3-2021

Ethical, Legal, and Social Issues (ELSI)

Andrea Jerkovic´
Center for European Security Studies

Alexander Siedschlag
Penn State Harrisburg, SIEDSCHA@erau.edu

Ethical, Legal, and Social Issues (ELSI)

Andrea Jerković and Alexander Siedschlag

Contents

Abstract

This chapter introduces the concept of ethical, legal, and social issues – known as ELSI – as it is relevant to security science research and security science-informed practice. After defining ethical, legal, and social issues, the chapter addresses main ELSI domains and discusses how to address those in security science. Arguments are illustrated using examples from domains such as critical infrastructure protection and novel coronavirus pandemic (COVID-19) response. Subsequently, the chapter demonstrates the relevance of ELSI analysis in security science for risk assessment and vulnerability analysis. It argues for a comprehensive approach to ELSI assessment and consideration in security science that actively involves members of the public in the process of exploring ethical, legal, and social issues. Selected public participation methods are recommended. Moreover, the chapter discusses the use of ELSI to address the security vs. liberty

A. Jerković (✉)
CEUSS | Center for European Security Studies and AMC Wirtschaftsakademie GmbH – Austrian Management Center, Vienna, Austria
e-mail: jerkovic@european-security.info

A. Siedschlag
School of Public Affairs, The Pennsylvania State University (Penn State), Penn State Harrisburg, Middletown, PA, USA
e-mail: siedschlag@psu.edu

A. J. Masys (ed.), *Handbook of Security Science*,
https://doi.org/10.1007/978-3-319-51761-2_37-1

dilemma in security science and the real-world security practice that it may inform and offers criteria for "good security science" that embeds assessing and addressing of ELSI throughout the research and dissemination process. The chapter concludes by arguing that security science should provide a better connection of the disciplines involved in its research undertakings. Security science should establish networked expertise to foster deliberate planning and well as rapid decision support capability for crisis management.

Introduction

The addressing of *e*thical, *l*egal, and *s*ocial *i*ssues (known as ELSI) in security science has gained significant relevance in the homeland security era (Hadjimatheou et al. 2015; Siedschlag 2017), the concept and its relevance pre-dating 9/11, though. Consideration of ELSI aspects in security science is an element of a moral discourse that derives from a global human security perspective and transcends national security research ecosystems (cf. Nyman and Burke 2016). ELSI emerged from deliberation about the interaction of technology and society in natural and life science-oriented security research but has gained increasing relevance throughout the entire disciplinary spectrum of security science.

ELSI as a specific concept was first introduced in the Human Genome Project (HGP), evaluating ethical, legal, and societal implications of the newfound genetic knowledge (Yesley and Roth 1993). Technology assessment of the effects of new products and processes on society and exploration of societal acceptance and ethical acceptability of emerging technologies was then applied to fields, such as nuclear technology, pharmacology, gene technology, or artificial intelligence, and others (Lucivero 2016). As well, ethics aspects have traditionally been addressed in strategic planning processes (Howe 1994). Broader applications relate ELSI to the entire spectrum of "emergency research ethics," addressing how the scientific study of individuals and populations experiencing calamity can and should "protect and promote the well-being and autonomy of research participants, researchers, science and society as a whole [. . .], while allowing and encouraging research to take place that will benefit members of society through the production of knowledge or new [. . .] interventions" (Selgelid and Viens 2012, p. xv).

By today, ELSI has become a universal concept used to address compliance and societal acceptance issues in military and security science, such as unanticipated military uses of technology and crossovers of military technological solutions to civilian use (Chameau et al. 2014). This, for example, includes informed consent, data protection, and risk-benefit assessment for research involving human subjects; ownership and use-to-purpose of data; potential of data to allow identification of individuals rather than just providing cluster information, thus supporting the right of individual self-determination; and assessing and addressing the potential for dual (civil and military) use and misuse (e.g., terrorist abuse) of research results. Typical ELSI mitigation methods include self-control by researchers and professional

associations; safeguards and codes of conduct, including addressing of wider (societal) impact of research results; institutional review and audit systems; as well as legally rooted mechanisms, such as data protection and harmonization of terminologies and legal standards to support compliance (Rath et al. 2014).

Defining Ethical, Legal, and Social Issues

ELSI analysis is indispensable in security science because it is a predominant factor in enabling us to ensure a sound balance between liberty and security (see Kowalski 2008). The three components of ELSI may be defined as follows:

Ethical issues – Ethical issues describe the space defined by the study of moral obligation that is available to achieve coherence of security with political and societal preferences (Selgelid and Viens 2012). That space can be broken down into three distinct systems (Zack 2009): *consequentialism* focuses on achieving action results of high moral value; *deontology* (or duty ethics) centers on always adhering to certain high moral principles in all of our actions, regardless of the specific outcome; *virtue ethics* are based on a moral system of common values. Specifically, ethical issues may be best mitigated by virtue (values ethics); legal issues by deontology; and social issues by consequentialism, focused on the actual effects on people. However, in practice, accurate addressing of ELSI in security science and practice will most likely be based on a combination of elements from all three moral systems.

Legal issues – As part of ELSI, reflection on legal issues mainly serves to duly consider the risk of security intrusion: encroaching of constitutionally protected civil rights and freedoms without a proportional security payoff, thus not serving the security of the people but infringing liberty (Kowalski 2008; Roach and Hufnagel 2012). Legal issues consideration addresses balancing of values as well as distributive justice: Security capabilities should not include as a consequence the uneven distribution of security in society, safeguarding some parts of it more than others, or securing some while making others more vulnerable (to hazards or an imbalance between security and liberty). Aspects such as dual-use (Rath et al. 2014) of security science research output and products (i.e., civilian technology applications that may also be used for military purposes or may be exploited for criminal terrorist abuse) demonstrate how legal aspects intertwine with other dimensions (such as ethical aspects) along the ELSI continuum.

Social issues – Whereas ethical aspects typically relate to the moral acceptability of security science, security technology, and security practice, social aspects often refer to their societal acceptance (Legran and McConnell 2012). This is an important perspective because technology not only can contribute to security but also create new vulnerabilities. Yet the social issues component in ELSI is still broader: It also relates to the all-hazards/whole-community approach to homeland security (Kilroy 2018) and the integrated approach to disaster resilience globally (Paton and Johnston 2017), as well as to comprehensively safeguarding and defending a society's commonly acquired values (Wolfers 1952, p. 485).

Important to consider in critical thinking about the response to the novel coronavirus pandemic (COVID-19), the "S" in ELSI also draws attention to the evidence-based security needs of society and disaster-struck communities, as opposed to the bureaucratic and political construction of disaster (Roberts 2013). It is indicative of the need for more awareness of, and delivery to, ELSI that accounts of "scientific response to COVID-19 and lessons for security" such as by Gronvall (2020) typically fail to address ethical, legal, and social (other than "social distancing") aspects of pandemic response and critical thinking about the future of security science(s). "Social distancing" is not a social but a physical matter and therefore should be more adequately referred to as physical distancing. This term that was in use in the public health discipline before COVID-19 (e.g., Glass et al. 2006) is a complete misnomer as well as an example of how relevant disciplines in security science do not interlock: For a thing to be "social," as we have known since Max Weber (1962), it has to be value-driven and meaning-loaden and oriented toward others' action, beyond mere co-orientation. If we refer to social distance, as we have known since Emile Durkheim and Georg Simmel (Karakayali 2009), we talk about in-grouping vs. out-grouping and trying to separate and seclude the values of one's own community from those of other communities. Also in times of crisis, terminology is not a luxury discourse but highly impactful on social outcomes.

The needs of all members of the whole community should be considered in the planning and execution of any disaster response, including pandemic response (Siedschlag 2020). Another consideration, also relatable to the COVID-19 response, is the following:

> Protecting people's security sometimes involves limiting the freedoms of a whole population. So long as the operation of these limitations is kept as short as possible and imposed in order to protect important rights, such as the right to life, even human rights law permits them. Human rights law recognizes the existence of emergencies that "threaten the life of the nation." [The] *International Covenant on Civil and Political Rights* (1966) recognize[s] this kind of emergency. Anticipating that declarations of emergency might be used opportunistically by governments as justification for the unnecessary limitation of rights, human rights law discourages the declaration of an emergency by governments, and requires the period of emergency to be as short as possible. Even in emergencies, certain human rights may not be limited, according to human rights law. These include the right not to be tortured and the right not to be discriminated against. (Hadjimatheou et al. 2015, p. 178)

Main ELSI Domains and How to Address Them in Security Science

Based on a literature review, primary domains of ELSI include the following (Siedschlag 2017):

- Balancing liberty and security in legislation as well as in policy implementation and disaster response
- Eternal or continuously extended emergency declarations that may ultimately run counter constitutional and democratic principles

- Ethical net assessment of technological and nontechnological security interventions: proportionality of the security measures related to the intended outcomes for society in comprehensive perspective
- Potential of abuse of technological security solutions, such as exploitation by criminals or terrorists
- Data mining and government surveillance of citizens, and the related aspects of right to privacy and legal limitations on intelligence gathering on own citizens
- Indiscriminate subjection of large parts of society to generalized suspicion and investigation, for example, based on profiling (such as racial profiling)
- Discriminatory security interventions that for example only mitigate risks and serve interest specific to a certain sector of society, as opposed to the whole community

Addressing ethical, legal, and social aspects in a way integrated into the very security research process itself is not only a requirement for good research. It also is of prior importance for the public perception of security science, its integrity, its discoveries and recommendations, and its overall impact on society, such as the creation of social asymmetry (Suchman et al. 2017). ELSI analysis thus contributes to the social legitimacy of that type of research, and society's acceptance and use of its results and products.

Conceptions of risk, security, and solutions to security problems vary according to the organization of political and social relations. Risks and security threats are selected as important because they reinforce established interpretations and relations within a culture, thus reproducing the symbolic foundations of a community: "Common values lead to common fears [. . .]. There is no gap between perception and reality" (Douglas and Wildavsky 1982, p. 8). In other words, there is no risk "out there," but risk is always selected from within a society, based on cultural backgrounds. This means following this interpretation that risk is a "social construct" and cannot be assessed against a (mistaken) "objective" or "factual" notion of the concept. This is where the concept of security culture comes in and can provide important guidance on addressing ELSI in security science.

Security culture (Siedschlag and Jerković 2018) is a deeper-rooted concept that goes beyond those approaches, based on a cognitive concept that looks into how groups of people perceive things and how this perception can be explained and to some extend predicted, as well as modified. A general assumption of cultural approaches is that the perception of (in)security depends on culturally embedded meanings of risk. For example, immigrant cultures may be interpreted as the cause of social radicalization processes that mount up to threats to internal security; differently, a user security culture may be interpreted as a social firewall against IT security offenses. A further relevant aspect of security culture is the cultural selection of risks. Different perceptions and disputes about risk and security can be linked to competing worldviews (Douglas and Wildavsky 1982, see above), as they tend to be paramount in multicultural cities.

Risk research has shown that people's assessment of risks and threats greatly depends on knowledge of precedents, frequency, and extent of risk experience as

well as perceived immediate effects on themselves (Kahneman et al. 1982). From those findings as well, important conclusions can be drawn for the COVID-19 pandemic response: For instance, as relates to a shift in public risk perception and resulting behavioral dispositions (Qin et al. 2021) or the challenge of basing mitigation strategies on evolving probabilistic information or on the role that social, political, and institutional rituals can play in enhancing or obstructing pandemic response effectiveness (Brown 2020).

Understanding, and building into research designs as well as policy recommendations emanating from security science research, risk perception constitutes an ELSI challenge of continuing and all-hazards relevance. For example, Coppola (2007, pp. 164–166) distinguished between fear-related and knowledge-related factors or risk perception and associated risk-taking behavior:

- Fear-related factors:
  - Risks causing pain and death are generally feared
  - Controllable risks tend to be feared less than uncontrollable risks
  - Disasters with global impacts are feared more than those with regional impacts
  - Lethal risks are feared more
  - Risks equal to all population groups are feared less than risks affecting particular sub-groups (especially children)
  - Collective risks are feared more than individual risks
  - Risks exceeding life spans are more alarming
  - Risks that are hard to prevent cause greater fear
  - Decreasing risks (e.g., due to effective mitigation) are feared less
  - Involuntary risks are feared more
  - Direct affection raises fear of risk
  - Avoidable risks cause less fear
- Knowledge-related factors:
  - Invisible risks (e.g., smoke vs. genetic engineering)
  - Risks with an unknown degree of exposure
  - Risks having delayed effects
  - New/unknown risks
  - Scientifically implausible risks

Further related to ELSI, as shown in Table 1, the World Health Organization pointed out that the perception of risk and resulting planning requirements to a considerable extent do not only depend on human mechanisms for processing information but also on social and cultural values (WHO 2005, pp. 110–111; for an in-depth discussion see Ammann 2006).

An interesting domain to illustrate how ELSI can be addressed proactively in the planning stage using different public participation methods is urban planning, with a focus on safe and secure – while open and livable – public spaces. Table 2 includes some well-tested and established methods, along with references to the *Urban Securipedia* open-access knowledge base (https://securipedia.eu), where those methods and their application are explained. Those methods are not restricted to

Table 1 Factors that affect people's perception of risk and risk-taking behavior, according to the World Health Organization (WHO)

Factor	Description with examples
Voluntariness	Risks from activities considered to be involuntary or imposed (e.g., exposure to chemicals and radiation from a terrorist attack using chemical weapons or dirty bombs) are judged to be greater and are, therefore, less readily accepted than risks from voluntary activities (such as smoking, sunbathing, or mountain climbing)
Controllability	Risks from activities considered to be under the control of others (such as the release of nerve gas in a coordinated series of terrorist attacks) are judged to be greater and are less readily accepted than those from activities considered to be under the control of the individual (such as driving an automobile or riding a bicycle)
Familiarity	Risks resulting from activities viewed as unfamiliar (such as travel leading to exposure to exotic-sounding infectious diseases) are judged greater than risks resulting from activities viewed as familiar (such as household work)
Fairness	Risks from activities believed to be unfair or to involve unfair processes (such as inequities in the location of medical facilities) are judged greater than risks from "fair" activities (such as widespread vaccinations)
Benefits	Risks from activities that seem to have unclear, questionable, or diffused personal or economic benefits (e.g., proximity to waste-disposal facilities) are judged to be greater than risks resulting from activities with clear benefits (e.g., employment or automobile driving)
Catastrophic potential	Risks from activities associated with potentially high numbers of deaths and injuries grouped in time and space (e.g., major terrorist attacks using biological, chemical, or nuclear weapons) are judged to be greater than risks from activities that cause deaths and injuries scattered (often apparently randomly) in time and space (e.g., household accidents)
Understanding	Poorly understood risks (such as the health effects of long-term exposure to low doses of toxic chemicals or radiation) are judged to be greater than risks that are well understood or self-explanatory (such as pedestrian accidents or slipping on ice)
Uncertainty	Risks that are relatively unknown or highly uncertain (such as those associated with genetic engineering) are judged to be greater than risks from activities that appear to be relatively well known to science (such as actuarial risk data related to automobile accidents)
Effects on children	Activities that appear to put children specifically at risk (such as drinking milk contaminated with radiation or toxic chemicals or pregnant women exposed to radiation or toxic chemicals) are judged to carry greater risks than more-general activities (such as employment)
Victim identity	Risks from activities that produce identifiable victims (such as an individual worker exposed to high levels of toxic chemicals or radiation, or children involved in accidents or terrorist attacks) are judged to be greater than risks from activities that produce statistical victim profiles (such as automobile accidents)
Dread	Risks from activities that evoke fear, terror, or anxiety due to the horrific consequences of exposure (e.g., to certain infectious diseases, radiation sickness, or cancer) are judged to be greater than risks from activities not arousing such emotions (e.g., to common colds or household accidents)

(continued)

Table 1 (continued)

Factor	Description with examples
Trust	Risks from activities associated with individuals, institutions, or organizations lacking in trust and credibility (e.g., chemical companies or nuclear power plants with poor safety records) are judged to be greater than risks from activities associated with trustworthy and credible sources (e.g., regulatory agencies that achieve high levels of compliance from regulated industries)
Media attention	Risks from activities that generate considerable media attention (such as anthrax attacks using the postal system or accidents at nuclear power plants) are judged to be greater than risks from activities that generate little media attention (such as occupational accidents)
Accident history	Activities with a history of major accidents or incidents as well as frequent minor accidents or incidents (such as leaks from waste-disposal facilities) are judged to carry greater risks than activities with little or no such history (such as recombinant DNA experimentation)
Reversibility	The risks of potentially irreversible adverse effects (such as birth defects from exposure to a toxic substance or radiation) are judged to be greater than risks considered to be reversible (e.g., sports injuries)
Personal stake	Activities viewed as placing people or their families personally and directly at risk (such as living near a waste-disposal site) are judged to carry greater risks than activities that appear to pose no direct or personal threat (such as the disposal of waste in remote areas)
Ethical and moral status	Risks from activities believed to be ethically objectionable or morally wrong (such as providing diluted or outdated vaccines for an economically distressed community) are judged to be greater than the risks from ethically neutral activities (such as the side effects of medication)
Human versus *natural origin*	Risks generated by human action, failure, or incompetence (such as negligence, inadequate safeguards, or operator error) are judged to be greater than risks believed to be caused by nature or "acts of god"

Source: WHO (2005, pp. 110–111), with adaptations

addressing the liberty vs. security/safety continuum in urban planning but are also applicable to other domains to ensure ELSI integration into security strategies and policies.

Legal aspects in security science specifically concern, but are not limited to, compliance issues in the research process itself. They also relate to the integration, typical of the homeland security era, of broad security aspects into the legal and political system in a socially feasible and ethically acceptable manner. This includes proper consideration of the impact of new security-related legislation on the public and private sectors (Anikeeff et al. 2003). A well-balanced consideration of ELSI further is relevant to avoid a legalist bias in security science and to the use of security science findings in practical decision-making. Using homeland security in the USA as an example, some of its critics argue that constitutional and legal considerations have sometimes prevailed over focused analyses of vulnerability gaps and development of new requirements for more efficient and effective security measures (cf. Beckman 2007). ELSI analysis can provide a context for placing relevant legal

Table 2 Public participation methods to integrate different ethical, legal, and social aspects into security considerations in the strategic planning of safe and secure public spaces

Public participation method	Short explanation	Urban Securipedia page
Activating Opinion Survey	Asks people about their views and attitudes; at the same time, encourages them to articulate and defend their interests and to contribute to solutions	https://securipedia.eu/mediawiki/index.php/Activating_opinion_surve
Advocacy Planning	Typically used at a regional or local level to appraise underrepresented segments of the population about planning issues and to involve them in developing suggestions to revolve contentious issues	https://securipedia.eu/mediawiki/index.php/Advocacy_planning
Citizen Jury	Using their everyday experience and knowledge, randomly selected members of the general public work together to produce an interest-free citizen assessment of a particular, often contentious, issue	https://securipedia.eu/mediawiki/index.php/Citizen_jury
Cooperative Discourse	Supports complex, conflictual decision-making processes combining different methods, such as mediation or Delphi survey; starts with participants from the affected communities developing criteria to assess different strategic/planning options; participants are then encouraged to actively bring their interests to the table in a mediation session; subsequently, experts analyze the decision alternatives identified by participants; finally, participants evaluate the options using their criteria set developed in the first step of the process, and recommend one alternative	https://securipedia.eu/mediawiki/index.php/Cooperative_Discourse
Dynamic Facilitation	This is a guided open group discussion, specially used to address emotionally loaded issues; participants are encouraged to be creative in exploring possible solutions, while also developing mutual trust	https://securipedia.eu/mediawiki/index.php/Dynamic_Facilitation
Experimental Participation Method	Series of professionally coordinated and facilitated meetings that serve as a link between decision-makers and those who will be affected by the decision; helps to improve problem awareness on both sides and can lead to discussion-driven consensus, with recommendations adopted by the relevant public sector agency/agencies	https://securipedia.eu/mediawiki/index.php/Experimental_participation_method
Focus Group	Framework for multistep, increasingly focusing deliberation on a specific issue in a goal-oriented fashion way, while also encouraging expression and addressing of emotion as well as group-dynamic processes	https://securipedia.eu/mediawiki/index.php/Focus_group

(continued)

Table 2 (continued)

Public participation method	Short explanation	Urban Securipedia page
Future Workshop	Dialogue-based micro-democratic processes to develop and test new ideas to solve common or shared problems	https://securipedia.eu/mediawiki/index.php/Future_Workshop
Local Open Dialogue	A set of different methods to improve risk communication, perception, and assessment through whole-community involvement; among other things, it may include roundtables (bringing representatives of different or segregated groups together that are affected by the same problem), citizen exhibitions (linguistic and visual expressions of those affected by a certain planning decision to create a fair discussion platform), or future workshops (see above)	https://securipedia.eu/mediawiki/index.php/Local_open_dialogue
Neosocratic Dialogue	A framework to address universal questions as involved in the planning/strategic decisions at stake with members of the public; this is then connected to participants' experience related to the underlying issues to establish a basis for further analysis responsive to the public's concerns and needs	https://securipedia.eu/mediawiki/index.php/Neosocratic_Dialogue
Participatory Diagnosis	A moderated small-group setting in which affected members of the public members discuss their most important questions or concerns about an issue/planning subject matter that is becoming ripe for decision making; a focus is on the expected impact on daily life and routines; based on this, priority topics are identified for subsequent research/policy analysis to support decision-making	https://securipedia.eu/mediawiki/index.php/Participatory_Diagnosis
Planning for Real	A community-oriented planning approach designed to activate people; based on a stepwise interactive process with different participation and interaction opportunities to overcome communication obstacles and identify existing (community) resources	https://securipedia.eu/mediawiki/index.php/Planning_for_Real
Safety Audit	Originally designed by the Metropolitan Action Committee on Violence Against Women and Children (METRAC), uses diverse, whole-community discussion groups to review public safety concerns and makes recommendations to local government	https://securipedia.eu/mediawiki/index.php/Safety_audit

foundations and compliance measures into the social context of the society whose values and way of life science and security interventions are meant to protect. Security always must be weighed against other values, such as liberty, freedom,

and privacy rights – but also accountability and freedom of discussion (Rosenzweig et al. 2012).

Another pertinent example of legal aspects within ELSI relates to civil rights in emergency management. The Federal Emergency Management Agency (FEMA 2021) published a *Community Vaccination Centers Playbook* that includes an annex on "Civil Rights Considerations During COVID-19 Vaccine Distribution Efforts." Civil rights considerations follow a checklist provided by FEMA's Office of Equal Rights (OER). The steps to ensure vaccine distributive justice for example include, but are not limited to:

- Identifying communities with limited English proficiency and languages needed for disseminating vaccination information
- Identifying, and assisting, communities with public transportation and functional needs to reach a vaccination center
- Identifying communities with internet access needs
- Organizing events to engage (with) communities without internet adaption or reliable internet access
- Addressing public concerns over vaccination site selection and accessibility
- Addressing people's religious and safety concerns
- Managing vaccination site compliance with legal accessibility requirements, such as following the Americans with Disabilities Act (ADA) in the USA

As this selection of examples of ELSI aspects demonstrates, the "E," "L," and "S" dimensions intersect. ELSI assessment in security science therefore should follow a comprehensive approach, as laid out in the subsequent section.

The Need for a Comprehensive Approach

There is more than the societal dimension of security, namely: *the societal creation of security.* The societal creation of security starts with a whole-community approach to vulnerability that includes ELSI aspects in vulnerability analysis and also considers vulnerable and protectable social infrastructure in addition to physical and institutional infrastructure (Cannon 2006). The interaction of anthropogenic systems with nature and natural hazards needs more thorough addressing by security science, whose projects and endorsements for a certain practice must increasingly consider societal impact, through proactive ESLI analysis. Critical thinking about the role of political privileged scientific advice in the context of the COVID-19 catastrophe has been demonstrated how ever more important this is in the present time (Brown 2020).

Here lies a problem with "science" or "data-driven" approaches to COVID-19 responses that many countries claim to follow (Siedschlag 2020). Typically, those approaches to the novel coronavirus pandemic almost exclusively focus on healthcare sector protection and preventing it, at seemingly almost any risked price, from demand overload. We know there is a tendency of risk avoidance (as

opposed to risk management) in the public health sector and also in public health sciences, as bioethics have criticized (Royo-Bordonada and Román-Maestre 2015). As the disaster ethics paradigm (Zack 2009) would posit, the "common good" (Rousseau's concept of what brings benefit to all of society) cannot be determined by realized in such an approach that neglects the needs of the entire rest of the whole community. Moreover, a public health metrics-focused data-driven approach to the COVID-19 response is limited. One shortcoming is that only pandemic data and projections appear to be used, with no adequately comprehensive set of indicators applied (cf. Wardman and Lofstedt 2020). Such a set would include, among others, social life data such as "social vulnerability" (Cannon et al. 2003).

More generally, reflecting the cross-border and cross-sector nature of current and emerging security threats and challenges, as well as the complexity of instruments and objectives in security policies and strategies, a comprehensive approach is needed to anticipate and effectively address ethical, legal, and social (ELSI) implications. The focus should be on recognizing and solving the actual security needs of the population, not only on mitigating the impacts of security interventions on public life. Integrated risk assessment (Ammann 2006), as discussed above, is one part of it. A comprehensive approach to security science and good societal security practice cognizant of security science discoveries should consider and address the public in an inclusive way, integrating people's perspectives into the research process, into the programming of security science itself, as well as into policies and strategies derived from security science discoveries (Rykkja 2018).

Security science should offer advice to authorities to make appropriate trade-offs between security and other valued societal objectives, while its research projects should make a well-defined and tangible contribution to the development of security science as a practically relevant discipline. The following example from the cybersecurity domain illustrates this postulation:

Since an increasing amount of health testing and monitoring is carried out digitally, a trend boosted by COVID-19, the security of e-health systems will be important to both governments and populations around the world. This might be a point of vulnerability to hostile attacks or a sort of blackmail of governments. In such cases, vulnerability is known to be reduced if numbers of networks are multiplied, but this is at the cost of interoperability. Research on the trade-offs between unified digital systems and vulnerability to cyberattacks will have ethical aspects, since less unity might in principle have a health cost, for example when medical records are inaccessible between regions as patients travel.

Moreover, addressing aspects of ethics is not only a requirement for good research. It is also of high importance for public perception of the scholastic integrity and societal impact of security science research. Addressing those aspects thus contributes to the social legitimacy of its scientific efforts, as well as society's acceptance and use of its results and products. There is a tendency to address ethical, legal, and broader sociocultural aspects of security and related scientific research via normative means: by enacting policies and procedures that reduce the risk of negative ethical and societal impacts. Security is a collective good that relates above all to society as a whole (Wolfers 1952). Without public acceptance and the

inclusion of the whole community in the creation of security and the "production" of solutions to security problems, such outcomes will be considerably limited in their effectiveness (Friedewald et al. 2017). As knowledge about how science works can increase public acceptance of its results and technological solutions (Weisberg et al. 2021), broad communication about ELSI integration into the research process in the field of security science can support its informed societal approval.

A recent example is the National Security Interim Strategic Guidance issued by President Biden in March 2021 that calls for a comprehensive approach with ELSI integration into the policy-making cycle:

> Because traditional distinctions between foreign and domestic policy – and among national security, economic security, health security, and environmental security – are less meaningful than ever before, we will reform and rethink our agencies, departments, interagency processes, and White House organization to reflect this new reality. We will ensure that individuals with expertise in science, technology, engineering, and mathematics, economics and finance, and critical languages and regions are fully integrated into our decision-making. Because the federal government does not, and never will, have a monopoly on expertise, we will develop new processes and partnerships to ensure that state, municipal, tribal, civil society, non-profit, diaspora, faith-based, and private sector actors are better integrated into policy deliberations. And we will develop new mechanisms to coordinate policy and implementation across this diverse set of stakeholders. (The White House 2021, p. 22)

The public planning participation methods assembled in Table 2 above provide some examples of how such integration of ELSI aspects into the national security policy-making cycle could be practically accomplished. However, fitting "expertise in science," as per the National Security Interim Strategic Guidance, into decision-making first should not be confined to the natural sciences and second poses its own specific challenges and creates dilemmas that political culture, prudence, and self-restraint will be better able to tackle than would the scientific construction of policy.

Dilemmas of Security Science in Practice

Adopting a security measure just because there is "science" that supports the measure works does not meet ELSI standards. Ethics and social issues consideration, as also demonstrated by COVID-19 responses and their criticism (Collins et al. 2020; Greer et al. 2020; Maor and Howlett 2020), still must achieve a balance between idealist behaviorism and realism. Idealist behaviorism was laid out by Charles Merriam, who also served as an advisor to several US presidents, in his *New Aspects of Politics* (Merriam 1925). Merriam had argued that political reasoning can be directly improved by improving methods of related research. Merriam advocated "politics as the science of constructive, intelligent social control," based on a well civics-educated rational public (Merriam 1925, p. 10). Hence, in this perspective, political decision-making should be based on scientific insight and crisis management should exert scholarly informed intelligent social control.

Arguing against Merriam and others, Hans J. Morgenthau (1947), in Scientific *Man* vs. *Power Politics*, explained how an emphasis on science and reason as routes to peace – and crisis and disaster management may be included – can have nations lose touch with their historic traditions of statecraft. As Morgenthau pointed out, science deals with probabilities but politics require prudent leadership. Morgenthau (1947, p. vi) argued that "belief in the redeeming powers of science" does not exempt the political leader from making the difficult choice of the lesser evil.

Good security science conscious of ELSI hence should:

- Be based on the understanding that security mainly refers to people and society, and that technical solutions are not effective without the acceptance and participation of the public
- Include advice to authorities to make appropriate trade-offs between security and other valued societal objectives
- Make a well-defined and tangible contribution to the evolution of security science as a societally relevant discipline
- Promote critical discussion of fundamental concepts – whether established or innovative and their societal impact
- Consider significant social, cultural, ethical, legal, and political aspects of security from the very beginning of the research and development activities, that is, not only in the implementation and in terms of public acceptance and ascribed legitimacy of research results and products
- Strengthen – especially against the backdrop of resilience – a whole-of-community and ownership approach to security
- Act as a socialization vector that builds resilience clusters, which wherever possible comprise technology/capability, first responders, and members of the general public
- Involve a track dedicated to quick response mechanisms for managing social stress resulting from interruption of supplies
- Strongly consider that new technological environments should support the self-help capacity of the general public and that new technologies can change the structure and perception of crises and their management
- Recognize that its technological innovations may also cause new societal vulnerabilities, or create different and unfair levels of security in society
- Make a specific contribution to the knowledge pool of the implementing organization(s) and the building of sustainable excellence of research and expertise, operational and effective beyond project lifetime
- Contribute to establishing institutionalized relations between those actors involved in realizing societal security

As discussed, ELSI considerations should also thoroughly inform risk and vulnerability assessment. By identifying vulnerabilities comprehensively, following an ELSI evaluation, security science can directly contribute to the strengthening of community resilience. In doing so, security science should follow a comprehensive approach to vulnerability, with a focus on social vulnerability:

> In order to understand how people are affected by disasters, it is clearly not enough to understand only the hazards themselves. Disasters happen when a natural phenomenon affects a population that is inadequately prepared and unable to recover without external assistance. But the hazard must impact on groups of people that are at different levels of preparedness (either by accident or design), resilience, and with varying capacities for recovery. Vulnerability is the term used to describe the condition of such people. It involves much more than the likelihood of their being injured or killed by a particular hazard, and includes the type of livelihoods people engage in, and the impact of different hazards on them.
>
> It is especially important to recognise this social vulnerability as much more than the likelihood of buildings to collapse or infrastructure to be damaged. It is crucially about the characteristics of people, and the differential impacts on people of damage to physical structures. Social vulnerability is the complex set of characteristics that include a person's
>
> - initial well-being (nutritional status, physical and mental health, morale;
> - livelihood and resilience (asset pattern and capitals, income and exchange options, qualifications;
> - self-protection (the degree of protection afforded by capability and willingness to build safe home, use safe site)
> - social protection (forms of hazard preparedness provided by society more generally, e.g. building codes, mitigation measures, shelters, preparedness);
> - social and political networks and institutions (social capital, but also role of institutional environment in setting good conditions for hazard precautions, peoples' rights to express needs and of access to preparedness). (Cannon et al. 2003, pp. 4–5)

For example, technological innovation and the further spread of networked structures will create new vulnerabilities, which will require increased societal awareness and resilience. Technology not only contributes to security but can by itself create new vulnerabilities. Technology also has the potential to change human behavior and to drive the evolution of security cultures. Public concern about being controlled by technology may change people's behavior. At the same time, it may bring a new impetus for community activities, such as crowdsourcing of information about hazards and disasters to support prevention, protection, mitigation, response, and recovery. As those examples indicate, the development and application of technology do not create security or new vulnerabilities out of the blue; rather, they – for example by providing frames – accentuate existing trends, processes, and repertoires of action that are socially rooted and connected to common values (Peterson 1991). Social networks play an increasingly important role in information dissemination, opinion-mining, and public decision-making. The unstructured and informal nature of social networks is a challenge for state authorities, which traditionally operate in a linear, top-down manner. This clash of cultures requires new procedures and training schemes for civil servants, officials, and volunteers. This is a significant dimension in the societal creation of security. There are no effective technological solutions without acceptance and public participation. With internal and external security becoming less and less separable in a variety of sectors, the public will have to be better involved in security processes.

At the same time, the further development of civil security cannot be conceived without technology, and technology will contribute to increasing societal resilience.

Another aspect is natural hazards and disasters. The risk they pose is co-defined by prevailing social conditions. Climate change to COVID-19 have taught us that the interaction of anthropogenic systems with nature and natural hazards need more thorough and more anticipatory addressing by security science.

With the dependency of society on critical infrastructure increasing, the complexity of the social consequences of critical infrastructure failure increases as well. Public entities and nations as a whole may be called on to assume security roles that focus on managing the social consequences of critical infrastructure breakdown. However, those possible future public roles will have their limitations in that people's crisis behavior considerably depends on predominant social patterns, security cultures, as well as the civic culture at large. This includes the perceived legitimacy of political, economic, and social institutions and the level of risk tolerance of the population as aspects of societal resilience.

Conclusion

As a universal, transdisciplinary, and whole-community enterprise, the output of security science must be planned for beyond the traditional research results utility criteria of advisory board pleasure, grant project officers' delight, and end-user satisfaction. It should anticipate and meet societal requirements and stimulate future demand, thus contributing to establish its own benchmarks instead of just meeting preset conventional standards.

Security itself does and will continue to play a role in a variety of discourses, but it remains a vague term that is under constant change. Therefore, security science should increasingly include perspectives from the humanities and social sciences to provide practical criticism of the evolution of the concept of security in different geographies, their cultures, and its impact on citizens and society. Security science should also provide a better connection of the disciplines involved in its research undertakings. It should establish networked expertise to foster deliberate planning as well as rapid decision support capability for crisis management. To meet growing ELSI expectations, security science should provide an analysis of societal security needs. It should also help make fair and sustainable trade-offs between security and other valued societal objectives.

Acknowledgments Parts of the original research results on that this chapter is based received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreements n° 261633 (FOCUS – Foresight Security Scenarios) and n° 261741 (VITRUV – Vulnerability Identification Tools for Resilience Enhancements of Urban Environments). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained therein. The authors would like to particularly acknowledge the contributions made to project deliverables used toward this chapter by Rosemarie Stangl and Florian Fritz, formerly Institute for Security Research, Sigmund Freud University Vienna; Juha Ahokas, Cross-border Research Association (CBRA); Brooks Tigner, SecEUR Sprl; Rachel Suissa, University of Haifa; and Tom Sorell, University of Warwick.

References

Ammann WJ (2006) Risk concept, integral risk management and risk governance. In: Ammann WJ, Danemann S, Vulliet L (eds) RISK 21. Coping with risks due to natural hazard in the 21st century. Taylor and Francis, London, pp 3–23

Anikeeff AH et al (2003) Homeland security law handbook. A guide to the legal and regulatory framework. Rowman & Littlefield, Lanham

Beckman J (2007) Comparative legal approaches to homeland security and anti-terrorism. Ashgate, Aldershot/Hampshire

Brown P (2020) Studying COVID-19 in light of critical approaches to risk and uncertainty. Research pathways, conceptual tools, and some magic from Mary Douglas. Health Risk Soc 22(1):1–14. https://doi.org/10.1080/13698575.2020.1745508

Cannon T (2006) Vulnerability analysis, livelihoods and disasters. In: Ammann WJ, Danemann S, Vulliet L (eds) RISK 21. Coping with risks due to natural hazard in the 21st century. Taylor and Francis, London, pp 41–50

Cannon T, Twigg J, Rowell J (2003) Social vulnerability, sustainable livelihoods and disasters. Report to DFID Conflict and Humanitarian Assistance Department (CHAD) and Sustainable Livelihoods Support Office. University College Benefield Hazard Research Centre, London

Chameau JL, Ballhaus WF, Lin HS (eds) (2014) Emerging and readily available technologies and national security. A framework for addressing ethical, legal, and societal issues. National Academies Press, Washington, DC

Collins A, Florin NV, Renn O (2020) COVID-19 risk governance. Drivers, responses and lessons to be learned. J Risk Res 23(7–8):1073–1082. https://doi.org/10.1080/13669877.2020.1760332

Coppola DP (2007) Introduction to international disaster management. Butterworth Heinemann, Oxford

Douglas M, Wildavsky A (1982) Risk and culture. An essay on the selection of technological and environmental dangers. University of California Press, Berkeley, CA

Federal Emergency Management Agency (FEMA) (2021) Community vaccination centers playbook. https://www.fema.gov/sites/default/files/documents/fema_community-vaccination-centers_playbook.pdf. Accessed 7 Mar 2021

Friedewald M, Burgess JP, Čas J, Bellanova R, Peissl W (eds) (2017) Surveillance, privacy and security. Citizens' perspectives. Routledge, London/New York

Glass RJ, Glass LM, Beyeler WE, Min HJ (2006) Targeted social distancing designs for pandemic influenza. Emerging Infect Dis [serial on the Internet]. https://doi.org/10.3201/eid1211.060255

Greer SL, King EJ, da Fonseca EM, Peralta-Santos A (2020) The comparative politics of COVID-19: the need to understand government responses. Globl Public Health 15(9):1413–1416. https://doi.org/10.1080/17441692.2020.1783340

Gronvall GK (2020) The scientific response to COVID-19 and lessons for security. Survival 62(3): 77–92. https://doi.org/10.1080/00396338.2020.1763613

Hadjimatheou K, Sorell T, Guelke J (2015) Ethical, legal, and social issues (ELSI) in homeland and civil security research and the European Union approach. In: Siedschlag A (ed) Cross-disciplinary perspectives on homeland and civil security. A research-based introduction. Peter Lang, New York, pp 177–194

Howe E (1994) The nature of ethical issues. Acting on ethics in planning. Rutgers University Press, New Brunswick

Kahneman D, Slovic P, Tversky A (1982) Judgement under uncertainty. Heuristics and biases. Cambridge University Press, Cambridge

Karakayali N (2009) Social distance and affective orientations. Sociol Forum 23(3):538–562

Kilroy RJ (ed) (2018) Threats to homeland security. An all-hazards perspective, 2nd edn. Wiley, New York

Kowalski KM (2008) A pro/con look at homeland security. Safety vs. liberty after 9/11. Enslow, Beverly Heights

Legran T, McConnell A (eds) (2012) Emergency policy. Routledge, New York

Lucivero F (2016) Ethical assessments of emerging technologies. Appraising the moral plausibility of technological visions. Springer, Heidelberg et al

Maor M, Howlett M (2020) Explaining variations in state COVID-19 responses. Psychological, institutional, and strategic factors in governance and public policy-making. Policy Des Practice 3(3):228–241. https://doi.org/10.1080/25741292.2020.1824379

Merriam C (1925) New aspects of politics. University of Chicago Press, Chicago

Morgenthau HJ (1947) Scientific man vs. power politics. University of Chicago Press, Chicago

Nyman J, Burke A (eds) (2016) Ethical security studies. A new research agenda. Routledge, New York

Paton D, Johnston D (2017) Disaster resilience. An integrated approach, 2nd edn. Thomas, Springfield

Peterson RT (1991) Technology, culture, and democratic politics. Centen Rev 35(1):31–49. http://www.jstor.org/stable/23740252. Accessed 23 Feb 2021

Qin H, Sanders C, Prasetyo Y (2021) Dynamic risk perception and behavior in response to the coronavirus disease 2019 (COVID 19). In: Natural Hazards Center quick response grant report series, 317. Natural Hazards Center, University of Colorado Boulder. https://hazards.colorado.edu/quick-response-report/dynamic-risk-perception-and-behavior-in-response-to-the-coronavirus-disease-2019-covid-19. Accessed 7 Mar 2021

Rath J, Ischi M, Perkins D (2014) Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. Sci Eng Ethics 20(3):769–790. https://doi.org/10.1007/s11948-014-9519-y

Roach K, Hufnagel S (eds) (2012) Emergency law. Routledge, New York

Roberts PS (2013) Disasters and the American state. How politicians, bureaucrats, and the public prepare for the unexpected. Cambridge University Press, New York

Rosenzweig P, McNulty TJ, Shearer E (eds) (2012) National security law in the news. American Bar Association, Chicago

Royo-Bordonada MA, Román-Maestre B (2015) Towards public health ethics. Public Health Rev 36(3). https://doi.org/10.1186/s40985-015-0005-0

Rykkja LH (2018) Societal security and crisis management. Governance capacity and legitimacy. Springer International Publishing, Cham

Selgelid MJ, Viens AM (eds) (2012) Emergency ethics. Ashgate, Farnham

Siedschlag A (2017) Ethical, legal, and social issues in homeland security. What they are and how to address them. In: Alperen MJ (ed) Foundations of homeland security. Law and policy, 2nd edn. Wiley, Hoboken, pp 29–54. https://doi.org/10.1002/9781119289142.ch3

Siedschlag A (2020) Pennsylvania's COVID-19 response vs. homeland security frameworks and research. Masking the whole community. Homel Secur Affairs 16(Article 10). http://www.hsaj.org/articles16350. Accessed 7 Mar 2021

Siedschlag A, Jerković A (eds) (2018) Homeland security cultures. Enhancing values while fostering resilience. Rowman & Littlefield International, Lanham

Suchman L, Follis K, Weber J (2017) Tracking and targeting. Sociotechnologies of (in)security. Sci Technol Hum Values 42(6):9831002. https://doi.org/10.1177/0162243917731524

The White House (2021) National security interim strategic guidance. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf. Accessed 7 Mar 2021

Wardman JK, Lofstedt, R (eds) (2020) COVID-19 Special Issue. J Risk Res 23(7–8). https://www.tandfonline.com/toc/rjrr20/23/7-8. Accessed 7 Mar 2021

Weber M (1962) Basic concepts in sociology (trans: Secher HP). Philosophical Library, New York

Weisberg DS, Landrum AR, Hamilton J, Weisberg M (2021) Knowledge about the nature of science increases public acceptance of science regardless of identity factors. Public Underst Sci 30(2):120–138. https://doi.org/10.1177/0963662520977700

Wolfers A (1952) “National security” as an ambiguous symbol. Polit Sci Q 67:481–502
World Health Organization (WHO) (2005) Effective media communication during public health emergencies. A WHO handbook. World Health Organisation, Geneva. http://www.who.int/csr/resources/publications/WHO%20MEDIA%20HANDBOOK.pdf. Accessed 10 Mar 21
Yesley MS, Roth MRJ (comp) (1993) ELSI bibliography. Ethical, legal & social implications of the human genome project. U.S. Department of Energy, Office of Energy Research. https://doi.org/10.2172/10108311
Zack N (2009) Ethics for disaster. Rowman & Littlefield, Lanham