frontiers | Frontiers in Political Science

TYPE Conceptual Analysis
PUBLISHED 07 January 2026
DOI 10.3389/fpos.2025.1749077

OPEN ACCESS

EDITED BY
Luiz Rogério Franco Goldoni,
Brazilian Army Command and General Staff College, Brazil

REVIEWED BY
Evelyn Téllez,
INFOTEC, Mexico
Mirosław Banasik,
War Studies University, Poland

*CORRESPONDENCE
Adam Farkas
✉ farkas.adam1@sze.hu

RECEIVED 18 November 2025
REVISED 06 December 2025
ACCEPTED 08 December 2025
PUBLISHED 07 January 2026

CITATION
Farkas A and Vikman L (2026) From totality to hybridity and beyond: The challenges of state security systems in the context of the info-communication revolutions.
Front. Polit. Sci. 7:1749077.
doi: 10.3389/fpos.2025.1749077

From totality to hybridity and beyond: The challenges of state security systems in the context of the info-communication revolutions

Adam Farkas* and Laszlo Vikman

Modern Technologies and Cybersecurity Law Department, Deak Ferenc Faculty of Law, Szechenyi Istvan University, Gyor, Hungary

Contemporary security is increasingly defined by a matrix of hybrid threats, driven by info-communication revolutions that blur the lines between war and peace. Mainstream literature typically explains these challenges through the concept of 'hybridity,' focusing on post-Cold War technological and tactical novelties. However, this approach often lacks deeper historical and state-theoretical grounding. This study proposes a new theoretical framework by drawing a parallel between the current security environment and the 20th-century transformations analyzed by Carl Schmitt. We argue that the defining characteristic of contemporary security is not 'hybridity' but 'totality.' By reinterpreting Schmitt's concepts of the 'total state' and the 'partisan,' we situate today's challenges within a longer historical process of societal and political totalization, accelerated by the info-communication revolution. The analysis employs a qualitative methodology combining theoretical synthesis, historical-comparative analysis, and conceptual critique. Our analysis identifies a 'total security environment' characterized by three key attributes: (1) the complete fusion of military, economic, social, and informational domains; (2) the collapse of spatial and temporal constraints on state and non-state action; and (3) the systemic vulnerability of the state's own normative and legal foundations. We demonstrate that hybrid threats are a logical manifestation of this total environment, representing 'total threats' that demand 'total responses.' By foregrounding 'totality' over 'hybridity,' this study provides a novel foundation for understanding and addressing contemporary security challenges. It suggests that effective solutions require moving beyond tactical countermeasures and rethinking statehood itself, focusing on systemic resilience, adaptable governance models, and societal preparedness. The historical experiences of previous security paradigm shifts offer crucial patterns for navigating this new era of total security.

KEYWORDS

hybrid threats, info-communication revolutions, security institutions, total state, total war

1 Introduction

The set of hybrid threats that define contemporary security, which permeates many areas of the technical and civil environment, appears in public discourse as an epochal change (Fridman et al., 2019; Giannopoulos et al., 2021; Garcia-Camargo and Bradshaw, 2021). This has been particularly reinforced by the effect that has shattered the post-Cold War perception of peaceful, or at least war-free, security in areas outside crisis zones (Bremmer, 2014, 2022).

To explain this phenomenon, security policy literature has developed an expanding theoretical framework, which is not without internal debates. The mainstream discourse sees the essence of hybrid warfare in deliberately created ambiguity and operations conducted in the "gray zone" between peace and war (Mumford and Carlucci, 2023; Krishnan, 2022). According to this view, the main driver of change is the cyber technology revolution, which enables remote, deniable, and asymmetric interventions (Steingartner and Galinec, 2021) and its main toolkit is a series of disinformation and cognitive operations targeting societies (Bachmann et al., 2023; Danyk and Briggs, 2023).

However, this dominant narrative emphasizes the novelty of the phenomenon and often fails to explore the deeper historical context. Although some of the literature recognizes the continuity with 20th-century, especially Soviet, political warfare practices (DeBenedictis, 2022) and also draws on Clausewitz's strategic principles, the emphasis is still on post-Cold War technology-driven changes. As critics of the literature point out, the concept of "hybrid warfare" has often spread as an "academic fad" without a deeper historical-theoretical foundation, and has become popular primarily as a result of NATO narratives after 2014 (Libiseller, 2023). According to our analysis, the real shortcoming is that the literature interprets contemporary challenges as an evolution of warfare tactics rather than as symptoms of a deeper structural transformation affecting the nature of the state.

Contemporary literature on hybrid warfare does not use Carl Schmitt's concepts as a central framework. Although Schmitt research deals with the topics of partisans (Engelking, 2025) and technology/cybernetics (Guilhot, 2020), it does so within its own political-philosophical debates, without analyzing the contemporary security policy phenomenon of hybrid warfare. These two discourses (hybrid warfare and Schmitt's interpretation) have so far existed side by side without any meaningful overlap. Even the most recent research examining state responses to hybrid threats (e.g., the concept of "total defense") typically works within other theoretical frameworks, such as Foucault's concepts of governmentality, without resorting to Schmitt's concept of the "total state" (Ljungkvist, 2024; Kaiser, 2021). This study aims to fill this dual gap—historical-theoretical and specifically Schmittian.

Consequently, the central research problem of this article is defined by two interrelated questions: (1) How can the Schmittian concept of 'totality' provide a more adequate explanatory framework for the structural transformation of the contemporary security environment than the currently dominant, phenomenon-based concept of 'hybridity'? (2) If the security environment is indeed becoming 'total,' what are the systemic consequences for the state's defense logic, moving beyond tactical countermeasures?

In contrast, it is important to see that the novelty of hybridity is, on the one hand, perhaps a misunderstood phenomenon (Kelemen and Farkas, 2025), and on the other hand, can also be understood as the continuation of a specific developmental trend. This trend is the process of totalization that defined the 20th century, during which society, politics, the state, and, as integral parts of these, defense and security underwent epochal changes (Hobsbawm, 1996a, 1996b, 1996c; Meadwell, 2001). However, a significant part of these changes were based on the technological, economic, and social changes of the so-called long 19th century, which, among many other areas, significantly transformed communication, the flow of information, and the formation of consciousness. These changes were accompanied by an acceleration of lifestyles due to the development of transportation, the gradual relativization of distances, and the increased interconnectedness of distant parts of the world, as well as the massification of politics. This process led to an epochal change in thinking and the exercise of power, which in turn brought about a historical shift. Eric J. Hobsbawm illustrated this change by calling the short 20th century, following the age of empires, the age of extremes (Hobsbawm, 1996d).

Carl Schmitt described the same change in relation to the state with his topos of the total state (Hjalmar, 2022; Arabaci, 2025). We supplement this framework with another of Schmitt's ideas, his theory of the partisan published in 1963 (Schmitt, 2007). If we examine the theory itself, it is clear that Schmitt described challenges and potential threats—at that time, even more so in the future—associated with partisans, which later became extremely relevant in international terrorism and, today, in the hybrid threat matrix and non-state security threats. This impact is reinforced by another thought experiment, also from the 1960s, which deals with the issue of power seizures and coups. Luttwak (2016) examines one of the outcomes of this type of challenge, systematically reviewing, among other things, the state's defense system and its challenges in a new security and power system.

In our view, therefore, the totalitarianism described by Schmitt, together with his theory of partisanship, provides a framework in which, in relation to hybrid threats, totalitarianism takes precedence over hybridity. With this, security threats have entered areas—traditionally non-military—that were not previously extensively and organically part of armed conflict. If this assumption can be substantiated, then hybrid threats are also total threats on a theoretical level, which brings with it the question of total defense and security. The aim of our study is to use this theoretical model as a basis for further research that can provide a suitable framework for practice-oriented governance, security policy, and strategic analyses.

2 Methodology and analytical framework

This study is a conceptual-theoretical research project that aims to develop a new interpretative framework for understanding contemporary security challenges. To this end, it employs a qualitative methodological approach based on three main pillars: theoretical synthesis, historical-comparative analysis, and conceptual analysis.

The starting point for the analysis is an interdisciplinary theoretical synthesis. The central analytical framework of the study is Carl Schmitt's political philosophy, in particular his topos of the total state and his theory of partisanship. We use relevant findings from political science, international relations, security policy, and military science to connect these theoretical ideas and adapt them to contemporary conditions. Our goal is to place Schmitt's concepts in the context shaped by the 21st-century information and communication revolution, building a bridge between classical state theory and modern security studies. In order to connect these theoretical ideas, our study projects theories from different fields of science onto Schmitt's topos of totality, and we attempt to supplement this theoretical construct with an approach based on practical, event-based analysis and categorization, typical of military science and security policy.

The study uses a historical-comparative method to show that the current "hybrid" security environment is not without precedent, but is the result of a longer technological, social, and political transformation rooted in the 19th and 20th centuries. We draw parallels between earlier paradigm shifts (e.g., the emergence of total war) and contemporary transformations. The purpose of the comparison is to identify the logic and potential pitfalls of possible state responses (regulatory, governance, defense) to current challenges based on patterns that can be drawn from past experiences. This approach helps to avoid the "present trap" (presentism) and places contemporary phenomena in a broader evolutionary arc.

The third pillar of the research is conceptual analysis. Within this framework, we critically examine the concept of "hybridity" and argue that "totalitarianism" is a more accurate and explanatory analytical category for describing the current security environment. The study deconstructs certain elements of the concept of hybridity and reinterprets them within the framework of totality. In the course of the analysis, we identify the defining attributes of the 21st-century "total security environment," thereby offering a new conceptual apparatus that can be used for further research.

The combined application of these three methodological elements allows the study not only to describe contemporary security challenges, but also to develop a new explanatory model based on solid theoretical and historical foundations, which can serve as a basis for further, even practice-oriented analyses.

3 Analysis: from the total state to the total security environment

This chapter contains the central analysis of the study, which examines the evolution of Carl Schmitt's concept of totality and its relevance in the 21st century. The argument proceeds in two steps. The first subchapter (3.1) presents the historical and theoretical foundations of totalitarianism through the concepts of the 20th-century total state and the partisan. The second subchapter (3.2) then analyzes how the information and communication revolution has fulfilled this logic and identifies the defining attributes of the total security environment that characterizes our times.

3.1 The historical and theoretical foundations of totalitarianism: the paradigm shift of the 20th century and the transformation of warfare

In our opinion, today's security environment, characterized by hybrid threats and paralleled by increasing geopolitical competition, forces states to maintain security and assert their interests in a much more dynamic environment that permeates all dimensions of social existence. Due to the technical and social interactions of our age, today's state is much more of a total state than the state of the early 20th century, for which Carl Schmitt developed the concept of the total state in response to the changes that were unfolding at the time. According to Schmitt's approach, the state and society mutually permeate each other, and everything that has hitherto been considered state affairs becomes social, and conversely, everything that has hitherto been considered 'only' social becomes state affairs, as is necessarily the case in a democratically organized community (Schmitt, 2002). It is important to emphasize that Schmitt's concept of the "total state" is primarily an analytical category that describes the merging of the state and social spheres and is not necessarily identical with a given totalitarian political system. However, it should also be noted that the totalitarian nature of this state lies in the fact that areas that were previously 'neutral'—religion, culture, education, economy—cease to be 'neutral' in a non-state and non-political sense. As a result, in a totalitarian state, everything is political, at least potentially, and reference to the state is no longer capable of justifying the special distinguishing feature of the 'political' (Schmitt, 2002, p. 16). From the perspective of security and its guarantee, the technical and social changes that form the basis of the total state have thus generated new types of security challenges and threats, or ones with a different impact and scope. In this environment, the value of information has also grown dynamically in terms of intelligence, subversion, and propaganda. This in itself has significantly increased the role of society in geopolitical competition, which has only been further expanded by the technology of total war and the desire to break the social support of the opposing side. However, the rapid rise in the importance of social components in the areas of defense and security, as well as in the confrontation with hard power tools, made the social dimension significant in other respects as well.

However, the social dimension was not only valued as a passive arena for confrontation between great powers. In the name of self-defense and resistance to new models of power, non-state actors emerged from society and played an increasingly important role, which Carl Schmitt identified as a new phenomenon in his theory of partisanship. But what characterized this new form of resistance/attack? Primarily, it was lawlessness, since classical international law did not recognize partisans as belligerents, meaning that the institutions restricting modern warfare did not apply to them. It follows from this, as Carl Schmitt correctly stated, that the modern partisan expects neither law nor mercy from the enemy. He has turned away from the conventional hostility of war, fortified by tamed defense institutions, and has turned toward another territory, the territory of the real enemy, which escalates with terror and counter-terror until destruction (Schmitt, 2002, p. 16).

With regard to the phenomenon of partisanship, and in particular its spread, two things must be noted. (1) On the one hand, total resistance resulted from the illegality of partisanship and its real hostility, which escalated into destruction, as Schmitt clearly explained, in a spiral of interaction and counteraction. This type of resistance knows no boundaries or conventions, only effectiveness and the achievement of the desired result. Today, this is also a relevant criterion in relation to terrorism, armed radicalism, and unconventional threats. It also determines the defensive responses of states to new challenges and threats. (2) On the other hand, it should also be noted that in previous historical examples, states were unable to take effective action against guerrilla fighters, particularly due to their social embeddedness. There is no general recipe for this, as the solutions and the tools themselves must be adapted to the specific situation and social milieu.

Attack and defense thus deviated from traditional military confrontation patterns in several respects due to the phenomenon of the total state, then total war, and finally guerrilla warfare, thereby increasing the role of non-military factors in an unprecedented manner, building on the effects of technological revolutions. From

today's perspective, we can say that when we look at the social implications of total war and the theory of guerrilla warfare together, we are faced with a hybrid scenario (Wissmann et al., 2021), but one that predates the widespread analysis of hybrid threats by many years. Thus, the totality of security was transformed in the same way as the state in Schmitt's theory at the beginning of the 20th century: many circumstances that were previously politically irrelevant became political, and almost all circumstances and areas of life that were previously irrelevant gradually became relevant in the confrontation between powers in the 20th century. According to Schmitt, in 1914 the peoples and governments of Europe rushed into World War I without a real enemy. The real hostility arose only from the war, which began as a traditional war between states under European international law and turned into a global civil war of revolutionary class antagonisms. The key question he then asks is: who will prevent the unexpected emergence of similar but infinitely more intense new types of enemies, whose appearance will lead to the formation of unexpected new partisan movements? While Schmitt originally envisioned a clear distinction between the partisan and the regular army, contemporary scholarship suggests that this 'new type of enemy' has evolved into a more diffuse and networked entity. In the context of hybridity, we rarely encounter a singular 'total enemy' in the traditional sense. However, recent analyses (Kiparenko, 2024; Bachmann et al., 2023) argue that the 'totality' of the enemy today lies not in its monolithic nature, but in its capacity to wage 'cognitive warfare' and create 'information disorder' that targets the legitimacy of the political order itself. Steingartner and Galinec (2021) and Ljungkvist (2024) further demonstrate that cyber and hybrid threats blur the lines between state and non-state actors to such an extent that the 'enemy' becomes a systemic condition rather than a discrete actor. Thus, the 21st-century 'total enemy' is defined by its omnipresence and its ability to operationalize ambiguity, posing an existential threat to the state's normative foundations without necessarily declaring open war. This characterization of guerrillas links them to terrorists, "little green men," and various radical armed groups, beyond their obvious similarities, and this is what makes it truly alarming for 21st-century policymakers (Schmitt, 2002, p. 162). This threat, which is largely independent of the state, highly effective, and directly embedded in social reality, has at its disposal a set of tools never before seen in the technological environment of the 21st century. The same is true, however, of the state's response and certain phenomena threatening the state from within, such as the coup threat examined by Edward N. Luttwak. While Luttwak assigns a key role to the armed factor, he essentially bases his theory on the expansion, professionalization, and "mechanization" of the total state outlined by Schmitt. According to Luttwak (2016), the prerequisite for a coup is a developed modern state apparatus and its self-motivation and effectiveness in the social sphere and its influence. Looking at the changes in attack and defense together, with the security implications of state and non-state factors and, in particular, the increased importance of the social field, we could say that totalitarianism "only" unfolded in the 20th century, but it is reaching its heyday in the information technology environment and hybrid threats of the 21st century, which raises a number of questions for us.

This 20th-century logic of totalitarianism was completed by the information and communication revolution, creating what we call a total security environment. If we approach totalitarianism from the perspective of the state as a complex entity surrounded and forced to operate by numerous environmental factors—such as the society that constitutes the state, national and international politics, natural influences, technological developments, the economy, various non-state actors, etc.—then we approach it from the perspective of the state's effectiveness on the one hand and the influences affecting the state on the other. Then we can approach it from the perspective of the comprehensiveness of the state's effectiveness on the one hand and the effects on the state in terms of space and time on the other. However, these approaches necessarily merge if we examine the relationship between the state and totality at a general level, abstracted from a given state, since all other states are thus classified as environmental influences.

The impact generated by other states is therefore one component of the extremely complex, multifaceted, and dynamic set of influences that make up the state's environment, in relation to which greater emphasis must also be placed on non-state actors. Carl Schmitt already drew attention to this in the context of defense and security with his famous question about guerrilla warfare, which has since become a self-fulfilling prophecy and a factor that significantly determines our security. However, it is also important to pay sufficient attention to the fact that, in terms of state security, in addition to gray zone operations (Dobias and Christensen, 2022; Mazarr, 2015), non-armed, non-violent influences are becoming increasingly important, meaning that we must imagine a more differentiated picture alongside or above guerrilla warfare. In this context, economic factors (Chen and Evers, 2023; Cha, 2023; Mohamed and Osman, 2022), the information environment (Wither, 2023; Briggs et al., 2021; Zhen et al., 2023) and the combination of all these factors are of paramount importance. However, in order to be able to interpret these factors properly in a comprehensive theoretical framework, whether in terms of hybrid threats or cyber threats, it is necessary to abstract the findings that have already been formulated in professional and scientific analyses in the security and military spheres, and which have appeared in various relevant strategies and, among others, in NATO decisions (Arkan, 2025; Janičatová and Mlejnková, 2021; Calmels, 2020; Csernatoni and Martins, 2023).

This complex security environment and matrix in itself influences the interpretation of totalitarianism in terms of security. Synthesized with the military-dominated conception of security that prevailed until the first half of the 20th century, this points to the fact that although the totality of war and the significant role played by partisans, guerrillas, and revolutionaries alongside state opposition were indeed novel in the previous century, it must also be recognized that at that time, the decisive arena for the systematic, malicious destabilization of states was still the state system. Guerrillas, and revolutionaries gained a significant role alongside state opposition, it must also be noted that at that time, violent, armed behavior was still the decisive factor in the systematic destabilization of states based on malicious intent, and that the increase in the role of non-military factors was a novelty in the second half of the 20th century. When the United States passed the National Security Act in 1947, Samuel P. Huntington, among others, identified military policy, which had previously been of a decisive nature, as an area of national security policy P. Huntington identified military policy, which had previously been of a decisive nature, as an area of national security policy (Huntington, 1957), they were responding not only to the changes of the Cold War, but also to the social and technological changes that were beginning to raise the totality of the state and war to a new level. However, the unfolding of

this change spilled over into the early 21st century. The main reason for this was that, despite the explosive development of technology in the first half of the 20th century, it had not yet reached the level where globalization could be interpreted as a matrix of real-time interactions covering the entire globe in both a physical and temporal sense, i.e., totalized. Thus, environmental impacts could not yet become total for the state, i.e., unlimited in space and time and immediately effective. Economic pressure, influencing societies through communication, or any other unconventional influence on the functioning of a state therefore presupposed some kind of direct physical presence or connection. Of course, the technological revolutions achieved up to that point gradually extended the state's influence and, ultimately, its offensive capabilities to new areas with an ever-increasing radius of action. With the development of transportation, economic capacity also grew stronger, while the development of air transportation brought about aerial warfare and, through observation and propaganda from aircraft, a new era of psychological and information warfare. Advances in chemistry and industry, as well as increased mechanization, increased the range of land warfare in terms of both artillery and mobility. These developments revolutionized the framework of confrontation and gave rise to the idea of total war (Ludendorff, 1940; Ludendorff, 1935), which (1) takes place simultaneously on land, sea, and air (more precisely, in all spaces accessible to technological advancement), (2) mobilizes and utilizes all living and non-living resources to completely defeat the enemy, (3) operates on the principle of a zero-sum game,[1] (4) blurs the lines between the home front and the front lines, between civilian and military, and between strategic and political-conspiratorial, and (5) can be described as having extraordinary escalation potential, coupled with the importance of propaganda or, in some cases, radio electronics for warfare and intelligence, thanks to technological advances. In terms of security as a whole, war became total in the first half of the last century, similar to the state, and then in the second half, with the increasing development of information technology and the slow erosion of the significance of physical barriers, intelligence warfare or information competition intensified. Thus, the next stage in the development of totalitarianism was the Cold War, which essentially constituted a transitional period between total war and a total security environment. Although the logic of military competition was decisive, the involvement of the social field and the information environment in the confrontation became increasingly important, in line with the broader grand strategy, or, if you will, national security policy.

By the 21st century, however, both technological developments and the trends on which Schmitt based his concept of the total state—the actual massification of politics and the associated broadening of the dissemination of related content—have undergone another explosive change, primarily due to the explosion of information and communication technology and the significance of cyberspace (Kostyuk and Gartzke, 2023; Baliga et al., 2020; Groenendaal and Helsloot, 2021; Puyvelde and Brantly, 2019; Kelemen and Farkas, 2020). Totalitarianism has thus taken on a new meaning in the security environment of the 21st century. The cornerstones of this are as follows:

- Through the development of information technologies, globalization has created real-time, essentially distance-independent opportunities for connection and influence across the entire globe, with cyberspace providing a significant dimension to this.
- The information revolution permeates the economic, industrial, political, non-political worldview, social functioning, state functioning, and thus essentially the entire security sphere. This means not only dynamism, increased efficiency, and rapid responsiveness, but also increased vulnerability of these systems and the creation of new opportunities for attack, intervention, and influence.
- By shifting the economy into the information and communication space, financial transactions can be initiated in real time from one point in the world to another, which also creates opportunities for abuse, both in terms of external financing of non-state actors (partisans) and crime.
- The increasing digitization of state operations and individuals' daily lives, as well as the so-called social networks formed in the information space, have increased the danger and effectiveness of influencing people with false or distorted news, as well as the vulnerability of the state to attacks from the information space.
- With further advances in technology, it can be achieved with live force from one side of the world to the other in a matter of hours, or even minutes with intercontinental missile systems and satellite technology.

Taking all this into account, we can see that totalitarianism has reached its full potential in the 21st century in terms of the state's environment, if we interpret it as the real-time and low-restriction possibility of the environment's effects in space and time. Environmental changes have thus made the state, and after the war, the security environment, total. Schmitt's topos of totality is therefore a reality that we live with in the field of security, which requires further interpretation. This change naturally poses new challenges for the state, especially its defense and security functions, as it must respond effectively to all of this without falling into the historical trap of excessive power and abuse.

To address the theoretical relationship between hybridity and totality, it is essential to distinguish between the modus operandi of the actor and the structural condition of the security environment. Drawing on recent scholarship, we argue that hybridity functions as a strategy, whereas totality defines the environment. Mumford and Carlucci (2023) posit that the essence of hybrid warfare lies in 'ambiguity.' They define it as a calculated 'operational design' used by great powers to generate a 'cognitive impasse,' allowing them to achieve political objectives below the threshold of conventional retaliation. In this framework, hybridity is a specific strategic choice—a tool of statecraft—rather than a description of the global order itself. In contrast, the concept of totality captures the broader structural context in which these strategies unfold. Ljungkvist (2024), analyzing the resurgence of 'Total Defence' in Sweden, describes this environment as a state of 'strategic non-peace.' In this condition, the distinction between peace and war is permanently blurred, necessitating an 'everyday total defence' where the civilian sphere is

1 In other words, one of the opposing parties can only gain an advantage during the war if the opposing party suffers a corresponding disadvantage. It is therefore not possible to gain profit or improve one's position without compromising one's interests.

increasingly 'martialised' to withstand constant, ambiguous pressure. Furthermore, Davies (2024) illustrates through the Russo-Ukrainian conflict that hybrid operations—driven by intelligence services and proxies—are not alternatives to, but often integral precursors of total war. As Davies notes, the escalation from hybrid subversion to high-intensity conflict demonstrates that hybridity is the tactical manifestation of a security environment that has become total in its scope and stakes. Therefore, in our model, the 'Total Security Environment' is the arena of 'strategic non-peace,' while hybrid warfare is the prevailing strategy used to navigate and exploit this totalized condition.

3.2 Totalitarianism in the 21st century: attributes of a total security environment

Based on our analysis, the contemporary essence of totalitarianism can be captured in three closely related attributes. On the one hand, because even in a technically and socially changing environment, today's state is still a totalitarian state, which exerts significant influence over many areas that at first glance appear to be independent of the state (economic activity, research and development, freedom of expression and religious practice, etc.). This trend will be further reinforced by armament and military developments due to the Russian-Ukrainian war, as well as other security measures. On the other hand, because in this 21st-century totalitarian state, many issues that at first glance do not fit into classical political thinking can become key political topics. Examples of this range from sexuality to the state of the ecosystem, from scientific progress to which technology companies' products can be considered safe or dangerous and according to what criteria, and what influence social media and other information service providers can exert on economic and social functioning. All these factors, intertwined with the politicizing nature of the total state, generate significant organizational and social psychological effects through the political determination of security, its connection to a friend-enemy binary code, and its combination with fear (Fluri et al., 2022; Gentry, 2017; Boucher and Gagnon, 2024). These, in turn, feed back into the guarantee and system of security through political processes. Thus, the total security environment, through the logic of the total state, mixes with political peculiarities and creates a new kind of spiral.

Within this spiral, it is crucial to define the 'total security environment' with precision, particularly regarding the digital domain. In the context of cyber-physical systems (CPS), 'total security'—understood as the complete elimination of risk—is an unattainable ideal. As Kure et al. (2022) emphasize regarding critical infrastructures, organizations cannot wholly avoid risk; rather, the objective is to keep risks to a minimum level while maintaining service delivery. Therefore, in our framework, 'total security' refers not to an achievable state of absolute invulnerability, but to the comprehensive scope of exposure. This exposure is amplified because traditional distinctions between risk types have collapsed. Michalec et al. (2022) argue that in modern operational technologies, the requirement for cyber security cannot be divorced from safety, as digital attacks now have direct consequences in the material realm. Expanding on this, Ji et al. (2021) provide empirical evidence that traditional independent risk analyses fail in this environment. They demonstrate that security threats and safety hazards often have an antagonistic relationship, where a cyber-threat explicitly evolves into a physical safety incident (e.g., via manipulated sensor data). Thus, the environment is 'total' because threats permeate the physical, digital, and cognitive domains simultaneously, necessitating a 'harmonized' rather than a siloed defense approach.

If this totalitarian state wishes to remain in power and establish the conditions for development and growth in its society, it is forced to operate in a complex security environment that can be described as truly global. As the sectoral theory of security has pointed out, this has many segments and dimensions in which non-military spheres are increasingly predominating. This does not mean, of course, that the importance of state agencies, which can be described as armed by nature, has diminished, firstly because their armed nature, which gives them *their specific difference*, is not their only characteristic, and on the other hand, because from international terrorism to organized crime to operations carried out in the information space, but if you like, from Syria through Ukraine to North Korea, it is clear that non-military spheres can be closely linked to violent and even armed events. This essentially captures one of the key aspects of hybrid threats. These must be countered in a coordinated manner, based on a specific defense and security logic. Returning to the environment in which the totalitarian state operates, we must recognize that it is a force field located at the intersection of extremely complex, multifaceted dimensions that operate according to their own specific laws in many respects. *The first attribute of the essence of totality is therefore that it can be described as a force field at the intersection of numerous dimensions and a specific system of operational relationships, in which the weight of the individual sub-force fields fluctuates dynamically, with great amplitude and unpredictably*. If you like, there is no sure formula for this, but while at the beginning of the 21st century economic impacts were the most important factors triggering state responses, in a short time they have become consequences or rather tools of security or health events, or even natural events. This has been confirmed by the COVID-19 pandemic, as well as by the effects of the Russian-Ukrainian war and the estimated costs of future reconstruction, and the global effects of geopolitical confrontation. It is important to note here that the use of hybrid tools accompanied each of these phenomena, with the aim of exerting geopolitical influence behind the scenes of the main challenges. This was accompanied by various information operations, economic warfare, and even changes in the balance of power in certain regions, such as Africa. However, with regard to the shift in focus between governance and crisis management, it should be noted that the neglect of defense and security capabilities, for example, cannot be corrected overnight in terms of technical conditions, personnel preparedness, or organization and regulation, meaning that their dismantling can lead to drastic losses in the event of a sudden change in the environment. It is almost certain that this kind of neglect causes serious cognitive disadvantages in times of dynamic change, even if the political will and unity to catch up are there. The right mindset and expertise can only develop and function properly over a long period of time and with continuous improvement. In other words, in addition to political will and economic resources, a well-functioning national security state or government is necessary—but without the right proportions and operating mechanisms, it is not necessarily sufficient—as is professional expertise ranging from the operational level to the strategic and policy levels. The timely recognition of the development toward a total security environment after total war cannot be said to have taken place in a timely manner, which is why we are only now

recognizing the consequences of the marginalization of defense and security developments in the course of the geopolitical transformation that is currently unfolding. Efforts to counteract this phenomenon are reflected in national military force development, military industrial development, broader national security capability and institutional development, NATO's steps to increase resilience and deterrence, but also initiatives aimed at creating an EU military force and establishing a unified EU-wide military industrial environment, and, in some respects, efforts to regulate information and communications and develop cybersecurity (Hulkó et al., 2025; Kour et al., 2024; Kello, 2013).

However, this force field, formed by the intersection of many sets, has an additional attribute associated with totalitarianism, which is based primarily on technological development, and within that, largely—but not exclusively—on the development of information technology and cyberspace. This is nothing less than the extremely intense relativization of space and time in relation to Earth. Due to the development of information technologies, it is now possible to exert economic, social, and political influence in real time from one point on Earth to another on the opposite side of the planet, and to a significant extent. On the one hand, this places established security concepts such as deterrence and restraint in a new perspective (Nye, 2017). On the other hand, due to the digitization of state organizations and the manufacturing and service sectors, operational disruptions equivalent to attacks can be caused from this distance, which was previously only possible through physical connection and with relative predictability. *The second attribute of totality is therefore that the constraints of space and time have lost their former limiting significance in terms of their impact on states, societies, and individuals*. From a security perspective, this means that threats crossing state borders will become increasingly common and the possibilities for prediction will be limited, while the initial cost of information-based operational capabilities is high, their maintenance and operating costs—and especially their loss value—will be much lower than those of traditional armed combat. This further reinforces the trend that the goal in confrontation is to prolong the period of sub-threshold conflict and to increase the exploitation of economic, social, and state operational vulnerabilities.

In addition to all this, it is important to consider the relationship between totalitarianism and the state in at least one respect. This is the relationship between effective, or if you like, good state functioning and totalitarianism. Today, when Western-style regulated statehood is spreading globally—although in many places this is only enforced as a formal requirement due to economic relations—the state's capabilities are important, but so is the appropriate regulation and regular functioning of those capabilities. The framework for this is open regulation based on legal certainty and global awareness through the information space. In a conflict situation, however, neglecting or failing to update this regulation and operation can be a vulnerability. Through accessibility, the opposing party can magnify the severity of any operational errors in the information space and turn them into a tool for political and social destabilization. This phenomenon is referred to in the literature as lawfare (Sari, 2020; Dunlap, 2001; Kittrie, 2016; Bachmann and Mosquera, 2015). Examples of this include the propagation on the World Wide Web of differing interpretations of international law in certain Far Eastern territorial disputes, the international legal interpretations of the Ukrainian crisis and, in particular, the annexation of the Crimean Peninsula, or even the analysis of the powers of law enforcement and military forces in the global press in the context of various crises. The updating of regulations designed to restrict the state and developed by the state has thus entered the realm of interpretation of the total security environment, alongside actual defense and security capabilities and non-military factors. *The third attribute of the essence of totality is therefore that the state's capacity to act and its stability are determined not only by its capabilities for action, but also by its regulatory and operational systems, i.e., the modernity of the state at the systemic level*, since its lack of modernity means vulnerability and exposure to attack both in terms of inter-state conflicts and non-state actors. In addition to the above examples, the need for dynamic development of counterterrorism regulations was also highlighted by after both 9/11 and the wave of terrorism in 2015–2016, as the attacks drew attention to the need for different, novel tools and procedures to maintain security (Jahankhani et al., 2020; Buchanan, 2020; Hamilton, 2016; Vanaga and Rostokos, 2019; Farkas, 2023). However, the corrections made after the attacks were typically radical responses, as the above examples also show.

Taking all this into account, it is clear that *the concept of totality has expanded and deepened to an extraordinary degree in relation to the state environment: the totality of the security environment has encompassed areas and phenomena that were not previously considered significant security threats or challenges*. The state and the law do not exist for their own sake, but are intended to guarantee the security, orderly functioning, and development of the nation and society that constitute the state. As Schmitt wrote: "… the performance of a normal state consists above all in creating complete satisfaction within the state and its territory, maintaining 'peace, security, and order,' and thus creating a normal situation…" (Schmitt, 2002; p. 31). Changes in the environment have therefore forced the state to respond to these changes in its own systems and to adapt to the environment in order to ensure its effective and efficient survival and to guarantee order, security, and peace. This is a law of the historical evolution of the state.

However, the state's capacity to guarantee this order is currently challenged by a critical limitation of the traditional Schmittian model. While the classic conception of totality focuses on the State and society, the infrastructure of the contemporary total security environment is largely owned by private technology giants. As Gu (2023) argues, these corporations have evolved into 'new data sovereigns' that form a 'digital empire' relatively independent of political authority. Kelton et al. (2022) define this challenge as 'virtual sovereignty,' where private control over the 'digital stack' allows corporations to exercise infrastructural power traditionally reserved for the state. Furthermore, Broeders et al. (2025) identify this phenomenon as 'digital corporate autonomy,' demonstrating that these entities act as independent geopolitical agents capable of navigating conflict on their own terms. Abels (2024) substantiates this with the case of Starlink in Ukraine, showing how private infrastructure owners can enable or restrict military operations based on a mix of profit-seeking and independent strategic preferences, rather than purely state directives. Consequently, the total state is no longer the sole master of the security domain but must negotiate its sovereignty within a symbiotic yet competitive relationship with these non-state leviathans.

Therefore, if Schmitt's assumption based on the topos of the total state is correct, that the complex developments of the past century have led from the total state through total war to total security challenges, then the total states of the present age must prepare themselves for the implementation of total defense and security within a similar interpretative framework, while at the same time ensuring that Western values of the rule of law are applied in a thoughtful and appropriate

manner. This suggestion is supported by the total defense concept of the Scandinavian and Baltic states, as well as by the further development of the American concept of the national security state (see Table 1).

4 Discussion: the consequences of a total security environment resource identification initiative

Considering the main features of totalitarianism identified above, Carl Schmitt's reinterpretation and further elaboration of the topos of totalitarianism in the 21st century seems reasonable. The theoretical model presented in the previous chapter not only serves to describe the contemporary security environment, but also highlights the key consequences that the modern state must face. In the following, we will explain these consequences, i.e., the practical and conceptual challenges arising from the total security environment, in more detail, along three main lines.

4.1 New challenges to state capacity: conclusions from the model

(1) *In order to ensure its survival, social order, stability and development, as well as the enforcement of individual rights (in short, security), the state must prepare itself in a complex manner for the influences coming from its environment, just as the security environment itself, which can be described as totalitarian, is complex, multifaceted and subject to changing dynamics*. On the one hand, this means that in the classic defense and security segments, increasing attention must be paid to non-military and non-violent factors and spheres, as well as cognitive characteristics. On the other hand, however, it is also necessary for non-military security sectors to show openness to increasing their security and defense awareness and to introducing and practicing the necessary protocols. Without this, true resilience is unimaginable. The synthesis of these two aspects can be achieved if, in addition to modernizing and developing its capabilities, the state also pays attention to the systematic renewal of its regulations and the coordinated management of the application of its capabilities, but in cooperation with civil actors.

(2) Given that totalitarianism has eliminated the classic limitations of space and time, primarily due to the widespread use and further spread of information technologies, *the state must exploit the advantages of digitalization and regulate private digitalization activities within its territory, so that, on the one hand, security is guaranteed in a meaningful way and, on the other hand, the most important—so-called vital—systems and services are ensured to function at the most necessary level even in the event of attacks from the information space or malfunctions occurring there*. Using an evolutionary example, even with all the advantages of civilization, the state must maintain the most basic instincts and routines of self-defense that have existed since the dawn of development: fight or flight. This necessarily implies that the state and the institutions and professionals responsible for its protection and security must be able to operate and think with a complexity and speed that breaks down the barriers of space and time, but also be equipped with a vision that becomes necessary when the information space becomes destabilized and the limitations of space and time are reinforced. This is because, given the changes in lifestyle brought about by digitalization, it can be predicted that this will have extraordinary social impacts, in addition to the possibility of other crises, threats, and attacks.

(3) In a total security environment, in addition to the capabilities of the state, its entire system, regulation, and fulfillment of its obligations also appear as factors that can be monitored, criticized, and attacked from anywhere in the world with attempts to influence the state-forming society. For this reason, it is crucial that the development and modernization of the state focus not only on capabilities, but also on modern regulatory and operational solutions and the reinforcement of commitments, as well as on the appropriate communication and awareness-raising of these within society. *The development of the state must therefore be approached systematically, because development interventions that focus on a single area or respond ad hoc to a single event are certain to lead to systemic inconsistencies and, from a security perspective, to vulnerability and the emergence of new attack surfaces*.

TABLE 1 Paradigm shift toward totality in the field of security.

Dimension	20th-century totalitarianism (age of total war)	21st-century totalitarianism (age of total security)
Defining technology	Industrial production, mechanization (railways, aircraft, tanks)	Information and communication technologies, cyberspace, global networks
The arena of conflict	Geographically defined fronts and rear areas (although borders are becoming blurred)	Global, borderless, taking place in both physical and virtual space
The nature of the conflict	Open, interstate armed conflict (total war)	Continuous, below-the-threshold, "gray zone" competition (hybrid warfare)
Key player (irregular)	Partisans tied to their territory (telluric)	Network-based "motorized guerrilla" (cyberterrorist, troll, etc.)
Main vulnerability	Industrial-military capacity, morale of the population	Critical infrastructure, information systems, social cohesion, normative order
The state's response	Total mobilization (military industry, conscription)	Total defense, social resilience, involvement of the civilian sphere

4.2 The imperative to respond: reinterpreting total defense

The present attempt to reinterpret totality and adapt it to 21st-century security, in my opinion, points to the fact that the

totalitarian state of the present age, with its broad political horizon, operates in the information age in a total security environment that requires a significantly different approach than in the past. Hybrid threats and warfare, illegitimate acts in the information space, intensifying geopolitical tensions, and their economic and social impacts thus place the state's defense and security system in a new perspective. If my assumption about the total security environment—a characteristic feature of which is hybridity—is correct, then the issue of total defense will also have to be reconsidered in the future.

This is now a recognized fact among NATO member states, but the concept is still often approached as a peculiar renaissance of the 20th-century military security concept rather than as a new phase of development. *In contrast, our model highlights that total defense in the 21st century must mean something radically different. The debate today revolves around two main models: the American-style national security state based on institutional coordination, and the Scandinavian-Baltic total defense concepts that emphasize social resilience. Our framework allows for criticism and further reflection on both models*.

Consequently, a modern interpretation of 'total defense' must transcend state-centric militarization and embrace a comprehensive approach rooted in societal resilience. Recent scholarship (Wither, 2020; Larsson, 2021) confirms that the Nordic model of total defense has evolved into a 'whole-of-society' strategy where civil preparedness is as critical as military readiness. This shift requires moving beyond top-down control to fostering a participatory security culture. As Kelemen et al. (2025) argue, resilience in the digital age is contingent upon public trust in institutions and the robustness of software supply chains, suggesting that technical and social resilience are mutually reinforcing. Furthermore, Kovács-Szépvölgyi et al. (2025) highlight that genuine societal resilience relies on the active participation and legal consciousness of citizens—including vulnerable groups like children—rather than their passive protection. Therefore, the 21st-century 'total defense' is not a return to the garrison state, but a model of 'comprehensive resilience' where the state facilitates, rather than dictates, the adaptive capacity of civil society.

The concept of the national security state also points in this direction, but instead of an integrative-coordinative approach, it may be advisable to develop a new approach, based in Hungary on the approach of Act XCIII of 2021 on the coordination of defense and security activities and the establishment of the new position of Chief National Security Advisor in March 2024. The question, however, is whether this development will go beyond the administrative approach and political control by senior leaders toward a material and institutional renewal in the field of defense and security.

In addition to multidisciplinarity, this may also require a rethinking of specific theoretical schemas, such as Carl Schmitt's topos of totality in politics, which goes far beyond the familiar friend-enemy dichotomy. The totalitarianism of our age, which is less limited in space and time and has an unprecedented scope and impact, and the primarily technological and secondarily economic, social, ecological, and psychological processes that fuel it, all make it necessary to think about the state and its development in a complex way, in line with changes in the external environment. This, in turn, may shift the focus in the future to the issue of national security governance and the transcendence of 20th-century institutional, conceptual, and methodological frameworks.

4.3 Theoretical contribution and future directions of research

The outline of the total security environment model goes beyond mere conceptual play; it creates an opportunity to place thinking about security on a deeper, theoretical foundation. The main theoretical contribution of our study is that it has built a bridge between classical 20th-century state theory and contemporary security studies. By focusing on the structural logic of "totalitarianism" rather than a phenomenon-centered description of "hybridity," we have shifted the debate from the tactical and technological surface to the deeper foundations of state and social theory. We have shown that, in addition to multidisciplinarity, there is a need to rethink specific theoretical schemas, such as Carl Schmitt's topos of totality—beyond the friend-enemy dichotomy that is far from unknown in politics.

The totalitarianism of our age, which is less limited in space and time and has an unprecedented scope and impact, and the primarily technological and secondarily economic, social, ecological, and psychological processes that fuel it, all make it necessary to think about the state and its development in a complex way, in harmony with changes in the external environment. This change in perspective will focus attention in the future on the issue of national security governance and the transcendence of 20th-century institutional, conceptual, and methodological frameworks.

This study has outlined a theoretical framework, which, of course, has its limitations. Since the focus was on conceptual model building, the research did not attempt to test the model in detail empirically. Future research could apply this framework to specific case studies, examining, for example, how the attributes of a total security environment manifest themselves in the specific defense strategies or legislative processes of individual states. Furthermore, the analysis was primarily based on the logic of Western-type states; further investigation is needed to determine how this new form of totalitarianism applies to non-Western state models.

5 Conclusion

This study has argued that contemporary security challenges, described in the literature as "hybridity," are the latest manifestations of a deeper and longer historical process of totalization. By reinterpreting Carl Schmitt's concept of totalitarianism, we have shown that the 21st-century information and communication revolution has created a total security environment in which the key concept is not tactical hybridity, but structural totalitarianism permeating all spheres of the state and society.

Consequently, our main conclusion is that an effective response to hybrid threats cannot be limited to the technical development of defense capabilities. A total security environment requires a total response from the total state, which necessitates a rethinking of the concept of total defense—a model that goes beyond 20th-century military logic and integrates social resilience, the protection of the normative order, and complex governance.

Based on all this, the big question for the future is not how states will combat individual hybrid threats, but whether they will be able to develop a new form of national security governance in an era of total security challenges that is both effective and preserves the rule of law. Moving beyond the institutional and conceptual solutions of the 20th century is no longer an option, but a necessity for survival.

Author contributions

AF: Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Resources, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. LV: Investigation, Writing – review & editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. The Article Processing Charge (APC) for this publication was funded by Széchenyi István University.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Abels, J. (2024). Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine. *Eur. J. Int. Relat.* 30, 842–866. doi: 10.1177/13540661241260653

Arabaci, G. Ç. (2025). The contestation of the sensible under populist authoritarianism: between silencing and seeking democratic rights. *Front. Polit. Sci.* 7:1648488. doi: 10.3389/fpos.2025.1648488

Arkan, Z. (2025). European security and hybrid threats. Cham: Palgrave MacMillan.

Bachmann, S. D., and Mosquera, A. B. M. (2015). Lawfare and hybrid warfare – how Russia is using the law as a weapon. *Amicus Curiae J. Soc. Adv. Legal Stud.* 2015, 25–28.

Bachmann, S.-D. D., Putter, D., and Duczynski, G. (2023). Hybrid warfare and disinformation: a Ukraine war perspective. *Glob. Policy* 14, 858–869. doi: 10.1111/1758-5899.13257

Baliga, S., de Bueno Mesquita, E., and Wolitzky, A. (2020). Deterrence with imperfect attribution. *Am. Polit. Sci. Rev.* 114, 1155–1178. doi: 10.1017/S0003055420000362

Boucher, V., and Gagnon, F. (2024). Partisanship and congressional intelligence oversight: the case of the Russia inquiries, 2017-2020. *Intell. Natl. Secur.* 1, 19–39. doi: 10.1080/02684527.2023.2249792

Bremmer, I. (2014). The centenary of the great war and today's G-zero world. *Horiz. J. Int. Relat. Sustain. Dev.* 1, 64–79. Available online at: https://www.jstor.org/stable/48573433

Bremmer, I. (2022). The power of crisis. New York: Simon & Schuster Paperbacks.

Briggs, C., Danyk, Y., and Maliarchuk, T. (2021). Security aspects of hybrid war, COVID-19 pandemic and cyber-social vulnerabilities. *Connect* 3-4, 47–72. doi: 10.11610/Connections.20.3-4.03

Broeders, D., Sukumar, A., Kello, M., and Andersen, L. H. (2025). Digital corporate autonomy: geo-economics and corporate agency in conflict and competition. *Rev. Int. Polit. Econ.* 32, 1189–1213. doi: 10.1080/09692290.2025.2468308

Buchanan, B. (2020). The hacker and the state. Cyber attacks and the new normal of geopolitics. Cambridge - London: Harvard University Press.

Calmels, C. (2020). NATO'S 360-degree approach to security: alliance cohesion and adaptation after the Crimean crisis. *Eur. Secur.* 29, 416–435. doi: 10.1080/09662839.2020.1795834

Cha, V. D. (2023). Collective resilience: deterring China's weaponization of economic interdependence. *Int. Secur.* 2023, 91–124. doi: 10.1162/isec_a_00465

Chen, L. S., and Evers, M. M. (2023). "Wars without gun smoke": global supply chains, power transitions, and economic statecraft. *Int. Secur.* 48, 164–204. doi: 10.1162/isec_a_00473

Csernatoni, R., and Martins, B. O. (2023). Disruptive technologies for security and defence: temporality, performativity and imagination. *Geopolitics* 29, 849–872. doi: 10.1080/14650045.2023.2224235

Danyk, Y., and Briggs, C. M. (2023). Modern cognitive operations and hybrid warfare. *J. Strateg. Secur.* 16, 35–50. doi: 10.5038/1944-0472.16.1.2032

Davies, P. H. J. (2024). Counterintelligence and escalation from hybrid to total war in the Russo-Ukrainian conflict 2014–2024. *Intell. Natl. Secur.* 39, 496–514. doi: 10.1080/02684527.2024.2329419

DeBenedictis, K. (2022). Russian 'hybrid warfare' and the annexation of Crimea: the modern application of soviet political warfare. London: I.B. Tauris.

Dobias, P., and Christensen, K. (2022). The 'Grey zone' and hybrid activities. *Connect* 2022, 41–54. doi: 10.11610/Connections.21.2.03

Dunlap, C. J. (2001). Law and military interventions: preserving humanitarian values in 21st century conflicts. Available online at: https://people.duke.edu/~pfeaver/dunlap.pdf (Accessed June 10, 2021).

Engelking, W. (2025). Partisan as Katechon: Carl Schmitt's myth of the earth. *Law Cult. Humanit.* doi: 10.1177/17438721251320319

Farkas, A. (2023). Babelic confusion?: systemic issues in the adaptation to defense and security challenges in the transatlantic states, with special regard to the Eurasia-idea as a special aspect of hybridity. *Iustum Aequum Salutare* 1, 17–31. Available online at: https://ias.jak.ppke.hu/20231sz/02_FarkasA_normal_IAS_2023_1.pdf

Fluri, P., Pataraia, T., and Tagarev, T. (2022). Leadership in the defense and security sector in the 21st century. *Connect* 1, 5–9. doi: 10.11610/Connections.21.1.00

Fridman, O., Kabernik, V., and Pearce, J. C. (2019). Hybrid conflicts and information warfare. New labels, old politics. Boulder-London: Lynne Rienner.

Garcia-Camargo, I., and Bradshaw, S. (2021). Disinformation 2.0: trends for 2021 and beyond. Helsinki: Hybrid CoE Working Paper 11. Available online at: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf (Accessed November 16, 2025).

Gentry, J. A. (2017). The intelligence of fear. *Intell. Natl. Secur.* 1, 9–25. doi: 10.1080/02684527.2016.1199348

Giannopoulos, G., Smith, H., and Theocharidou, M. (2021). The landscape of hybrid threats: a conceptual model. Luxembourg: Publications Office of the European Union.

Groenendaal, J., and Helsloot, I. (2021). Cyber resilience during the COVID-19 pandemic crisis: a case study. *J. Conting. Crisis Manag.* 29, 439–444. doi: 10.1111/1468-5973.12360

Gu, H. (2023). Data, big tech, and the new concept of sovereignty. *J. Chin. Polit. Sci.* 29, 591–612. doi: 10.1007/s11366-023-09855-1

Guilhot, N. (2020). Automatic leviathan: cybernetics and politics in Carl Schmitt's postwar writings. *Hist. Hum. Sci.* 33, 128–146. doi: 10.1177/0952695119864244

Hamilton, D. S. (2016). Forward resilience. Protecting society in an interconnected world. Washington: Johns Hopkins University, Center for Transatlantic Relations.

Hjalmar, F. (2022). The modern Epimetheus: Carl Schmitt's katechontism as reactionary chronopolitics. *Front. Polit. Sci.* 4:957094. doi: 10.3389/fpos.2022.957094

Hobsbawm, E. J. (1996a). The age of revolutions. New York: Vintage Books.

Hobsbawm, E. J. (1996b). The age of empire. New York: Vintage Books.

Hobsbawm, E. J. (1996c). The age of capital. New York: Vintage Books.

Hobsbawm, E. J. (1996d). The age of extremes. New York: Vintage Books.

Hulkó, G., Kálmán, J., and Lapsánszky, A. (2025). The politics of digital sovereignty and the European Union's legislation: navigating crises. *Front. Polit. Sci.* 7:1548562. doi: 10.3389/fpos.2025.1548562

Huntington, S. P. (1957). The soldier and the state. Cambridge: Harvard University Press.

Jahankhani, H., O'Dell, L. M., Bowen, G., Hagan, D., and Jamal, A. (2020). Strategy, leadership, and AI in the cyber ecosystem. Cambridge: Academic Press.

Janičatová, S., and Mlejnková, P. (2021). The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemp. Secur. Policy* 42, 312–344. doi: 10.1080/13523260.2021.1885921

Ji, Z., Yang, S.-H., Cao, Y., Wang, Y., Zhou, C., Yue, L., et al. (2021). Harmonizing safety and security risk analysis and prevention in cyber-physical systems. *Process. Saf. Environ. Prot.* 148, 1279–1291. doi: 10.1016/j.psep.2021.03.004

Kaiser, A.-B. (2021). Carl Schmitt, the chameleon. *Philos. Soc. Crit.* 47, 158–162. doi: 10.1177/0191453720974735

Kelemen, R., and Farkas, A. (2020). "To the margin of the theory of a new type of warfare: examining certain aspects of cyber warfare" in Hungarian yearbook of international law and European law (2019). eds. M. Szabó, L. Gyeney and P. L. Láncos (The Hague: Eleven International), 203–226.

Kelemen, R., and Farkas, A. (2025). "The connections between social media platforms and hybridity" in Bridging the digital divide: perspectives on inequality and discrimination in the digital age. eds. O. P. de la Fuente and J. Skrzypczak (Cham: Springer Nature Switzerland), 105–123.

Kelemen, R., Squillace, J., Medvácz, Á., Cappella, J., Bucko, B., and Mazuch, M. (2025). Cybersecurity regulations and software resilience: strengthening awareness and societal stability. *Soc. Sci.* 14:578. doi: 10.3390/socsci14100578

Kello, L. (2013). The meaning of the cyber revolution: perils to theory and statecraft. *Int. Secur.* 38, 7–40. doi: 10.1162/ISEC_a_00138

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., and Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *Int. Aff.* 98, 1977–1999. doi: 10.1093/ia/iiac226

Kiparenko, K. (2024). The conception of political of Carl Schmitt. *Doxa* 42, 73–82. doi: 10.18524/2410-2601.2024.2(42).333059

Kittrie, R. F. (2016). Lawfare. Law as a weapon of war. New York: Oxford University Press.

Kostyuk, N., and Gartzke, E. (2023). Fighting in cyberspace: internet access and the substitutability of cyber and military operations. *J. Confl. Resolut.* 68, 80–107. doi: 10.1177/00220027231160993

Kour, R., Karim, R., Dersin, P., and Venkatesh, N. (2024). Cybersecurity for industry 5.0: trends and gaps. *Front. Comput. Sci.* 6:1434436. doi: 10.3389/fcomp.2024.1434436

Kovács-Szépvölgyi, E., Tóth, D. A., and Kelemen, R. (2025). From voice to action: upholding children's right to participation in shaping policies and laws for digital safety and well-being. *Societies* 15:243. doi: 10.3390/soc15090243

Krishnan, A. (2022). Fifth generation warfare, hybrid warfare, and gray zone conflict: a comparison. *J. Strateg. Secur.* 15, 14–31. doi: 10.5038/1944-0472.15.4.2013

Kure, H. I., Islam, S., and Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Comput. Applic.* 34, 15241–15271. doi: 10.1007/s00521-022-06959-2

Larsson, O. L. (2021). The connections between crisis and war preparedness in Sweden. *Secur. Dialogue* 52, 306–324. doi: 10.1177/0967010620936849

Libiseller, C. (2023). 'Hybrid warfare' as an academic fashion. *J. Strateg. Stud.* 46, 858–880. doi: 10.1080/01402390.2023.2177987

Ljungkvist, K. (2024). The military-strategic rationality of hybrid warfare: everyday total defense under strategic non-peace in the case of Sweden. *Eur. J. Int. Secur.* 9, 533–552. doi: 10.1017/eis.2024.18

Ludendorff, E. v. (1935). Der totale Krieg. Munich: Ludendorffs.

Ludendorff, E. v. (1940). Apostle of the "total war". *Living Age*, March 1940, 22–25.

Luttwak, E. N. (2016). Coup d'état. A practical handbook – Revised edition by Esward N. Luttwak. Cambridge: Harvard University Press.

Mazarr, M. J. (2015). Mastering the gray zone: understanding a changing era of conflict. Carlisle: Army War College Press.

Meadwell, H. (2001). The long nineteenth century in Europe. *Rev. Int. Stud.* 27, 165–189. Available online at: http://www.jstor.org/stable/45299509

Michalec, O., Milyaeva, S., and Rashid, A. (2022). When the future meets the past: can safety and cyber security coexist in modern critical infrastructures? *Big Data Soc.* 9. doi: 10.1177/20539517221108369

Mohamed, B. H., and Osman, A. B. (2022). The rise of China as a hegemonic power: the case for a partial peaceful rise. *J. Reg. Secur.* 2, 187–207. doi: 10.5937/jrs0-31562

Mumford, A., and Carlucci, P. (2023). Hybrid warfare: the continuation of ambiguity by other means. *Eur. J. Int. Secur.* 8, 192–206. doi: 10.1017/eis.2022.19

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *Int. Secur.* 41, 44–71. doi: 10.1162/ISEC_a_00266

Puyvelde, D. V., and Brantly, A. F. (2019). Cybersecurity: politics, governance and conflict in cyberspace. Cambridge: Polity Press.

Sari, A. (2020). Legal resilience in an era of grey zone conflicts and hybrid threats. *Cambridge Rev. Int. Aff.* 33, 846–867. doi: 10.1080/09557571.2020.1752147

Schmitt, C. (2002). A politikai fogalma [The concept of the political]. Budapest: Osiris – Pallas Stúdió – Attraktor.

Schmitt, C. (2007). Theory of partisan. New York: Telos Press Publishing.

Steingartner, W., and Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. *Acta Polytech. Hung.* 18, 25–46. doi: 10.12700/APH.18.3.2021.3.3

Vanaga, N., and Rostokos, T. (2019). Deterring Russia in Europe. Defense strategies for neighboring states. London – New York: Routledge.

Wissmann, M., Nilsson, N., Palmerz, B., and Tunholm, P. (2021). Hybrid warfare. Security and Assymetric conflict in international relations. London: IB TAURIS.

Wither, J. K. (2020). Back to the future? Nordic total defence concepts. *Def. Stud.* 20, 61–81. doi: 10.1080/14702436.2020.1718498

Wither, J. K. (2023). Hybrid warfare revisited: a battle of 'buzzwords'. *Connect* 1, 7–27. doi: 10.11610/Connections.22.1.02

Zhen, L., Yan, B., Tang, J. L., Nan, Y., and Yang, A. (2023). Social network dynamics, bots, and community-based online misinformation spread: lessons from anti-refugee and COVID-19 misinformation cases. *Inf. Soc.* 39, 17–34. doi: 10.1080/01972243.2022.2139031