worthwhile, however, to muse about Boff's thoughts on the third and fourth level and to compare his anticipations in the year 2006 with current trends.

1. "Human cognitive and physical capabilities may be enhanced well outside the range of normal biological variation, thereby altering traditional boundary constraints on the adaptability of humans in complex system design." Boff's statement in a scientific journal article 8 years ago is publicly discussed today in quality news magazines [43], [44] and seems to become a technological option within reach.
2. "The DARPA Augmented Cognition Program is aimed at maximizing human cognitive abilities through the unification of humans and computational systems." The reader of this statement might associate tele-operated and partially automated unmanned aerial and robotic vehicles or threat evaluation and weapon assignment systems which are established in military operations.
3. "Never mind restoring impaired cognitive functions, the race is on to bring the next Viagra, only this drug will be for the brain and will be used to boost cognitive normals into a hyper-range of capabilities." Besides memories of Aldous Huxley's "Brave New World," where drugs psychologically stabilize a dystopic society [45], today's university and professional life is actually confronted with the phenomenon of "mental doping" [46].
4. "Predictably enough, the market for cognitive enhancement is extremely high. The same market may lead to a new frontier for elective medicine: Cosmetic Neurology." In view of the enormously growing market of cosmetic surgery, Boff's vision of cosmetic neurology for "alpha plus intellectuals" according to Huxley taxonomy or, less ambitiously, "the rich and beautiful" seems to be not unrealistic an anticipation.

Apparently, human enhancement engineering seems to be detaching themselves from the purposes that have originally stimulated the development of human assistance systems, such as defense, safety, and security, or, in a more recent step, vehicle driver assistance. It is going to penetrate many aspects of human life, including even "cosmetic" desires, as Boff anticipates. Questions may arise, whether it is really desirable to follow the technological path Boff predicts, under which preconditions pursuing its destination might be ethical at all, or which alternative destinations should be chosen.

At any rate, technological progress is by no means a "natural" process obeying deterministic laws beyond human control. Quite in the contrary, future technology is shaped by human beings acting freely at present and being inescapably responsible of their actions, wherever and whenever they act, i.e., as decision makers, sponsors, researchers, system engineers, or end users defining requirements. The triple strategy with its systemic approach of technological, legal, and actuarial measures may be useful in this context and counter even risks caused by inconsiderate technology developments. Much will depend on justly chosen aims and on just attitudes to reach them, i.e., on a moral habit that is aware of ethical and societal implications to be "encoded" in appropriately designed technical and legal design principles and systematic, "actuarial" quantification of residual risks and their coverage. Not unexpectedly, "meta-technological" thoughts, personal convictions, and beliefs beyond science and technology are quite naturally involved in such debates.

REMARKS ON TECHNO-ROMANTICISM

Boff's visions, which are based on sober analysis and describe apparently possible options, call for a deeper understanding of philosophical ideas that consciously or subconsciously may drive technological progress towards a direction we might not actually want. Considering the attitude towards nature and human beings that seems to be visible in Boff's dystopian anticipations, the author is reminded of Friedrich Nietzsche who has crossed our path in the very beginning: "*Hubris* is our whole attitude to nature nowadays, our violation of nature with the help of machinery, and all the unscrupulous ingenuity of our scientists and engineers," he writes in his influential *On the Genealogy of Morals* and continues: "*Hubris* is our attitude to God, that is, to some alleged teleological and ethical spider behind the meshes of the great trap of the causal web. *Hubris* is our attitude to ourselves — for we experiment with ourselves in a way that we would not allow with any animal, and with pleasure and curiosity open our soul in our living body: what matters now to us the *salvation* of the soul?" [47].

Nietzschean thinking seems to have a strong hidden presence in modern pop culture shaping a sort of intercultural subconscious using technological metaphors and fictional anticipations. In his science fiction movie *Blade Runner* [48], for example, a cult movie retelling the myth of Zeus and his child Athena conceived of and birthed from his own mind, the prominent English movie director Sir Ridley Scott (b.1937) stresses not only the industrial dimensions of "human enhancement engineering," but provides an explicit reference to Nietzsche when explaining the famous last speech of Roy Blatty, a "replicant": "Philosophically, he is the authentic 'being' and Nietzsche's *Mad Man*" [49]. Blatty's functional definition "combat, colonization defense program" is apparently related in a sense to the public security topic. But also the phenomenon of cinematic "superheroes" and their technological aids show a strange connotation to public safety and security and provide a direct link to Nietzsche's *Overhuman* that is being discussed in the contemporary philosophic literature [50].

These societally subconscious philosophical and moral attitudes in modern pop culture seem to have their counterparts in engineering communities. Looking at human deficiencies and the nameless suffering they are inflicting and in search of some "superhuman authority," the mathematician and physicist Sir Roger Penrose (b.1931) asks himself: "Can robots save our troubled world?" [51]. If we are to believe in the claims of prominent computer scientists, Penrose considers skeptically, the potential of computers and computer-guided robots will ultimately exceed our own intelligence: "We could then turn to these superior intelligences, they claim, for advice and authority in all matters of concern – and the humanity induced troubles of the world could at last be resolved."

In the vision of *Overhumans* ruling a society of "slaves," human enhancement engineering seems to be a means to reach "transhuman" powers. "We can conclude that Nietzsche and the transhumanists share many aspects in their general anthropologies and their values," summarizes a contemporary philosopher. "Their concept bears many significant similarities to that of Nietzsche's *Overhuman*" [52]. A leading university text book on artificial intelligence speaks of "transhumanism" as an "active social movement that looks forward to this future in which humans are merged with – or replaced by – robotic and biotech inventions" and comments dryly: "Suffice it to say that such issues present a challenge to most moral theorists, who take the preservation of human life and the human species to be a good thing" [53]. Currently, even an ongoing process of inserting these ideas into a new and globally active political movement can be observed [54].

"What idea, if embraced, is the world's most dangerous idea?" asks Francis Fukuyama (b.1952), political scientist, in view of this development and answers: "Transhumanism, a strange liberation movement, whose crusaders aim at much higher than civil right campaigners, feminists, or gay-rights advocates. This movement wants nothing less than to liberate the human race from its biological constraints" [55]. "Francis Fukuyama thinks so," replies Nick Bostrom (b.1973), transhumanist philosopher and director of the *Future of Humanity Institute* at Oxford University, "but the only real danger it poses is to reactionary bioconservativism" [56]. Such visions seem to despise human nature altogether with all of its fundamental limitations and is opposed to an anthropology that accepts human nature which in its very polarity (material and spiritual) is a good not an evil needing "liberation."

Quite disturbingly, the very notion of the identity and agency of human subjects is at the same time challenged by re-

cent philosophical strands. "Obviously, the concept of 'human agency' is a prime example of an essentially contested concept, meaning that there is no consent about the content of the notion between different users of the term," summarizes a recent volume on the philosophy of law and technology [57]. In particular, poststructuralist orientations, often attributed to Michel Foucault (1926–1984), who was strongly influenced by Nietzschean thinking, seem to discard the notion of human agency altogether, declaring the "death of the subject," or deconstructing the subject as a product of textual interpellations according to Jacques Derrida (1930–2004).

A powerful technology fallen into the hands of techno-ideologists with strange visions of the future destiny of the "human race" can indeed become dangerous. At least Germans know only too well what can happen to even educated societies with significant cultural achievements, when "black romanticism," fond of technology and Nietzsche, grasps at power. Perhaps we can ban these evil spirits by calling them by their very names. In this sense, appropriate names for societally subconscious techno-romanticism seem to be narcissism, megalomania, and above all hubris that may seduce our society to "experiment with ourselves in a way that we would not allow with any animal" [47].

ON POSSIBLE CONCLUSIONS

Quite obviously, any beneficial use of "cognitive tools" that augment human capabilities beyond their "natural" range sensitively depends on a commonly agreed idea of what human beings actually are and what is right for them to do, in other words, on the very foundations of law. As recalled in the very beginning, the notion of an individual human subject born with free will, capable of and accountable for deliberate intentional action, and the idea of inalienable fundamental rights to which a subject is inherently entitled simply because she or he is a human being are the very hallmarks of Western democracy and the basic assumptions of Western legal systems.

Only if these foundations are really clear, commonly agreed upon, and societally conscious, their transformation in a legal system, the second pillar of the triple strategy for safety and security, is possible. The *Reflections on the Foundations of Law* [58] that Benedict XVI presented in the German parliament seem worth considering in this context: "To serve right and to fight against the dominion of wrong is and remains the fundamental task of the politician," he reminded in 2011 the German politicians framing German laws and characterized the present situation: "At a moment in history when man has acquired previously inconceivable power, this task takes on a particular urgency. Man can destroy the world. He can manipulate himself. He can, so to speak, make human beings and he can deny them their humanity. . . . There is also an ecology of man. Man too has a nature that he must respect and that he cannot manipulate at will" [59].

All those with care of the common good, one could conclude, have the obligation to use their authority not for their personal benefit but for the common good. The amassing of great quantities of data evidently has a benefit for the safety and security element of the common good, but there is a real danger of it being converted for private good. The misappropriation of the common resource of the data to private gain may thus lead to perversions of government such as tyranny or oligarchy. Embedded into appropriately framed and truly human legal structures, however, and along with actuarial residual risk assessment, properly designed law-compliant technologies such HAMLeT are indeed likely become key modules of comprehensive systems that satisfy the quite legitimate desires for individual and societal safety and security.

And in a safe and secure and truly human society we may harvest the fruits that are only ripening in protected habitats: mental liberality, cultural achievements, calculable economic and societal processes, social balancing, and stable industries, the sources of material prosperity. Therefore, it does not seem unrealistic to anticipate a significant need for security assistance systems and related "big business" finding its path between the Scylla and Charybdis of utopian [60] or dystopian visions [61].

We thus naturally conclude that a modular approach for safety and security assistance systems needs to be encouraged that explicitly includes legal and other metadata to assess the utility-cost-privacy impact for each system module and the overall system. Only then we will be able to exploit the rapidly increasing number of sensors, volume of information, and processing capabilities within a framework that recognized the essential need to respect the privacy, dignity, and other fundamental rights of the individual.

In view of these considerations, we may reread Schopenhauer's recommendation: "But let our maxim be: for being safe and secure, sacrifice to the evil demons! . . . The clearest example of this rule is the ~~insurance premium~~ [the triple strategy of public safety and security]. . . . It is a sacrifice publicly offered up. That means we should not avoid a certain effort of labor, time, money, or difficulties to shut the door to the possibility of calamities" [62]. ◆

ACKNOWLEDGMENTS

The author wishes to thank four anonymous reviewers for their valuable comments and insightful suggestions. To one of them in particular, he is very much indebted.

REFERENCES AND NOTES

[1] Lampert, L. *Nietzsche and Modern Times: A Study of Bacon, Descartes, and Nietzsche*. New Haven, CT: Yale University Press, 1995.

[2] Nietzsche, F. *The Gay Science* (Trans. Walter Kauffman). Aphorism 283. Cambridge: Cambridge University Press, 2001. German: *Die Fröhliche Wissenschaft*. In *Friedrich Nietzsche. Werke II*, Karl Schlechta, Ed. Frankfurt a. M.: 1969, p. 166.

[3] van Beethoven, L. *Billet to Freiherr Ignaz von Gleichenstein* (Translated by the author). 1808, cited in: Koch, P. *Der geistesgeschichtliche Hintergrund der Versicherungswirtschaft* [Intellectual Background of Insurance Industry]. In: *Beiträge zur Geschichte des deutschen Versicherungswesens*, Heinz Leo Müller-Lutz et al., Eds. Karlsruhe: 1982/1995, p. 161.

[4] Schopenhauer, A. *Parerga and Paralipomena* (Chapter V, A.50. Transl. E. F. J Payne). Oxford: Oxford University Press, 2003. German: *Parerga und Paralipomena*. In *Gesammelte Werke. Band V*, Arthur Hübscher, Ed. Bonn: 1946/1951, p. 503.

[5] Freud, S. *Civilization and Its Discontents*. Penguin, 1929/2011. German: *Das Unbehagen in der Kultur*. In *Gesammelte Werke. Band XIV*, Anna Freud et al., Eds. London: 1948, p. 474.

[6] Zweig, S. *The World of Yesterday* (Transl. Anthea Bell). University of Nebraska Press, 1942/2013. German: *Die Welt von Gestern. Erinnerungen eines Europäers*. Frankfurt a. M.: 1970, p. 15.

[7] Maslow, A. A theory of human motivation. In *Psychological Review*, Vol. 50(4), 1943, pp. 370–396, available online.

[8] Hayes, R. E. (Ed.). *Campaigns of Experimentation: Pathways to Innovation and Transformation*. Washington, DC: CCRP Publication Series, 2005. See also: Honekamp, W. *Experimentieren in komplexen Organisationen – Ein Update der Erfahrungen aus der praktischen Anwendung von Concept Development & Experimentation* [Experimentation in Complex Organizations – Practical Applications of Concept Development & Experimentation]. Remscheid: 2010.

[9] Hildebrandt, M., and Rouvroy, A. *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*. Abington, UK: Routledge, 2011, p. 3.

[10] Human rights. Wikipedia, http://en.wikipedia.org/wiki/Human_rights, last access March 25, 2014.

[11] Benedict XVI, Pope Emeritus. "Unlike other great religions, Christianity has never proposed a revealed law to the State and to society, that is to say a juridical order derived from revelation. Instead, it has pointed to nature and reason as the true sources of law – and to the harmony of objective and subjective reason, which naturally presupposes that both spheres are rooted in the creative reason of God. Christian theologians thereby aligned themselves with a philosophical and juridical movement that began to take shape in the second century B.C." The listening heart. Reflections on the foundations of law. Address to the German Parliament, Reichstag Building, Berlin, Sept. 22, 2011.

[12] Benedict XVI, Pope Emeritus. The listening heart. Reflections on the foundations of law. Address to the German Parliament, Reichstag Building, Berlin, Sept. 22, 2011.

[13] The first digital computer in insurance industry was introduced in 1954 by the Metropolitan Life Insurance Company, New York, while the first computer for German insurance applications was installed by Allianz in 1956. See: Koch, P. *Geschichte der Versicherungswirtschaft in Deutschland* [History of Insurance Industry in Germany]. Karlsruhe: 2012, p. 379f.

[14] Zuse, K. *The Computer – My Life* (Transl. P. McKenna and J. A. Ross). Springer, 1968/1993.

[15] Bundesministerium für Wirtschaft und Technologie (Ed.). *Master Plan Civil Safety & Security Industry*. Sept. 20, 2013. [Online] http://www.bmwi.de/DE/Mediathek/publikationen,did=600562.html, last access March 25, 2014.

[16] Gesamtverband der Deutschen Versicherungswirtschaft e.V (Ed.). *Die deutsche Versicherungswirtschaft. Jahrbuch 2012* [German Insurance Economy. Year Book 2012]. [Online].

[17] See for example: von Drobnig, U. *Principles of European Law: Security Rights in Movables*. Oxford University Press, 2014, or *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*.

[18] Rabinovitch, N. *Probability and Statistical Inference in Ancient and Medieval Jewish Literature*. University of Toronto Press, 1973.

[19] For example: Koch, W. *Tracking and Sensor Data Fusion. Methodological Framework and Selected Application*s. Springer Mathematical Engineering Series, 2014.

[20] *The Ultimate General Art*. See: Künzel, W., and Cornelius, H. *Die* Ars generalis ultima *des Raymundus Lullus: Studien zu einem geheimen Ursprung der Computertheorie* [The *Ars generalis ultima of Raymundus Lullus*. Studies on an Unknown Origin of Computer Theory]. Advanced Studies in Modern Philosophy and Computer Science, Berlin: 1989. Lullus is honored a Catholic martyr, beatified in 1857 by Pope Pius IX.

[21] Buonanno, R. *The Stars of Galileo Galilei and the Universal Knowledge of Athanasius Kircher* (Vol. 399). Springer Astrophysics and Space Science Library, 2014.

[22] Knobloch, E. et al. (Eds.). *Gottfried Wilhelm Leibniz. Hauptschriften zur Versicherungs- und Finanzmathematik* [Main Works on Actuarial and Financial Mathematics]. Oldenbourg: 2000. See also: Koch, P. *Geschichte der Versicherungswissenschaft in Deutschland* [History of Actuarial Science in Germany]. Karlsruhe: 1998, p. 58ff.

[23] Lauritzen, S. *Thiele. Pioneer in Statistics*. Oxford University Press, 2002, p. 249.

[24] *Op. Cit*., p. 57ff.

[25] See, for example: *On the Mathematical Theory of Risk* (1930) and *Collective Risk Theory* (1955). In: *Harald Cramér. Collected Works I.* Springer Collected Works in Mathematics, 2013.

[26] Creifelds et al. (Eds.). *Rechtswörterbuch* [Juridical Dictionary]. München: 2007.

[27] European Commission. Mobility and Transport. *Road Safety*, http://ec.europa.eu/transport/road_safety/specialist/statistics/, last access Mar. 25, 2014.

[28] *Verkehrsunfälle*. Statistisches Bundesamt, https://www.destatis.de/DE/ZahlenFakten/Wirtschaftsbereiche/TransportVerkehr/Verkehrsunfaelle/Verkehrsunfaelle.html, last access Mar. 25, 2014.

[29] Waldvogel. S. et al. *Simple and sensitive online detection of triacetone triperoxide explosive*. *Elsevier Journal on Sensors and Actuators B: Chemical*, Vol. 143, 2 (7 January 2010), 561–566.

[30] Wieneke, M., and Koch, W. (2009). *Combined Person Tracking and Classification in a Network of Chemical Sensors*. Elsevier International Journal of Critical Infrastructure Protection Vol. 2 (2009), 51–67.

[31] Koch, W., Kaul, P., Snidaro, L., Waldvogel, S. et al. (2008). *A Security Assistance System Combining Person Tracking with Chemical Attributes and Video Event Analysis*. In Proceedings of the 11th International Conference on Information Fusion, Cologne, 2008.

[32] Mahler, R. *Statistical Multisource-Multitarget Information Fusion*. Artech House, 2007.

[33] Streit, R. *Poisson Point Processes: Imaging, Tracking, and Sensing*. Springer, 2010, and M. Schikora, Koch, W., Streit, R., and Cremers, D. A sequential Monte Carlo method for multi-target tracking with the intensity filter. In *Advances in Intelligent Signal Processing and Data Mining. Theory and Applications,* Mila Mihaylova et al., Eds. Springer, 2013, chapter 3.

[34] Streit, R., and Luginbuhl, T. E. Probabilistic multi-hypothesis tracking. Naval Undersea Warfare Center Dahlgreen Division, Research Report NUWC-NPT/10/428, 1995.

[35] Wieneke, M. Hazardous material localization and person tracking. Ph.D. thesis, Bonn University. In *Advances in Sensor Data and Information Fusion* (Vol. 3), Wolfgang Koch, Ed.

[36] 2014 Nuclear Security Summit. Wikipedia, http://en.wikipedia.org/wiki/2014_Nuclear_Security_Summit, last access Mar. 25, 2014.

[37] Wieneke, M., and Koch, W. *Localization and Tracking of Radioactive Source Carriers in Person Streams*. In Proceedings of the 15th International Conference on Information Fusion, Singapore 2012.

[38] See, for example, the European Union project CATO (A comprehensive holistic answer centered on an integrated CBRN toolbox). http://www.cato-project.eu, last access Mar. 25, 2014.

[39] Arkin, R. C. *Governing Lethal Behavior in Autonomous Robots*. CRC Press, 2009.

[40] For example: Isaac Asimov's *Three Laws of Robotics*. In Asimov, I. *Runaround*, 1941. Short story published in: A. Asimov (1950). *I, Robot*. Harper Voyager Books, 1950/2013.

[41] Liggins, M. E., Hall, D. L., Llinas, J (Eds.). *Handbook of Multisensor Data Fusion—Theory and Practice, 2nd Edition*. Boca Raton, FL: CRC Press, 2008, p. 24.

[42] USAF, Chief Scientist, Human Effectiveness Directorate, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio. http://www.af.mil/AboutUs/Biographies/Display/tabid/225/Article/107678/dr-kenneth-r-boff.aspx, last access March 25, 2014.

[43] Boff, K. R. Revolutions and shifting paradigms in human factors and ergonomics. *Elsevier Journal of Applied Ergonomics*, Vol. 37 (2006), 391–399.

[44] See for example: Grolle, J. *Die Hirningenieure. Die Ära der Maschinenmenschen bricht an*. DER SPIEGEL, 49/2013, 28.11.2013 (*The Brain Engineers*), available online.

[45] Huxley, A. ". . . there is always soma, delicious soma, half a gramme for a half-holiday, a gramme for a week-end, two grammes for a trip to the gorgeous East, three for a dark eternity on the moon; returning whence they find themselves on the other side of the crevice, safe on the solid ground of daily labour and distraction." *Brave New World*. Vintage, 1932/2004.

[46] Trenkamp, O. *Neue Studie zu Hirndoping: Jeder fünfte Student putscht sich auf*. [A New Study on Brain Doping. Every Fifth Student is Using It]. SPIEGEL Online, 31.01.2013, available online.

[47] Nietzsche, F. *On the Genealogy of Morals* (Transl. Walter Kaufmann and R. J. Hollingdale). Vintage, 1887/1989. German: *Zur Genealogie der Moral. Eine Streitschrift*. In *Friedrich Nietzsche. Werke III*. Karl Schlechta, Ed. Frankfurt a. M.: 1969, p. 854.

[48] *Blade Runner*. Directed by Ridley Scott. Warner Bros, 1982. Final cut: 2007.

[49] Pate, A. *Nietzsche's Ubermensch in the Hyperreal Flux: An Analysis of Blade Runner, Fight Club, and Miami Vice*. Master's Thesis, 2009, Dissertations and Graduate Research Overview. Paper 15, available online.

[50] Anton, A. *The Nietzschean Influence in* The Incredibles *(2004)*. In *The Amazing Transforming Superhero! Essays on the Revision of Characters in Comic Books, Film and Television*. Terrence R. Wandtke, Ed. McFarland & Co, 2004/2007. See also the globally successful TV series *24* telling the deeds of counter terrorist agent Jack Bauer analyzed in: Snyder, S. *Truth and Illusion in* 24*: Jack Bauer, Dionysus, and Apollo*. In *24 and Philosophy. The World According to Jack*, Jennifer Hart Weed et al., Blackwell Philosophy and Pop Culture Series, Eds., 2008.

[51] Penrose, R. *Shadows of the Mind. A Search for the Missing Science of Consciousness*. Vintage, 2004/2005, p. 8ff.

[52] Sorgner, S. L. Nietzsche, the overhuman, and transhumanism. *Journal of Evolution and Technology*, Vol. 20, 1 (2009). See also the Special Issue *Nietzsche and European Posthumanism*, Vol. 21, 1 (2010).

[53] Russell, S. J., and Norvig, P. *Artificial Intelligence. A Modern Approach* (3rd ed.).Pearson, 2010, p. 1038. See also: Sloterdijk, P. *Regeln für den Menschenpark: Ein Antwortschreiben zu Heideggers Brief über den Humanismus*. Frankfurt a. M., 1999; und H.-P. Horn *Brauchen wir Tabus? Antwort auf die Preisfrage der Deutschen Akademie für Sprache und Dichtung vom Jahr 2000*. Göttingen, 2000/2003.

[54] See for example: http://transhumanity.net/news/entry/transhumanity.net-endorses-the-pirate-party, last access Mar. 25, 2014. The German branch of the "Pirate Party" is an opposition party in the German provincial parliaments of Berlin, North Rhine-Westphalia, Schleswig-Holstein, and Saarland.

[55] Fukuyama, F. The world's most dangerous idea: transhumanism. *Foreign Policy*, Vol. 144 (2004), 42–43.

[56] Bostrom, N. *Transhumanism: The World's Most Dangerous Idea?*, http://www.transhumanism.org/index.php/WTA/more/bostrom-responds-to-fukuyama/, last access Mar. 25, 2014.

[57] *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology*, S. 5.

[58] Benedict XVI, Pope Emeritus. The listening heart. Reflections on the foundations of law, 2011.

[59] Benedict XVI, Pope Emeritus, (2006). Benedict has apparently been aware of the ethical problems related to cognitive tools: "The contemporary context seems to give primacy to an *artificial intelligence* that becomes ever more dominated by experimental techniques, and in this way forgets that all science must always safeguard man and promote his aspiration for the authentic good." In: Benedict XVI. *Address at the Pontifical Lateran University*, Rome, October 21, 2006, available online.

[60] Kurzweil, R. *The Singularity is Near: When Humans Transcend Biology*. New York: Viking, 2005.

[61] Heidegger, M. *The Question Concerning Technology, and Other Essays*. New York: Garland, 1953/1977.

[62] Schopenhauer, A. Parerga and paralipomena. In *Short Philosophical Essays* (Vol. I), 1851, p. 503.