Kruck, Andreas; Weiss, Moritz

Article — Published Version

Disentangling Leviathan on its home turf: Authority foundations, policy instruments, and the making of security

Regulation & Governance

Suggested Citation: Kruck, Andreas; Weiss, Moritz (2024) : Disentangling Leviathan on its home turf: Authority foundations, policy instruments, and the making of security, Regulation & Governance, ISSN 1748-5991, John Wiley & Sons Australia, Ltd, Melbourne, Vol. 19, Iss. 1, pp. 146-160, https://doi.org/10.1111/rego.12594

Regulation & Governance

Regulation & Governance (2025) 19, 146–160 doi:10.1111/rego.12594

Disentangling *Leviathan* on its home turf: Authority foundations, policy instruments, and the making of security

Andreas Kruck and Moritz Weiss

Geschwister-Scholl-Institute of Political Science, LMU Munich, Munich, Germany

Abstract

Making security has been *Leviathan's* home turf and its prime responsibility. Yet, while security states in advanced democracies share this uniform purpose, there is vast variation in how they legitimize and how they make security policies. First, the political authority of elected policy-makers is sometimes superseded by the epistemic authority of experts. Second, states make security, in some instances, by drawing on their own capacities, whereas in other fields they rely on rules to manage non-state actors. Based on this variation in authority foundations and policy instruments, we disentangle *Leviathan* into different types of (i) positive, (ii) managing, (iii) technocratic, and (iv) regulatory security states. Our typology helps better understand contemporary security policy-making; it advances regulatory governance theory by conceptualizing the relationship between expertise and rules in a complex and contested issue area; and it provides insights into the "new economic security state" and the domestic underpinnings of weaponized interdependence.

Keywords: authority, expertise, rules, security, state.

1. Introduction

The provision of security is *Leviathan*'s home turf. In fact, the core function of the state has always been to "provide security within a geographically defined territory against both internal and external threats" (Paul & Ripsman, 2010, p. 1). Yet, while today's security states in advanced Western democracies share this primary purpose, there is vast variation in who actually makes security policies, by what means, and on what legitimating grounds. A variety of public and private actors, whose interests both converge and diverge, interacts in multi-level policy-making processes. For instance, the provision of cybersecurity involves different actors than policy-making in arms procurement or in military operations, which creates distinct interest and power constellations, and eventually diverse policy trajectories. In short, the *making of security*—and the shape of the *security state*[1]—is both complex and contested (Avant & Haufler, 2018; Gheciu & Wohlforth, 2018; Hofmann, 2013; Neumann & Sending, 2018). Defying notions of a monolithic *Leviathan*, contemporary security states empirically vary with regard to their main authority foundation and their primary policy instruments (Kruck & Weiss, 2023; see Paul & Ripsman, 2010, p. 11).

First, the making of security is sometimes based on the political authority of elected politicians (see Zürn, 2018), while in other instances it relies on the epistemic judgment of experts (see Haas, 1992; Slayton, 2020, 2021; Slayton & Clark-Ginsberg, 2018). For instance, military strategy and operational planning are often reserved to a state's civil-military leadership, who command the political authority to make vital decisions based on institutional entitlement and democratic procedures. Yet, frequently private security experts are also involved in the development of doctrine and in the design of military operations (Leander, 2005; Pratt, 2018). Claims to superior expertise and performance render such private experts authoritative. In short, the foundations of authority vary.

Second, states employ different policy instruments to make security. In some instances, they draw on their own coercive capacities (see Hanson & Sigman, 2021); on other occasions, they rather set rules to incentivize

Correspondence: Andreas Kruck, Geschwister-Scholl-Institute of Political Science, LMU Munich, Oettingenstr. 67, D-80538 Munich, Germany. Email: andreas.kruck@gsi.uni-muenchen.de

Accepted for publication 10 April 2024.

governance contributions from other actors (see Genschel & Zangl, 2014; Levi-Faur, 2005; Majone, 1994, 1997; Schilde, 2023). For instance, the gathering of intelligence about adversaries has always been crucial for protecting states against imminent threats. To do so, governments have built up massive signals intelligence installations to intercept worldwide communications by themselves. However, they have also commissioned and regulated private firms, such as network operators, search engines, and cloud services, to intercept worldwide communications for them. In this instance, national authorities have imposed rules on these private providers, so that they deliver information that governments rely on to provide national security. In short, policy instruments vary.

Despite widespread empirical evidence of this variation, complexity and contestation, most analyses of global security have—implicitly or explicitly—remained wedded to the established notion of the Westphalian state, which monopolizes the political authority to make collectively binding decisions about security and draws on vast state capacities for their autonomous implementation (Brooks, 2005; Huntington, 1957; Paul & Ripsman, 2010). As a consequence, scholars lack adequate tools to re-conceptualize and empirically map the variation in contemporary security policy-making. We seek to fill this conceptual gap by arguing that various types of security states, constituted by distinct configurations of authority foundations and policy instruments, co-exist in different polities and fields of security. We provide a novel typology that helps to capture the contested complexity in the making of security in advanced Western democracies. By combining the distinctions between political and epistemic authority as well as between capacities and rules (as policy instruments), we conceptualize *four different ideal-typical security states*: (i) positive, (ii) managing, (iii) technocratic, and (iv) regulatory. This allows mapping the making of security in different *polities* and different *fields* at different *points in time*. To back up our conceptual arguments, we draw on illustrative examples, suggesting how our typology can help to approach sectoral, cross-country, and intertemporal variation in various security states.

Our reconceptualization makes three contributions. First, it adds to regulatory governance theory (Abbott et al., 2017, 2020; Genschel & Zangl, 2014; Jordana & Levi-Faur, 2004; Lavenex et al., 2021; Levi-Faur, 2005; Majone, 1994, 1997; Vogel, 1998). On the one hand, introducing insights from regulatory governance scholarship to the domain of global security helps to shed light on important but insufficiently understood variation in (i) the foundations of authority and (ii) the prevailing policy instruments for security policy-making. On the other hand, we theoretically advance regulatory governance approaches. Existing scholarship has usually considered particular authority foundations and particular policy instruments in implicit conjunction (Abbott et al., 2020; Genschel & Jachtenfuchs, 2013, 2023; Krahmann, 2008, 2017; Leander, 2005). By contrast, we differentiate between both analytical dimensions and demonstrate their distinct importance. Different alignments on these two dimensions suggest different types of statehood. The type that is most distant from the traditional Westphalian state—the regulatory security state—only prevails when epistemic authority is linked to regulatory policy instruments. Second, our typology of security states also contributes to the research program on weaponized interdependence and "new economic statecraft" (Farrell & Newman, 2019, 2023) by studying the interplay between sub-systemic types of security states and the systemic conditions of weaponized interdependence. Third, our differentiation of the Westphalian state into security states opens up productive empirical-analytical research avenues regarding the causes of variation in types of security states as well as of shifts from one type to another.

In the remainder, we first distinguish two major authority foundations for making security. Second, we show that, besides the employment of state capacities, the promulgation of rules to manage non-state actors can be another prevailing policy instrument for making security. Based on our conceptualization of possible variation on these two key dimensions, we suggest a differentiation of the uniform Westphalian state into different types: positive, managing, technocratic, and regulatory security states. We lay out their attributes and illustrate them with evidence from a core domain of security policy, that is, the use of military force. We conclude by explicating the value-added of our typology for several research avenues.

2. Variation in authority foundations

The first major variation in how states provide security refers to different authority foundations: *who* predominates in the process of policy-making and *why* are these actors recognized to make collectively binding decisions? Our approach to these questions draws on David Lake's notion of relational authority that "arises from an exchange between governor and governed in which A provides a political order of value to B sufficient to offset

the loss of freedom incurred in his subordination to A, and B confers the right on A to exert the restraints on his behavior necessary to provide that order" (Lake, 2010, pp. 595–596; see Abbott et al., 2020). By contrast to formal-legal notions of authority, a relational understanding starts out from this exchange relationship between the ruler and the ruled. Control is traded against order. Relational authority, then, serves as the common ground for more specific forms of authorities, which reflect two distinct answers to the *who*- and *why*-questions.

First, states may draw on political justifications to make security policy, such as using military force (Zürn, 2018, p. 51). In this case, the source of governments' ("who") authority is the recognized claim that they are in the rightful institutional position to make collectively binding decisions on how to protect community members from security threats. The governed accept this claim to authority to the extent that they accept the need for collectively binding decisions to promote order and to the extent that they recognize the institutional position of the governor as the one who *ought* to make such decisions ("why"). From this follows that political authority primarily rests on political entitlement and procedural legitimacy (Tallberg & Zürn, 2019, p. 594). Those in power can make security policies because they have reached this position in accordance with widely accepted procedures (e.g., democratic elections) (Genschel & Zangl, 2014; Majone, 1997; Scharpf, 1999).

Second, states may also draw on expertise or even enlist expert bodies ("who") to make security. The source of the epistemic authority of experts is the recognized claim that experts are most competent to produce a security-relevant good or a standard of behavior and, thus, political order ("why") (Esterling, 2004; May & Koski, 2013; Sending, 2015). While elected policy-makers may remain formally in charge of making policies, they as well as the governed accept experts' claim to authority to the extent that they acknowledge the experts' superior knowledge (Bode & Huelss, 2023; Dunn Cavelty & Smeets, 2023; Haas, 1992; Slayton & Clark-Ginsberg, 2018). This form of epistemic authority, then, rests on substantive legitimacy, that is, the perceived effectiveness of policy-making (Majone, 1997; Rietig, 2014; Scharpf, 1999). Those in power make and justify security-relevant policies on the promise that these policies are based on superior expertise, thus outperforming alternative suggestions (Abbott et al., 2020; De Silva & Holthoefer, 2023; Grassiani, 2018; Tanczer et al., 2018).

We thus suggest that epistemic authority prevails when governments defer to the authority of experts to make security. Political decision-makers' deference to experts implies, on the one hand, that experts have institutionally guaranteed access to policy-making and possess considerable independence from political interference (i.e., their institutional basis of epistemic authority). On the other hand, widely accepted justifications for policies are based on evidence-based, "expertocratic" reasoning (i.e., their discursive basis of epistemic authority). Epistemic authority prevails if institutional prerogatives for experts and their discursive dominance extend beyond the problem definition and agenda setting phases of the policy cycle, where experts have always provided their input (Lasswell, 1956; Sabatier, 1978; Weible & Sabatier, 2018), to the decision-making and implementation phase. Full delegation of decision-making power to expert bodies is a strong indication of epistemic authority, but the latter is also prevalent when political decision-makers cannot ignore the advice of experts for functional or legitimacy-related reasons. Orders rest on epistemic authority as long as key stakeholders recognize experts' claim to knowledge and competence.

Yet, we also suggest that experts' promises of superior effectiveness will not necessarily be fulfilled. Knowledge claims may be informed by political or economic self-interest, they may be contested, and they are often intertwined with unequal material power positions that privilege some knowledge claims at the expense of others (Slayton & Clark-Ginsberg, 2018). Whose expertise and knowledge claims count is often part of political contestations and struggles (Dunn Cavelty & Smeets, 2023). Orders based on expertise are neither politically neutral nor necessarily geared toward actually serving the common good (Bode & Huelss, 2023). Corporate experts, such as big-tech companies may capture the policy-making process through a combination of their expertise and their material-structural power—at the detriment of effective and legitimate policies (Obendiek & Seidl, 2023). In short, orders based on epistemic authority are no ideal(ist) panacea for security policy-making.

While our conceptual disentanglement of *Leviathan* on its home turf challenges the uniform notion of the Westphalian state as a monopolist of authority, it corresponds to numerous empirical observations (see Avant & Haufler, 2018). For instance, multi-actor networks and "security assemblages" are engaged in benchmarking and so-called evidence-based making of security (Abrahamsen & Williams, 2010). These experts are enlisted to produce superior outcomes and thus allegedly better security at a lower cost. While governments remain formally in charge, they need to "sell" security policies to their constituencies on the basis of expertise. In military

contracting, oversight bodies of experts are involved in monitoring outsourcing efforts in military operations (Kruck, 2020). They often work at arm's length from elected politicians, and decisions are routinely taken on the basis of experts' advice (Krahmann, 2010; Leander, 2005).

Deviations from the state as a monopolist security supplier, which relies on political authority, are the more pronounced, the more we turn to historically less established forms of security policy such as the protection of the digital space. Technological innovation provides manifold opportunities not only for distinct actors ("who"), but also for different justifications for governing ("why") (Tanczer et al., 2018; Weiss, 2018). More specifically, the "technification" of the digital domain makes epistemic claims prevail over competing arguments (Maurer, 2018; Obendiek & Seidl, 2023; Owen, 2015). Governments enlist technical experts for their advice so that "the legitimacy granted to experts and the epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown" (Hansen & Nissenbaum, 2009, pp. 1166–1167). This technification not only entitles expert actors on the basis of their superior knowledge, but also expands the scope of their expert claims (Slayton, 2020, 2021).

In sum, the foundations of authority—and, therefore, the answers to the *who*- as well as the *why*-question about making security—vary. In real-world processes of security policy-making, political and epistemic authority often co-exist and may even reinforce each other. Nonetheless, we may fruitfully ask whether security policies in a particular polity and field are made primarily on the basis of decision-makers' political entitlement and procedural legitimacy, or whether democratically elected governments defer to the epistemic authority of experts. The second scenario becomes the more empirically prevalent, the more we move beyond historically established fields of military security.

3. Variation in policy instruments

A second major variation relates to *how* states make security. In line with regulatory governance approaches that study other issue areas (Braithwaite, 2000; Jordana & Levi-Faur, 2004; Levi-Faur, 2005; Majone, 1994, 1997), we differentiate between two policy instruments: States may employ their own coercive capacities, or they may set regulatory incentives for other non-state actors to make security.

First, states may draw on their own capacities to respond to security threats (Huntington, 1957; Tilly, 1975). Beyond extractive and administrative capacities, coercive capacities comprise the standing action resources manifested in the armed forces, the police, and the intelligence services (Genschel & Jachtenfuchs, 2023; Hanson & Sigman, 2021; Skocpol, 1985). Capacities-based governance relies on unilateral command-and-control, which allows state institutions to autonomously implement their policies (Bruin, 2020; Paul & Ripsman, 2010). In the traditional notion of the Westphalian state, the build-up and direct use of coercive state capacities takes clear precedence over employing other policy instruments in making security (Genschel & Zangl, 2014).

Second, states may draw on rules and rely on indirect modes of security provision involving non-state actors. This includes legislative, bureaucratic-administrative, and judicial rule-making and rule implementation in national and transnational settings.[2] These rules incentivize intermediary third parties, which states try to nudge into making security in line with their interests (Abbott et al., 2017, 2020; Avant, 2004, 2005; Jordana & Levi-Faur, 2004; Schilde, 2023; Weiss & Jankauskas, 2019). On the one hand, *general* rules, such as legislative acts, are directed at a broad range of addressees and apply to all of them in the same way. Given their general scope and applicability, these prescriptions have a widespread impact, but usually provide their addressees with some leeway in how to implement them (Herr, 2021). On the other hand, states may also regulate by setting *specific* rules and criteria through contracts, as illustrated by the contractual privatization of state-owned security suppliers (Markusen, 2003; Weiss, 2021). Their specific nature limits the diffusion of these rules, but they exert a more direct influence on the contract party. The implementation of rules is, thus, monitored more tightly.

Similar to the potential repercussions of epistemic authority, indirect rules-based governance may also facilitate capture of the policy-making process by non-state actors. Private actors may use their economic resources and their structural power position in indirect security policy-making to pursue their particularistic economic or political interests rather than the common good (see Carpenter & Moss, 2013). In fact, indirect rules-based governance often comes with the promise of more efficient governance but with the risk of states' losing control to private actors over the policy-making process and its outcomes (Abbott et al., 2020). By contrast, the migration management literature has pointed out that non-state entities may also be co-opted by state actors, turning into

"hand-maidens" of the state that enhance state authority and maneuver (see Lahav, 1998; Lori & Schilde, 2021; Torpey, 2000).[3]

Independent from its consequences on state control, rules-based security policy-making is at odds with the uniform notion of a Westphalian state that primarily draws on its own coercive capacities to make security. Nonetheless, it is an empirical reality in contemporary security policy-making. For instance, given that most advanced democratic states do not autonomously produce military goods and services (Kruck, 2014; Weiss, 2021), a diverse set of private actors is involved in the preparation and use of armed force (Avant & Haufler, 2018). The more security is made by markets, the more rules proliferate to (re-)regulate private actors (see also Vogel, 1998). Governments buy military goods from privately owned companies, regulate their exports, and hire private contractors to maintain the weapons in question: "Without contractor support, the United States would not be able to arm and field an effective fighting force" (Schwartz et al., 2018, p. 1).

Rules-based security policy-making is the more pronounced, the more we turn to those domains, where governments lack own capacities and hardly have any choice but to draw on third parties that help them design and implement policies. An example is states' attempt to secure cyberspace, where most states lack the option of capacity-based approaches. Governments need to collaborate with telecommunication companies to protect hardware, and also with firms that control the exchange of information (e.g., search engines, cloud services) (Glen, 2018, pp. 121–142; Harris, 2014, pp. 134–135). They thus turn to a more indirect provision of digital security, relying on private actors and their regulation (Boeke, 2018; Weiss & Jankauskas, 2019).

To sum up, rules-based security policies may not only supplement states' capacities-based governance, as has often been the case. They may even to a large extent substitute for states' reliance on their own coercive capacities.[4] Independent from the general or specific nature of rules, states may "steer" the making of security, while non-state actors take over the "rowing", that is, provide capacities that states lack (Braithwaite, 2000; Jordana & Levi-Faur, 2004; Levi-Faur, 2005). Indirect provision of security empowers third parties in general and private actors in novel domains of security in particular. Not only the *who* and *why*, but also the *how* of providing security varies in contemporary security policy-making.

4. A typology of security states

We argue that these variations in the foundations of authority and in prevailing policy instruments are not only relevant in their own right, but that considering the former *in conjunction* with the latter allows us to conceptually grasp and empirically study the differentiation of *the* Westphalian state into *different types of security states*. Such conceptual efforts help to map the "contested complexity" in contemporary security policy-making and allow us pointing out distinct logics of how states provide security in the 21st century.

The main objective of our typology of security states is to capture the prevailing type of security state in a given polity and in a particular field of contemporary security politics. To be sure, we may also ask whether a particular polity—a sovereign state or an international organization such as the EU[5]—*in toto* is predominantly a regulatory security state or another type. Yet, more frequently, it will be fruitful to study whether a polity is a particular type of security state with regard to a *specific policy field* of security. This implies that a given polity—such as a sovereign state or an international organization—can be a regulatory security state in one policy field, but a positive security state in another.

Our two dimensions constitute ideal-typical distinctions that may overlap in practice. Any security state in the real world may, for instance, rely on a mix of political and epistemic authority as the foundation for its exercise of power. Similarly, any security state in the real world may employ a combination of capacity and rules in order to pursue policy objectives. No real-world security state has ever been completely autarchic; no security state has fully abandoned state capacity and draws solely on rules in its effort to provide security. Moreover, some combination of epistemic and political authority as well as of rules-based and capacity-based governance may be necessary to provide effective and legitimate security policies (Genschel & Jachtenfuchs, 2023).

Yet, our goal is not to provide a recipe for effective and legitimate security statehood. We seek to capture distinct logics of how states *do* make security rather than how they *should*. We claim that our ideal-typical distinctions will help to better map the observable variation in contemporary security policy-making. On their basis, we can answer questions such as: Which type of security state is *prevailing* at a particular point in time, within a

specific polity, and in a particular field of security? Which type of authority and policy instrument is *predominant* at a given point in time? Is the relative importance of one type of authority or policy instrument *increasing relative* to the other? How does the predominant type of security state vary across different *fields of security*? Our conceptual distinctions enable us to study not only variation across states and fields, but also allow us approaching the question of continuity and change. Ultimately, we seek to disentangle *Leviathan* on its home turf.

To do so, we combine the distinctions between political and epistemic authority and between capacity and rules to build four types of security states: (i) positive, (ii) managing, (iii) technocratic, and (iv) regulatory (see Fig. 1). The different types capture significant variation in *who* governs security, by what *means*, and on what *justificatory grounds*. To demonstrate the empirical applicability of our typological categories, we not only introduce the abstract characteristics of the four types but further specify observable indicators for the domain of using military force, which is conventionally regarded as *the* core domain of security policy (see Table 1). Therefore, it constitutes a hard case for our claim that the Westphalian state is differentiating into different types. If we can point to empirical indications that suggest we find different types of security states even in the domain of "use of military force," we should expect to find them even more so in less traditional domains of security, such as the protection of digital critical infrastructures or individual human security. Therefore, we illustrate the four security states with examples from different countries and fields, which are all situated in the broad domain of use of military force. These empirical instances exemplify our abstract concepts and support our overarching claim about the differentiation of the Westphalian state in the making of security.

First, the *positive* security state (PSS) is the classical security state (Huntington, 1957) that is still taken for granted by most scholars of global security (Bruin, 2020; Gilli & Gilli, 2019; Paul & Ripsman, 2010). When scholars refer to the Westphalian security state, they normally have a PSS in mind. We do not dismiss its continued relevance. However, we do claim that a narrow and exclusive notion of the PSS is no longer adequate as it discounts the growing empirical prevalence of the other three types. The PSS draws on political authority and nationally owned and controlled coercive capacities to produce security-relevant collective goods itself. In the PSS, state actors effectively claim the exclusive right to govern security matters based on their recognized institutional position as rightful political authorities. At least in the liberal constitutional state, this political entitlement stems from democratic procedures and involves legal constraints (Lake et al., 2021). The PSS relies on state capacities as key policy instruments to pursue security goals.

When it comes to the use of military force, the PSS builds up, sustains, and directly employs vast coercive state resources in the form of large standing armies and state-owned defense industries. The means of force are in the hands of bureaucratic institutions and the state conducts all vital military activities on its own and without significant involvement of non-state actors. It exercises command and control over the armed forces and directly controls the provision of the means of force (Huntington, 1957; see also Montgomery, 2020; Narang, 2017). For example, *India's* defense sector, esp. when it comes to the *provision of the means of force*, can be considered such a PSS. The Indian state has even preferred government-to-government imports of weaponry rather than

Four types of security state		***Policy instrument***	
		Capacities	Rules
Foundation of authority	Political authority	**I) Positive security state (PSS)**	**II) Managing security state (MSS)**
	Epistemic authority	**III) Technocratic security state (TSS)**	**IV) Regulatory security state (RSS)**

FIGURE 1 Four types of security states.

exploiting the numerous market advantages of government-to-firm deals (Weiss, 2019, pp. 571–574). Political authorities in India justify their exclusive right to make decisions over the provision of the means of force based on legal and procedural arguments. This has been firmly entrenched in the historical set-up of India's civil-military relations (Cohen & Dasgupta, 2010). Politically accountable actors and institutions have for long governed the production of force in a statist mode of governance.

Second, the *managing* security state (MSS) bases its claim to govern on political authority, just as the PSS does. Politically accountable actors assert and justify the bindingness of their decisions with the claim that they are in the rightful institutional position and act in the interest of the common good. They are recognized as the ones who *ought* to make collectively binding decisions. However, in contrast to the PSS, the MSS relies more strongly on rules and the enlistment of non-state actors rather than on its own capacity as a key policy instrument (Genschel & Zangl, 2014). Therefore, a large number of—often powerful and sometimes competing—non-state actors is involved in the production of the means of force and their use.[6] The role of the security state is focused on coordinating, overseeing, steering and most importantly regulating the governance contributions of non-state actors (Genschel & Zangl, 2014; Jordana & Levi-Faur, 2004; Levi-Faur, 2005). Political authorities indirectly control the use and means of force through the promulgation and enforcement of rules.

In the domain of use of military force, the MSS features lean armies and bureaucracies, as most defense and security industries for military goods and services are privatized. State actors strongly rely on private contractors as non-state contributors of indirect governance (Kruck, 2014, 2020), while both general and specific rules to govern their relations proliferate. Western European allies of the United States in so called "nuclear sharing" arrangements in the context of NATO provide an example of this type, as states such as Germany or Italy heavily rely on the contributions by private defense contractors and their regulation when they fulfill their countries' responsibilities in the nuclear sharing arrangement with the United States. While the production, maintenance, and modernization of nuclear force capabilities as such follows a PSS regime, the potential delivery systems (e.g., fighter aircraft) of Western European partner states in nuclear sharing are neither developed nor produced by those countries' state capacities, but by private entities according to certified requirement schemes.

As a consequence, states such as *Germany* and *Italy*, which are involved in the field of *nuclear sharing*, are MSSs, as they heavily draw on non-state providers of security services, such as defense contractors rather than state-owned laboratories or state-run arms manufacturers. Moreover, nuclear sharing arrangements have a strong regulatory component, as they are not only characterized by specific rules between public and private actors that govern their economic exchange relations, but they also depend on general rules, such as technical standards and certification schemes.[7] Thus, political decision-makers in partner states involved in nuclear sharing rely on rules for private commercial actors to make nuclear sharing work. At the same time, states do clearly not defer to non-state experts' authority in making decisions about nuclear force. Rather, as typical of MSSs, they mainly retain hierarchical control over non-state providers of security. Reaffirming their political right and prerogative to decide over nuclear force, state actors effectively call the shots while collaborating with private actors as instruments for the pursuit of their political goals.

Third, the *technocratic* security state (TSS) bases its claim to exercise authority on expertise, while using capacity-based instruments. In this type of security state, the possession—or attribution—of expertise, which is claimed to lead to better performance and more effective security policies at a lower cost, is the key foundation of authority. Whereas the PSS is characterized by a high level of centralization, a unified and generalist civil service, and expansive hierarchical bureaucracies, the TSS relies more heavily on specialized expert agencies and expert commissions operating at arm's length from central government (Dunn Cavelty & Smeets, 2023; Hansen & Nissenbaum, 2009, pp. 1166–1167; Rittberger & Wonka, 2013). However, much like the PSS, the TSS draws on capacities. It builds up and further enhances its own capacities for the direct production of collective security goods. Where experts from both public and private sides are involved in policy-making, private experts largely remain under hierarchical state control (Slayton & Clark-Ginsberg, 2018), and state actors seek to keep or insource crucial capabilities.

In the domain of use of military force, specialized expert institutions *within* the TSS directly shape the use and means of force rather than primarily relying on non-state actors' contributions. Take the example of the *UK*

in the field of *intelligence*, in general, and crisis warning, in particular (Meyer et al., 2020, pp. 56–57). The UK has built strong state capacities in the form of specialized resource-strong intelligence agencies. They are located within the state apparatus—rather than being outside of it as would be typical of an MSS. At the same time, their expert authority does not replace but supersedes the political authority of elected decision-makers in the UK to make authoritative calls about crises. While the intelligence experts in the competent British state agencies do not always successfully persuade political decision-makers, the latter face severe difficulties to ignore their advice. The reason is that these intelligence experts normally justify their right to shape decisions over the use of force in terms of superior knowledge and performance in "warning about war" rather than political entitlement and democratic procedures (Meyer et al., 2020). As a consequence, resource-rich "expertocrats" from within the state apparatus govern the provision of intelligence about (and for) the use of force.

Fourth, the *regulatory* security state (RSS) relies on epistemic authority as its main foundation and employs rules as the predominant policy instrument for achieving its security goals. It is legitimated by claims to expert knowledge by both private actors and state regulators. Independent expertise thus serves as the basis for making binding decisions on the use and the means of force (see Majone, 1997, p. 154). The RSS is characterized by the proliferation of public, private and hybrid security actors and institutions with a specialization in a fairly narrow range of policy issues. These diverse actors may have both converging and diverging interests, ranging from the pursuit of national security to pecuniary economic concerns and the consolidation of political power. Thus, the level of contested complexity is arguably highest in the RSS.

Multi-actor networks and "security assemblages" (Abrahamsen & Williams, 2010; Tanczer et al., 2018) complement and partly even replace the generalist bureaucracy prevailing in the PSS with its bureaucratic command-and-control mode. The RSS employs—general and specific—rules to incentivize and manage governance contributions from non-state actors. Regulation is key for state actors who will regularly have to worry about private intermediaries pursuing their own economic or political agendas the more assertively, the more indispensable they become for the state in indirect governance (Abbott et al., 2020; Kruck, 2020). Thus, rule-making and rule-enforcement, rather than the autonomous build-up of capacities, are key priorities and activities of the RSS (Majone, 1997, pp. 143–144; see also Weiss, 2021). Formal contracts and contractual legal obligations govern public–private coordination.

With regard to the domain of use of military force, state institutions of the RSS heavily rely on non-state actors to support and conduct warfare. They employ legal contracts, rules, and litigation with private security providers to safeguard ultimate state control over the use of force. Yet, unlike in the MSS, non-state actors are not mere vehicles of decision-makers' political authority but, due to their expert authority, recognized co-producers of decisions and activities related to warfare. Consider middle powers, such as *Germany*, but also the superpower *United States* in the field of *cyber warfare* as an example of RSSs: In these polities, "the private sector is not a 'partner' of government, but the 'supported command'" (Healey, 2013, p. 25), when it comes to cyber warfare. As political actors, such as democratically elected governments, have been latecomers in cyberspace, this has guaranteed private companies a comparative advantage in setting the rules of the game and acquiring epistemic authority in this field: "Cybersecurity differs from most other security fields in that a private market for cybersecurity services and tools already existed by the time governments really started to consider cyberspace a domain for military operations" (Maurer, 2018, p. 71).

Such a powerful position of private corporate experts, which, together with a strong reliance on rules- rather than capacities-based governance, characterizes the RSS, applies not only to middle powers, such as Germany, but even to those state actors that are considered to be the most powerful ones in setting the rules of cyberspace. The US National Security Agency (NSA) "is dependent on corporations that build software and hardware and that own and operate portions of the Internet. The agency would find itself generally out of the surveillance and cyber warfare business without the cooperation of these companies" (Harris, 2014, p. 88). In other words, private digital experts have acquired the authority to shape the rules and thus the conduct of cyber warfare in the United States and most democratic military powers.

Table 1 summarizes key observable attributes of the four types, in particular for the domain of use of force. We highlight commonalities and differences across the different types. This helps to designate in empirical research the (ideal-)type of security state to which a real-world entity most closely approximates in a particular field of security.

TABLE 1 Attributes of different types of security states

	I) Positive security state	II) Managing security state	III) Technocratic security state	IV) Regulatory security state
Who makes security decisions?	Political actors are in charge and have direct control over large standing armies, numerous and generalist bureaucratic staff, and state-owned defense industries.	Political actors are in charge and largely have control over lean armies and bureaucracies, as most defense and security industries for military goods and services are privatized.	Though political actors remain formally in charge, they have difficulty in deciding against advice from public experts. De facto, specialized expert agencies within the state control decision-making.	Though political actors remain formally in charge, expertise gaps and the institutional independence of expert bodies render them unable to act against public and private experts' advice. De facto, experts control complexes of specialized (public, private and hybrid) institutions.
Why are actors recognized to make these decisions?	Those in charge procedurally justify their right to make security decisions on the basis of their institutional position that rightfully empowers them to do so. They stress the monopolist nature of their political authority.	Those in charge procedurally justify their right to make security decisions on the basis of their rightful institutional position. Yet, the importance and influence of non-state contributors is widely accepted.	Specialized expertise and expected performance justify the right to shape effective decisions, which remain the formal responsibility of elected politicians.	Superior expertise, the expectation of effective decisions and thus performance claims justify the right to impose collectively binding security decisions, even if those are still formally taken by elected politicians.
How do state actors govern warfare?	State actors themselves deploy coercive capacities in the form of operational resources without significantly involving non-state actors.	Both general and specific rules proliferate. State actors rely on non-state contributors to warfare, but hierarchical control is maintained.	State actors consult with private experts, but private expertise is hierarchically controlled by the state. Expert agencies within the state serve as operational resources; rules are secondary.	General and specific rules predominate. Conflicts over their enactment are resolved by litigation. State actors strongly rely on non-state contributors based on contractual relationships.

5. Conclusion: What can we learn by moving from "*the*" Westphalian state toward *types* of security states?

This paper has shown that making security may rely on epistemic as well as political authority and on capacities as well as rules. Taking empirically observable variations in authority foundations and policy instruments seriously requires overcoming the notion of a uniform Westphalian state and replacing it with a new conceptual vocabulary of different types of security state. We argue that this typology is analytically productive because it opens up new research avenues for explaining variation in the making of security policies. It also advances the prominent research program on "new economic statecraft" by specifying the domestic institutional foundations for weaponized interdependence (Farrell & Newman, 2019, 2023). Furthermore, its conceptualization of epistemic authority advances research on regulatory governance by conceiving of it as a distinct constitutive dimension of particular security states.

First, our typology paves the way for a systematic study of the causes of the emergence of PSSs, MSSs, TSSs, and RSSs. This may include cross-country or cross-regional analyses of global trends and divergent patterns in the prevalence of different types; cross-sectoral explanations of commonalities and differences across fields of security; or the tracing of continuities and disruptions in the emergence of security states over time. While our

main ambition in this article is conceptual, we consider particular structural drivers as promising first cuts for theorizing variations in types of security states and shifts from one type to another.

Technological change has historically challenged existing patterns of how to provide security (Bode & Huelss, 2018; Horowitz, 2010; Weiss, 2018). Ceteris paribus, technological innovation increases the relevance of epistemic authority in policy-making. For example, the advance of information technologies has created an enhanced demand for technical expertise in security states (Dunn Cavelty & Wenger, 2020). When political actors are responsible for, but hardly capable of, mitigating threats arising from technological innovation, they will empower more competent experts (Abbott et al., 2020) inside the state or enlist expertise from outside the bureaucratic apparatus.

Besides technological innovation, different types of security pressures might invite different ways of organizing the provision of security policies (Genschel & Jachtenfuchs, 2023; Kelemen & McNamara, 2022). Ceteris paribus, we would expect that direct military threats foster the build-up of coercive state capacities. Moreover, the presence of a direct military threat should also bolster the political authority of decision-makers via the creation of mass support. By contrast, when facing diffuse security risks, state actors will be more inclined to rely on incentivizing and regulating contributions from non-state third parties specialized in addressing these risks, while deferring to their expert judgment (Weiss & Biermann, 2022; Weiss & Jankauskas, 2019).

However, public and private security actors may interpret and politically channel technology- and threat-driven demands in different ways. The supply of different security states will be shaped by varying interest and power constellations, institutions, and prevailing ideas (Hall, 1997; Hay, 2004; Majone, 1997; Moe, 2019; Thatcher & Stone Sweet, 2002). Our typology enables in-depth theoretical and empirical investigations into the *politics* of security state reforms. Different types of security state entail distinct winners and losers, who will fight for the realization of their varying preferences and ideas. Different groups of actors—political decision-makers, bureaucracies, specialized agencies, non-state experts, business actors, and others—will push for distinct designs of the security state, which are conducive to their respective interests and reflect their ideas. They will promulgate different definitions of threats and varying conceptions of adequate policy responses. Therefore, one may theorize that the type of security state resulting from discursive struggles and "quiet politics" depends on those actors' interests that are able to deploy superior bargaining and discursive power.

Our second main contribution is that our typology sheds light on how different types of states are associated with the systemic conditions of weaponized interdependence. Scholars of the "new economic security state" (Farrell & Newman, 2023) have identified the security consequences of global economic networks, when "some states are able to leverage interdependent relations to coerce others" (Farrell & Newman, 2019, p. 45; see also Drezner et al., 2021). Our typology of security states facilitates research on how, on the one hand, different types of security states may drive—or constrain—the emergence of weaponized interdependence; and how, on the other hand, exposure to weaponized interdependence may shape security state reform in targeted states toward different types.

Globalization is the driving force behind the formation of powerful economic networks of private actors, which, in turn, can be manipulated and used by states for political coercion. Whereas weaponized interdependence research has so far highlighted the structural effects of globalization on the rise of networks of powerful private actors, we can specify important sub-systemic conditions that enable or constrain the emergence of these networks in the first place. Different types of security states will be more or less inclined toward employing strategies of weaponized interdependence (Bach & Newman, 2007). The PSS primarily engages in more traditional strategies and tactics of asymmetric interdependence, as we know them from the classical literature (Keohane & Nye, 1973). Power is important; yet, it is mostly exercised in direct and often bilateral ways between states. By contrast, the more global security issues are governed by states relying on expertise and rules, the more a network constellation may evolve and the more network effects (e.g., chokepoints) may become conceivable.

Thus, the TSS and, in particular, the MSS and the RSS drive the emergence of weaponized interdependence. They all empower experts and non-state actors so that the network effects theorized by weaponized interdependence become conceivable. TSSs promote the creation and expansion of transnational and transgovernmental networks of experts (i.e. agencies). The rules these networks make and spread globally are an important source of state power as they reflect and promote different states' interests to different degrees (Büthe & Mattli, 2011). The MSS typically promulgates politically motivated regulation and standardization via non-state intermediaries, which are particularly prone to network effects. Given the combination of powerful

non-state actors and rule-setting with great potential for economies of scale, the RSS is particularly conducive to the emergence of networks, which, in turn, provide manifold opportunities for weaponized interdependence. Take the prominent SWIFT (i.e., Society for Worldwide Interbank Financial Telecommunication) network under Belgian law as an instance of how the RSS subsumes formerly economic sectors under a security logic. Control over SWIFT basically allows to cut states off from the global financial settlement system. The combination of rules-based governance and epistemic authority has helped to convert these forces of globalization into a political weapon, which has been heavily employed by the United States and the EU to compel Russia in the context of its 2022 invasion of Ukraine (Sanger & Crowley, 2021; Shalal et al., 2021).

Our typology also invites theoretically and politically important research on how security states may *respond* to pressures from weaponized interdependence. When a state, in a particular field, is facing another state's use of networked coercion, how will it try to cope with this? On the one hand, the state may try to re-shape control over global networks in a way that provides the state with more leverage over the networks. Seeking to improve its own ability to use networked coercion, the state may also reform its domestic institutional structures in a way that is conducive to its exercise of weaponized interdependence. Previous literature on global market governance suggests that the RSS is particularly well positioned to employ—and deal with—networked coercion (Bach & Newman, 2007) due to its proficiency in indirect, rules-based governance as well as its strong public-private ties to business actors. This would imply that pressures from weaponized interdependence in particular fields and polities will reinforce the emergence of RSSs in these fields and countries as they try to get more competent at playing the game of weaponized interdependence.

On the other hand, states may respond to the expected deployment of weaponized interdependence by trying to isolate themselves from harmful global networks. Reducing dependence on global business networks, for instance in the trade of semi-conductors, suggests enhancing the security state's own autonomous capacities, for example, in the production and maintenance of critical digital infrastructures. Thus, efforts to withdraw from global networks and become more self-sufficient may spark reform toward the PSS as the targeted states try to (re-)build the capacities for playing a different kind of game. Future research could fruitfully explore under what conditions states' expected exposure to weaponized interdependence will spur reform toward the RSS (i.e., enhancing states' ability to employ networked coercion) or the PSS (i.e., enhancing states' ability to evade networked coercion).

Third, disentangling "the" security state into different types not only contributes to research on weaponized interdependence and allows for a better understanding of the contested complexity in contemporary security policy-making. It also contributes to advancing regulatory governance theory. We conceptualize the role of experts in a normally contested issue area as a constitutive attribute of particular types of security states and thus separate it conceptually from regulation as a policy instrument. On the one hand, this highlights that expertise-based governance does not have to be rules-based governance as epistemic authority may also combine with capacities in a TSS (e.g. within intelligence agencies). Yet, the independence of experts in TSSs is different than what we know about experts in other policy fields that regulatory governance scholars have analyzed (e.g., Benish & Levi-Faur, 2020; Guidi et al., 2020): TSSs regularly preserve some hierarchical control over their capacities. On the other hand, our conceptualization emphasizes that an RSS is not only constituted by the predominant use of rules as policy instrument, but that reliance on epistemic authority is also necessary for this mode of making security in a complex and contested policy domain (Bode & Huelss, 2023; Obendiek & Seidl, 2023). In the RSS, *Leviathan* not only employs rules, it also defers to security experts.

Acknowledgments

For comments on earlier versions of this paper, we thank Felix Biermann, Michael Blauberger, Myriam Dunn Cavelty, Philipp Genschel, Tim Heinkelmann-Wild, Gunther Hellmann, Markus Jachtenfuchs, David-Levi-Faur, Yagnyashri Kodaru, Markus Kornprobst, Hugo Meijer, Katharina Meissner, Jeremy Richardson, Berthold Rittberger, Chiara Ruffa, Andrea Schneiker, Lorenz Sommer, Bernhard Zangl, and Eva Ziegler. We are also grateful to the contributors of our 2023 *JEPP* special issue on "The Regulatory Security State in Europe" as well as the participants of panels at the Academic Convention of the German Political Science Association (DVPW, online, 2021), the 11th Biennial Conference of the SGEU in the ECPR (Rome, 2022), the Annual Conference of the European Initiative for Security Studies (Berlin, 2022), the Conventions of the International Relations

(Friedrichshafen, 2023) and Political Economy (Berlin, 2022) Sections of the DVPW, the colloquium of the DVPW's Foreign and Security Policy Group (online, 2021) and research colloquia in Munich, Salzburg and Odense for their feedback. Kathrin Will, Aliaa Aly, Maya von Ahnen, and Simon Zemp provided excellent research assistance. We gratefully acknowledge funding from the Fritz Thyssen Foundation (project "The Making of National Security: From Contested Complexity to Types of Security States," Az. 10.23.2.001.PO). Open Access funding enabled and organized by Projekt DEAL.

Conflict of interest statement

The authors declare no conflicts of interest.

Data availability statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Endnotes

[1] First, our understanding of *security* encompasses not only the protection of individuals and political collectivities against direct violent threats, but also safeguarding their ability to act as purposive entities in, for instance, digital spaces (see Börzel & Zürn, 2021, 293; Farrand & Carrapico, 2022; Wolfers, 1962, 150–151). Second, *making security* involves all stages of the policy cycle (Lasswell, 1956; Weible & Sabatier, 2018); however, due to our focus on authority and the ultimate choice of policy instruments we pay particular attention to the decision-making stage. Third, we conceive of *security states* as national or supranational polities that can make collectively binding decisions within a distinct security field at a certain point of time (Kruck & Weiss, 2023; see Section 4).

[2] By contrast, some scholars of regulatory governance adopt a narrower understanding of regulation as "bureaucratic and administrative rulemaking" (Levi-Faur, 2011, see also Koop & Lodge, 2017).

[3] We thank an anonymous reviewer for highlighting this point.

[4] We consider it an open question whether and when rules-based security governance is an effective and legitimate way of providing security or whether rules-based governance necessarily has to be complemented by state capacities to produce effective and legitimate policies.

[5] Our notion of *security states* applies to both national and supranational polities in which governors exchange the provision of security for the right to rule over the governed. Such "states" may be, but are not necessarily, based on national sovereignty, so that the European Union (EU) can be as much a security state as the United States or Singapore (see Kruck & Weiss, 2023).

[6] For developments in the issue area of security which we subsume under the MSS, see Avant (2005), Betz and Stevens (2011), Boeke (2018), Dunigan and Petersohn (2015), and Owen (2015).

[7] As long as NATO states, such as Germany or Belgium, seek to participate in nuclear sharing and they operate certified delivery systems, one may speak of a conventional exchange relationship between public and private actors in the use of military force. Similar to standard-setting in the world economy (Büthe & Mattli, 2011), however, rules-based governance in particular unfolds its relevance over time. Nuclear sharing is based on strict certification schemes, which critically reduces the number of available suppliers of delivery systems. It may come as no surprise then that, today, NATO's nuclear sharing countries have the choices of either buying American or engaging in highly costly certification processes with uncertain prospects to succeed both technically and legally.

References

Abbott, K. W., Genschel, P., Snidal, D., & Zangl, B. (2020). Competence versus control: The governor's dilemma. *Regulation and Governance*, 14(4), 619–636.

Abbott, K. W., Levi-Faur, D., & Snidal, D. (2017). Theorizing regulatory intermediaries: The RIT model. *The Annals of the American Academy of Political and Social Science*, 670(1), 14–35.

Abrahamsen, R., & Williams, M. C. (2010). *Security beyond the state: Private security in international politics*. Cambridge University Press.

Avant, D. (2004). The privatization of security and change in the control of force. *International Studies Perspectives*, 5(2), 153–157.
Avant, D. (2005). *The market for force: The consequences of privatizing security*. Cambridge University Press.
Avant, D., & Haufler, V. (2018). Public–private interactions and practices of security. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford handbook of international security*. Oxford University Press.
Bach, D., & Newman, A. L. (2007). The European regulatory state and global public policy: Micro-institutions, macro-influence. *Journal of European Public Policy*, 14(6), 827–846.
Benish, A., & Levi-Faur, D. (2020). The expansion of regulation in welfare governance. *The Annals of the American Academy of Political and Social Science*, 691(1), 17–29.
Betz, D. J., & Stevens, T. (2011). *Cyberspace and the state: Toward a strategy for cyber-power*. Routledge.
Bode, I., & Huelss, H. (2018). Autonomous weapons systems and changing norms in international relations. *Review of International Studies*, 44(3), 393–413.
Bode, I., & Huelss, H. (2023). Constructing expertise: The front- and back-door regulation of AI's military applications in the European Union. *Journal of European Public Policy*, 30(7), 1230–1254.
Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, 31(3), 449–464.
Braithwaite, J. (2000). The new regulatory state and the transformation of criminology. *British Journal of Criminology*, 40(2), 222–238.
Brooks, S. G. (2005). *Producing security: Multinational corporations, globalization, and the changing calculus of conflict*. Princeton University Press.
Bruin, E. d. (2020). Mapping coercive institutions: The state security forces dataset, 1960–2010. *Journal of Peace Research*, 58(2), 315–325.
Börzel, T. A., & Zürn, M. (2021). Contestations of the liberal international order: From liberal multilateralism to postnational liberalism. *International Organization*, 75(2), 282–305.
Büthe, T., & Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton University Press.
Carpenter, D., & Moss, D. A. (2013). *Preventing regulatory capture: Special interest influence and how to limit it*. Cambridge University Press.
Cohen, S. P., & Dasgupta, S. (2010). *Arming without aiming: India's military modernization*. Brookings Institution Press.
De Silva, N., & Holthoefer, A. (2023). Hidden figures: How legal experts influence the design of international institutions. *European Journal of International Relations*, 30, 52–77. https://doi.org/10.1177/13540661231210931
Drezner, D., Farrell, H., & Newman, A. L. (Eds.). (2021). *The uses and abuses of weaponized interdependence*. Brookings Institution Press.
Dunigan, M., & Petersohn, U. (Eds.). (2015). *The markets for force: Privatization of security across world regions*. University of Pennsylvania Press.
Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, 30(7), 1330–1352.
Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5–32.
Esterling, K. (2004). *The political economy of expertise*. University of Michigan Press.
Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31(3), 435–453.
Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79.
Farrell, H., & Newman, A. L. (2023). The new economic security state: How de-risking will remake geopolitics. *Foreign Affairs*, 102(6), 106–122.
Genschel, P., & Jachtenfuchs, M. (2013). *Beyond the regulatory polity? The European integration of core state powers*. Oxford University Press.
Genschel, P., & Jachtenfuchs, M. (2023). The security state in Europe: Regulatory or positive? *Journal of European Public Policy*, 30(7), 1447–1457.
Genschel, P., & Zangl, B. (2014). State transformations in OECD countries. *Annual Review of Political Science*, 17(1), 337–354.
Gheciu, A., & Wohlforth, W. C. (2018). The future of security studies. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford handbook of international security* (pp. 3–13). Oxford University Press.
Gilli, A., & Gilli, M. (2019). Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security*, 43(3), 141–189.
Glen, C. M. (2018). *Controlling cyberspace: The politics of internet governance and regulation*. Praeger.
Grassiani, E. (2018). Between security and military identities: The case of Israeli security experts. *Security Dialogue*, 49(1–2), 83–95.
Guidi, M., Guardiancich, I., & Levi-Faur, D. (2020). Modes of regulatory governance: A political economy perspective. *Governance*, 33(1), 5–19.
Haas, P. M. (1992). Introduction: Epistemic communities and international policy coordination. *International Organization*, 46(1), 1–35.
Hall, P. (1997). Institutions, interests and ideas in the comparative political economy of the industrialized nations. In M. Lichbach & A. Zuckerman (Eds.), *Comparative politics: Rationality, culture and structure* (pp. 174–207). Cambridge University Press.
Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, 53(4), 1155–1175.

Hanson, J. K., & Sigman, R. (2021). Leviathan's latent dimensions: Measuring state capacity for comparative political research. *The Journal of Politics*, 83(4), 1495–1510.
Harris, S. (2014). *War: The rise of the military-internet complex*. Houghton Mifflin Harcourt.
Hay, C. (2004). Ideas, interests and institutions in the comparative political economy of great transformations. *Review of International Political Economy*, 11(1), 204–226.
Healey, J. (2013). *A fierce domain: Conflict in cyberspace, 1986 to 2012*. CCSA.
Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. *Regulation & Governance*, 15(1), 98–114.
Hofmann, S. C. (2013). *European security in NATO's shadow: Party ideologies and institution building*. Cambridge University Press.
Horowitz, M. C. (2010). *The diffusion of military power: Causes and consequences for international politics*. Princeton University Press.
Huntington, S. P. (1957). *The soldier and the state: The theory and politics of civil–military relations*. Harvard University Press.
Jordana, J., & Levi-Faur, D. (2004). *The politics of regulation: Examining regulatory institutions and instruments in the age of governance*. Edward Elgar.
Kelemen, R. D., & McNamara, K. R. (2022). State-building and the European Union: Markets, war, and Europe's uneven political development. *Comparative Political Studies*, 55(6), 963–991.
Keohane, R. O., & Nye, J. S. (1973). Power and interdependence. *Survival*, 15(4), 158–165.
Koop, C., & Lodge, M. (2017). What is regulation? An interdisciplinary concept analysis. *Regulation & Governance*, 11(1), 95–108.
Krahmann, E. (2008). Security: Collective good or commodity? *European Journal of International Relations*, 14(3), 379–404.
Krahmann, E. (2010). *States, citizens and the privatization of security*. Cambridge University Press.
Krahmann, E. (2017). Legitimizing private actors in global governance: From performance to performativity. *Politics and Governance*, 5(1), 54–62.
Kruck, A. (2014). Theorising the use of private military and security companies: A synthetic perspective. *Journal of International Relations and Development*, 17(1), 112–141.
Kruck, A. (2020). Governing private security companies: Politics, dependence, and control. In K. W. Abbott, P. Genschel, D. Snidal, & B. Zangl (Eds.), *The governor's dilemma: Indirect governance beyond principals and agents*. Oxford University Press.
Kruck, A., & Weiss, M. (2023). The regulatory security state in Europe. *Journal of European Public Policy*, 30(7), 1205–1229.
Lahav, G. (1998). Immigration and the state: The devolution and privatisation of immigration control in the EU. *Journal of Ethnic and Migration Studies*, 24(4), 675–694.
Lake, D. A. (2010). Rightful rules: Authority, order, and the foundations of global governance. *International Studies Quarterly*, 54(3), 587–613.
Lake, D. A., Martin, L. L., & Risse, T. (2021). Challenges to the liberal order: Reflections on international organization. *International Organization*, 75(SI 2), 1–33.
Lasswell, H. (1956). *The decision processes: Seven categories of functional analysis*. University of Maryland Press.
Lavenex, S., Serrano, O., & Büthe, T. (2021). Power transitions and the rise of the regulatory state: Global market governance in flux. *Regulation & Governance*, 15(3), 445–471.
Leander, A. (2005). The power to construct international security: On the significance of private military companies. *Millennium: Journal of International Studies*, 33(3), 803–825.
Levi-Faur, D. (2005). The global diffusion of regulatory capitalism. *The Annals of the American Academy of Political and Social Science*, 598(1), 12–32.
Levi-Faur, D. (2011). Regulatory networks and regulatory agencification: Towards a single European regulatory space. *Journal of European Public Policy*, 18(6), 810–829.
Lori, N., & Schilde, K. (2021). Muddying the waters: Migration management in the global commons. *International Relations*, 35(3), 510–529.
Majone, G. (1994). The rise of the regulatory state in Europe. *West European Politics*, 17(3), 77–101.
Majone, G. (1997). From the positive to the regulatory state: Causes and consequences of changes in the mode of governance. *Journal of Public Policy*, 17(2), 139–167.
Markusen, A. R. (2003). The case against privatizing national security. *Governance*, 16(4), 471–501.
Maurer, T. (2018). *Cyber mercenaries: The state, hackers and power*. Cambridge University Press.
May, P. J., & Koski, C. (2013). Addressing public risks: Extreme events and critical infrastructures. *Review of Policy Research*, 30(2), 139–159.
Meyer, C. O., De Franco, C., & Otto, F. (2020). *Warning about war: Conflict, persuasion and foreign policy*. Cambridge University Press.
Moe, T. M. (2019). *The politics of institutional reform: Katrina, education, and the second face of power*. Cambridge University Press.
Montgomery, E. B. (2020). Primacy and punishment: US grand strategy, maritime power, and military options to manage decline. *Security Studies*, 29(4), 769–796.
Narang, V. (2017). Strategies of nuclear proliferation: How states pursue the bomb. *International Security*, 41(3), 110–150.
Neumann, I. B., & Sending, O. J. (2018). Expertise and practice: The evolving relationship between the study and practice of security. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford handbook of international security* (pp. 29–40). Oxford University Press.
Obendiek, A. S., & Seidl, T. (2023). The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. *Journal of European Public Policy*, 30(7), 1305–1329.

Owen, T. (2015). *Disruptive power*. Oxford University Press.
Paul, T. V., & Ripsman, N. M. (2010). *Globalization and the national security state*. Oxford University Press.
Pratt, S. F. (2018). What should we make of elite American mercenaries in Yemen? *War on the Rocks*. Available from URL: https://warontherocks.com/2018/10/what-should-we-make-of-elite-american-mercenaries-in-yemen/. Accessed April 19, 2024.
Rietig, K. (2014). "Neutral" experts? How input of scientific expertise matters in international environmental negotiations. *Policy Sciences*, 47(2), 141–160.
Rittberger, B., & Wonka, A. (2013). *Agency Governance in the EU*. Routledge.
Sabatier, P. (1978). The acquisition and utilization of technical information by administrative agencies. *Administrative Science Quarterly*, 23(3), 396–417.
Sanger, D., & Crowley, M. (2021). "Greetings, Mr. President": Biden and Putin hold 2-hour virtual summit. *New York Times. Available from URL:* https://www.nytimes.com/2021/12/07/us/politics/biden-putin-ukraine-summit.html. Accessed April 19, 2024.
Scharpf, F. W. (1999). *Governing in Europe: Effective and democratic*? Oxford University Press.
Schilde, K. (2023). Weaponising Europe? Rule-makers and rule-takers in the EU regulatory security state. *Journal of European Public Policy*, 30(7), 1255–1280.
Schwartz, M., Sargent, J. F., & Mann, C. T. (2018). Defense acquisitions: How and where DOD spends its contracting dollars. https://sgp.fas.org/crs/natsec/R44010.pdf
Sending, O. J. (2015). *The politics of expertise: Competing for authority in global governance*. University of Michigan Press.
Shalal, A., Holland, S., & Osborn, A. (2021). Biden warns Putin of sanctions, aid for Ukraine military if Russia invades. *Reuters. Available from URL:* https://www.reuters.com/markets/currencies/biden-putin-set-crucial-call-over-ukraine-2021-12-07/. Accessed April 19, 2024.
Skocpol, T. (1985). Bringing the state back in: Strategies of analysis in current research. In P. B. Evans, D. Rueschemeyer, & T. Skocpol (Eds.), *Bringing the State Back in* (pp. 3–37). Cambridge University Press.
Slayton, R. (2020). Performing cybersecurity expertise: Challenges for public utility commissions. *Berkeley Technology Law Journal*, 35(3), 757–792.
Slayton, R. (2021). What is a cyber warrior? The emergence of US military cyber expertise, 1967–2018. *Texas National Security Review*, 4(1), 61–96.
Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation & Governance*, 12(1), 115–130.
Tallberg, J., & Zürn, M. (2019). The legitimacy and legitimation of international organizations: Introduction and framework. *Review of International Organizations*, 14(4), 581–606.
Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and global cybersecurity: How technical experts support science diplomacy. *Global Policy*, 9, 60–66.
Thatcher, M., & Stone Sweet, A. (2002). Theory and practice of delegation to non-majoritarian institutions. *West European Politics*, 25(1), 1–22.
Tilly, C. (1975). *The formation of national states in Western Europe*. Princeton University Press.
Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state*. Cambridge University Press.
Vogel, S. K. (1998). *Freer markets, more rules: Regulatory reform in advanced industrial countries* (1st paperback ed.). Cornell University Press.
Weible, C. M., & Sabatier, P. (2018). *Theories of the policy process* (4th ed.). Routledge.
Weiss, M. (2018). How to become a first mover? Mechanisms of military innovation and the development of drones. *European Journal of International Security*, 3(2), 187–210.
Weiss, M. (2019). From wealth to power? The failure of layered reforms in India's defense sector. *Journal of Global Security Studies*, 4(4), 560–578.
Weiss, M. (2021). Varieties of privatization: Informal networks, trust and state control of the commanding heights. *Review of International Political Economy*, 28(3), 662–686.
Weiss, M., & Biermann, F. (2022). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform*, 26(3), 250–267.
Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. *Governance*, 32(2), 259–275.
Wolfers, A. (1962). *Discord and collaboration: Essays on international politics*. Johns Hopkins University Press.
Zürn, M. (2018). *A theory of global governance: Authority, legitimacy, and contestation*. Oxford University Press.

