European Journal of International Security (2025), page 1 of 20
doi:10.1017/eis.2025.10012

EJIS

RESEARCH ARTICLE

Digital im/materiality and the securitisation of cyber

Håvard Rustad Markussen

Nordic Institute for Studies in Innovation, Research and Education (NIFU), Oslo, Norway
Email: haavard.markussen@nifu.no

(Received 12 June 2024; revised 9 April 2025; accepted 19 May 2025)

Abstract

This article conducts a theoretical exploration of how the materiality of 'the digital', and, more specifically, the immaterial nature of 'the digital', imposes on the securitisation of cyber. Starting from the observation that the implementation of new, draconian cybersecurity policy – illustrated with the Norwegian bulk interception controversy – is legitimised with reference to the immateriality of digital threats and digital transformations, I ask how may we understand the material agency of immaterial matter in the context of cybersecurity. To address this problem, I turn to existing constructivist and new materialist accounts of the immateriality of cyber (in)security, and build on these to offer my own account of digital immateriality. In particular, I mobilise Yuk Hui's reading of Jean-Francois Lyotard's notion of im/materials to suggest that 'the digital' can be seen as a material force which concretises imperceptible relations by keeping the invisible invisible, and hence by abstracting and obscuring cyber threats and digital insecurities. In this way, 'the digital' engenders a new logic of cyber securitisation which I label 'exceptionality without urgency', where cybersecurity policy is aimed at countering fundamental, long-term, and rather vague transformations of politics and society rather than immediate, concrete threats.

Keywords: bulk interception; cybersecurity; im/materiality; new materialism; securitisation

Introduction

A number of Western European and North American countries have implemented so-called bulk interception regimes for data-gathering and surveillance. Bulk interception means intercepting and storing in bulk data streams that cross state borders in fibre optic cables. The implementation of such regimes has sparked hefty debates, and, in particular, their potential violation of human rights has been hotly contested. Opponents of bulk interception claim that mass surveillance and large-scale privacy breaches happen at the moment of bulk storage, while proponents argue that bulk interception is mere storage and that privacy-invasive surveillance occurs only if pieces of data stored in bulk are assembled by the intelligence services without proper justification. Crucially, moreover, proponents of bulk interception also tend to emphasise the need for improved digital security and more specifically control with digital communication to combat various security threats in the cyber domain.[1] Hence, they mobilise securitisation discourses, i.e. representations

[1] Greg Nojeim, 'Not a secret: Bulk interception practices of intelligence agencies', Center for Democracy and Technology, available at: {https://cdt.org/insights/not-a-secret-bulk-interception-practices-of-intelligence-agencies/}; Nóra Ní Loideáin, 'Bulk surveillance: Europe's recent landmark judgements', Digital Freedom Fund, available at: {https://digitalfreedomfund.org/bulk-surveillance-europes-recent-landmark-judgements/}.

© The Author(s), 2025. Published by Cambridge University Press on behalf of The British International Studies Association. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

of digital communication as a security issue,[2] in order to neutralise arguments about bulk interception's potentially human-rights-violating nature.

What is curious about these efforts to securitise digital communication in the legitimation of bulk interception, however, is the way in which notions of 'the digital' figure in the debates. In Norway, which is the empirical focus of this article, tropes like 'we cannot have an analogue defence in a digital world'[3] were, for instance, repeated by the defence minister in parliamentary and media debates, suggesting that digitalisation in itself justified the implementation of a bulk interception regime. As other politicians and various stakeholders who participated in the parliamentary debates engaged more with the content of digital threats, moreover, they often and strikingly relied on references to their immaterial qualities. One parliamentarian for instance stressed the invisibility of digital threats, while others emphasised insecurity associated with the speed, complexity, reach, scope, and general ubiquity of 'the digital'.[4] The emphasis on immaterial qualities of 'the digital' in the securitisation discourse represents a puzzle: how does the immateriality of 'the digital' impose materially on securitisation processes? In other words: how may we understand the material agency of immaterial matter in the context of cybersecurity?

Security studies and securitisation theory are rich with scholarship that engages with the securitisation of cyber[5] and with how the materiality of digital threats influences securitisation processes and the production of (in)security.[6] Furthermore, this scholarship also addresses – more or less explicitly – the immateriality of digital threats and discusses how the intangible and imperceptible nature of such threats influences the way in which cyber (in)security is produced discursively

[2] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Reiner, 1998); Thierry Balzacq, 'Enquiries into methods: A new framework for securitization analysis', in Thierry Balzacq (ed.), *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge, 2010), pp. 45–68.

[3] Bjørn Arild Gram, 'Vi kan ikke ha et analogt forsvar i en digital verden', NRK, 31 October 2022, available at: {https://www.nrk.no/ytring/vi-kan-ikke-ha-et-analogt-forsvar-i-en-digital-verden-1.16159366}.

[4] Stortinget, 'Stortinget torsdag 11. juni 2020 kl. 10.00: Video fra møte 11. juni kl. 10.00–1/2', available at: {https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/videoarkiv/Arkiv-TV-sendinger/?meid=10598&msid=3952}; Stortinget, 'Åpen høring i Stortingets utenriks- og Forsvarskomitè torsdag 28. mai 2020 kl. 11.28: Video fra høring 28. mai. Kl. 12.15–2/2', 28 May 2020, available at: {https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/videoarkiv/Arkiv-TV-sendinger/?h=10004169&dateid=10004428&del=2&rtid=120919&msid=341}; Stortinget, 'Stortinget tirsdag 6. juni 2023 kl. 10.00', 6 June 2023, available at: {https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/videoarkiv/Arkiv-TV-sendinger/?meid=11213&del=1&rtid=095800&msid=120}.

[5] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2007); Myriam Dunn Cavelty, 'Cyber-terror: Looming threat or phantom menace? The framing of the US cyber-threat debate', *Journal of Information Technology & Politics*, 4:1 (2008), pp. 19–36; Myriam Dunn Cavelty, 'From cyber-bombs to political fallout: Threat representations with and impact in the cyber-security discourse', *International Studies Review*, 15:1 (2013), pp. 105–22; Elgin M. Brunner, and Myriam Dunn Cavelty, 'The formation of in-formation by the US military: Articulation and enactment of infomanic threat imaginaries on the immaterial battlefield of perception', *Cambridge Review of International Affairs*, 22:4 (2009), pp. 629–46; Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, 53:4 (2009), pp. 1155–75; 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; Lars Gjesvik, and Kasper Szulecki, 'Interpreting cyber-energy-security events: Experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout', *European Security*, 31:1, pp. 104–24; Noran Fouad, 'Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation', *European Journal of International Security*, 9:4 (2024), pp. 553–73.

[6] Thierry Balzacq and Myriam Dunn Cavelty, 'A theory of actor-network for cyber-security', *European Journal of International Security*, 1:2 (2016), pp. 176–98; Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge: Cambridge University Press, 2016); Andrew Dwyer, 'Cybersecurity's grammars: A more-than-human geopolitics of computation', *Area*, 55:1 (2021), available at: {https://doi.org/10.1111/area.12728}; Noran S. Fouad, 'Entropic security: Information, materiality, and cybersecurity', thesis, University of Sussex (2020); Noran S. Fouad, *Theorising Cyber (In)Security: Information, Materiality, and Entropic Security* (London: Routledge, 2024); Tobias Liebetrau and Kristoffer Kjærgaard Christensen, 'The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces', *European Journal of International Security*, 6:2 (2020), pp. 25–43; Myriam Dunn Cavelty, 'The materiality of cyber threats: Securitization logics in popular visual culture', *Critical Studies on Security*, 7:2 (2019), pp.138–51; Jan Harris and Paul Taylor, *Digital Matters: The Theory and Culture of the Matrix* (London: Routledge, 2005).

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

and materially. However, this literature lacks sustained attention to the immaterial qualities of 'the digital' in itself and tends to overlook how 'the digital' and not only its component parts acts materially in and upon securitisation processes. In this article, I conduct a theoretical exploration of the materiality of 'the digital', and how it influences the securitisation of digital communications and, ultimately, helps legitimise the implementation of new and more invasive mass surveillance regimes.

I do so in four steps. First, I turn to constructivist cyber securitisation theory which studies the discursive construction of cyber threats and how these enable the production of cybersecurity policy. While generally concerned with speech acts and the intertextual construction of cyber, some cyber securitisation scholarship also pays moderate attention to the material aspects of cyber and, indeed, its immaterial qualities like invisibility and complexity.[7] These approaches only take us thus far in excavating the immateriality of digital materiality, however, since they ultimately give analytical privilege to discourse over matter and hence tend to understand immateriality as a limit of representation rather than an agentic property of 'the digital'.

Second, and in seeking to more soundly account for the material agency of 'the digital', I mobilise new materialist approaches to big data and digital politics. This literature analyses the material components – artefacts, devices, and infrastructures, but also code and software – which make up 'the digital' and, relatedly, investigates how digital materiality animates cybersecurity practices. Importantly, some of this research highlights the immaterial quality of cyber threats, for instance by theorising malware as cybersecurity actants.[8] Noran Shafik Fouad's theory of how the simultaneously physical and non-physical nature of information leads to the governance of cybersecurity through a logic of noise is particularly helpful, as it provides clear and compelling answers to how the immateriality of digital threats impacts securitisation directly.[9] Yet new materialist cybersecurity scholarship leaves open the question of how 'the digital' in itself – rather than its component parts – acts in and upon securitisation processes and, more than that, tends to overlook the long-term exceptionality imposed by 'the digital' on cybersecurity discourses.

Third, I offer my own account of digital immateriality. I do so by mobilising philosopher of technology Yuk Hui's reading of Jean-Francois Lyotard's notion of immateriality to suggest that the material agency of cyber threats lies in the immateriality of the digital.[10] According to Lyotard, telecommunications technology confronts us with a new kind of material which he labels immaterial: physical things which are unperceivable for the human.[11] This, Hui holds, captures the nature of and may even be epitomised by 'the digital', since the digital consists of concrete, physical relations between data that cannot be sensed by the human without specialised concretisation-tools. The digital is thus at the same time material and non-material; an im/material which is made up of matter while remaining an essentially abstract phenomenon. We know it is there, but we cannot grasp it. It is all around us but impossible to see or touch. Whereas other technologies concretise relations by making them graspable and perceptible, then, 'the digital' has the material effect of keeping invisibles invisible and hence of further obscuring and abstracting digital threats.[12]

Fourth, I discuss how Hui's Lyotardian notion of 'the digital' as im/material acts in and upon processes of securitisation. In particular, I explain how the im/materiality of 'the digital' differs from the non/physicality of digital threats, and, accordingly, how 'the digital' enables a mode of cyber securitisation different from one that governs through a logic of noise like that suggested by

[7] Invisibility: Hansen and Nissenbaum, 'Digital disaster'; complexity: Dunn Cavelty, *Cyber-Security*; Stevens, *Cyber Security*.

[8] Balzaq and Dunn Cavelty, 'A theory'; Dwyer, 'Cybersecurity's grammars'.

[9] Fouad, 'Entropic security'; Fouad, *Theorising Cyber*.

[10] Yuk Hui, 'Towards a relational materialism: A reflection on language, relations and the digital', *Digital Culture and Society*, 1:1 (2015), available at: {https://doi.org/10.14361/dcs-2015-0109}.

[11] Jean-Francois Lyotard, 'Jean-Francois Lyotard: After six months of work … (1984)', in Yuk Hui and Andreas Broeckmann (eds), *30 Years after* Les Immateriaux: *Art, Science, and Theory* (Lüneburg: Meson Press, 2015 [1984]), pp. 29–66; see also Robin Mackay, 'Immaterials, exhibition, acceleration', in Yuk Hui and Andreas Broeckmann (eds), *30 Years after* Les Immateriaux: *Art, Science, and Theory* (Lüneburg: Meson Press, 2015), pp. 215–42.

[12] Hui, 'Towards a relational materialism'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

Fouad.[13] Instead of enabling security governance through a logic of noise, I argue, which responds to urgency without existentiality, 'the digital' enables a securitisation of cyber which conversely responds to existentiality without urgency. By concretising relations through keeping the invisible invisible, and hence abstracting and obscuring digital threats, 'the digital' acts by legitimising long-term, draconian security measures to mediate fundamental and exceptional changes to society and politics.

The article contributes to debates in critical security studies which directly or indirectly engage with the immateriality of 'the digital', and how this immateriality influences the securitisation of cyber. As indicated above, research about the immaterial qualities of cyber threats can be found across different theoretical approaches to cybersecurity. The article contributes to these separately, and, more than that, to the debates about immateriality which unite them. In this way, the article also contributes to efforts that aim to bring cybersecurity literature into closer conversation with International Relations (IR).[14] By theorising how the immaterial properties of 'the digital' are active in the production of cyber (in)security, I also engage with important IR questions about how globalised digital technologies impact the development of international security.

Before beginning the theoretical exploration, I will start by giving a more detailed account of the Norwegian bulk interception controversy. I understand 'controversy' in line with Linda Monsees's broad definition of controversies as 'the contestation of values and identities but even more so the problem definition as such'.[15] The Norwegian case was chosen because it is the most recent case of bulk interception implementation, and more importantly, because the implementation of bulk interception in Norway took place after the clarification of the legal status of bulk interception regimes in the European Court of Human Rights (ECtHR). The ECtHR ruling established that bulk interception may be legal if national authorities deem such a regime necessary to protect national security and if the regime contains sufficient safeguards against breaches of privacy rights.[16] As a result, debates about the legality of bulk interception in the Norwegian case very consciously revolved around the balance between concerns for liberty and security. This makes the Norwegian bulk interception controversy a clear case of attempted securitisation and, more concretely, of how 'the digital' acts in and upon securitisation processes. The case will be discussed throughout the article to engage with the different theoretical propositions and as an illustration for the article's main claim about the immateriality of 'the digital' and its securitising effects.

The Norwegian bulk interception controversy

Following a number of other Western European and North American countries, Norway has recently implemented a so-called bulk interception regime, which allows its foreign intelligence service to harvest in bulk all data that crosses state borders in fibre optic cables.[17] The suggestion for a new Intelligence Act which included a bulk interception provision sparked a heated debate. Proponents of bulk interception insisted that the foreign intelligence service needed better – and more specifically digital – tools to prevent and counter the security threats of the day. Opponents, on the other hand, were sceptical about bulk interception given its privacy-invasive and potentially human-rights-violating nature. After the first round of parliamentary proceedings in 2018 and 2020, the Intelligence Act was passed, but the bulk interception provision was postponed in order to

[13] Fouad, 'Entropic security'; Fouad, *Theorising Cyber.*

[14] Linda Monsees and Tobias Liebetrau, 'Cybersecurity and International Relations: Developing thinking tools for digital world politics', *International Affairs*, 100:6 (2024), pp. 2303–15.

[15] Linda Monsees, 'A war against truth: Understanding the fake news controversy', *Critical Studies on Security*, 8:2 (2020), pp. 116–29 (p. 119).

[16] Eliza Watt, 'Much ado about mass surveillance: The ECtHR Grand Chamber 'opens the gates of an electronic "Big Brother in Europe in Big Brother Watch v UK"', *Strasbourg Observer* (28 June 2021), available at: {https://strasbourgobservers.com/2021/06/28/much-ado-about-mass-surveillance-the-ecthr-grand-chamber-opens-the-gates-of-an-electronic-big-brother-in-europe-in-big-brother-watch-v-uk/}.

[17] Nojeim, 'Not a secret'; Ní Loideáin, 'Bulk surveillance'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

wait for clarification about the legality of such a regime from the European Court of Human Rights. Reacting to these clarifications, an altered bulk interception provision which strengthened control mechanisms to ensure the law was within Norway's human rights commitments, was presented to parliament in 2023, after which the bulk interception provision was eventually passed.[18]

In the second parliamentary debate, which addressed whether to include bulk interception in the already-passed Intelligence Act, representative Liv Signe Navarsete from the Centre Party (SP) offered a first example of how 'the digital' figured in the securitisation process when she stated the following:

> The digital space, cyberspace, communication across state borders has acquired a different role in securing Norwegian interests … In short, we can say that the security situation in our geographical proximity is drastically worsened. The report … that the Foreign Intelligence Service published in February this year points to a continued increase in Russian capacities and to an enlargement, not only of the known capacities, but also – and we, especially those of us who have reached my age, have to realise, that the technological development is about more than tanks and planes. That which is perhaps most difficult to combat is that which we do not see; that which absolutely happens everywhere in society and between countries, but that which we do not see.[19]

Of particular note here is Navarsete's discursive linking of the dangers associated with digital threats to the *invisibility* of digital communication. By contrasting digital threats with physical objects on the military battlefield such as tanks and planes, and, more importantly, by describing digital threats as 'that which we do not see', Navarsete placed great emphasis on the material quality of the digital when securitising digital communication. For Navarsete, digital communication was dangerous and in need of a strong policy response precisely because it is an activity which operates in registers that evade our senses. Due to this immaterial materiality, she even argued that digital communication is the threat which is 'most difficult to combat'. By this account, the invisibility of the digital was a reason not merely to securitise, but also to implement extra invasive surveillance and, more specifically, to give the intelligence services extra-wide authority in terms of access to commercial data.

Playing into Navarsete's representation of digital threats as invisible and strengthening the overall impression of digital threats as materially imperceptible, many also represented 'the digital' as *ubiquitous*. First of all, Navarsete herself linked the invisibility representation with the notion of the ubiquity of 'the digital' by stressing that 'that which we do not see' 'absolutely happens everywhere in society'. By this account, the ubiquity of digital threats in a sense contributes to their invisibility: the digital is impossible to see because it is all around us. Making a similar discursive move, FFI, a military research institute invited to the open hearing, said in their consultation response that

> digitalisation has brought a fundamental, pervasive change in the entire society's ecosystem. And everything hangs together, connected by the internet which is by nature border-crossing, very large, and complex. This digital ecosystem is used by nearly all societal functions, communication and infrastructure, and it is therefore absolutely necessary to understand, manage, make use of, and protect. We are of the opinion that a new Intelligence Act is necessary because the rapid technological development has created and will continue to create new and significant vulnerabilities and risks for state security.[20]

[18] Stortinget, 'Lov om Etterretningstjenesten (etterretningstjenesteloven)', available at: {https://www.stortinget.no/no/Saker-og-publikasjoner/Saker/Sak/?p=79451}; Jakob Bjørnøy, 'E-tjenesten får snart lagre nær all datatrafikk i Norge' *Nettavisen*, available at: {https://www.nettavisen.no/nyheter/flertall-pa-stortinget-apner-for-masseovervaking-i-norge/s/5-95-1120292}; Olav Døvik, 'Ny lov for e-tjenesten blir vedtatt.' *NRK*, 26 October 2020, available at: {https://www.nrk.no/norge/flertall-pa-stortinget-for-ny-etterretningstjenestelov-1.15045224}.

[19] Stortinget, 'Stortinget torsdag 11. juni'; all translations from Norwegian are my own.

[20] Stortinget, 'Åpen høring'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

In this way, FFI substantiated Navarsete's linking of invisibility with ubiquity through the notion of omnipresence and, more specifically, added texture to this construction by representing the digital as 'pervasive', 'border-crossing', and 'very large'. By stating these digital attributes as reasons to update the Intelligence Act (implicitly involving the bulk interception provision), moreover, FFI also mobilised the immaterial quality of digital threats in their efforts to securitise digital communications. By FFI's account, it was necessary to put in place stronger security and surveillance policies due to the material quality of the digital, and, more specifically, since the digital is difficult to grasp and control given its immaterial ubiquity.

While linking invisibility to ubiquity, moreover, FFI also linked invisibility to *complexity*, which may be seen as yet another immaterial quality of the digital which makes digital communications seem threatening and demanding strong policy response. Similarly, representative Bengt Fasteraune (SP) stated in the second parliamentary debate that

> we see that threat actors in digital spaces exploit opportunities which arise due to new technology and new patterns of use. … The new act with the proposed changes provides important tools in order to reveal and combat threats in the digital, complex space".[21]

For FFI and Fasteraune, then, not only size but also complexity describes the nature of the internet and processes of digitalisation, since complexity, like ubiquity and invisibility, makes the digital virtually ungraspable. As such, complexity adds further nuance to the material imperceptibility of the digital, and importantly, gives yet another reason to securitise digital communications. Note also how Fasteraune places the hostile activities of real and tangible threat actors in complex, digital spaces, thus making activities which are possible to ground in a physical reality seem mysterious and enigmatic and hence difficult to detect, respond to, and even fully understand.

Finally, the notion of *speed* also seems to have played into and reinforced the impression of digital threats as imperceptible and thus demanding securitisation. The following quotes illustrate this. The first is given by NUPI, a foreign affairs research institute, in the open hearing, and the second by Christian Tybring Gjedde from the Progress Party (FRP) in the first parliamentary debate.

> the digitalisation of society is so pervasive and in so many fields that the foreign intelligence services need to pay attention to these things, and have tools to follow this development which is exponential and extremely fast, and thus we cannot have an act which is outdated tomorrow.[22]

> digitalisation is happening faster and faster, and that is mostly for the better, and we cannot stop it in an open, modern society. Therefore it is only natural that thugs and foreign operators become more digitalised and work better. And it is then also obvious that we too, to defend ourselves, need better tools to stop that.[23]

Here, NUPI and Tybring-Gjedde both argue that the speed with which digital technologies are developing is a reason to give the intelligence services surveillance tools that enable the harvesting, storage, and potential monitoring of digital communications. Speed, for them, seems to accentuate the dangers already associated with digital threats, since digital threats may be even more dangerous in the near future due to rapid technological progress. The tempo of development is thus represented as a material quality inherent in digital technologies, which makes security threats that manifest in digital activities require policy response.

The statements cited here, whether they refer to the invisibility, ubiquity, complexity, or speed of 'the digital', represents 'the digital' as a unitary yet vaguely defined force which in and of itself seems to constitute a threat and thus require securitisation. FFI's statement that an update

[21] Stortinget, 'Stortinget tirsdag 6. juni'.

[22] Stortinget, 'Åpen høring'.

[23] Stortinget, 'Stortinget torsdag 11. juni'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

of the Intelligence Act (which included the bulk interception provision) was ‘necessary because the rapid technological development has created and will continue to create new and significant vulnerabilities and risks for state security’ is emblematic of this. It shows with clarity that the nature of concrete threats, risks, and vulnerabilities is a secondary concern, and that it is the digital revolution in itself that must be secured against. Similarly, Tybring-Gjedde indirectly discusses threats when he contends that as a result of speedy digitalisation, it is ‘natural that thugs and foreign operators become more digitalised and work better’. Here too, the nature of the threats in question remains vague, and it is ‘the digital’ that is highlighted as that which needs securitisation.

In the following, I explore how ‘the digital’ may be seen to act in and upon the securitisation of digital communication by consulting and engaging a number of different theoretical approaches to the material production of cybersecurity. The material presented above by no means constitutes a full account of the securitisation of communication and legitimisation of mass surveillance through bulk interception in Norwegian policy discourse. Nonetheless, the material shows that notions of ‘the digital’ figured quite prominently in the discourse and that its immaterial qualities played a part in enabling the legitimation of bulk interception. Off the back of this observation, it is necessary to ask, as I do in this article and as will be explored in the sections below, how we can best account for the ways in which ‘the digital’ acts in and upon securitisation processes through its immaterial qualities.

Matter as condition: Constructivist approaches to digital immateriality

Constructivist securitisation theory has been interested in the securitisation of cyber for a long time. While it has speech acts and the discursive, intersubjective construction of cyber threats as its main object of study, constructivist cyber securitisation scholarship also pays moderate attention to the materiality of cyber threats and, indeed, to their immaterial qualities.

In her seminal book on the securitisation of cyber threats, *Cyber-Security and Threat Politics*, Myriam Dunn Cavelty examines the myriad ways in which cyber threats have been perceived and constructed by US policymakers.[24] In conceptualising how cyber threats operate, Dunn Cavelty develops a matrix of means and targets of cyber attacks. Here, she separates between means and targets that exist in the physical domain, such as cables, servers, backhoes, and hammers, and those which exist in the cyber domain, such as networks and hacking. According to Dunn Cavelty, means and targets in the cyber domain are ‘immaterial’ as opposed to the material means and tools in the physical domain in the sense that they are ‘very elusive’.[25] These elusive immaterials of the cyber domain, she further explains, make up ‘the information and the content that flows through the infrastructure’.[26]

Moreover, Dunn Cavelty also contends that ‘there are some hard facts grounded in real-life experiences when it comes to the information infrastructure and what we can do with it’.[27] More specifically, she points to the speed, complexity, and reach of cyber threats and shows how these qualities – all of which are expressions of digital immateriality – play an important part in deciding how threats are constructed.[28] Dunn Cavelty, for instance, argues that the speed of future technological development of digital tools and infrastructures makes it almost impossible to completely dismiss cyber threats even in the absence of concrete previous incidents or likely future scenarios. She also suggests that the complexity of digital information systems, networks, and infrastructures, and the difficulty of fully understanding how ‘the digital’ hangs together and operates, enable the construction of cyber threats as a permanent uncertainty which requires continuous

[24] Dunn Cavelty, *Cyber-Security*.

[25] Dunn Cavelty, *Cyber-Security*, p. 22.

[26] Dunn Cavelty, *Cyber-Security*, p. 22.

[27] Dunn Cavelty, *Cyber-Security*, p. 18.

[28] Dunn Cavelty, *Cyber-Security*, p. 19; see also Dunn Cavelty, ‘From cyber bombs’.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

securitisation.[29] Complexity, Dunn Cavelty further demonstrates, is exacerbated by the global scope of 'the digital' and global reach of cyber threats.[30]

Related arguments have been made in critical security studies and surveillance studies literatures that emerged as a response to the Snowden revelations. Notably, Bauman et al. emphasise the 'complex and rhizomatic character of interconnected networks of surveillance tools' and highlight how this complexity demands a rethinking of the security politics involved in contemporary mass surveillance.[31] Hence, they call to our attention how immaterial material qualities not only of 'the digital' as such, but also of contemporary digital surveillance systems in particular (rhizomatic complexity), determine how we can and should make sense of digital surveillance today (in terms of new lines of flight and structures of authority). Similarly, David Lyon suggested that the Snowden leaks demonstrated the liquidity of contemporary surveillance, i.e. ubiquitous gathering and exploitation of uncontained and uncontrolled flows of data.[32]

Tim Stevens, moreover, conducts a narrative analysis of the temporal logics after which security politics operates.[33] While also located firmly in constructivist security studies, as he examines intersubjective, discursive construction of cybersecurity in epistemic communities, Stevens's approach explicitly makes room for taking into account the material aspects of cybersecurity as well. Laying out his approach to the securitisation of cyber, Stevens explains that 'cyber security is not only a set of rules or policies but is also instantiated through hardware: the material infrastructures of the global information grid'.[34] In this way, he suggests – much like Dunn Cavelty[35] – that the physical attributes of 'the digital' make up the conditions for how cybersecurity can be envisaged and represented. Moreover, Stevens also holds that cybersecurity constitutes an assemblage in the sense that it is made up of a wide variety of human and non-human components, which relate and interact in unpredictable and heterogeneous ways. He focuses his analysis on how this assemblage is imagined by human actors but acknowledges the agency of non-humans as well. For Stevens, human actors are the immaterial component of the cybersecurity assemblage, while the physical objects of cybersecurity make up its material component.[36]

Furthermore, Lene Hansen and Helen Nissenbaum have notably argued that cyber threats lend themselves to hypersecuritisation, in the sense that they target networks of digital and physical infrastructures and thus may 'cause society, financial, and military break-down'.[37] More so than Dunn Cavelty[38] and Stevens,[39] Hansen and Nissenabaum take an explicitly critical constructivist approach. They even distance themselves from materialist understandings of cybersecurity, explaining that they view security as 'a discursive and political practice rather than a material condition or verifiable fact' and state that they are not 'convinced … that the material conditions of the communications environment will determine the winning discourse as this constitutes material structures as outside and above political decisions and discursive processes'.[40] For Hansen and Nissenbaum, even the physical components of 'the digital' are discursively constructed and given

[29] Dunn Cavelty, *Cyber-Security*; see also 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.

[30] Dunn Cavelty, *Cyber-Security*.

[31] Zygmunt Bauman, Dider Bigo, Paulo Esteves, et al., 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology*, 8:2 (2014), pp. 121–44 (p. 124).

[32] David Lyon, 'Surveillance, Snowden and Big Data: Capacities, consequences, critique', *Big Data & Society*, 1:2 (2015), available at: {https://doi.org/10.1177/2053951714541861}.

[33] Stevens, *Cyber Security*.

[34] Stevens, *Cyber Security*, p. 29.

[35] Dunn Cavelty, *Cyber-Security*.

[36] Stevens, *Cyber Security*, p. 33

[37] Hansen and Nissenbaum, 'Digital disaster', p. 1164.

[38] Dunn Cavelty, *Cyber-Security*.

[39] Stevens, *Cyber Security*.

[40] Hansen and Nissenbaum, 'Digital disaster', p. 1162, note 6.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

meaning in a cybersecurity context only through the ways in which they are represented in text and image.[41]

Still, Hansen and Nissenbaum's emphasis on the difficulty of representing cyber threats visually, and on the instantaneous cascading effects of cyber attacks, seems to suggest otherwise; that even if the physical components of 'the digital' are constructed discursively, the materiality of these components, at least to some extent, also matters. In particular, the argument that cyber threats are difficult to represent visually, and that this leads to hypersecuritisation, implies that the material quality of invisibility impacts the way in which cyber threats are securitised. Likewise, the argument that cyber attacks have instantaneous cascading effects, which also contributes to enabling hypersecuritisation, implies that the material property of speed has an impact on the securitisation of cyber as well.

Similar to Hansen and Nissenbaum, moreover, Stevens also includes in his analysis an argument about the difficulties in representing cyber threats due to their invisibility.[42] In contrast with Hansen and Nissenbaum, however, he suggests that what leads to securitisation is not the lack of visual representations, but rather attempts at representing cyber threat scenarios visually. Such attempts, which often consist of cybersecurity exercises and simulations and may also come through popular culture, engender catastrophe scenarios which are typically worse than likely, real-world situations. Stevens stresses, though, that there is an important difference between exercises and simulations on the one hand, and popular cultural representations on the other. In this way, the invisibility of cyber threats may, through efforts to what Stevens calls 'materialising the virtual', function to enable security practitioners and politicians to raise the security-stakes in the liberty/security-trade-off and thus legitimise new and more invasive security policy.[43]

Presenting a complementary explanation, Claudia Aradau and Tobias Blanke show how anthropocentric understandings of cybersecurity enable the lowering of liberty stakes in the liberty/security trade-off by giving the impression that data-gathering does not constitute mass surveillance since personal data is only viewed and analysed by computers.[44] Aradau and Blanke even engage directly with the example of bulk interception and show how arguments about the absence of humans in data analysis have been leveraged to make the case for why bulk interception is not harmful from a privacy perspective.[45] Their approach is part of a larger body of 'data politics' literature which tends to treat data as part of the material conditions for the production of cybersecurity and more specifically the legitimation of surveillance. Most notably, Evelyn Ruppert, Engin Isin, and Didier Bigo, who coined the concept of data politics, argue that data has world-making effects in the sense that it creates new spaces for the enactment of security politics.[46] In making this argument, they emphasise the invisibility of data by highlighting how the language of the internet 'is hardly visible or even comprehensible to those who do not write such code'. In this way, Ruppert, Isin, and Bigo suggest that the writers of invisible code hold a certain power in the production of digital politics and accordingly imply that the invisibility of data in itself plays an important part in making possible such productive processes. Aradau and Blanke also emphasise the power that lies in managing largely invisible datapoints, as they argue that algorithmic governance makes digital subjects knowable through 'othering' based on anomaly rather than abnormality.[47]

[41] See also Brunner and Dunn Cavelty, 'The formation' and Fouad, *Theorising Cyber*.

[42] Stevens, *Cyber Security*, pp. 153, 160.

[43] Stevens, *Cyber Security*, p. 153.

[44] Claudia Aradau, and Tobias Blanke, 'The (Big) Data-security assemblage: Knowledge and critique', *Big Data & Society*, 2:2 (2015), available at: {https://doi.org/10.1177/2053951715609066}.

[45] See also Claudia Aradau and Emma Mc Cluskey 'Making digital surveillance unacceptable? Security, democracy, and the political sociology of disputes', *International Political Sociology*, 16:1 (2022), available at: {https://doi.org/10.1093/ips/olab024}.

[46] Engin Isin, Evelyn Ruppert, and Didier Bigo, 'Data politics', *Big Data & Society*, 4:2 (2017), available at: {https://doi.org/10.1177/2053951717717749}.

[47] Claudia Aradau and Tobias Blanke, 'Governing others: Anomaly and the algorithmic subject of security', *European Journal of International Security*, 3:1 (2018), pp. 1–21. available at: {https://doi.org/10.1017/eis.2017.14}.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

In exploring how digital immateriality acts in securitisation processes, these constructivist approaches to cybersecurity undoubtedly offer important insights. By making the case for taking into account how discursive representations of cyber threats are shaped by the materiality of 'the digital', they all – albeit in different ways – demonstrate how matter may function as a *condition* for the intersubjective meaning-making that goes into the securitisation of cyber. They show that immaterial qualities of 'the digital' such as complexity, speed, reach, and invisibility make possible certain representations of cyber (in)security. More specifically, they seem to suggest that these immaterial qualities enable the construction of cyber threats as a kind of insecurity which requires the urgent and swift implementation of security measures, even in the absence of concrete threats.

Constructivist approaches to cyber securitisation thus also provide a useful framework for analysing the Norwegian bulk interception controversy. Indeed, we saw in the presentation of the Norwegian bulk interception controversy above that parliamentarians and other stakeholders represented 'the digital' with references to many of the immaterial digital qualities highlighted by e.g. Dunn Cavelty,[48] Stevens,[49] and Hansen and Nissenbaum.[50] Recall for instance how Navarsete argued that 'that which we do not see' constitutes the most serious security threat,[51] invoking the invisibility that Hansen and Nissenbaum call to our attention when arguing that cyber threats hypersecuritise in part because they are difficult to represent visually. Recall also how FFI emphasised how 'the digital' and more concretely the internet as a central digital infrastructure is 'by nature, border-crossing, very large, and complex',[52] thus mobilising imaginaries of reach and complexity that Dunn Cavelty highlights as central 'hard facts' of 'the digital'. And recall, finally, how NUPI contended that the intelligence services must 'have tools to follow this [the digital] development which is exponential and extremely fast',[53] and as such, justified the implementation of bulk interception with reference to the speed of digitalisation that Stevens raises as an important condition for the governance of cybersecurity.

Still, seeing digital materiality as a conditioning force limits our understanding of how 'the digital' acts in and upon securitisation processes. Specifically, the understanding of material agency in terms of passive conditioning, which is more or less explicitly put forth by constructivist cyber researchers, prevents us from properly interrogating how digital immateriality may play a more active role in the production of cybersecurity. By giving analytical privilege to discourse over matter, even when acknowledging the importance of the hard facts and materials of cybersecurity, they miss how 'the digital' is not only acted upon but also acts itself. For while the statements revisited here illustrate how digital matter functions to condition discursive representations about cybersecurity, they also give the impression that something more is in play, and, concretely, that 'the digital' imposes on rather than structures the discourse.

Active matter: New materialist approaches to digital immateriality

In seeking to account for the more active intervention of digital immateriality in securitisation processes, I now turn to new materialist scholarship on cyber (in)security and discuss how this literature has addressed the material agency of immaterials. As opposed to constructivist securitisation theory, which concentrates on the discursive construction of cyber threats, new materialist approaches emphasise the material properties and agential capacities of matter and hence show how the immateriality of digital matter not only conditions securitisation but plays an active part in the production of cyber (in)security.

One prominent new materialist approach is Thierry Balzacq and Dunn Cavelty's actor-network theory for cyber security.[54] Actor-network theory posits that all actants – human and non-human –

[48] Dunn Cavelty, *Cyber-Security*.

[49] Stevens, *Cyber Security*.

[50] Hansen and Nissenbaum, 'Digital disaster'.

[51] Stortinget, 'Stortinget torsdag 11. juni'.

[52] Stortinget, 'Åpen høring'.

[53] Stortinget, 'Åpen høring'.

[54] Balzacq and Dunn Cavelty, 'A theory'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

have ‘capacity for agency’[55] and that they are involved in, come into being through, and have productive effects via interactions with other actants. Balzacq and Dunn Cavelty theorise malware, i.e. malicious software, as the central actant of cyber (in)security and argue that it *creates* spaces which ‘have implications for the way we conceptualise cyber-security, the process that brings actors together, and the type of interventions that are made possible’.[56] In other words, malware acts by creating the spaces within which cybersecurity policy can operate. Concretely, Balzacq and Dunn Cavelty suggest that malware creates three kinds of spaces through its disruptive performance: regional, networked, and fluid spaces. On the one hand, the creation of regional and networked space keeps cyber (in)security manageable, since malware in such cases perform cyber (in)security as confined within stable geographical or computerised spaces, both of which are physical. The creation of fluid space, on the other hand, happens when malware succeeds in breaking down systems to the extent that components in an actor-network no longer have stable relations to each other. This is when ‘networks start to panic’ and cyber insecurity spills over into the public and political realms.[57] In this way, the creation of fluid space may lead to digital hysteria or ‘or strong over-reactions in government circles’.[58] According to Balzacq and Dunn Cavelty, moreover, severe disruptions and their creation of fluid space mark ‘the moment when malware becomes perceptible, sometimes even literally *visual*’,[59] which also contributes to enabling strong cybersecurity policy responses.[60]

To some extent, Balzacq and Dunn Cavelty’s actor-network theory for cyber (in)security is similar to the constructivist approaches. In the quote reproduced above, they claim that malware’s creation of space has ‘implications for the way we conceptualise cyber-security’.[61] Elsewhere, they contend that ‘in order to understand the role (and agency) of cyber-incidents, we must understand what they do – how they *perform* – in their environment, before they are interpreted by actors in political processes’.[62] In this way, Balzacq and Dunn Cavelty suggest that malware acts in securitisation processes by establishing the structures and frames within which policy responses to cyber insecurity are possible. In particular, the assumption of a chronological relationship between immaterial action and discursive construction, where the latter follows the former, reproduces the notion of digital immateriality as condition. Moreover, Balzacq and Dunn Cavelty’s argument that the creation of fluid space through malware activity enables digital hysteria and exaggerated policy responses is reminiscent of Hansen and Nissenbaum’s[63] and Stevens’s[64] contentions that the invisibility and speed of ‘the digital’ make possible the justification of draconian cybersecurity policy. By both accounts, the immateriality of ‘the digital’ lays the material foundations for public perception and political response.

At the same time, however, Balzacq and Dunn Cavelty’s approach differs significantly from constructivist accounts of digital immateriality by front-footing the *activity* of malware. For Balzacq and Dunn Cavelty, malware acts not only by conditioning conceptualisation but also by mediating relations and transforming the networks of which it is part. More concretely, seeing malware as a mediator in cybersecurity actor-networks entails seeing malware as an actant which ‘affects whatever flows through’ it, and, as such, as an immaterial cyber component which not only circulates

[55] Balzacq and Dunn Cavelty, ‘A theory’, p. 183.

[56] Balzacq and Dunn Cavelty, ‘A theory’, p. 178.

[57] Balzacq and Dunn Cavelty, ‘A theory’, p. 191.

[58] Balzacq and Dunn Cavelty, ‘A theory’, p. 190.

[59] Balzacq and Dunn Cavelty, ‘A theory’, p. 181, emphasis in original.

[60] See also Tobias Liebetrau and Kristoffer Kjærgaard Christensen, ‘The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces’, *European Journal of International Security*, 6:1 (2020), pp. 25–43, and Clare Stevens, ‘Assembling cybersecurity: The politics and materiality of technical malware and the case of Stuxnet’, *Contemporary Security Policy*, 41:1 (2020), pp. 129–52.

[61] Balzacq and Dunn Cavelty, ‘A theory’, p. 178.

[62] Balzacq and Dunn Cavelty, ‘A theory’, p. 180, emphasis in original.

[63] Hansen and Nissenbaum, ‘Digital disaster’.

[64] Stevens, *Cyber Security*.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

but also 'affects circulation in cyberspace'.[65] Thus, Balzacq and Dunn Cavelty's actor-network-theory-inspired approach allows us to see how digital immateriality imposes materially on the securitisation process in ways that are 'detached from the "intent" of the person who wrote the code'.[66] In other words, malware lives a life of its own and contributes to the production of cyber (in)security in unpredictable and uncontrollable ways.[67]

Providing an account of cyber (in)security that more explicitly brings new materialist perspectives on digital immateriality to bear on theories of securitisation, Noran Shafik Fouad argues that the agency of information (and more precisely the actions of code and software) produces what she calls entropic security – a security characterised by uncertainty and disorder.[68] Fouad argues, moreover, that entropic (cyber)security is constituted by three interrelated logics. First, the logic of negentropy marks the need to respond to the entropic nature of cyber (in)security. Negentropy means 'negative entropy' and describes anti-entropic security practices which aim to counter the entropic force of information-related threats. In practice, this entails accepting the inherent uncertainty of information and directing security practices towards risk prioritisation rather than elimination. Second, the logic of emergence refers to how the randomness and non-linear activity of information forces cybersecurity practices to redirect their attention away from easily defined enemies and instead towards more complex assemblies consisting of self-organising technical systems and agentic malware as well as human actors and/or states. Finally, the logic of noise describes how cyber (in)security is more mundane than exceptional given the simultaneous physicality and non-physicality of information. Taken together, Fouad holds, these three logics of cyber (in)security should lead us to think differently about the securitisation of cyber threats. In particular, she argues that the notion of entropic security highlights how cybersecurity practices are legitimised through more complex processes where a multitude of actors are involved and interact with the materialities of information and crucially, where the construction of threats is not reliant upon references to enmity and emergency.

For the purposes of this article, Fouad's (2020) theorisation of information and digital threats in terms of the '*simultaneous* physicality and non-physicality' of information, and her suggestion that this leads to the governance of cyber (in)security through a logic of noise, is particularly useful.[69] In theorising information as simultaneously physical and non-physical, Fouad particularly highlights how 'the digital is made of binary codes embedded in machines and are not visible to human beings' and explains how 'codes/software hide their complexity in user-friendly interfaces'.[70] She also demonstrates how even the tangible components of digitality are elusive. For instance, users of digital technologies often have the impression that their data is 'stored in a virtual place', while in reality data centres are 'massively physical'.[71] Likewise, wireless and hence invisible digital connections are 'supported by a huge infrastructure of cable systems, under soil or under sea'.[72]

The non/physicality of digital information, Fouad further argues, enables the governance of cyber (in)security through a logic of noise, since it limits 'existentiality perceptions'[73] in the security discourse by showing that cyber threats are '*disruptive* rather than *destructive*'.[74] For Fouad, cyber threats and their inherent non/physicality make noise in the sense of always disrupting digital systems. Hence, they do not represent existential threats that require the suspension of normal politics to implement draconian security policy, but instead mundane threats which can

[65] Balzacq and Dunn Cavelty, 'A theory', p. 183.

[66] Balzacq and Dunn Cavelty, 'A theory', p. 183.

[67] See also Dwyer, 'Cybersecurity's grammars'; Andrew Dwyer, Clare Stevens, Lilly P. Muller, et al., 'What can a critical cyber security do?', *International Political Sociology*, 16:3 (2022), available at: {https://doi.org/10.1093/ips/olac013}.

[68] Fouad, 'Entropic security'; Fouad, *Theorising Cyber*.

[69] Fouad, 'Entropic security', p. 150, emphasis in original.

[70] Fouad, 'Entropic security', p. 150.

[71] Fouad, 'Entropic security', p. 157.

[72] Fouad, 'Entropic security', p. 160.

[73] Fouad, 'Entropic security', p. 169.

[74] Fouad, 'Entropic security', p. 184, emphasis in original.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

be addressed through normal politics and by implementing security policies that continuously hinder and limit disruptions.[75] In Fouad's words, a 'cyber attack is the noise that threatens the system but does not necessarily challenge its existence'.[76] In this way, the non/physicality of digital information and its creation of system-threatening noise produces what Fouad calls a condition of 'urgency without existentiality'.[77] On Fouad's account, then, the securitisation of cyber is influenced by the immaterial materiality of 'the digital' in the sense that the non/physicality of information enables the swift and urgent securitisation of threats even in the absence of existentiality.

As an advance from critical constructivist securitisation theory, and its view of the immateriality of 'the digital' as a conditioning force, the new materialist approaches to digital immateriality discussed here take us one step further in understanding the role of immaterial agency in securitisation processes. By highlighting the non-human agency of malware and of information more generally, the new materialist scholars discussed here demonstrate how immaterial digital materials act in securitisation processes not only by establishing the foundations for the discursive construction of threats but also by taking an active part in that construction by continuously interacting with the human security actors who formulate threat representations.

Applied to the Norwegian bulk interception controversy, moreover, new materialist approaches to digital immateriality provide further insights into how the new surveillance regime was legitimised. Most importantly, Fouad's notion of noise as a logic of cybersecurity governance offers a promising way of conceptualising how the immateriality of digital materials imposed on the securitisation of communication in the bulk interception controversy.[78] From Fouad's perspective, the non/physicality of communication (a kind of digital information) represented disruptive noise in the securitisation discourse and enabled the implementation of a surveillance regime meant to continuously address this noise and hinder or limit disruptions. This can be seen, for instance, in FFI's consultation response, where they stated that the 'digital ecosystem is used by nearly all societal functions, communication and infrastructure and it is therefore absolutely necessary to understand, manage, make use of and protect', and that the implementation of a new Intelligence Act which included a bulk interception bill was 'necessary because the rapid technological development has created and will continue to create new and significant vulnerabilities and risks for state security'.[79]

At the same time, though, the Norwegian bulk interception controversy also demonstrates that there may be more in play in the immaterial production of cyber (in)security than existing new materialist approaches suggest. Specifically, the securitisation of communication in the case of the Norwegian bulk interception controversy seems to invoke some sort of existentiality, and hence, Fouad's notion of noise-governance as security policy that responds to 'urgency without existentiality'[80] does not provide a precise enough description of the immaterial's role in the securitisation process. The FFI-quote reproduced above, for instance,[81] is indeed imbued with a wish to implement policy which responds to the fundamental, long-term transformation of society and threat politics which digitalisation represents. Moreover, the legitimisation of bulk interception also appears to have been enabled not only by the digitality of threats but also by the threatening nature of 'the digital' in itself. As such, accounts of cyber securitisation that refer to malware agency and noisy cyber attacks do not capture the full breadth of the problem.

[75] See also Jef Huysmans, *Security Unbound: Enacting Democratic Limits* (London: Routledge, 2014).

[76] Fouad, 'Entropic security', p. 172.

[77] Fouad, 'Entropic security', pp. 18, 84, 147.

[78] Fouad, 'Entropic security'; Fouad, *Theorising Cyber*.

[79] Stortinget, 'Åpen høring'.

[80] Fouad, 'Entropic security', pp. 18, 84, 147.

[81] Stortinget, 'Åpen høring'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

Digital im/materiality: Abstraction and obfuscation

In order to discern the materiality of 'the digital' and subsequently to make sense of how this materiality imposes on securitisation processes, I turn to postmodern philosopher Lyotard's[82] notion of immateriality and, more specifically, to philosopher of technology Yuk Hui's[83] reading of Lyotard in light of recent digital transformations. Lyotard's concept of the immaterial stems from an exhibition he set up alongside designer Thierry Chaput at the Centre Pompidou in 1984/5. The exhibition was a response to the development of new telecommunications technology and aimed to thematise how it puts into question modern notions of humans' relation to their material – often technological – surroundings.

More specifically, Lyotard suggests the concept of the immaterial to capture how seemingly non-material technologies that have a physical fundament confronts us with a new kind of matter which is neither material nor non-material but rather something in between and a bit of both.[84] For Lyotard, then, the concept of the immaterial 'defines the realm of the physically imperceptible';[85] it is material in the sense that it consists of physical components and non-material in the sense that it cannot be immediately perceived by the human senses. Hence, it is best captured by the term immaterial, which mobilises the prefix 'im' to negate the notion of a binary relationship between that which is material and that which is not. Since it operates in spatiotemporal registers that evade our senses, moreover, the immaterial refuses control and becomes unmasterable, meaning it constitutes a technology which cannot easily be manipulated by human actors but instead acts upon humans in mysterious and largely ungraspable ways.[86]

Revisiting Lyotard's notion of the immaterial around 30 years after the *Les Immateriaux* exhibition, Hui suggests that the immaterial is helpful for understanding what the digital *is* materially, as it has evolved since the revolution in telecommunications that Lyotard reacted to in the 1980s.[87] To arrive at an immaterial ontology of the digital, however, Hui begins by elaborating on traditional ways of understanding the digital in digital physics and in media theory.

The digital physics approach understands the digital in terms of 1s and 0s. Inspired by Leibniz's monadology and seeking to establish a metaphysics of simple substances, this approach posits that 'any digital being … can be reduced to its binary composition'.[88] On this account, the digital consists materially of the tiniest bits and pieces which constitutes it and is given its characteristic features by the concrete ways in which these bits and pieces relate and are organised. While helpful, Hui argues, this approach is limited since it ultimately conceptualises the digital in highly abstract terms. Understanding the digital in terms of 1s and 0s may seem like a radical concretisation of digital materiality, but in effect it conceals the digital's material foundations by leaving the *concept* of the digital abstracted. The digital physics approach, Hui claims, presupposes the question of materiality, i.e. the question of what the digital *is* materially in the sense that it prioritises 'information [as organised by 1s and 0s] over matter and energy [the material foundations of the digital]'.[89]

Media theory, on the other hand, instead reduces the digital to its physical components, i.e. the materials that support the digital and make possible its practical operation. One influential media-theoretical approach called forensic materiality advocates for 'analysing traces in a computer, going beyond what is visible on the screen'.[90] Forensic materiality thus decomposes digital objects in order to reveal and make visible and tangible the material foundation that undergirds the abstract concept of the digital. Hui sees this approach as a necessary corrective to the digital physics approach,

[82] Lyotard, 'Jean-Francois Lyotard'.

[83] Hui, 'Towards a relational materialism'.

[84] Bernard Blistene, '*Les Immateriaux*: A conversation with Jean-Francois Lyotard', *Flash Art*, 121 (1985), pp. 32–9.

[85] Christina Grammatikopoulou, 'Shades of the immaterial: Different approaches to the "non-object"', *Interartive: A Platform for Contemporary Art and Thought*, available at: {https://interartive.org/2012/02/shades-of-the-immaterial}.

[86] Lyotard, 'Jean-Fancois Lyotard', pp. 37–8.

[87] Hui, 'Towards a relational materialism'.

[88] Hui, 'Towards a relational materialism', p. 133.

[89] Hui, 'Towards a relational materialism', p. 134.

[90] Hui, 'Towards a relational materialism', p. 135.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

since it renders the concrete matter of the digital visible instead of concealing it. For Hui, however, this approach is also limited since it makes the digital almost too physical, which in a sense also conceals the materiality of the digital. By emphasising the tangibility of all digital matter, media theory makes the error of understanding the 'condition of being material … a synonym of its materiality',[91] i.e. it confuses materiality with physicality. While forensic materiality can helpfully 'be applied to any kind of technical object' in order to show how technical objects and their often imperceptible operations are composed of physical matter, it contributes little to 'the clarification of the digital'.[92]

To clarify the digital, then, Hui suggests turning to Lyotard's notion of the immaterial. The immaterial, Hui holds, is precisely what we normally refer to as the digital today and, as such, can cast light on what the digital *is*. Lyotard's notion of the immaterial occupies a middle ground between the digital physics and media theory approaches as it rejects both the abstraction of 1s and 0s and the concretisation of technical objects and instead insists on the simultaneous materiality and non-materiality of digital matter. In occupying this middle ground, moreover, the immaterial offers a radically different way of thinking about digital materiality as such. It does so not only by rejecting exaggerated abstraction and concretisation, but also by refusing to take the question of substance as the starting point for its critique. Both digital physics and media theory 'start with and end up with substance',[93] in the sense that they build their account of digital materiality from observations of the physical existence of binary code and technical objects respectively. The immaterials approach, meanwhile, seeks to move away from substance and approach digital matter as constituted by relations instead. This means that it takes digital materiality to consist not of the digital's physical components but rather of the energy produced by the ways in which these components interact.

Crucially, moreover, Hui argues that the digital stands out from other immaterials such as Lyotard's telecommunications technology since the interactional energy it produces and hence its material force consists of *data*.[94] Technology has a general tendency, Hui explains, to concretise relations and in this way render 'the invisibles visible'.[95] For instance, 'writing puts thoughts and perceptions on paper; pulleys, wheels and chains concretise imaginary movements in mechanical terms; the vapour engine instantiates flows of energy in the relations between water, fuels, pipes and gears'.[96] The concretisation of relations through data, on the other hand, is different since it does not render invisibles visible but rather *keeps invisibles invisible and abstract even in concretised form*, since data – while technically physical – is for all intents and purposes imperceptible.

As such, the digital constitutes a materiality which is not conditioned by 'the subjective grasp of relation',[97] meaning it acts as a material force independent of human perception and understanding of the relations it concretises. Indeed, it is precisely in the elusiveness of the digital, and in the digital's capacity to evade the human senses while it is knowingly physically present, that the material agency of the digital lies. As Mark Weiser famously argued: 'The most profound technologies are those that disappear.'[98] As Hui's reading of Lyotard's concept of the immaterial shows, the concretisation of relations in data form is one particularly effective way for technologies to disappear, and, following Weiser, thus also a powerful way for digital technologies to act in and upon processes of social and political ordering.

Importantly, though, data as a site for the production and enactment of politics has been explored before. Recall for instance Isin, Ruppert, and Bigo's argument that data has world-making

[91] Hui, 'Towards a relational materialism', p. 135.
[92] Hui, 'Towards a relational materialism', p. 136.
[93] Hui, 'Towards a relational materialism', p. 137.
[94] Hui, 'Towards a relational materialism', pp. 138–40.
[95] Hui, 'Towards a relational materialism', p. 138.
[96] Hui, 'Towards a relational materialism', p. 138.
[97] Hui, 'Towards a relational materialism', p. 141.
[98] Mark Weiser, 'The computer for the 21st century', *Mobile Computing and Communications Review*, 265:3 (1991), pp. 3–11 (p. 94).

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

effects and that the invisibility of data plays into how it makes worlds.[99] Moreover, a relational ontology, and more specifically an emphasis on the relationality of data, is nothing new either: new materialist approaches to cyber (in)security all assume that humans and non-humans do not have a pre-relational existence and form but rather emerge from and gain political salience through their interactions with other components of the actor-network or assemblage. For instance, Balzacq and Dunn Cavelty's theory of cybersecurity actor-networks relies on a 'generalised ontological symmetry', meaning it takes 'different kinds of entities (humans and nonhumans) [to be] involved in relational productive activities'.[100]

Different from previous 'data politics' and relational approaches to cyber (in)security, though, Hui's argument that 'the digital' consists of data relations and the energy produced by data interactions highlights how 'the digital' may act as a unitary entity and material force in its own right and not only via the material relationality of its component parts, and through the interactions between these components and human security actors.[101] Through this focus on data relationality, moreover, Hui's approach also brings out the distinctly *im/material* quality of digital matter, which often gets sidelined in existing new materialist approaches. Focusing on the im/material (material but intangible; simultaneously physical and non-physical) elements of 'the digital' (like code and software) and how they interact with the human actors involved in cybersecurity, new materialist approaches locate the political salience of digital immateriality in relations between humans and non-humans. Hui, on the other hand, locates the political salience of 'the digital' in relations between data, and the immaterial energy produced through such relations, since it is in the im/materiality of 'the digital' and not in the relations between the material and immaterial components of digitality that the primary material force of 'the digital' and its capacity for political action lies. This does not mean that 'the digital' does not interact with human actors through its material components, but rather that 'the digital' in itself – a category of technology rather than a concrete technology, e.g. in the form of a device or a piece of equipment – interacts with humans and influences how they socially construct policy issues by imposing its energetic presence on the discourse. Different from the way in which concrete technologies like smartphones or the internet or artificial intelligence would impact their own construction by interacting directly with the human actors who represent them, 'the digital' impacts the construction of policy issues (like security) by providing an entirely new lens through which we view and make sense of them.

Indeed, the material and immaterial quality of 'the digital' has – as we saw above – also been addressed in the literature, most explicitly by Fouad, who conceptualises digital information in terms of the simultaneous physicality and non-physicality of code and software.[102] However, Hui's understanding of 'the digital' in terms of its data ontology differs significantly from Fouad's understanding of 'the digital' in terms of its information ontology, in the sense that it emphasises how 'the digital' acts through the im/material properties of data rather than through the material properties of immaterial digital components like code and software.[103] This is shift in perspective is important not only because it brings out how 'the digital' acts in its own right and not only through the relations between its component parts and human actors, but also because it shows how the political agency of 'the digital' lies in its capacity to concretise relations through further abstraction and obfuscation.

Im/material securitisation: Exceptionality without urgency

What does it then mean to invoke 'the digital' in a security controversy, and more precisely, in efforts to securitise cyber threats? How does immaterial materiality impose on and animate the

[99] Isin, Ruppert, and Bigo, 'Data politics'.

[100] Balzacq and Dunn Cavelty, 'A theory', p. 183.

[101] Hui, 'Towards a relational materialism'.

[102] Fouad, 'Entropic security'; Fouad, *Theorising Cyber*.

[103] Hui, 'Towards a relational materialism'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

securitisation process? One clue can be found in Lyotard's suggestion that the *Les Immateriaux* exhibition was meant to generate unease, indicating that immaterials engender cyber insecurity by invoking a vague and permanent kind of uncertainty.[104] Another (and more important) clue can be found in Hui's argument that the political stake in an immaterial concept of the digital is connected to the use of data for commercial as well as intelligence purposes, which suggests that digital immateriality may primarily produce cross-sectorial, society-wide insecurity.[105] As such, the immateriality of 'the digital' may at first sight be seen to contribute to what Jef Huysmans has called the unbinding of security, whereby insecurities are scattered and diffused across societal domains and permeate everyday life, and, hence, where securitisation turns mundane matters such as digital communication into issues of security.[106] Yet Hui's notion and political reading of 'the digital' points in the direction of a more precise diagnostic of the securitising dynamics at play when 'the digital' acts.

Hui argues that an im/material conception of 'the digital' reveals a political condition in which material relations concretised as data and metadata are profitable for commercial as well as state actors. Hui thus implies that by appreciating the im/material quality of 'the digital' we may see how digitalisation enables what he has elsewhere described as a 'new mode of reification and control'.[107] To clarify this point, Hui also writes that the 'criticality' of this new political condition 'is also in the process of disappearing'.[108] By this he does not mean – I take it – that the criticality of data-governed politics and society is currently disappearing in the sense of losing relevance or potency, but rather that the criticality of such a politics lies precisely in its continuous act of disappearing. That is, the digital is a powerful political force because it systematically avoids capture. As such, Hui invokes Weiser's famous dictum referenced above, which posits that disappearing technologies are the most pervasive, since they become invisible through ubiquity and powerful through being taken for granted.[109]

On this account, 'the digital' can be seen to construct security threats precisely by obscuring them and hence contributes to the production of cyber (in)security by disappearing into the background, a position from which it presents an ever-present, atmospheric source of insecurity and unease. By concretising immaterial components of cyber (in)security through keeping the invisible invisible and hence by abstracting and obscuring that which is technically physical and tangible, 'the digital' represents a threat in itself. This perspective contrasts Stevens's argument that attempts at representing digital threats visually function to 'materialize the virtual'[110] and hence typically have the effect of raising the stakes involved in cybersecurity policy by constructing cyber (in)security in overly apocalyptic terms.

Informed by Hui's data-ontological approach, we can see that 'the digital' acts in and upon the securitisation process by raising the security stakes in the liberty/security-tradeoff, not by allowing for the construction of catastrophe scenarios, but by representing a threat in and of itself. By continuously disappearing into the background and representing an ever-present and looming danger, 'the digital' acts through further abstraction and obfuscation, rather than through enabling concrete representations. In a way, then, a Hui-informed approach to securitisation is more in line with Hansen and Nissenbaum's argument that it is the invisibility of digital threats, rather than attempts at compensating for that invisibility, that leads to securitisation.[111] At the same time, a

[104] Paul Boye, 'The inhuman conditions: Jean-Francois Lyotard's *Les Immateriaux* and technological sublime', *Currents Journal*, 1 (2020), available at: {https://currentsjournal.net/The-Inhuman-Condition}.

[105] Hui, 'Towards a relational materialism', p. 145.

[106] Huysmans, *Security Unbound*.

[107] Yuk Hui, 'Anamnesis and re-orientation: A discourse on matter and time', in Yuk Hui and Andreas Broeckmann (eds), *30 Years after* Les Immateriaux: *Art, Science, and Theory* (Lüneburg: Meson Press, 2015), pp. 179–202 (p. 201).

[108] Hui, 'Towards a relational materialism', p. 145.

[109] Weiser, 'The computer'.

[110] Stevens, *Cyber Security*, p. 153.

[111] Hansen and Nissenbaum, 'Digital disaster'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

Hui-informed approach departs from Hansen and Nissenbaum's constructivism by showing how invisibility is not a limit of representation but rather an agentic property of 'the digital'.

Seeing 'the digital' through Hui's lens, then, seems to enable the governance of cyber (in)security and more precisely influence securitisation of digital communication by saturating the cybersecurity discourse with permanent and indeed existential uncertainty. By disappearing into the background and thus constituting an omnipresent and foundational threat, 'the digital' functions to legitimise the implementation of draconian security policies, meant as a response not to immediate and concrete threats, but to a drastically changed security situation, where a digital atmosphere of lasting uncertainty makes invasive mass surveillance seem natural and necessary. Instead of enabling the governance of cyber (in)security through the logic of noise and a sense of urgency without existentiality, 'the digital' thus conversely enables the governance of cyber (in)security through a sense of *existentiality without urgency*. Through its invisible and complex omnipresence, and via the promise of speedy development and ubiquitous impact, 'the digital' creates a security situation which requires invasive robust action that offers to build a digitally resilient defence, but which does not – and for the very same reasons – require swift and urgent implementation. Indeed, the Norwegian bulk interception controversy, and in particular the Norwegian parliament's decision to postpone the inclusion of the bulk interception clause in the Intelligence Act in lieu of a clarification of the potentially human rights-violating of bulk interception regimes generally from the ECtHR, indicates that the threat of digitalisation is of a type that demands solid grounding and thus cannot operate through a suspension of normal politics, like classical securitisation theory might suggest.

To further explicate what kind of securitisation the im/material agency of 'the digital' enables, and more specifically, to further detail how cyber securitisation as response to existentiality without urgency may operate, we can locate the Hui-informed approach to cyber (in)security in relation to two prominent logics of cyber risk governance recently identified and presented by Sarah Backman and Tim Stevens.[112] Backman and Stevens argue that governance of risk and uncertainty in the cyber domain operates after two main logics: risk as potential threat and risk as uncertainty. Risk as potential threat means that the risk to which cybersecurity policy responds is understood in terms of a potential threat that *may* be actualised in the future. Risk as uncertainty, on the other hand, entails an understanding of cyber (in)security in terms of the constitutive uncertainties and, more precisely, the socio-technical vulnerabilities of digital systems and infrastructures.

Hui's notion of 'the digital' as im/material, and, consequently, the role that 'the digital' plays in processes of securitisation, carries elements of both of the security logics identified by Backman and Stevens and may thus be seen to sit somewhere on a spectrum between them. On the one hand, im/material securitisation responds to potential threats in the sense that 'the digital' is a vehicle for unpredictable future threats. Specifically, the im/material quality of 'the digital' makes potential cyber threats seem more ominous since it obscures and abstracts the nature of such threats. In the bulk interception controversy, we saw this e.g. through Navarsete's emphasis on the invisibility of digital threats and her argument that 'that which we do not see' is 'more difficult to combat'.[113] On the other hand, im/material securitisation also responds to longer-term uncertainties in the sense that 'the digital' represents a fundamental change in the conditions for the governance of cyber (in)security. In particular, the im/material quality of 'the digital' makes uncertainties seem more ubiquitous and complex. This is perhaps best captured by, for example, Gram's argument that 'we cannot have an analogue defence in a digital world'.[114]

The contention that statements from the Norwegian parliamentary debates about bulk interception – such as Navarsete's or Gram's referenced here – show that 'the digital' acts in and upon securitisation processes requires qualification, however. I have made the case that 'the digital' acts

[112] Sarah Backman and Tim Stevens, 'Cyber risk logics and their implications for cyber security', *International Affairs*, 100:6 (2024), available at: {https://doi.org/10.1093/ia/iiae236}.

[113] Stortinget, 'Stortinget, torsdag 11. juni'.

[114] Gram, 'Vi kan ikke'.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

through its im/material properties and suggested that such action is visible in discursive representations. This raises an important methodological question about how we can discern and recognise material agency in discourse, and in securitisation discourses more specifically. More concretely, how can we tell if and to what extent, for example, Navarsete's and Gram's statements cited above were influenced by the im/material agency of 'the digital'?

To address this question, Tom Lundborg and Nick Vaughan-Williams's notion of radical intertextuality is helpful. They argue that the new materialist turn in IR and security studies is problematic since its emphasis on 'the politics of materiality over that of language and representation perpetuates rather than challenges the notion of a prior distinction between language and materiality'. To overcome this problem, they suggest turning to the materialist sensitivity that lies latent in poststructuralist discourse theory. Of particular use for the present article is Lundborg and Vaughan-Williams's analysis of Derrida's notion of 'force'. For Derrida, they explain, materiality and language are characterised by a 'mutual imbrication', which means that 'it is impossible to assume any sort of "pure material" realm that is uncontaminated by language (and vice versa)'. 'Matter "is" not anything', they continue, and can 'only be understood as part of a complex and radical intertextuality' or 'the generalised text'. Animating the generalised text, moreover, are what Derrida calls forces: 'often invisible or impalpable' political moves that cut across the language/materiality divide and which 'entail closures in the attempt to delimit a specific context'.[115]

From the perspective of radical intertextuality, the question of whether we can discern the effect of material agency in discursive representation makes little sense. Language and materiality are 'mutually imbricated' and hence cannot be separated analytically. We cannot know, then, if statements given by parliamentarians about digital security are a result of the im/material agency of 'the digital' per se. Importantly, though, this is not a methodological concession, but an acknowledgement of the complexity of discursive/material meaning-making. Taking seriously this complexity, we should not identify signs of discernible material agency in discursive representations but instead try to look for the activity of force within the generalised text. Seeing 'the digital' as a force in Derrida's sense, representations of 'the digital' in security discourses express, not the exact effect of digital im/materiality on the securitisation of cyber, but the im/material activity of 'the digital' in producing the conditions of possibility for security politics.

Exceptionality without urgency can thus be seen as a mode of securitisation which is enabled, in part, by the im/material force of 'the digital'. 'The digital' is a force that acts in and upon securitisation processes by making current threats abstract and obscure, and by making future threat scenarios more uncertain. In this way, 'the digital' makes possible the implementation of a security policy which maximises data access for the intelligence services to use for calculating and pre-empting risk and, crucially, the long-term legitimation of such policy, since digital development constitutes a fundamental and permanent uncertainty.

Conclusion

In this article, I have explored how the immateriality of 'the digital' acts materially in and upon securitisation processes, and, in particular, how the agential capacities of 'the digital' influences the securitisation of cyber threats. Existing research about the production of cyber (in)security provides important insights into how the immateriality of 'the digital' imposes on securitisation processes. Constructivist securitisation theory accounts for how digital matter, and in particular its immaterial aspects such as invisibility, ubiquity, speed, and complexity, conditions discursive representations of cyber threats, while new materialist approaches account for how immaterial components of cyber threats such as malware act on their own to create political spaces, practices, and effects. Arguing that both these theoretical approaches to the immateriality of cyber

[115] Tom Lundborg and Nick Vaughan-Williams, 'New Materialisms, discourse analysis, and international relations: A radical intertextual approach', *Review of International Studies*, 41:1 (2015), pp. 3–25. available at: {https://doi.org/10.1017/S0260210514000163}.

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press

securitisation provide insufficient answers as to how the immateriality of 'the digital' operates in securitisation processes, the article turned to Yuk Hui's reading of Jean Francois Lyotard's notion of immateriality to suggest that 'the digital' imposes on securitisation processes by abstracting and obscuring digital threats.[116] As opposed to other technologies, 'the digital' concretises imperceptible relations by keeping the invisible invisible and hence makes cyber threats disappear into the background, from where they represent an ominous, existential, and permanent uncertainty. Through Hui's notion of digital immateriality, I argue, we can see how not only digital threats, but also 'the digital' in itself, seen as a material entity and force, act to produce (in)security. Crucially, moreover, I have made the case that the capacity of 'the digital' to abstract and obscure cyber insecurity engenders a new logic of cyber securitisation, where instead of governing noise created by the non/physicality of information through an urgency without exceptionality,[117] security policy governs the obscurity created by the im/materiality of data through a logic of exceptionality without urgency. The theoretical argument is illustrated by the Norwegian bulk interception controversy, which gives an example of a securitisation process where vague and abstract notions of 'the digital', and, importantly, heavy reference to the immaterial nature of 'the digital', play an important part in legitimising the implementation of a new and more invasive surveillance regime.

Acknowledgements. Many thanks to two anonymous reviewers for generous and insightful comments on the manuscript.

Håvard Rustad Markussen is a senior researcher at the Nordic Institute for Studies in Innovation, Research and Education. Markussen holds a PhD in political science and specialises in how science, technology, and innovation influence international security politics and vice versa. His work has appeared in *Security Dialogue, Review of International Studies, International Political Sociology, Critical Studies on Security, Democracy and Security*, and *Issues in Science and Technology*.

[116] Hui, 'Towards a relational materialism'.

[117] Fouad, 'Entropic security'; Fouad, *Theorising Cyber*.

Cite this article: Håvard Rustad Markussen, 'Digital im/materiality and the securitisation of cyber', *European Journal of International Security* (2025), pp. 1–20. https://doi.org/10.1017/eis.2025.10012

https://doi.org/10.1017/eis.2025.10012 Published online by Cambridge University Press