Cyber risk logics and their implications for cybersecurity

SARAH BACKMAN AND TIM STEVENS*

Risk has long been the object of theorization and discussion within International Relations (IR) and security studies. Scholars have identified and sought to explain shifts in state and corporate practices that have moved risk to the heart of decision-making in international affairs across defence, security, intelligence, diplomacy and the wider political economy of private–public interactions. Recent years have also seen an increasing number of risk-themed contributions within cybersecurity/IR scholarship. While these contributions have provided valuable insights into 'cyber risk' and associated topics, they have often reflected a general IR approach to risk that assumes an overarching logic in its derivation and expression, particularly as related to its nominal counterpart, security. There have been few studies exploring the simultaneous existence of different cyber risk logics within a given organizational or political setting. We see this as problematic, as it may underplay or mask the plurality of risk practices and the interaction between different risk rationalities and modalities in the same organizational or political context. It also potentially overdetermines the relationship between risk and security. In this article, we aim to move the conversation forward by offering a more heterogeneous view of cyber risk. Specifically, we propose that at least two logics can be discerned in cyber risk: one threat-oriented (risk as potential threats), and one systems-oriented (risk as uncertainty). A central aspect of the elevation of cybersecurity from a technical to a traditional threat politics issue has been to interlink an outward-looking focus on external threats with a more inward attention to systems and vulnerabilities.[1] Through the application of our risk typology, we can explore the role of risk in this process.

Our article is structured in six sections. The first argues that risk is more internally diverse than is sometimes portrayed in the risk literature within IR. We propose that multiple risk logics may coexist, interact and compete in practice and

* This article is part of a special section in the November 2024 issue of *International Affairs* on 'Cybersecurity and International Relations: developing thinking tools for digital world politics', guest-edited by Tobias Liebetrau and Linda Monsees. The authors are grateful to the guest editors, journal editors and three peer reviewers for their constructive comments and suggestions on draft versions of this article.

[1] Myriam Dunn Cavelty and Andreas Wenger, 'Introduction: cyber security between socio-technological uncertainty and political fragmentation', in Myriam Dunn Cavelty and Andreas Wenger, eds, *Cyber-security politics: socio-technological transformations and political fragmentation* (Abingdon and New York: Routledge, 2022), pp. 1–13 at p. 3.

International Affairs **100**: 6 (2024) 2441–2460; DOI: 10.1093/ia/iiae236

policy contexts, each with a different relationship to 'conventional' threat-based security. In the second section, we specifically focus on this multiplicity of risk in the context of cybersecurity. We propose the existence of two distinct 'cyber risk logics' along a continuum based on their relationship with threat politics: cyber risk as potential threats and cyber risk as uncertainty. The third section outlines a provisional case-study of the United Kingdom, showing how these logics are presented in the UK's public guidance on cyber risk management, as well as in cybersecurity policy documents. We examine how these logics coexist and interact in this context. We then discuss how the configuration of different cyber risk modalities can play a role in connecting the technical, inward and systems focus to traditional threat politics. We conclude by, first, exploring the implications of our differential risk logic argument for IR theory and practice, in respect of the identification of plural risk rationalities and the relationship between risk and security, and then discuss the role of cyber risk in comprehending and constructing 'the international'.[2]

Risk in International Relations

Risk has evolved in a complex fashion and is closely interlinked with developments in technology, economy, politics and culture.[3] The overall trajectory of risk studies in IR is from the localized risks of early modernity to the global and systemic risks of the twenty-first century.[4] In the 1990s, IR began to take risk seriously as an object of disciplinary attention. This was partly driven by an appreciation that 'security' should be conceptualized more expansively than a conventional focus on military threats allowed. This 'broadening' move brought political theory back into security, whereby security could be extended to 'referents' beyond and below 'national security' and 'the state'.[5] It expanded the range of threats that affect a given referent and the diversity of responses to conditions of insecurity, situating 'risk' and 'risk management' as complementary to, or competitive with, 'security' as the principal mode of engagement with problems of war, terrorism, migration, environmental degradation and so on.[6] Two other intellectual developments furthered the translation of risk into IR. First, the sociological theorization of 'risk society' published in English in the early 1990s; and second, the formalization of 'securitization theory' later that decade.

[2] Linda Monsees and Tobias Liebetrau, 'Cybersecurity in International Relations: developing thinking tools for digital world politics', *International Affairs* 100: 6, 2024, pp. 2303–14, https://doi.org/10.1093/ia/iiae232.

[3] Peter L. Bernstein, *Against the gods: the remarkable story of risk* (Hoboken, NJ: John Wiley & Sons, 1996); Robert Deuchars, *The international political economy of risk: rationalism, calculation and power* (Abingdon and New York: Routledge, 2004).

[4] Nigel Gould-Davies, *Tectonic politics: global political risk in an age of transformation* (Washington DC and London: Brookings Institution Press and Royal Institute of International Affairs, 2019); Virginia Haufler, *Dangerous commerce: insurance and the management of international risk* [1997] (Ithaca, NY: Cornell University Press, 2019).

[5] Ken Booth, *Theory of world security* (Cambridge, UK: Cambridge University Press, 2007), pp. 149–81; Barry Buzan and Lene Hansen, *The evolution of international security studies* (Cambridge, UK: Cambridge University Press, 2009), pp. 187–225.

[6] Buzan and Hansen, *The evolution of international security studies,* pp. 250–1; Karen Lund Petersen, 'Risk analysis—a field within security studies', *European Journal of International Relations* 18: 4, 2012, pp. 693–717, https://doi.org/10.1177/1354066111409770.

In their formulations of the 'risk society', Ulrich Beck and Anthony Giddens led a sociological turn in the theorization of risks.[7] In modern society, they argued, risks have changed fundamentally. Risks are no longer relatively localized and are therefore less controllable and calculable than in the past: modern risks are characterized by their global, anthropogenic and incalculable nature. Beck made a clear distinction between 'calculable risk' and novel 'manufactured uncertainties' that are not geographically bound; the consequences of the latter are impossible to calculate and their effects may be irreversible.[8] The risk society that emerges in a world of manufactured uncertainties is therefore the 'uninsurable society', beyond the capacity of historical management practices to control and calculate.[9] The risk society framing became influential in IR and was adopted in several subfields, including that of Strategic Studies, in which proactive risk management of uncertainty through military force displaced the traditional strategic rationale of responding to known threats.[10]

Securitization theory sparked further debates regarding the relationship between risk- and threat-based approaches to security. Classic Copenhagen School securitization concerns the construction of threats as immediate, identifiable and possible to eliminate by exceptional measures exercised outside normal political deliberations.[11] Questions as to where risk sits in relation to this process (and threat-based security more broadly) produced at least two different strands of argument. The first (associated with critical security and governmentality perspectives) sees risk as another mode of threat-based security, one which expands the boundaries of 'threat' and allows claims of 'security' to encompass the unlikely, the long-term and the speculative.[12] The other, more classical, 'Copenhagen' perspective argues that risk politics and threat politics differ: although risk and threat as security logics often overlap in practice, they are not mutually identifiable.[13] Olaf Corry proposed that the adoption of risk postures portends a 'riskification' of security, whereby actors construct entities politically as 'risks' rather than 'threats'.[14]

[7] Anthony Giddens, *The consequences of modernity* (Cambridge, UK: Polity, 1990); Ulrich Beck, *Risk society: towards a new modernity* [1986] (London: SAGE, 1992).

[8] Ulrich Beck, *World at risk* (Cambridge, UK: Polity, 2009), p. 294.

[9] Ulrich Beck, *World risk society* (Cambridge, UK: Polity, 1999), pp. 31–4.

[10] Mikkel Vedby Rasmussen, 'Reflexive security: NATO and international risk society', *Millennium: Journal of International Studies* 30: 2, 2001, pp. 285–309, https://doi.org/10.1177/03058298010300020901; Yee-Kuang Heng, *War as risk management: strategy and conflict in an age of globalised risks* (Abingdon and New York: Routledge, 2006); Mikkel Vedby Rasmussen, *The risk society at war: terror, technology and strategy in the twenty-first century* (Cambridge, UK: Cambridge University Press, 2006); Christopher Coker, *War in an age of risk* (Cambridge, UK: Polity, 2009).

[11] Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: a new framework for analysis* (Boulder, CO: Lynne Rienner Publishers, 1998).

[12] Claudia Aradau and Rens van Munster, 'Governing terrorism through risk; taking precautions, (un) knowing the future', *European Journal of International Relations* 13: 1, 2007, pp. 89–115, https://doi.org/10.1177/1354066107074290; Jessica Kirk, 'From threat to risk? Exceptionalism and logics of health security', *International Studies Quarterly* 64: 2, 2020, pp. 266–76, https://doi.org/10.1093/isq/sqaa021.

[13] Ole Wæver, 'Politics, security, theory', *Security Dialogue* 42: 4–5, 2011, pp. 465–80, https://doi.org/10.1177/0967010611418718.

[14] Olaf Corry, 'Securitisation and "riskification": second-order security and the politics of climate change', *Millennium: Journal of International Studies* 40: 2, 2012, pp. 235–58, https://doi.org/10.1177/0305829811419444.

One difference between these perspectives centres on 'exceptionalism', drawing on Carl Schmitt's sovereign suspension of the rule of law in times of crisis or perceived need.[15] In classical securitization, as in 'riskification', exceptional measures embrace coercive and other means outside 'normal' governance to manage a perceived 'threatening other', such as through military and intelligence operations.[16] Governmentality perspectives focus instead on management activities beyond militarism and within the scope of non-exceptional 'normalcy', including routinized practices of bureaucratic risk analysis, assessment and management.[17] Scholars have challenged the strictly Schmittian interpretation of exceptionalism, which is also connected to the perceived dichotomy between risk and threat security, as well as between the 'politicized' and 'securitized'. Jessica Kirk suggests that while security and risk may differ in certain aspects (not least the scope and scale of exceptional measures), risk, like security, may also make claims of exceptional danger that demand (albeit minor) alterations of political, legal and social norms.[18] From this viewpoint, risk and threat security are not counter-concepts demarcated by (non-)exceptionalism, but lie on opposite ends of the same spectrum while being intertwined in diverse ways 'in the middle'.[19] Similarly, Jef Huysmans argues that exceptionalism is not a static and rigid state (as understood by, for example, classical securitization), but can be conceptualized as a continuum along which politics shift and slide over time.[20] Exceptionalism can thus prosper by the gradual accumulation of mundane security procedures and technologies ('little security nothings').[21]

Andrew Neal has examined explicitly the perceived division between security and politics. Neal contends that characterizing security as anti-politics, emphasizing the distinction between 'normal' politics and security (including binaries like norm/exception and politicized/securitized), is an outdated notion, one which may have been an accurate description of security politics once but is no longer.[22] While security politics may involve states of exception and exceptional measures, a majority of security politics is now happening inside the 'normal' political sphere as an institutional site of professional political practice.[23] This could entail the accumulation of 'little security nothings' within the realms of 'normality', but not by default. According to Neal, the development of security as politics is not unambiguously good or bad, but its transition to something more

[15] Michael C. Williams, 'Words, images, enemies: securitization and international politics', *International Studies Quarterly* 47: 4, 2003, pp. 511–31, https://doi.org/10.1046/j.0020-8833.2003.00277.x.
[16] Wæver, 'Politics, security, theory'; Corry, 'Securitisation and "riskification"'.
[17] Didier Bigo, 'Globalized (in)security: the field and the ban-opticon', in Didier Bigo and Anastassia Tsoukala, eds, *Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11* (Abingdon and New York: Routledge, 2008), pp. 10–48.
[18] Kirk, 'From threat to risk?', p. 267.
[19] Kirk, 'From threat to risk?', p. 267.
[20] Jef Huysmans, 'Minding exceptions: the politics of insecurity and liberal democracy', *Contemporary Political Theory*, vol. 3, 2004, pp. 321–41 at p. 330, https://doi.org/10.1057/palgrave.cpt.9300137.
[21] Huysmans, 'Minding exceptions', p. 337; Jef Huysmans, 'What's in an act? On security speech acts and little security nothings', *Security Dialogue* 42: 4–5, 2011, pp. 371–83, https://doi.org/10.1177/0967010611418713.
[22] Andrew W. Neal, *Security as politics: beyond the state of exception* (Edinburgh: Edinburgh University Press, 2019), p. 7.
[23] Neal, *Security as politics*, p. 10.

multifaceted and complex challenges our traditional conceptions and analytical delineations of security.[24]

The question of the relationship between risk and threat security has generated a rich and valuable literature in IR; however, it has also contributed to a tendency to conceptualize risk as a rationality with a relatively stable relationship to security. It is either different from security, or it is categorically interwoven with security in theoretical and practical terms. We see this as problematic, as it may underplay or mask a richer and more complex genealogy of risk and the relationship between risk and security.[25] For example, as Mitchell Dean suggested in his critique of the 'risk society', 'risk and its techniques are plural and heterogeneous and its significance cannot be exhausted by a narrative of a shift from a quantitative calculation of risk to the globalization of incalculable risks'.[26] Reifying risk as one form or another ignores the fact that multiple risk logics or rationalities exist (and have always existed) in any given spatiotemporal context.[27]

In this article, we develop a more heterogeneous view of risk logics and their relationship to threat security. We do so by proposing a typology of (cyber) risk modalities in the form of two 'logics': 'cyber risk as potential threats' and 'cyber risk as uncertainty'. As we will show, these conceptual and analytical frameworks can help provide theoretical focus to scholarly enquiry, but they are also risk logics which can be studied empirically in their discursive and material formations. Nor should we think of them as mutually exclusive, as they can coexist and interact in organizational and wider social settings at multiple levels of governance and fields of practice. Scholars have been able to distinguish between contrasting risk and security rationalities within the same organization, such as the concurrence of risk- and threat-based security logics in European Union cybersecurity governance.[28] They have also been able to identify differential cyber risk models and conceptualizations of cyber risk between states.[29] However, there have been few studies identifying the simultaneous existence of different cyber risk logics within a given organizational or political setting.[30]

Our risk typology describes two distinct risk logics. We see 'logics' as intersubjective modalities or approaches that draw upon shared material and symbolic resources, carry pronounced conceptualizations and assumptions, and can be

[24] Neal, *Security as politics*, pp. 9–11.
[25] Lund Petersen, 'Risk analysis'.
[26] Mitchell Dean, *Governmentality: power and rule in modern society* (London: SAGE, 2009), p. 191.
[27] Mitchell Dean, 'Risk, calculable and incalculable', in Deborah Lupton, ed., *Risk and sociocultural theory: new directions and perspectives* (Cambridge, UK: Cambridge University Press, 1999), pp. 131–59; Dean, *Governmentality*, pp. 217–18.
[28] Sarah Backman, 'Risk vs. threat-based cybersecurity: the case of the EU', *European Security* 32: 1, 2023, pp. 85–103, https://doi.org/10.1080/09662839.2022.2069464. See also Myriam Dunn Cavelty, 'Cybersecurity between hypersecuritization and technological routine', in Eneken Tikk and Mika Kerttunen, eds, *Routledge handbook of international cybersecurity* (Abingdon and New York: Routledge, 2020), pp. 11–21.
[29] Aaron F. Brantly, 'Risk and uncertainty can be analyzed in cyberspace', *Journal of Cybersecurity* 7: 1, 2021, https://doi.org/10.1093/cybsec/tyab001; Monica Kaminska, *To retaliate or not: a matter of cyber risk perception*, PhD diss., University of Oxford, 2021.
[30] Myriam Dunn Cavelty and Florian J. Egloff, 'Hyper-securitization, everyday security practice and technification: cyber-security logics in Switzerland', *Swiss Political Science Review* 27: 1, 2021, pp. 139–49, https://doi.org/10.1111/spsr.12433.

detected through discourses and practices. Each risk logic is future-oriented, of course, and is concerned with protecting a referent object, but they differ in important ways, namely: problem focus; analytical concerns; aims; and associated practices (and what actors are involved in carrying them out). Importantly, this also means that they differ in their relationship to security.

The following sections unpack the two risk logics, including their key characteristics, how they have been approached analytically and how they manifest in cybersecurity. We then explore these risk logics in practice, including how they interact with and relate to security, using the empirical case-study of the UK. We analyse the public-facing guidance on cyber risk management as issued by the National Cyber Security Centre (NCSC), founded in 2016 to provide government advice and support to British public- and private-sector organizations. We assess NCSC guidance against the background of key cyber policy documents, including four UK national cybersecurity strategies (from 2009, 2011, 2016 and 2022), and the *Government cyber security strategy* (2022). The UK is selected in part due to the authors' familiarity with the case, but also because the UK has one of the longest institutional histories of cyber policy development, much of which has negotiated the shifting relationships between cyber risk and cybersecurity.[31]

Cyber risk logics

Cybersecurity is unusual in that it seeks to regulate an environment ('cyberspace') that is global, transnational and more or less ubiquitous in its material dimensions and in its mutual dependencies with other socio-technical and political domains. Perceptions of risk and uncertainty are endemic to international affairs but, as Aaron Brantly notes, they take on additional inflections in cyberspace due to environmental complexity, unpredictability of effects, the ability of actors to shield their identities, and the frequent difficulties of translating technical knowledge across functional boundaries.[32] As a form of security, a principal mode of cybersecurity remains the tackling of immediate threats, which include cybercrime, digital espionage, state military and intelligence threats, and non-state political actors. Given epistemic and structural uncertainty, risk has emerged as an increasing form of engagement with cyber problems, such that we might argue for an overall 'riskification' of cybersecurity that has helped produce cybersecurity as a distinct field of policy and practice.[33]

To date, there is little work on the internal differentiation of cybersecurity risk and how risk conceptions relate to or support cyber security politics, although the fact that risk- and threat-based security logics coexist in cybersecurity is recog-

[31] Tim Stevens, 'United Kingdom: pragmatism and adaptability in the cyber realm', in Scott N. Romaniuk and Mary Manjikian, eds, *Routledge companion to global cyber-security strategy* (Abingdon and New York: Routledge, 2021), pp. 191–200.

[32] Brantly, 'Risk and uncertainty'.

[33] Karsten Friis and Erik Reichborn-Kjennerud, 'From cyber threats to cyber risks', in Karsten Friis and Jens Ringsmose, eds, *Conflict in cyber space: theoretical, strategic and legal perspectives* (Abingdon and New York: Routledge, 2016), pp. 27–44.

nized well.[34] The following discussion introduces a typology of risk that we apply to cybersecurity: 'risk as potential threats' and 'risk as uncertainty'.

Risk as potential threats

Framing risk as potential threats is endemic to IR treatments of risk. For example, Strategic Studies scholars have argued that war has been reinvented in terms of risk management.[35] They define risk management through military means as the 'anticipation of threats', coupled with practices geared to preventing an undesirable threat scenario 'from becoming real'.[36] While threats are definable, identifiable, immediate and often connected to specific threatening actors, risks are connected to future potentialities or scenarios ('what could happen').[37] This approach aims to render risks knowable, manageable and controllable, although their proliferation means that not all risks can be controlled. Emphasis is therefore placed on judgement—decision-makers have to choose which risks to 'manage'—and on actions that attempt to forestall the materialization of possible threats. Faced with 'infinite risks' in the shape of potential threats, risk management becomes about foreseeing and disciplining the future through scenarios, estimation, models, and pre-emptive and preventive measures aimed at countering the actualization of threat scenarios.[38] Risk as a response to potential threats is also the principal object of critique in critical risk and governmentality studies. For instance, Claudia Aradau et al. define risk as 'the probability of an undesirable event happening in the future'.[39] Inherent in risk, therefore, are efforts to foresee an event (speculation) and to tame uncertainty through calculation and control. Analytical focus is directed on the technologies deployed to manage, control and pre-empt potential threats within the realms of 'normalcy'.

These approaches treat risk conceptually as 'the anticipation of threats' and therefore study risk practices that try to make the incalculable calculable, that imagine future scenarios and that legitimize threat-oriented pre-emptive measures.[40] A central premise of our argument is that although the 'risk as potential threats' logic is prominent—perhaps even dominant—in security politics and governance, risk practices are more heterogeneous than can be captured by this

[34] Myriam Dunn Cavelty, 'From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse', *International Studies Review* 15: 1, 2013, pp. 105–22, https://doi.org/10.1111/misr.12023. See also Helena Farrand Carrapico, Narzanin Massoumi, William McGowan and Gabe Mythen, 'Disputing security and risk: the convoluted politics of uncertainty', in Ian Scoones and Andy Stirling, eds, *The politics of uncertainty: challenges of transformation* (London: Routledge, 2020), pp. 151–63.

[35] Heng, *War as risk management*; Rasmussen, *The risk society at war*; Coker, *War in an age of risk*.

[36] Rasmussen, *The risk society at war*, p. 4; William Clapton, *Risk and hierarchy in international society: liberal interventionism in the post-Cold War era* (Basingstoke: Palgrave Macmillan, 2014), pp. 29–35.

[37] Michael J. Williams, *NATO, security and risk management: from Kosovo to Kandahar* (Abingdon and New York: Routledge, 2009), p. 66.

[38] Heng, *War as risk management*.

[39] Claudia Aradau, Luis Lobo-Guerrero and Rens van Munster, 'Security, technologies of risk, and the political: guest editors' introduction', *Security Dialogue* 39: 2–3, 2008, pp. 147–54 at p. 148, https://doi.org/10.1177/0967010608089159.

[40] Claudia Aradau and Rens van Munster, *Politics of catastrophe: genealogies of the unknown* (Abingdon and New York: Routledge, 2011).

perspective alone. We will address the contrasting logic of 'risk as uncertainty' subsequently, but how do potential threats propel risk thinking and practice in cybersecurity?

A 'risk as potential threats' approach understands risks as the anticipation of threats or threatening events, which can be controlled and pre-empted through interventions external to the object of protection. In cybersecurity, this risk logic prioritizes cyber threats and antagonists 'in' global cyberspace, such as advanced persistent threats and ransomware groups, rather than, for example, the internal vulnerabilities of digital socio-technical systems that might be exploited by those actors. The combination of an emphasis on cyber threats and cyber risk mitigation as a threat-oriented challenge of actionable information leads to intelligence-centred risk mitigation measures: monitoring of (potential) cyber threats; cyber threat modelling; threat scenario building; and cyber threat intelligence.[41] In practice, this is reflected in the close alignment between national technical authorities for cybersecurity (and other centres of adjacent expertise) and signals intelligence (SIGINT) agencies.[42]

The overarching aim is to identify, calculate and pre-empt potential cyber threats or potential disruptive activities of known threat actors. In other words, to turn what is viewed as the incalculable into calculable information and thereby generate a knowledge base with which decisions can be made.[43] This risk logic deploys pre-emptive and precautionary activities directed at mitigating or eliminating potential cyber threats, especially when they can be linked to identifiable threat actors. In national policy, this logic is materialized in activities to achieve 'cyber deterrence', precautionary development of offensive cyber capabilities, or by policies of 'persistent engagement' with adversaries in cyberspace.[44] All feature variously in the cyber postures and policies of democratic states. The cyber risk as potential threats logic is scenario-driven and preoccupied with imaginative speculation of the potential negative effects of future possible cyber attacks and other malign cyber eventualities.[45] Historically, it is striking how hypothetical cyber disaster scenarios have been used in cybersecurity discourse, reflecting an extreme reliance on visualizations of future threats to legitimatize securitizing moves (hypersecuritization tendencies).[46] The shifting empirical reality of cyber

[41] Troy Mattern, John Felker, Randy Borum and George Bamford, 'Operational levels of cyber intelligence', *International Journal of Intelligence and CounterIntelligence* 27: 4, 2014, pp. 702–19, https://doi.org/10.1080/08850607.2014.924811; Martin Lee, *Cyber threat intelligence* (Hoboken, NJ: John Wiley & Sons, 2023).

[42] John Ferris, *Behind the enigma: the authorised history of GCHQ, Britain's secret cyber-intelligence agency* (London: Bloomsbury, 2020), pp. 687–713.

[43] Aaron F. Brantly, *The decision to attack: military and intelligence cyber decision-making* (Athens, GA: University of Georgia Press, 2016); Brantly, 'Risk and uncertainty'.

[44] Michael P. Fischerkeller, Emily O. Goldman and Richard J. Harknett, *Cyber persistence theory: redefining national security in cyberspace* (New York: Oxford University Press, 2022); Max Smeets, *No shortcuts: why states struggle to develop a military cyber-force* (London: Hurst, 2022); Erica D. Borghard and Shawn W. Lonergan, 'Deterrence by denial in cyberspace', *Journal of Strategic Studies* 46: 3, 2023, pp. 534–69, https://doi.org/10.1080/01402390.2021.1944856.

[45] Myriam Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age* (London: Routledge, 2007); Sean T. Lawson, *Cybersecurity discourse in the United States: cyber-doom rhetoric and beyond* (Abingdon and New York: Routledge, 2020).

[46] Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly* 53: 4, 2009, pp. 1155–75 at p. 1164, https://doi.org/10.1111/j.1468-2478.2009.00572.x. See

incidents has contributed to adjusting discourses away from ideas of 'cyber doom'.[47] Nevertheless, socio-technical imaginaries of 'cyber disasters' and ideas about preventing them through externally oriented countermeasures remain vital in contemporary sense-making of cyber risk and threats.[48]

Risk as uncertainty

In contrast, a 'risk as uncertainty' logic treats risks as systemic and inherent, with an emphasis on socio-technical vulnerability. Rather than trying to pre-empt potential threats or potentially consequential operations by threat actors through scenarios, intelligence generation, quantification and control, this risk logic integrates to a greater extent an acceptance of the unknown. Consequently, it is not oriented around attempts to 'tame' uncertainty and 'control' risk through methodologies of quantification and prediction, but considers longer-term strategies that recognize the value and limitations of forecasting under conditions of epistemic uncertainty and socio-technical change.[49] In this formulation, uncertainty is not what is left over—a residual—after calculable risk is measured and managed, but an intrinsic feature of all socio-technical systems.[50] Instead of measures aimed at threat mitigation and elimination, its energies are directed internally towards resilience, adaptation and reliability, and to the ability to 'cope with' and 'bounce back from' diverse unexpected and negative events, whether these are caused by accidents, errors or any other harmful phenomena that arise in complex socio-technical settings.[51]

In contrast to the logic of risk as potential threats, the logic of risk as uncertainty has been less commonly addressed in IR, despite widespread recognition of the epistemic uncertainty engendered by asymmetric information pertaining to actors' intentions and by imperfect knowledge of the structural conditions of international dynamics.[52] When it has been addressed, it has often been through the

also, Myriam Dunn Cavelty, 'The materiality of cyberthreats: securitization logics in popular visual culture', *Critical Studies on Security* 7: 2, 2019, pp. 138–51, https://doi.org/10.1080/21624887.2019.1666632.

[47] Miguel Alberto Gomez and Christopher Whyte, 'Breaking the myth of cyber doom: securitization and normalization of novel threats', *International Studies Quarterly* 65: 4, 2021, pp. 1137–50, https://doi.org/10.1093/isq/sqab034.

[48] Lars Gjesvik and Kacper Szulecki, 'Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout', *European Security* 32: 1, 2023, pp. 104–24, https://doi.org/10.1080/09662839.2022.2082838.

[49] Myriam Dunn Cavelty, 'From predicting to forecasting: uncertainties, scenarios, and their (un-)intended side effects', in Andreas Wenger, Ursula Jasper and Myriam Dunn Cavelty, eds, *The politics and science of prevision: governing and probing the future* (London: Routledge, 2020), pp. 89–103.

[50] Peter J. Katzenstein and Lucia A. Seybert, eds, *Protean power: exploring the uncertain and unexpected in world politics* (Cambridge, UK: Cambridge University Press, 2018). See also, Darryl S. L. Jarvis, 'Theorising risk and uncertainty in International Relations: the contributions of Frank Knight', *International Relations* 25: 3, 2011, pp. 296–312, https://doi.org/10.1177/0047117811415485.

[51] Christian Fjäder, 'The nation-state, national security and resilience in the age of globalization', *Resilience: International Policies, Practices and Discourses* 2: 2, 2014, pp. 114–29, https://doi.org/10.1080/21693293.2014.914771; Myriam Dunn Cavelty, Mareile Kaufmann and Kristian Søby Kristensen, 'Resilience and (in)security: practices, subjects, temporalities', *Security Dialogue* 46: 1, 2015, pp. 3–14, https://doi.org/10.1177/0967010614559637.

[52] Brian C. Rathbun, 'Uncertain about uncertainty: understanding the multiple meanings of a crucial concept in International Relations theory', *International Studies Quarterly* 51: 3, 2007, pp. 533–57, https://doi.org/10.1111/j.1468-2478.2007.00463.x; Jeffrey M. Kaplow and Erik Gartzke, 'The determinants of uncertainty in Interna-

concept of resilience, which has found its way to IR through ecology, psychology, public administration and crisis management studies.[53] Resilience is generally defined as the ability of a system to withstand turbulence through robustness, adaptation and recovery.[54] While resilience is popular in the public administration literature, the IR literature has usually taken a more critical stance, pointing to the tendency of resilience approaches to co-opt neo-liberal governmentality and methodologies of control.[55] In turn, some authors have challenged this view by arguing that resilience is not universally or necessarily tied to neo-liberalism, and have called for critique to be more context-specific.[56]

While uncertainty has been addressed in IR cybersecurity discussions, the concept of cyber resilience has emerged relatively recently, coinciding with an increasing interest in infrastructure and complex socio-technical systems.[57] Some contributions have, for example, focused on the ways in which the concept of cyber resilience connects individuals with aggregate socio-technical systems.[58] Others have discussed cyber resilience as one of several interpretations of cyber risk arising from specific configurations of knowledge and power circulating in socio-technical systems.[59]

A risk as uncertainty approach understands risks as disruptive hazards which are not necessarily connected to specific threat actors or events. It is internally rather than externally oriented. In the context of cybersecurity, this means placing focus on (internal) systemic and conditional sources of danger, such as complex vulnerabilities developing through human-machine interactions in socio-technical systems, rather than through (external) antagonists and their capabilities.[60] In practice, this risk logic focuses on socio-technical and systemic vulnerabilities created by the combination of hyperconnectivity and digital dependencies. The platforms and protocols that establish common operating conditions across global networks also enable the distribution of problems when shared vulnerabilities are identified and exploited, as in the recent case of Log4j, described by NCSC as 'potentially the

tional Relations', *International Studies Quarterly* 65: 2, 2021, pp. 306–19, https://doi.org/10.1093/isq/sqab004; Brantly, 'Risk and uncertainty'.

[53] Jeremy Walker and Melinda Cooper, 'Genealogies of resilience: from systems ecology to the political economy of crisis adaptation', *Security Dialogue* 42: 2, 2011, pp. 143–60, https://doi.org/10.1177/0967010611399616.

[54] Arjen Boin and Martin Lodge, 'Designing resilient institutions for transboundary crisis management: a time for public administration', *Public Administration* 94: 2, 2016, pp. 289–98, https://doi.org/10.1111/padm.12264.

[55] Patrick O'Malley, 'From risk to resilience: technologies of the self in the age of catastrophes', in Bernard Harcourt, ed., *Neoliberalism and risk: the future of risk*, The Carceral Notebooks, vol. 7, 2011, pp. 41–68; Julian Reid and Brad Evans, *Resilient life: the art of living dangerously* (Cambridge, UK and Malden, MA: Polity, 2014); David Chandler and Julian Reid, *The neoliberal subject: resilience, adaptation and vulnerability* (Lanham, MD: Rowman and Littlefield, 2016).

[56] Olaf Corry, 'From defense to resilience: environmental security beyond neo-liberalism', *International Political Sociology* 8: 3, 2014, pp. 256–74, https://doi.org/10.1111/ips.12057.

[57] Lewis Herrington and Richard Aldrich, 'The future of cyber-resilience in an age of global complexity', *Politics* 33: 4, 2013, pp. 299–310, https://doi.org/10.1111/1467-9256.12035.

[58] Myriam Dunn Cavelty, Christine Eriksen and Benjamin Scharte, 'Making cyber security more resilient: adding social considerations to technological fixes', *Journal of Risk Research* 26: 7, 2023, pp. 801–14, https://doi.org/10.1080/13669877.2023.2208146.

[59] Tim Stevens, *Cyber risk: hyperconnectivity and the political economy of uncertainty*, SSRN Scholarly Paper (Social Science Research Network, 2022), http://doi.org/10.2139/ssrn.4280577.

[60] Friis and Reichborn-Kjennerud, 'From cyber threats to cyber risks'; Dunn Cavelty and Wenger, 'Introduction'.

most severe computer vulnerability in years'.[61] Its associated measures are aimed at generating adaptive capacity rather than control.[62] Adaptive capacity includes activities which increase robustness and resilience, meaning enhancing system capability to withstand turbulence of different sorts (cyber 'attacks', but also accidents, mistakes or effects of natural disasters). Since this risk approach tends to acknowledge the limits of predictive knowledge, it is less inclined to lean on the identification, quantification and control of individual risks.

Unlike the risk logic associated with potential threats, which requires intelligence activities and capabilities to identify potential threat actors and events, risk as uncertainty is associated with inward-looking activities which can be conducted largely without specialized (cyber threat) intelligence capabilities. For example, these might include activities such as: gaining and maintaining trust in system performance; ensuring privacy by design and default; and enhancing system redundancy and resilience. Each requires a different type of expertise and a different set of competencies. All of this also means that risk as uncertainty is not as prone to speculation about scenarios of threatening cyber events or cyber-induced disasters. Rather, this logic is oriented towards 'everyday' and 'mundane' compliance activities: making sure systems are maintained through patches and updates; that standards are implemented; and that data and privacy laws are adhered to.

Each of these cyber risk logics is a response to fundamental uncertainty about the world. Yet each reflects different assumptions as to the extent to which uncertainty can be 'tamed' or transformed into 'certainty', whether the main source of danger is external or internal, and what measures key actors deem appropriate in response. These logics are not mutually exclusive, but can coexist within the same political or organizational setting.

Case-study: the United Kingdom

Risk has been a central component of UK cybersecurity since the first iteration of the country's national cybersecurity strategy, in 2009. Indeed, the 2009 strategy puts 'safety, security and resilience' at the top of its agenda, which indicates that tackling known threats has never been the sole motivation behind UK cybersecurity.[63] The attention to risk has intensified in the three subsequent national cybersecurity strategies published by the UK government.[64] This is consistent with UK national security policy and decision-making since the 2010 national security strategy, titled *A strong Britain in an age of uncertainty*, which adopted an overtly

[61] National Cyber Security Centre, 'Log4j vulnerability: what everyone needs to know', https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 12 Sept. 2024).

[62] Dunn Cavelty et al., 'Making cyber security more resilient'.

[63] HM Government, Cabinet Office, *Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space*, 2009, https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf.

[64] A rough proxy for the significance of 'risk' in high-level UK cybersecurity policy can be established by the frequency of its occurrence in the four national cybersecurity strategies to date: 2009 (risk = 29), 2011 (32), 2016 (60) and 2021 (102).

risk-based methodology and approach to 'national security risk assessment'.[65] Risk does not replace a threat-based approach to UK security, but it does represent a 'significant rearticulation' of the 'grammar' of national security.[66] The latest *National cyber strategy* (2022) and *Government cyber security strategy* (2022) define cyber risk as the 'potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm'.[67] This conceptualizes cyber risk as dependent on the identification (and calculation) of a *given* threat, which reflects the external, threat-dependent (and calculative) orientation of a 'risk as potential threats' logic. Risk language also appears several times in relation to the description of threat mitigation, pre-emptive activities and deterrence. When discussing the use of offensive cyber operations, for example, the *National cyber strategy* (2022) identifies '[r]educing the risk of harm to UK armed forces by degrading adversary weapons systems' as an operational activity that could be performed by the National Cyber Force,[68] and considers a desirable (but not yet achieved) outcome of cyber deterrence to be that it has 'fundamentally altered the risk calculus of attackers'.[69]

Nevertheless, a substantial number of risk-related problem statements and measures are also inward and systems-oriented. These are often described under headings such as 'approaching systemic risk', 'cyber assurance' and achieving 'cyber resilience'. The *Government cyber security strategy* defines 'cyber resilience' as the 'ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events'.[70] A key aspect here is the use of the phrase 'cyber events' rather than 'cyber attacks' or 'cyber threats', the former being non-specific and the latter more threat-oriented. 'Cyber assurance' activities include inward-facing and systems-oriented activities such as updating legacy technology, hardening systems, achieving security by design and default, configuring technology, implementing classification and standards, and management of vulnerabilities.[71]

The NCSC is the UK government's principal vector of cybersecurity advice and support. It does not use a consistent definition of risk but, as a government organization, in part respects a common definition of risk across UK government as 'the effect of uncertainty on objectives … usually expressed in terms of causes, potential events, and their consequences'.[72] It also notes that (according

[65] HM Government, *A strong Britain in an age of uncertainty: the national security strategy*, 2010, https://assets.publishing.service.gov.uk/media/5a74cb2de5274a3cb286738d/national-security-strategy.pdf.
[66] Neal, *Security as politics*, p. 243.
[67] HM Government, Cabinet Office, *National cyber strategy 2022: pioneering a cyber future with the whole of the UK*, 2021, https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022, p. 126; HM Government, Cabinet Office, *Government cyber security strategy 2022–2030: building a cyber resilient public sector*, 2022, https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030, p. 79.
[68] HM Government, *National cyber strategy 2022*, p. 43. See also HM Government, National Cyber Force, *Guidance: responsible cyber power in practice*, 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html, p. 4.
[69] HM Government, *National cyber strategy 2022*, p. 25.
[70] HM Government, *Government cyber security strategy 2022–2030*, p. 19.
[71] HM Government, Government Security, 'GovAssure Overview', 2023, https://www.security.gov.uk/guidance/govassure/overview.
[72] National Cyber Security Centre, 'The fundamentals and basics of cyber risk', https://www.ncsc.gov.uk/collection/risk-management/the-fundamentals-and-basics-of-cyber-risk.

to one dictionary) the core meaning of risk is 'the possibility of something bad happening'[73] and that risk can be specified as 'possible future outcomes that we can describe in terms of their chances of occurrence, and the impact they would have if realised'.[74] Noting the need to 'assess, analyse and address' the various components of risk, the NCSC thinking in this space reflects an understanding of risk in terms of speculation (defining possible future outcomes and effects) and as something quantifiable (probabilities of occurrence, measurement of impacts). This aligns with a risk approach that prioritizes potential threats. Additionally, the NCSC's risk management guidance defines the benefits of good risk management in relation to decision-making and creating 'a foundation to adapt and respond to new threats and opportunities as they emerge'.[75] The NCSC's Cyber Assessment Framework highlights the importance of risk assessments being based on 'a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function(s) and your sector' and the performance of 'detailed threat analysis'.[76] This indicates both an external orientation (potential/new threats or opportunities) and the organizational aim of achieving a semblance of control through risk management (threat response).

The overall mission statement of the NCSC reflects an internal and adaptive focus more aligned with risk as uncertainty than with potential threats. It emphasizes activities such as understanding and distilling knowledge into practical and available guidance, responding to cyber incidents and reducing harm, using expertise to nurture cybersecurity capabilities, and reducing risks by securing networks.[77] This is discernible in both the NCSC's component-driven risk perspective, a bottom-up approach to identifying technical vulnerabilities, and its top-driven systemic risk perspective, used for analysing interdependence and potential interaction failures of large complex systems.[78]

The 'risk as uncertainty' logic is particularly evident in the NCSC's cyber risk assurance approach. Instead of focusing on risk in terms of (potential) external threats or threatening events, risk assurance promotes measures to gain and maintain confidence in system reliability.[79] The NCSC outlines several types of cyber risk assurance—intrinsic, extrinsic, implementation and operational—all involving activities intended to foster confidence and trust in cyber-related processes and services from development to implementation and maintenance. For example, this can mean ensuring a product or service goes through a recognized, independ-

[73] National Cyber Security Centre, 'The fundamentals and basics of cyber risk'.
[74] National Cyber Security Centre, 'Glossary', https://www.ncsc.gov.uk/section/advice-guidance/glossary.
[75] National Cyber Security Centre, 'Risk management', https://www.ncsc.gov.uk/collection/10-steps/risk-management.
[76] National Cyber Security Centre, 'Principle A2 risk management', https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-a-managing-security-risk/principle-a2-risk-management.
[77] National Cyber Security Centre, 'What we do', https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.
[78] National Cyber Security Centre, 'Introducing system and component driven risk management approaches', https://www.ncsc.gov.uk/collection/risk-management/introducing-system-and-component-driven-risk-management-approaches.
[79] National Cyber Security Centre, 'How to gain and maintain assurance', https://www.ncsc.gov.uk/collection/risk-management/how-to-gain-and-maintain-assurance.

ent evaluation scheme appropriate to its function and anticipated use.[80] Examples of operational assurance activities include: monitoring for the emergence of new vulnerabilities concerning a product, system or service; applying patches when available to address known security vulnerabilities; training relevant personnel in how to monitor for and apply security patches; and testing whether security patches or updates have been applied and whether these address known vulnerabilities.[81]

A cyber risk as potential threats logic is scenario-driven, preoccupied with potential threats and with imaginative speculation of potential negative effects of cyber attacks. This focus is reflected in several of the NCSC's recommended risk management measures, such as the use of 'attack trees' to explore a chain of events that might lead to a successful attack. These enable risk professionals 'to build a structured and logical image of the cyber security risk to a system from the perspective of possible successful attacks' and provide, a 'visualisation of the problem' that facilitates discussion and the crafting of pre-emptive and preparatory countermeasures.[82] It also recommends the use of 'threat modelling' to identify potential technical threats and attack vectors. Threat modelling serves to 'better understand how a system or service might be attacked or otherwise go wrong'.[83] The adoption of 'an adversarial perspective' by system developers channels the common information security mantra 'to think like the enemy' and consider who might wish to attack a system and how they might do so. Penetration testing is widely considered industry best practice, and is a mode of evaluation that requires 'red teams' to adopt the adversarial posture of a speculative attacker and probe for technical vulnerabilities and organizational flaws ahead of possible future network intrusions.[84] 'Cyber security scenarios' should be used to understand challenges to organizational cybersecurity and develop robust response and readiness frameworks. These tend to involve non-technical as well as technical personnel and encourage people 'to think differently about the future, so they can plan for cyber security risks and outcomes that might currently seem implausible or far-fetched'.[85] The general intention is 'to map out different potential futures' as a guide to decision-making but not to 'overestimate the potential realism of the futures investigated'.[86]

Coexistence and interaction of cyber risk logics

So far, our analysis has identified the coexistence of two 'cyber risk logics' in the UK's cyber policies and the public-facing guidance on cyber risk manage-

[80] National Cyber Security Centre, 'How to gain and maintain assurance'.
[81] National Cyber Security Centre, 'How to gain and maintain assurance'.
[82] National Cyber Security Centre, 'Using attack trees to understand cybersecurity risk', https://www.ncsc.gov.uk/collection/risk-management/using-attack-trees-to-understand-cyber-security-risk.
[83] National Cyber Security Centre, 'Threat modelling', https://www.ncsc.gov.uk/collection/risk-management/threat-modelling.
[84] National Cyber Security Centre, 'Penetration testing', https://www.ncsc.gov.uk/guidance/penetration-testing.
[85] National Cyber Security Centre, 'Using cyber security scenarios', https://www.ncsc.gov.uk/collection/risk-management/using-cyber-security-scenarios.
[86] National Cyber Security Centre, 'Using cyber security scenarios'.

ment by the NCSC. One logic treats risk as contingent on potential threats or threatening events, with associated measures mostly outward-facing in terms of defining, anticipating and/or pre-empting threats/threat events. The other logic frames risk with respect to (systems) vulnerability and uncertainty, with associated measures—resilience, adaptability and reliability—being focused on internal entities, processes and structures. Distinguishing between these risk logics allows detailed attention to what types of risk understandings are prioritized, which risk measures are seen as appropriate over others, which actors are seen as the relevant risk 'managers', and the precise effects of these risk–security assemblages.

We found multiple indications of a 'risk as uncertainty' logic in UK cybersecurity policy and in the risk definitions and recommendations of the NCSC. This is specifically reflected in guidance referring to 'systemic risks', 'achieving resilience' and 'information assurance'. These guidelines minimally reference specific threats or threat actors, advocate for bottom-up measures to mitigate risk, and emphasize the systemic origins of vulnerability. Nonetheless, a significant portion of risk-related sections in UK cyber policy and strategy and NCSC risk management guidance still reflects a threat-based and outward-facing posture aligned with the overall threat-dependent risk definition of recent UK cybersecurity strategy. Of course, this cannot be divorced from the institutional context from which these risk logics emerge and within which they are reproduced. The organizational context of a given entity is likely to influence its understanding of risk.

The NCSC is part of the Government Communications Headquarters (better known by its initials—GCHQ), the UK's signals intelligence agency, whose primary mission is to 'identify, analyse and disrupt threats to the UK'.[87] GCHQ's strategic and operational priorities are set by the National Security Council (chaired by the Prime Minister), as well as by the ongoing advice of the Joint Intelligence Committee. The decision to found and then situate the NCSC within the GCHQ hierarchy was taken in 2015, the major factor being GCHQ's existing cybersecurity expertise and capacity.[88] The NCSC therefore operates under the umbrella of an organization which is by default oriented towards understanding risks as potential threats.[89] We have noted the possible institutional constraining and enabling effects of the NCSC's situation within the UK intelligence community, and the influence of GCHQ over the NCSC and UK cybersecurity has long been questioned. Such views are normally animated by a desire to involve a greater range of stakeholders in cybersecurity decision-making and delivery, although issues of classification, secrecy and institutional mindset also play their part.[90] Read through the prism of competing and complementary risk logics, we can add

[87] Government Communications Headquarters, 'Overview', https://www.gchq.gov.uk/section/mission/overview.

[88] Robert Hannigan, *Organising a government for cyber: the creation of the UK's National Cyber Security Centre* (London: Royal United Services Institute, 2019), https://static.rusi.org/20190227_hannigan_final_web.pdf.

[89] Richard J. Aldrich, 'From SIGINT to cyber: a hundred years of Britain's biggest intelligence agency', *Intelligence and National Security* 36: 6, 2021, pp. 910–17, https://doi.org/10.1080/02684527.2021.1899636.

[90] Kristan Stoddart, 'UK cyber security and critical national infrastructure protection', *International Affairs* 92: 5, 2016, pp. 1079–1105 at pp. 1090–91, https://doi.org/10.1111/1468-2346.12706; Stevens, 'United Kingdom', p. 193.

a potential drift towards more subtle expressions of 'threat security' that emerge from the bureaucratic cultures of intelligence in the UK.

Discussion

Risk is not expressed in a singular logic or discrete set of unified activities but is a multimodal assemblage of competing or complementary logics and associated practices. We have introduced a typology of cyber risk which includes two main modalities or 'logics'— risk as potential threats, and risk as uncertainty. Each carries different meanings of cyber risk which embed different measures, priorities and hierarchies. These differences also lead to particular 'security' outcomes, themselves affected by the relative balance of risk logics in specific contexts and over time.

A key aspect of making cybersecurity a traditional threat politics issue has been to connect an inward focus on technical systems to an outward focus on threats and threat actors.[91] We suggest that risk (or, more precisely, the configuration of the different risk modalities that shapes the overall understanding of risk) has a role in this process, which supports the elevation of cybersecurity from a technical issue to a tool for the pursuit of political security goals. Central to this role is the 'risk as potential threats' logic. We argue that this risk modality is more likely to involve activities that resemble or enable classical security actions, even if their impulse lies within the field of risk and its management. This applies to exceptionalism in a strict Copenhagen School interpretation, as expressed in preventive and pre-emptive military-intelligence offensive cyber operations. The United States' 'persistent engagement' cyber doctrine, for instance, signifies a conceptual and operational shift from reaction to proaction and the use of impressive national cyber capacity to manage risks in and through cyberspace.[92] Indeed, risk language is also used by the UK to legitimize the increase of cyber-related intelligence activities and offensive cyber operations to 'mitigate' and 'prevent' threatening events. Less dramatic security activities are also identified in the broader frameworks offered by governmentality perspectives. These identify routinized practices of monitoring, calculation and control, and intelligence-centred activities that manage possible cyber threats and are constituted in 'tiny transgressions' of law, ethics and norms within the realms of 'normalcy'. In aggregate, these constitute a whole greater than the sum of its parts.[93]

Most cybersecurity activities are still low-level, mundane and routine practices, often in the shape of risk activities that reflect a focus on vulnerabilities, technical maintenance and resilience. The 'risk as potential threats' logic is located somewhere between this inward focus on systems and 'classical' security focused

[91] Dunn Cavelty and Wenger, 'Introduction', p. 3.

[92] James A. Lewis, 'Risk, resilience, and retaliation: American perspectives on international cybersecurity', in Tikk and Kerttunen, *Routledge handbook of international cybersecurity,* pp. 252–59; Monica Kaminska, 'Restraint under conditions of uncertainty: why the United States tolerates cyberattacks', *Journal of Cybersecurity* 7: 1, 2021, https://doi.org/10.1093/cybsec/tyab008.

[93] Kirk, 'From threat to risk?', p. 272; Huysmans, 'What's in an act?'.

on external threats. Through this 'middle' position (still identified as 'risk' rather than 'security'), it can strengthen and mainstream the connection between risk and classical threat-oriented security, and function as a 'bridge' and conceptual 'glue' between resilience-oriented risk and threat politics. In practice, this establishes a connection between traditional security actors and activities on the one hand, and the local, technically oriented and basic 'everyday practices' of cybersecurity practitioners on the other—as exemplified by the UK NCSC. The legislation that supported the founding of the NCSC explicitly allowed (for the first time) the translation of secret (threat) intelligence into the public domain.[94] This has one function in communicating threats to non-government stakeholders (the private sector and the general public) but another in shaping overall risk management advice and guidance to all stakeholders, including public-sector organizations and other security and intelligence agencies.

In the UK, a shift towards risk as a mode of national security does not equate to 'dovishness', in cyber or otherwise, but to the wide incorporation of security into the everyday, including the forms of 'little security nothings' that are integral to the logic of risk as potential threats.[95] Indeed, risk and its 'objective' political technologies, like national risk registers that feature cyber threats and risks, are vehicles for the circulation of unease and perceptions of persistent and inevitable insecurity.[96] Risk is therefore not necessarily equivalent to the desecuritization of cybersecurity, despite the use of less heightened language around threats and risks, but a rationality and set of practices that run alongside more conventional cybersecurity measures.[97]

Conceptual and policy implications

The tendency to treat cyberspace and cybersecurity as entities apart from the mainstream of world affairs and disciplinary IR is no longer—if indeed it ever was—practical or sensible.[98] Cybersecurity is not an optional extra in the theory or practice of international affairs, but an integral aspect of it, one that affects, supports and enables wider security ambitions. Cybersecurity is 'not restricted to the security of information and information technologies but is the means through which other forms of security may be pursued, as well as being a condition of that greater security'.[99] Importantly for IR, cybersecurity 'evades the state as the natural polit-

[94] Legislation.gov.uk, 'Investigatory Powers Act 2016', https://www.legislation.gov.uk/ukpga/2016/25/section/251/enacted.

[95] Neal, *Security as politics*, p. 276.

[96] Jonas Hagmann and Myriam Dunn Cavelty, 'National risk registers: security scientism and the propagation of permanent insecurity', *Security Dialogue* 43: 1, 2012, pp. 79–96, https://doi.org/10.1177/0967010611430436.

[97] On the potential desecuritization of cybersecurity, see Joe Burton and Clare Lain, 'Desecuritising cybersecurity: towards a societal approach', *Journal of Cyber Policy* 5: 3, 2020, pp. 449–70, https://doi.org/10.1080/23738871.2020.1856903.

[98] Johan Eriksson and Giampiero Giacomello, 'Introduction: closing the gap between International Relations theory and studies of digital-age security', in Johan Eriksson and Giampiero Giacomello, eds, *International relations and security in the digital age* (Abingdon and New York: Routledge, 2007), pp. 1–28; Monsees and Liebetrau, 'Cybersecurity in International Relations'.

[99] Tim Stevens, *Cyber security and the politics of time* (Cambridge, UK: Cambridge University Press, 2015), p. 23.

ical fulcrum of security politics'.[100] The distributed nature of cybersecurity objects and agents—virtual, material, embodied or ideational—provides numerous opportunities to illuminate existing problems in IR. The focus on differential risk logics and rationalities can contribute to this disciplinary project in productive ways, three of which we outline below: plural risk rationalities; the risk–security relationship; and the embeddedness of cyber risk in 'the international'.

The first contribution concerns the rationalities of risk and risk management operating in international affairs. This pluralizing move is applicable to IR as a whole, which, despite decades of risk-oriented research, still tends to view risk as a unitary world-view drawn from sociological theorizing about the risk society. There are notable exceptions, particularly in the governmentality and critical security literature, but this research programme deserves further elaboration and exploration. Disentangling multiple rationalities within the larger risk assemblage can shed light on the complexities of national and international security, foreign policy, diplomacy, governance, war and conflict. As we have shown in the case of the NCSC, different modes of risk and risk management coexist within the same organization. By extension, this should also apply to state apparatuses and multilateral organizations like NATO and to regional political blocs like the EU.[101] Multiple risk rationalities and processes of 'riskification' imply the existence of differential structuring and constraining effects of risk and risk management, which complement and conflict with one another in empirically discernible ways in space and over time. Attention might be paid to how differential risk modalities are negotiated and contested, leading to specific configurations of organizational risk logics. These are unlikely to be static arrangements, and analyses should address the topological and temporal dynamics of intra-risk assemblages. Risk logics of varied orientation still 'meet' through empirically identifiable activities, methods or instruments. How, where and when do different risk logics become commingled or enmeshed?

A second opening allows us to re-examine the risk–security relationship. Risk is internally complex. Some risk approaches bear little resemblance to traditional threat politics; others are closely aligned, as in our category of risk as potential threats. As we have argued, the latter may function as a 'bridge' between inward and systems-oriented cybersecurity activities and classical threat-oriented security, paving the way to invest everyday objects and relations with insecurities ordinarily associated with threat security. In the case of cybersecurity, an enhanced appreciation of different risk logics can help us understand better the 'grammar' of cybersecurity, as well as its ontological politics: how dynamic and unstable socio-material entanglements condition different understandings and 'security arrangements'.[102] We suggest that this dynamic is generalizable

[100] Kristoffer Kjærgaard Christensen and Tobias Liebetrau, 'A new role for "the public"? Exploring cyber security controversies in the case of WannaCry', *Intelligence and National Security* 34: 3, 2019, pp. 395–408 at p. 396, https://doi.org/10.1080/02684527.2019.1553704.

[101] See Benjamin Farrand, Helena Carrapico and Aleksei Turobov, 'The new geopolitics of EU cybersecurity: security, economy and sovereignty', *International Affairs* 100: 6, 2024, pp. 2379–97, https://doi.org/10.1093/ia/iiae231.

[102] Hansen and Nissenbaum, 'Digital disaster'; Tobias Liebetrau and Kristoffer Kjærgaard Christensen, 'The

beyond the specific context of UK cyber risk management and cybersecurity, a proposition that can be tested empirically. As Tobias Liebetrau and Kristoffer Christensen have argued, if we do not appreciate the multiplicity of agents and practices operating beyond or outside conventional security frameworks, 'we run the risk of being blindsided by those practices of security that do not, in and of themselves, amount to high politics or exceptional politics'.[103] The risk logics presented here fall into this category, which lends their identification and analysis an additional normative imperative in terms of democratic accountability and legitimacy.

Communicating the ubiquity of cyber risk and cyber risk management in international ordering is a third opportunity for disciplinary engagement and 'opens up' the field to a more diverse set of actors and practices and their contributions to the international. Cybersecurity scholars are comfortable with thinking of cybersecurity and cyber risk as transnational, socio-technical and materially embedded in multiple socio-economic contexts. Absent cybersecurity and cyber risk management, both the present and future well-being of global information networks are imperilled, with substantial effects on global stability and prosperity. This is not a parochial plea for wider recognition of a niche field of enquiry, but a fact of life in digitally enabled modernity. In both material and functional terms, cyberspace enables 'the international' in significant ways. It is not the only enabler, of course, but the global fabric of digital interconnectivity is, objectively, a key socio-material infrastructure of contemporary international life.[104] Logically, therefore, we can perform a double epistemic move: understanding 'cyber' through international theory (as we currently do) and understanding 'the international' through cyber (as we should do next).[105] There is a compelling case that the cybersecurity–cyber risk complex at the heart of cyber politics is therefore consequential to our comprehension of international dynamics in IR and allied fields like International Political Economy. This has implications for understanding, *inter alia*, the emergence of 'big tech' actors in international affairs, the 'de-risking' of technological geopolitical competition, and discussions of cyber and digital sovereignty.[106]

ontological politics of cyber security: emerging agencies, actors, sites, and spaces', *European Journal of International Security* 6: 1, 2021, pp. 25–43 at pp. 25–26, https://doi.org/10.1017/eis.2020.10.

[103] Liebetrau and Christensen, 'The ontological politics of cyber security', p. 42.

[104] Mark A. Raymond, 'Cyber entanglement and the stability of the contemporary rules-based global order', in Robert Chesney, James Shires and Max Smeets, eds, *Cyberspace and instability* (Edinburgh: Edinburgh University Press, 2023), pp. 217–39.

[105] See Corneliu Bjola and Markus Kornprobst, eds, *Digital International Relations: technology, agency and order* (Abingdon and New York: Routledge, 2024).

[106] Rocco Bellanova, Helena Farrand Carrapico and Denis Duez, 'Digital/sovereignty and European security integration: an introduction', *European Security* 31: 3, 2022, pp. 337–55, https://doi.org/10.1080/09662839.2022.2101887; Henry Farrell and Abraham Newman, 'The new economic security state: how de-risking will remake geopolitics', *Foreign Affairs* 102: 6, 2023, pp. 106–22; Tobias Liebetrau and Linda Monsees, 'Assembling publics: Microsoft, cybersecurity, and public-private relations', *Politics and Governance* 11: 3, 2023, pp. 157–67, https://doi.org/10.17645/pag.v11i3.6771.

Conclusion

We have argued that risk is more internally heterogeneous than sometimes assumed in IR. Treating risk as a single rationality contributes to an oversimplification of risk and overlooks the multiplicity and complexity of risk modes and practices. It may also mask subtle changes in the relationship between risk and threat security. Although risk has recently featured more prominently in cybersecurity discussions within IR, there has been little work on the internal differentiation of cybersecurity risk and how risk conceptions relate to or support cybersecurity politics. In this article, we have aimed to address this gap by proposing a new typology of cyber risk relative to notions of 'potential threats' and 'uncertainty'. Through this typology, we were able to identify distinct but coexisting risk rationalities in UK cyber policy and practice contexts. We argued that these risk rationalities can 'bridge' the focus on internal technical and systems attributes—including resilience—on the one hand, and the emphasis on external threats and threat actors on the other. This bridge helps to connect 'everyday' and 'mundane' cybersecurity practices with high-level cyber threat politics and actors. The risk–security relationship will continue to be an important area of scholarly inquiry, not least due to the rise of risk approaches and rationalities in security contexts. Acknowledging differential risk logics and rationalities can contribute to a more finely grained understanding of this relationship and move the risk debate within cybersecurity studies and IR forward in productive ways.