PUBLIC INTEGRITY
https://doi.org/10.1080/10999922.2021.1932144

Routledge
Taylor & Francis Group

From Threat to Risk: Changing Rationales and Practices of Secrecy

Marlen Heide

Università della Svizzera italiana

ABSTRACT

This article explores how risk rationales affect and alter national security secrecy. While the transformation of defense and security policy has been widely discussed by security theorists, transparency scholars have not yet considered the notion of risk in their conceptualizations of national security secrecy. This article draws on security studies literature to outline the divergences between conventional and risk-based security. The empirical section investigates how the difference between both rationales manifests in secrecy practices by investigating conventional and risk-based classification frameworks (in Germany compared to the United Kingdom). In a risk security setting, information is increasingly seen as an asset and therefore subject to proactive management and exploitation. This requires a shift from a bureaucratic risk aversion in classification practices toward sharing, exploitation, and availability of information. Further, information governance is no longer about the separation between sensitive and nonsensitive information, but instead a comprehensive evaluation of all government assets for risks. These shifts ultimately change conventional understandings of secrecy as an "exemption" and a "necessity," impelling new debates about the legitimacy of secrecy practices.

KEYWORDS

classification, risk, secrecy, security

Heretofore, security scholars have noted that risk management techniques, such as screening, profiling, or precautionary measures, have increasingly determined security practices. Risk rationales often prevail over conventional "realist" approaches to security. While the field of security studies has grappled extensively with these transformations, academic debates on national security secrecy widely disregard the diffusion of risk. Instead, secrecy continues to be justified along realist lines as a "necessity" and "exception." Recent classification reforms, however, show that risk is also alternating the way in which secrecy is thought and practiced. This raises new questions concerning the legitimacy of categorization and restriction of information as sensitive.

This article explores how risk rationales alter the conceptualization national security secrecy and the potential problems arising from such a shift. To begin, the dividing points between conventional security rationales and risk-security will be determined based on existing scholarship from the field of security studies. The empirical section contrasts secrecy practices in a conventional security context (Germany) versus a risk-security context (United Kingdom). By applying an "analytics of government" approach, the analysis investigates the classification frameworks of both countries to trace "regimes of practice"—the ways in which secrecy is conceived,

CONTACT Marlen Heide heidem@usi.ch Institute of Communication and Public Policy, Università della Svizzera italiana, Lugano, Switzerland.

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

represented, and managed. The article concludes by discussing the implications of risk-security on the concept and practice of national security secrecy.

The analysis finds that a risk-centered approach to security does impact secrecy practices. Classification is no longer merely about the protection of sensitive information but also serves as information management. Such a shift implies a departure from bureaucratic risk aversion, by promoting individual responsibility and information sharing. Moreover, the emergence of "risk secrecy" questions the conceptualization of secrecy as an "exemption" and "necessity," instead embedding it into a broader framework of information management. While this opens new avenues for information disclosure and accountability, it also allows a more encompassing justification for secrecy in areas previously untouched.

Problem setting and the objective of the article

Secrecy represents a persistent problem in the scholarship on democratic governance. While openness and accountability are heralded as a *sine qua non,* even fierce transparency advocates concede exceptions to the norm of transparency (Coliver, 1998, p. 2). One of the more important exceptions is nondisclosure, or active concealment, in order to implement protective policies—measures concerning safety, security, and defense (Thompson, 1999). Such "national security secrecy" is embedded in the realist idea that security is an overarching societal value: it is a precondition for governance itself.

While security serves as a constitutive element of exceptionalism, the conceptualization and understanding of security itself poses a major challenge: "The polyvalent meaning of national security ultimately translates into an uncertainty what exactly constitutes information that are too sensitive to be disclosed: As there is no universally accepted definition of national security, there exists no common understanding of which kind of information may endanger national security if released" (Amiri, 2014, p. 20). In addressing this persistent question, scholars rarely draw on security studies for an adequate appreciation of security as a concept in itself or critical discourses on the notion of "necessity" embedded in security claims. Instead, contributions on the issue of "national security secrecy" rely primarily on a realist conceptualization of security, perpetuating the understanding of secrecy as a "necessary exemption" from the norm of transparency. This article provides an entry point for a more critical discussion of how the understanding of security relates to claims for secrecy by arguing that the increasing importance of risk rationales in security governance challenges conventional assumptions about secrecy.

The first part of the article outlines the conceptual differences between conventional and risk-security rationales by drawing on a rich literature by critical security scholars that discusses the shift from exceptionalism toward risk management techniques in security governance (Aradau, 2016; Corry, 2012; Rasmussen, 2006). The empirical section of this article compares secrecy in a country following largely conventional security rationales (Germany) and a country that largely adopted notions of risk-security (United Kingdom). The analysis of both cases determines if and how secrecy practices differ between these systems. The article concludes with a discussion of the potential implications of risk security on the conceptualization of national security secrecy. It proposes that with the shift toward risk security, secrecy can no longer be thought of merely as an exemption from normal democratic rules when risk-security thinking is not determined by the immediacy of crisis and threat.

National security secrecy and the logic of realist security

While rarely made explicit, national security secrecy is primarily conceptualized along realist lines. Here, the notion of survival facilitates the idea of a "necessary exception": during crises, decision making and policy implementation might need to depart from otherwise established processes in order to safeguard the (democratic) system itself (Schoenfeld, 2010). Security precedes other considerations of democratic systems, such as transparency and accountability. Secrecy is a hallmark of the politics of exception, limiting the number of authoritative speakers and facilitating speedy decision making (Corry, 2012, p. 248). It provides strategic and technical advantages vis-à-vis opponents and reduces the vulnerabilities of the defense apparatus (Herman, 1996; Sunstein, 1986). Secrecy is considered legitimate, as it "works to protect information that would pose an identifiable threat to the security of the nation by compromising its defense or the conduct of its foreign relations. . . . [T]he public interest is served when this type of information remains secure" (Aftergood, 2009, p. 399). Thus, national security secrecy falls under the "necessity rationale" for government secrecy, whereby information protection is required for policy implementation (Curtin, 2014, p. 689).

Critical security studies, notably scholarship on securitization, allow us to map the rationale of realist security (and, by extension, secrecy). Justifications for enhanced security measures, it is argued, follow a "grammar of security," which relies on the construction of threats in the form of adversaries that pose an imminent and existential threat to a valued referent object—classically, a state (Buzan, Wæver, & de Wilde, 1998). Key terms are "existential threat," "survival," "urgency," or motivation of friend-enemy logics (Corry, 2012). Huysmans (1998, p. 571) describes securitization as "a technique of government which retrieves the ordering force of the fear of violent death by a mythical replay of the variations of the Hobbesian state of nature." Such patterns serve equally to justify nondisclosure and enhance secrecy measures.

While conventional security along realist rationales has perpetuated secrecy practices in past, recent scholarship from the field of security studies suggests that the notion of security itself is undergoing a fundamental transformation. In recent years, security policy has examined risk rationales, thus not only modifying strategic thinking but also the language in which security is considered. Discussions on the interdependencies between secrecy and security remain widely untouched by these changes. Yet, the prevalence of risk rationales in security affairs has influenced thought about secrecy practices, potentially challenging its conceptualization as an exemption to the democratic norm of transparency.

Risk-security rationales

Recent years have seen a diffusion of risk logics within the field of security policy. Frequently, security scholars perceive risk-security as an extension of conventional security, making security more encompassing and thus extending state power (Bigo, 2012). Risk-security, it is argued, is no longer a matter of emergency politics, but routine procedures (Corry, 2012). Such a paradigmatic shift in security affairs might likely reflect in related secrecy practices, in turn challenging conventional notions of its justification and underlying rationale.

Logic of risk

Risk-thinking is pervasive, permeating diverse aspects of life, from insurance to business operations, health, and—indeed—security. Beck (1986) famously coined the term "risk society" to describe the *zeitgeist* of late modernity. The term "risk" refers to the probability of an adverse event of some magnitude (Hardy & Maguire, 2016 p. 80). Risk "implies the ex-ante possibility that things can go wrong or not turn out as expected" (Power, 2004, p. 60). Risk refers to anticipated hazards as opposed to immediate problems, since "the mode of existence of risks does not consist in being real but in becoming real" (Beck, 2009, p. 67). Risk is conventionally conceptualized in opposition to "uncertainty," referring to the indeterminacy of the future and thus the limits of knowing. In contrast, risk is a form of "measurable uncertainty," making the future knowable through statistical and probabilistic reasoning. Risk "amalgamates knowledge with non-knowing within the semantic horizon of probability" (Beck, 2009, p. 5), and has hence been described as "calculative rationality"

(O'Malley, 2010, p. 467). Consequently, the management of risks entails predicting and pre-empting future hazards by rendering latent dangers ascertainable.

Risk rationales in security

Risk security scholars argue that the concept of risk is also becoming an important determinant of security governance (Petersen, 2012, p. 703). Security discourses and practices are increasingly dominated by potential risks rather than imminent threats—survival, confrontation, and competition (Hammerstad & Boas, 2015, p. 478). Risk security emerged against the background of a new strategic environment after the Cold War. Territorial, interstate conflicts were largely replaced by a defense paradigm focusing on "risks of international terrorism, nuclear proliferation, economic stability, organized crime, cyber-attacks, climate change and natural hazards, crisis management and protection of critical infrastructure" (Földes, 2014, p. 6). Beck (2009, p. 148) notes that the "old wars" were conducted symmetrically in the sense that the actors "behave in predictable ways as regards the political goals and the threat potential." In contrast, recent years have seen an increasing focus on hybrid, nonstate threat actors in security governance, and thus reflect the changing patterns of security governance.

The core characteristic of a security risk compared to conventional security is the absence of a threatening enemy, which depersonalizes danger by describing *attributes* of a threat actor rather than actual enemies (Aradau, Lobo-Guerrero, & Van Munster, 2008, p. 148), such as the practice of risk profiling that identifies typical characteristics of terrorists (Corry, 2012, p. 244). Thus, risk security tends to "depersonalise danger" (Hammerstad & Boas, 2015, p. 278). Further, the language of risk highlights "the conditions of possibility," wherein a risk could transform into actual harm (Hammerstad & Boas, 2015, p. 478). Conventional security "deals with direct causes of harm, whereas risk-security is oriented towards the conditions of possibility or constitutive causes of harm" (Corry, 2012, p. 235). Whereas in a conventional understanding of security threats are tangible and instantaneous, risk security turns toward the uncertain future.

This changing understanding of threats has altered security governance itself, by reorienting it toward risk detection and prevention. The management of risk security relies on the security practices of precaution ("better safe than sorry") and pre-emption ("strike first"). For Rasmussen (2006, p. 109), the purpose of security policy is no longer to stop immediate threats but to filter a risk matrix by probability of harm. This translates to the implementation of approaches such as screening, profiling, or proactive interventions in order to manage uncertainty and prevent the materialization of threats (Aradau, 2016).

The turn toward detection and prevention changes the provision of security from emergency response toward bureaucratic routines (Aradau, 2016, p. 292); it has become a matter of long-term governance aimed at controlling uncertainty (Corry, 2012, p. 245). Krahmann points to the perpetual demands created by risk thinking: "Risks require permanent surveillance, analysis, assessment and mitigation … [T]he potential range of imaginable risks is infinite" (2011, p. 356). The ubiquity and normalization of security governance has, in turn, marginalized the question of survival, such that many current security practices deal with threats below the level of existential danger and survival (Corry, 2012, p. 244). Agamben notes, "in all of Western democracies, the declaration of the state of exception has gradually been replaced by an unprecedented generalization of the paradigm of security as the normal technique of the government" (2004, p. 14). Against this background, critical security scholars have cautioned against the diffusion of security into the day-to-day business of government.

Analytical approach

Case selection

The analysis explores whether and how the shift from conventional to risk security has impacted secrecy practices by investigating two distinctive cases, each representing one of the two rationales: Germany and the United Kingdom. The selection was determined by the prevalence of risk and threat management language and techniques in security policy and governance more generally. The analysis of both cases determines if and how secrecy practices differ between the systems.

A number of crises triggered the adoption of risk governance in the United Kingdom, after which public sector organizations began importing management tools from the private sector (Power, 2004, p. 60). By now, the term "risk" and "at risk" are used in association with just about any routine event. In Germany, risk management techniques are slow to take place and implementation is rudimentary, which is caused by a lack of centralized planning as well as a lack of expertise in this field (Budäus & Hilgers, 2009).

The difference is also reflected in general practices of security governance. Germany generally counts as a late adopter of post-Cold War security environments. Frequently criticized for being slow in technical and strategic transformation, White Papers for defense planning have only reluctantly included new notions of security, starting as late as 2006. Despite a comprehensive project for the armed forces, their strategic mindset still points toward deterrence and territorial defense (Junk & Daase, 2013, p. 142). In the United Kingdom, the post-Cold War transformation happened faster and more efficiently than in other countries. Transformation efforts aimed at creating versatile forces ready for deployment on a global scale at short notice were concluded by 2004. The approach reflects risk rationales by using the "core risk-security terminology such as uncertainty, vulnerability, resilience, flexibility and preparedness" (Hammerstad & Boas, 2015, p. 482). Observers also notice an increasing usage of the language of risk in the UK National Security Strategy, referring to the "age of uncertainty" (Hammerstad & Boas, 2015, p. 484) and of "new and unforeseen threats" (Aradau, 2016, p. 292).

Terminology, though not a perfect analogue, can thus be measured to isolate a country's position along a scale between absolute adoption of risk rationales and complete attachment to conventional rationales for security and governance, where the United Kingdom leans more toward the former and Germany to the latter. As other authors have noted, the United Kingdom, despite a comprehensive adoption of risk terminology, still shows patterns of conventional defense thinking (Hammerstad & Boas, 2015). Germany displays some adoption of risk rationales, with its 2016 strategic concept having emerged to be more vocal about "new threats," like cybersecurity or economic threats, even if the usage of risk language remains scarce.

Data analysis

The analysis of secrecy systems in the United Kingdom and Germany will be guided by the main analytical question, "How do risk rationales alter the conventional logic of national security secrecy?" The analysis follows an "analytics of government" approach. Analytics of government investigates specific situations in which the activity of governing is "problematized"—in this case, state secrecy. The focus is not on the empirical activity of government, but rather on the organized practices through which a society is governed and governs itself (Lawlor & Nale, 2014). Against this background, this analysis investigates the rationales through which secrecy is rendered governable, tracing the principles that organize the selection and protection of sensitive information.

The analytics of government investigates "regimes of practice" (i.e., coherent, organized, and routine ways of going about governmental activities). Regimes of practice include, for instance, how the sphere to be governed is conceived and represented, the forms of knowledge and techniques applied to specific governance problems, as well as the goals, outcomes, and consequences of governmental policies. Regimes of practice can thereby focus on specific policy problems or problematize institutional practices themselves, such as in the case of state secrecy. This analysis treats classification provisions—the most prominent technique of state secrecy—as a regime of

TABLE 1. Analytical Components.

	Conventional security	Risk rationale
Conception of security	State-centric; political independence, territorial integrity; military logic; symmetrical threats	Constitutive conditions of harm; depersonalized danger; dispersed hazards; economic stability, organized crime, cyber-attacks, climate change
Grammar of security	Threat, survival, enemy, urgency, imminence	Uncertainty, vulnerability, resilience, flexibility and preparedness
Governance techniques	Security as a question of force; prevent threats; deter opponents	Bureaucratic routines of monitoring probability calculations, pre-emption, mitigation

practice and explores its mechanisms by determining types of information considered for classification, determinants of sensitivity, the objective of information protection, and the relation between classification and openness provisions.

Classification provisions are the main data source for this analysis, constituting the primary provision for state secrecy. Thus, the analysis refers primarily to the UK Government Security Classification (Version May 2018) and the German General Regulation for Material and Organizational Protection of Classified Documents (Verschlusssachenanweisung). Governmentality analysis focuses on the routines of bureaucracy: theories, programs, knowledge, and expertise that composes a field to be governed and the ways of seeing and representing that field embedded in the practices of government. Thus, the approach takes policy papers, official publications, legal texts, and academic publications as its sources.

The analysis takes an interpretive approach, paying close attention to the language and problem representation applied in the abovementioned documents, and, specifically, whether and how threat and risk terminology are applied. Indicator terms, such as threat, danger, mention of concrete threats, territorial defense, survival, and so forth versus probability, risk, uncertainty, and the like, are drawn from existing security studies literature, specifically securitization and risk-security scholarship (see Table 1). The analysis was done through inductive manual coding of data, relying on double coding to ensure intercoder reliability. The rationales displayed in the core data itself were complemented by drawing on secondary data (e.g., policy statements or academic literature on policy directives in the country) to obtain a more comprehensive understanding.

Empirical section

Selective versus comprehensive approach to secrecy

The German approach to classification relies on the *ex-ante* specification of types of official information that qualify for protective marking. According to the regulatory framework pertaining to document classification, "protective markings concern information related to external and internal security, foreign relations and third-party interests entrusted to the government" (BMI, 2006, p. 27). Endangerments, damages, and disadvantages must be demonstrated conclusively and refer to concrete scenarios (BMI, 2006). As a consequence of preselecting types of information that qualify for classification, nonsensitive information does not feature as part of the classification system. Thus, the majority of official information is left unmarked. The German classification regime reflects how security rationales motivate governments' information privilege, establishing a legitimate space for official action under the veil of secrecy. Further, information protection in the German case relates to a specific *field of governance*—activities in foreign and security policy, both of which are usually understood as "high politics," in which the executive and military technocrats are granted a prerogative in decision making.

The United Kingdom pursues a quite different approach to classification regimes. Here, the official nature of a document might render it part of the classification system, not a specific threat or danger associated with it. The idea that the official nature of information constitutes its membership in a classification system does not presuppose an increase in official secrecy; rather, it signifies a shift in understanding the instrumentality of official information altogether. The Government Security Classifications Policy refers to "all information that government collects, stores, processes, generates or shares" (Cabinet Office, 2018b, p. 3). Thus, the lowest level of classification, information marked as "official," is applicable to "all routine public sector business, operations and services." The underlying understanding is one of risk management, as all government activities attract risks that "need to be assessed by government organisations so that they can make informed, practical and business enabling decisions" (Cabinet Office, 2018a, p. 5).

The difference between the German and UK approaches suggests a fundamental rethinking of national security secrecy. In the conventional approach, sensitive information needs to be distinguished from nonsensitive information. The separation between secrets and nonsecrets reflects the distinction between normal and exceptional politics within a conventional understanding of security. It is here transferred to information management, inasmuch as *some* information from the bulk of public information is selected as worthy of protection, thus creating an exception to the norm of unprotected information. The risk management approach to information security assumes a liability of information *per se,* reflecting what risk authors have called a pervasiveness and perpetuation of information management outside of less-than-existential threats.

Degree of sensitivity vs. type of sensitivity

Both classification regimes apply a graded system in which the level of information sensitivity—and therefore secrecy—depends on the severity of harm that its unauthorized release might cause. Different, however, are the determinants of what constitutes harm in each case.

The German regulation considers the extent of damage inflicted upon national security; that is, the institutions, processes, and policies that comprise the system of defense and external relations for the country at large. The unauthorized release of classified information might either "endanger the existence of vital interests," "endanger security or severely damage the interests," "damage interests," or "create disadvantages" for the Federal Republic and the federated states, depending on whether they are classified as "top secret," "secret," "confidential," or "for official use only." The logic applied here is one of gradation; the object of harm remains constant, while the gravity of harm magnifies. The German approach thus reflects a conventional logic in several regards, engaging a language of survival and national interest or escalatory language, pointedly described by securitization theory.

The UK classification regime considers multiple factors in grading the sensitivity of information, such as areas of government activity, type of threat actors, as well as type of damage. For instance, information classified as "top secret" might be the target of advanced state actors using significant technical, financial, and human resources. The consequence of unauthorized release might incur widespread loss of life. The release of "secret" information could damage military capabilities or the investigation of serious organized crime. Threat actors on this level are nation-state actors or criminal organizations. Even official-level information displays vulnerabilities, being the target of hacktivists, single issue pressure groups, investigative journalists, competent individual hackers, and the majority of criminal individuals and groups (specified as attackers with bounded capabilities and resources). The undue release of such information might infringe upon the regular business of government.

The distinction between both frameworks reflects the initially outlined distinction between conventional and risk security. Germany applies a system of signaling danger and sensitivity, thus pointing toward the escalating dynamics of emergency. Thereby, the threat itself is unspecified, but is likely to change according to the prevailing security assessment. The UK approach adopts the language of escalation to some degree, but moves beyond gradation in terms of damage gravity. The classification stages take into consideration descriptive factors, such as types of threats to be expected as well as the concrete nature of the damage. Following Corry, “the key difference between risks and threats lies not so much directly in the perceived gravity of a danger or its imminence or the de-personalised nature of it but rather in *what kind of causality* a danger is constructed in terms of” (Corry, 2012, p. 246).

Information as a liability versus information as an asset

While information protection is a natural aim of implementing classification regimes, the comparative analysis suggests that the purpose and boundaries of information protection might vary. Broadly speaking, the objective of the German classification system is the protection of sensitive information. In the United Kingdom, information protection is complemented and supported by proactive information management and effective exploitation of information. The difference of approach between both countries suggests a shift from risk aversion to risk management.

The divergence of both approaches is reflected in the stated objective of the respective classification frameworks. The German guidelines set out to “provide material and organizational protection for classified information” (BMI, 2006, p. 2) and for “agencies and institutions working with classified documents to provide a protective framework as well as personnel with access to classified documents and thus have to consider protective measures” (BMI, 2006, p. 2). The UK classification scheme describes the “administrative system for the secure, timely and efficient sharing of information” (Cabinet Office, 2018b, p. 4). Further, the policy specifies how information assets are classified to “ensure they are appropriately protected, support Public Sector business and the effective exploitation of information” (Cabinet Office, 2018b, p. 3). The mention of “national security” is notably avoided—thus departing from the conventional rationale for official secrecy.

The example of German classification systems treats information primarily as a liability. The UK classification system suggests that information is not only seen as a vulnerability as suggested by conventional security logics, but as an *asset,* too, for anticipating and managing future risks, thus enhancing the governance capacity of information itself. In contrast to the German example, UK classification guidelines suggest that vulnerabilities are dispersed and require ongoing assessment and management. Further, the focus of information classification shifts from foreign and security policy to a wide array of hazards and vulnerabilities.

The emphasis of the German classification guidelines is placed on various measures to handle and protect sensitive information, thus providing a tool for official process management. The guidelines describe a system for documenting classification activities, re- and declassification, infrastructure for information protection, and quality control that allows safe handling of sensitive information. Further, the guidelines assign authority not only for the production of classifications but also for the access of sensitive information, thus pointing to the notion of insiders and outsiders.

The classification guidelines in the United Kingdom and the German display some similarities, inasmuch as they provide a guide to handle, store, and protect sensitive information, designate authorities and responsibilities, or provide guidance for the identification and marking of sensitive information. However, the UK guidelines also serve as a tool for self-regulation, addressing the problem of over-classification and risk aversion. The guidelines caution that “applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls” (Cabinet Office, 2018b, p. 13). Information management needs to be “business-enabling,” meaning proactive and responsible, allowing for not only information protection, but also information availability and usage. The guidelines emphasize that “information needs to be trusted and available to the right people at the right time. The failure to share or exploit information can impede effective government business” (Cabinet Office, 2018b, p. 5). In consequence, UK officials are entrusted with the responsibility and accountability of information appropriation, thus contributing to the broader task of government security.

Most importantly, the role of information appears to change. In conventional security, information is one component of security governance; in risk-security, information is a means for constituting security: the former perceives information as a vulnerability, and the latter as an asset.

Secrecy prerogative versus complementing transparency and secrecy

The relationship between classification and access to information provisions is an essential component of information security. Both cases display fundamental differences in their perspectives on said relationship. While Germany mostly treats these as different areas of government, the UK approach could be described as two sides of the same coin.

The UK classification places secrecy provisions within the framework of other applicable legislations, including the Freedom of Information Act 2000. Provisions for information disclosure and protection thereby exist in parallel:

> Classification markings can assist in assessing whether exemptions to the Freedom of Information Act 2000 (FOIA) may apply. However, it must be noted that each FOI request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. (Cabinet Office, 2018b, p. 15)

Thus, the classification status of a document does not immediately lead to its nonrelease.

The German classification framework makes no mention of the *Informationsfreiheitsgesetz* ([Freedom of Information Act] IFG, 2006) that came into force in 2006. The IFG in turn entails a general exclusion of classified information from release in Germany, pointing to an understanding of state prerogative in information protection. State secrecy provisions clearly override information access.

In the United Kingdom, the release or concealment of information is subject to continuous evaluation, balancing harm with interest for disclosure. Security exemptions are largely subject to an interest test: “To justify withholding information, the public interest in maintaining the exemption would have to outweigh the public interest in disclosure” (ICO, 2017). These assessments do not feature as part of the German IGF law.

The German approach points to a system of legitimate exemption, hence an acknowledged power function of the state in a particular area of government. It provides a curated space for government and bureaucracies to operate in sensitive areas according to their best judgment. On the contrary, the UK classification system emphasizes the continuous assessment and management of information for the benefit of performance and security of government operations. Information management here entails the diligent assessment of information through rigid guidelines as well as assessing potential lingering risks to a polity or constituency.

Summary of findings

The foregoing analysis compares secrecy practices in a context displaying a primarily conventional approach to security (Germany) compared to one dominated by risk rationales (United Kingdom). The empirical section presented a variety of differences between both cases regarding the conceptualization of information sensitivity and the execution of secrecy management; notably, risk rationales appear as a determining factor in the recently reformed UK classification framework. Table 2 provides a summary of the points of comparison identified in the previous section.

The patterns identified in the case of the United Kingdom represent a departure from conventional secrecy practices that still persist in Germany. Even when characteristics pertain, such as

TABLE 2. Summary of Empirical Results.

	Germany	United Kingdom
Scope of classification	Classification pertains only to "sensitive information"	Classification system includes *all* information
Information categorization	Degree of information sensitivity based on gravity of harm	Gravity of harm *and* characteristics of damage, perpetrator and government activity
Objective of classification	Classification as framework of information management	Framework for information management *and* staff management
	Focus on information protection	Information protection *and* information exploitation, sharing
Relation FOI–classification	Separated spheres, classified assets are "exempted" from disclosure	Both embedded in information governance, interdependent

the objective to manage and protect information, these are complemented by new patterns, which in turn shape the face of secrecy governance. The most remarkable aspects observed in the United Kingdom are the applicability of the classification provision to all information, the shifting focus from protection from outsiders to internal staff conduct, and finally, the emphasis to effectively use and potentially share information. These patterns indicate a paradigmatic shift in the way secrecy is not only practiced but also thought, diverging from its realist roots as outlined initially.

By drawing on the immediate comparison between the German and the UK classification system, this analysis identified several trends that challenge the conventional conception of secrecy: (1) The conception of sensitive information as "exempt," embedded in the exceptionalism of realist security, is rendered obsolete by the comprehensiveness of risk-based classification, blurring the boundary lines between secretive and transparent; (2) the emphasis on information exploitation and sharing directly counters patterns of bureaucratic risk aversion conventionally associated with secrecy management—staff deterrence for the benefit of information protection is replaced with an emphasis on the responsibilization of individual staff; (3) the notions of "imminence" and "necessity" typically ascribed to secrecy are replaced by routine management in which all state data are continuously scanned for inherent risks.

Similar patterns identified here paradigmatically for the case of the United Kingdom have also been recorded in other contexts, indicating the potential emergence of a new standard. Ultimately, the emergence of new rationales—"risk secrecy," as we shall call it—does not only impact information management and classification practice but also entails broader implications for questions of accountability and the legitimacy of secrecy.

Implications of "risk secrecy"

The logic of risk secrecy described in this article through the case of the UK classification framework has a number of potential consequences regarding questions of accountability and legitimacy of government secrecy. In fact, it might challenge the way in which secrecy is thought, justified, and scrutinized.

As previously noted, risk security relies on monitoring, forecasting, and probability calculations, because in contemporary security governance, "information is the key to victory" (Strickland, 2005, p. 436). The analysis in this article suggests that an information-centered approach to security also alters secrecy practices. The conventional understanding of secrecy as a means for protecting sensitive areas of government, such as defense and foreign affairs ("high politics"), which still applies in the case of Germany, implies a distinction between secrets and nonsecrets. The case of the United Kingdom suggests a departure from such a dichotomous understanding. Information control is no longer limited to a few selected pieces of sensitive information; all information features as part of the classification apparatus ("comprehensive approach"). Intuitively, such a development suggests an increasing challenge for ensuring the accountability of secrecy. Indeed, various critical scholars have previously cautioned that risk security techniques are a means to further expand state power, or what Bigo (2012, p. 277) has called a "permanent state of emergency." The inclusion of all public sector information into the classification framework renders the potential for concealment universal. Every piece of information is subject to classification, since unclassified assets no longer exist.

At the same time, information classification based on risk rationales, as seen in the United Kingdom, can offer new avenues for accountability. Traditionally, bureaucracies have been described as secretive due to their tendency toward risk aversion, blame avoidance (Hood, 2007), and bureaucratic politics (McClean, 2011, p. 59). Reforms to the UK classification system in 2014 were directly driven by this specific concern about risk aversion and blame avoidance. The new classification guidelines lay out that an "emphasis upon personal responsibility and accountability that underpins the new policy is a key feature" (Cabinet Office, 2018a, p. 2). Agencies should aim for "staff who are well trained to exercise good judgement, take responsibility and be accountable for the information they handle" (UK Cabinet Office, 2018a, p. 2). The UK classification framework, while still addressing the protection of sensitive information vis-à-vis outsiders, is also a tool for ensuring due process and effective management within the framework. This falls in line with the observation that with the rise of risk management, "the mechanisms of government themselves are subject to problematization, scrutiny and reformation." (Dean, 1999, p. 193)

Moreover, the case of the United Kingdom suggests a departure from the static "locking up" of information in favor of an ongoing assessment of information regarding their sensitivity status, either through the evaluation of information "assets," the scanning and categorizing information "risks," or conducting harm/public interest tests. This creates a dynamic process in which the status of documents is subject to change, thus creating new potentials for disclosure. Further, such evaluations and their justification to outside audiences equally create transparency of process. In that regard, secrecy itself is subject to accountability.

Further, the emergence of risk secrecy has conceptual implications for scholarly discussions on state secrecy. Conventionally, secrecy is seen in opposition to democratic values, such as transparency and accountability. In the context of risk secrecy, the boundary lines distinguishing between information protection and information provision become increasingly blurred. The British Security Policy Framework illustrates this idea: "The security of information is essential to good government and public confidence" (Cabinet Office, 2018a, p. 6). Efficient information management, as seen, facilitates not only information protection but also upstream transparency through increased information integrity and availability.

Conclusion

Besides the immediate reflections on the changing nature of national security secrecy, this article also introduces a wider discussion on the rise of risk rationales and risk management techniques in the public sector and their implications for the legitimacy of governance. The analysis illustrates that the "calculative rationality" of risk constitutes a mixed blessing: on the one hand, it enhances the objectivity of decision making and provides new avenues for accountability; on the other hand, risk serves as a powerful rationale by which decisions can be justified in a top-down manner.

Thereby, it should be noted that the notion of risk primarily provides a cognitive scheme through which the world is perceived, constituting an alternative, but not an absolute mode of ordering reality. As Ewald (1991) notes, nothing is a risk *per se* (e.g., Ewald, 1991), but serves as a way of "representing events in a certain form so they might be made governable in particular ways, with particular techniques and for particular goals." (Dean, 1999, p. 206). These goals are multifaceted: frequently, using risk rationales and practices serve as a legitimizing function in itself, providing seemingly “objective” criteria for governance decisions. In other instances, risk management is instituted as a way to ensure integrity in the public sector, to identify risks of deviance and power abuse (OECD, 2020).

Yet, risk has a depoliticizing effect, favoring data-driven probability calculations over political debate and consent. What’s more, power actors might foster consensus and bolster authority by harnessing risk as a cognitive scheme. Thus, when the notion of risk is introduced into political discourse, its role as a substantive as opposed to a power function requires continuing evaluation.

These problems provide an interesting agenda for future research. While the notion of risk in governance has been problematized by a variety of scholars, avenues for ensuring integrity and accountability in an age of risk governance are yet to be explored.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Aftergood, S. (2009). Reducing government secrecy: Finding what works. *Yale Law & Policy Review*, *27*(2), 399–416. Retrieved from https://digitalcommons.law.yale.edu/ylpr/vol27/iss2/4

Agamben, G. (2004). *State of exception*. Chicago, IL: University of Chicago Press.

Amiri, A. P. (2014). *Freedom of information and national security. A study of judicial review under US law*. München, Germany: Utz.

Aradau, C. (2016). Risk, in(security) and international politics. In A. Burgess, A. Alemanno, & J. Zinn (Eds.), *Routledge handbook of risk studies* (pp. 290–298). New York, NY: Routledge.

Aradau, C., Lobo-Guerrero, L., & Van Munster, R. (2008). Security, technologies of risk, and the political: Guest editors’ introduction. *Security Dialogue*, *39*(2–3), 147–154. https://doi.org/10.1177/0967010608089159

Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt, Germany: Suhrkamp.

Beck, U. (2009). *World at risk*. Cambridge, UK: Polity Press.

Bigo, D. (2012). Security, surveillance and democracy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook on surveillance studies* (pp. 277–284). New York, NY: Routledge.

Budäus, D., & Hilgers, D. (2009). Öffentliches Risikomanagement. Zukünftige Herausforderungen an Staat und Verwaltung. In F. Scholz, A. Schuler, & H. Schwintowski (Eds.), *Risikomanagement der öffentlichen Hand* (pp. 17–77). Heidelberg, Germany: Physica.

Bundesministerium des Inneren [BMI]. (2006). Allgemeine Verwaltungsvorschrift zum Materiellen und Organisatorischen Schutz von Verschlusssachen. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSA_pdf.pdf?__blob=publicationFile.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Cabinet Office. (2018a). HMG security policy framework. Retrieved from https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.

Cabinet Office. (2018b). Government security classifications. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf.

Coliver, S. (1998). Commentary to: The Johannesburg Principles on national security, freedom of expression and access to information. *Human Rights Quarterly*, *20*(1), 12–80. https://doi.org/10.1353/hrq.1998.0005

Corry, O. (2012). Securitisation and “riskification.” *Millennium: Journal of International Studies*, *40*(2), 235–258. https://doi.org/10.1177/0305829811419444

Curtin, D. (2014). Overseeing secrets in the EU: A democratic perspective. *Journal of Common Market Studies*, *52*(3), 684–700. https://doi.org/10.1111/jcms.12123

Dean, M. (1999). *Governmentality: Power and rule in modern society*. London, UK: Sage.

Ewald, F. (1991). Insurance and risk. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 197–210). Chicago, IL: University of Chicago Press.

Földes, A. (2014). Classified information. A review of current legislation across 15 countries. *Transparency International Corruption Risks Series*. Retrieved from http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf.

Gesetz zur Regelung des Zugangs zu Informationen des Bundes [IFG]. (2006). Retrieved from https://www.gesetze-im-internet.de/ifg/BJNR272200005.html.

Hammerstad, A., & Boas, I. (2015). National security risks? Uncertainty, austerity and other logics of risk in the UK government's National Security Strategy. *Cooperation and Conflict*, *50*(4), 475–491. https://doi.org/10.1177/0010836714558637

Hardy, C., & Maguire, S. (2016). Organizing risk: Discourse, power, and "riskification". *Academy of Management Review*, *41*(1), 80–108. https://doi.org/10.5465/amr.2013.0106

Herman, M. (1996). *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Hood, C. (2007). What happens when transparency meets blame-avoidance? *Public Management Review*, *9*(2), 191–210. https://doi.org/10.1080/14719030701340275

Huysmans, J. (1998). Desecuritisation and the aesthetics of horror in political realism. *Millennium: Journal of International Studies*, *27*(3), 569–589. https://doi.org/10.1177/03058298980270031301

Information Commissioners Office [ICO]. (2017). The guide to freedom of information. Retrieved from https://ico.org.uk/media/for-organisations/guide-to-freedom-of-information-4-9.pdf.

Junk, J., & Daase, C. (2013). Germany. In H. Biehl, B. Giegerich, & A. Jonas (Eds.), *Strategic cultures in Europe: Security and defense policies across the continent* (pp.139–152). Wiesbaden, Germany: Springer.

Krahmann, E. (2011). Beck and beyond: Selling security in the world risk society. *Review of International Studies*, *37*(1), 349–372. https://doi.org/10.1017/S0260210510000264

Lawlor, L. & Nale, J. (Eds.). (2014). *The Cambridge Foucault lexicon*. Cambridge, UK: Cambridge University Press.

McClean, T. (2011). *Shackling leviathan. A comparative historical study of institutions and the adoption of freedom of information* (Doctoral dissertation). The London School of Economics and Political Science, London, UK. Retrieved from http://etheses.lse.ac.uk/3102/.

O'Malley, P. (2010). Uncertain subjects: Risks, liberalism and contract. *Economy and Society*, *29*(4), 460–484. https://doi.org/10.1080/03085140050174741

Petersen, K. L. (2012). Risk analysis—A field within security studies? *European Journal of International Relations*, *18*(4), 693–717. https://doi.org/10.1177/1354066111409770

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London, UK: Demos.

Rasmussen, M. V. (2006). *The risk society at war: Terror, technology and strategy in the twenty-first century*. Cambridge, UK: Cambridge University Press.

Schoenfeld, G. (2010). *Necessary secrets: National security, the media and the rule of law*. New York, NY: Norton & Co.

Strickland, L. S. (2005). The information gulag: Rethinking openness in times of national danger. *Government Information Quarterly*, *22*(4), 546–572. https://doi.org/10.1016/j.giq.2006.01.005

Sunstein, C. (1986). Government Control of Information, California Law Review, *74*(3), 889–921. https://doi.org/10.2307/3480399

Thompson, D. F. (1999). Democratic secrecy. *Political Science Quarterly*, *114*(2), 181–193. https://doi.org/10.2307/2657736