Received: 6 September 2020 | Revised: 17 March 2021 | Accepted: 6 May 2021

DOI: 10.1111/area.12728

AREA Royal Geographical Society with IBG — WILEY

SPECIAL SECTION

More than words: Geopolitics and language

Cybersecurity's grammars: A more-than-human geopolitics of computation

Andrew C. Dwyer

Department of Geography, University of Durham, Durham, UK

Correspondence
Andrew C. Dwyer, Department of Geography, University of Durham, Lower Mountjoy, South Road, Durham DH1 3LE, UK.
Email: andrew.dwyer@durham.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Number: CDT in Cyber Security (University of Oxford) EP/P0

Abstract

On one June afternoon in 2017, during an autoethnography of a malware analysis and detection laboratory, NotPetya quickly caused destruction. This malware has since been characterised as a key geopolitical event in cybersecurity, causing billions of dollars in damage as it rendered inoperable computers across the world. The hunt to identify those who had written NotPetya occurred almost immediately. However, this paper rearticulates this event through grammar, in a close reading of computation, to urge for a more-than-human reading of cybersecurity. By exploring the written propositions of the hackers, various computational materials – including hardware, code, and machine learning algorithms – as well as their ecologies, cybersecurity is understood to be part of an ecology of language-practice. Engaging with N. Katherine Hayles' study of non-human cognition and choice, computation has an ability to read, interpret, and act, and thus intervene. NotPetya is thus not only a tool of hackers but is a political actor which, alongside others, transformed the contours of the geopolitics of cybersecurity. By focusing on grammars, geopolitics does not wholly derive from the (white, male, rational) hacker, analyst, or intelligence agent, but rather from a distributed set of actors that speak to one another. Grammars permit a nuanced appreciation of cyber-attacks, the hacker's handling of computational cognition and choice, as well as conceptualising the relation between author and computation and the risks of machine learning. Cybersecurity, through grammar, then becomes one of co-authorship where security is not only performed by humans but is contorted by an alien politics of computation.

KEYWORDS

autoethnography, computation, cybersecurity, machine learning, more-than-human, NotPetya

1 | INTRODUCTION

A warm cup of tea, some now forgotten software disassembly,[1] a hum of the computers in the background, sunlight streaming through the glass façade. Adam[2] ran into the malware analysis laboratory at around 2.15pm, full

of analysts sitting in rows of desks analysing software for maliciousness, writing detections. He was breathless, speaking fast.

(Research diary)

On 27 June 2017, I first encountered the malicious software NotPetya. This was during a seven-month autoethnography of the malware analysis and detection laboratory at the UK headquarters of Sophos in Oxfordshire, which provides protection against malware.[3] Here, I immersed myself in analysing and detecting what are sometimes known as computational viruses and worms across various computational infrastructures supporting big data analysis and visualisation, the maintenance of 'engines' to distribute detections to customers, as well as its office space, air-conditioning for servers, on segregated and 'safe' networks. NotPetya spread fast that day, with Adam running into the laboratory, Twitter exploding with snippets of news, amid shouting across rows of computers and malware analysts. *We* posted information on a shared page and a detection was quickly distributed to customers. It is this close working with malware at Sophos that informs my thinking of cybersecurity as a more-than-human endeavour. That is, the various materials, the analysts, the hackers, all perform together to produce what I argue are grammars.

NotPetya became infamous through its propagation from a modified update to a popular accounting software used in Ukraine, wiping and rendering inoperable computers across the country, eventually affecting international businesses from FedEx to the pharmaceutical giant Merck. This was subsequently attributed to the Russian military (the GRU) amid claims of the violation of Ukraine's sovereignty. It also exposed vulnerabilities in the everyday, yet geopolitically essential, shipping business Mærsk, as the attack limited systems processing the loading and unloading of cargo ships.

This paper delves into NotPetya as grammar to rearticulate how we attribute responsibility, and understand the geography of cyber conflict and the practices of cybersecurity. Through exploring grammars as a set of language practices that interweave hackers and computational cognition across various ecologies, I demonstrate alternative relationships in cybersecurity that portend to both the complexity of the enactment of attacks and defending against these. Rather than understanding cyber-attacks as linear relationships between hacker intent and resultant impacts through malware as tool or collateral damage, computation instead becomes a political actor and intervenes in what is possible. As computational capacity has grown, as demonstrated through machine learning algorithms, cybersecurity must recognise what grammars can actualise in more-than-human ways, where computation 'speaks' back. For geopolitics, this means that computation cannot be treated as a tool exclusively awaiting human activation, but instead as an actor that shapes geopolitics.

This paper then opens this conversation by: (1) introducing the utility of grammars for understanding computation's role in geopolitics and cybersecurity; (2) offering a reading of NotPetya that continues throughout the paper; (3) detailing what a geopolitics of computation through an understanding of grammars may look like; (4) explaining how computation can be understood as a political actor through its ability for cognition and choice; and concluding by (5) assessing the implications of greater risks for cybersecurity and geopolitics made possible through grammars.

2 | ARTICULATING GRAMMARS

NotPetya has been described as 'the most devastating cyberweapon in the history of the internet' (Greenberg, 2019, p. 180). Yet, like many readings of malware, Greenberg's *Sandworm* locates the locus of NotPetya's agency with its authors. I instead diverge from such a human-dominant perspective to offer a computational language-practice, consisting of texts and performance, as grammar. Through a non/representational appreciation of language (Daya, 2019), I understand malware to per/form particular grammars by adapting the interpretations of McQuillan (2017) and Amoore (2020). In my reading, grammars consist of three primary elements: (1) written *propositions* from computational 'texts' – hardware, software, and code – that guide the parameters of possibility through their arrangement by authors (Amoore, 2013, 2020, pp. 9–13; Wittgenstein, 1969); (2) a more-than-human politics through *computational, non-human cognition* by developing on N. Katherine Hayles' (2017, 2019) work; and (3) how various environments, politics, and other geopolitical arrangements – henceforth *ecologies* (Hörl, 2017) – condition what is per/formed.

Grammars are momentary alignments based on shared language-practices, which render cybersecurity and geopolitics more-than-human. To demonstrate this, I trace NotPetya, crisscrossing the propositions of Russian hackers, how they are *read*, *interpreted*, and *acted* on through computational cognition, as well as various ecologies, including a blackout in Ghana. This is in order to argue that computation has a capacity to be political (Thornton, 2017) through its cognitive abilities. When propositions are written by hackers and then processed through computational cognition in different ecologies, computation interprets and per/forms choices. Grammars then link representational computational texts such as software, hardware as material artefacts, and ecologies that simultaneously form new relations and potentials that cannot be wholly known in advance.

Yet, computational cognition and their resultant choices should not be considered the same as a reflexive human practice of decision, as much as this is always partial and multiple. Rather computational choices should be understood as alien (Fazi, 2019), where grammars cannot be opened up to our representational forms of scrutiny. Grammars – in more-than-human ways – produce arrangements of who and what counts in unequal, and sometimes racist and enduring colonial formations (Elwood, 2020; Mbembe, 2017; Noble, 2018). So, although here I turn my attention to cybersecurity, one element in the task of accounting for computation as a geo/political actor is to develop new methods to address their 'outputs' as choices that are not reduced to representational adjustment of propositional arrangement.

As I witnessed at Sophos, it is not always clear how propositions in the 'texts' of malware lead to certain choices and thus grammars. For cybersecurity, this has important implications, such as when a human should be held responsible for a grammar (e.g., in attribution, see Egloff & Wenger, 2019), or how modifying an ecology can assist in defending against an offensive cyber operation. As Louise Amoore argues in *Cloud Ethics* (2020), it is not possible to simply read the code of machine learning algorithms to adequately identify a point where the propositions (the learning data and software) lead to a certain output. I further argue that grammars, at least partially, are not open to representational examination, due to computational language-practice obscured by differing forms of non-human cognition based on calculative modes, inaccessible to human representation(s). This means that we can never truly grasp the more-than-human politics of a cyber-attack or machine learning-informed detection, but only glimpse at its grammars. That means cybersecurity is full of risks, unknown parts, and this is only becoming more so as 'automated' systems are deployed. When thinking of malware, grammars 'work' – attacks, compromise, and intrusion happen all too frequently – so this is not a claim that computational cognition and its choices are excessive. Propositions matter, they have meaning, but only come to matter in certain performances, in certain places, at certain times to per/form grammars.

3 | NOTPETYA

NotPetya caused such great damage across Ukraine and beyond because it *writes* over crucial code in the 'master boot record' (MBR), preventing the computer from booting up. On that Tuesday morning in June, NotPetya was released through a backdoor[4] to the Ukrainian accounting software, M.E. Doc, causing havoc across the country as it swiftly propagated across internal corporate networks. For many, conducting attribution and understanding its geopolitical implications – from interstate conflict, the disruption of global shipping, to the fragility of 'critical national infrastructure' – would be the totality of this event. However, by considering NotPetya as per/forming a grammar, it is possible to offer a more-than-human and wholly more unsettling account.

The hackers, in this more-than-human reading, arranged a set of propositions to infiltrate M.E. Doc in order for its distribution as part of a 'routine' update (albeit another grammar in itself!). NotPetya could then enter a computer and its network to per/form in these ecologies. NotPetya then *read* these as it encountered different malware detection products. This included Kaspersky ('avp.exe'), which if *read* by NotPetya, was *interpreted* based on its propositions, and *acted* based on these to prevent the wiping of the computer's MBR. Here, we can ask if the hackers wished to protect certain computers – the ecologies – of those using Kaspersky? Likewise, if the Norton ('ns.exe') or Symantec ('ccSvcHst.exe') detection products were *read* and *interpreted*, NotPetya would not use EternalBlue[5] (Sood & Hurley, 2017) to propagate. Was this because EternalBlue would have been *read* and *interpreted* by these detection products, leading them to dectect NotPetya and stop it per/forming its grammars? At Sophos, I read these tightly defined propositions written by the hackers; but this is not, and cannot be, the whole story.

As I have hinted at, NotPetya did not per/form its grammars in isolation but across a mêlée of other computational grammars that, partially, form a broader ecology of materials that include business investment decisions, efforts to segregate networks, and electricity infrastructures. This then makes it difficult to ascertain *where* and *how* (geo)politics emerges. NotPetya did not propagate much beyond internal networks, as the hackers wrote propositions to shape grammars, but not exactly how they come to per/form across ecologies. Therefore, when discussing malware, who and *what* does the geopolitics; is it the hackers, the lack of defensive segregation of (computational) ecologies that resulted in the loss of billions of dollars (see US Department of Justice, 2020; US$1bn), or rather was it the alien politics of computational cognition? It is in the formation of grammars that we see the geopolitical arise, where political actors (human and computational) work with and through the ecologies that they are interwoven with. By understanding this as a language-practice, because there is a reading of texts, their interpretation and action *by* and *through* computation, a wider polity of cybersecurity and geopolitics emerges. The hackers had an approximate idea where their propositions would intersect with computational cognition and their resultant choices, but not where it would precisely take them. It is unlikely that the hackers explicitly intended to severely damage the shipping and logistics business Mærsk or FedEx, but the range of propositions, computational cognition, and choices, as well as the ecology came together to lead to these grammars of 'collateral damage.'

4 | A GEOPOLITICS OF COMPUTATION

Critical geopolitics has attended extensively to language, representation, and discourse (Müller, 2008). This paper advocates for computation to be similarly understood through a per/formative language-practice alongside an embrace of materiality. As Vicky Squire notes, critical geopolitics has conventionally focused on the representational and discursive, and calls for an embrace of more-than-humanism that acknowledges 'the limits of a critical geopolitics that over-invests the representational, cultural, and the interpretive dimensions of geopolitics' (2015, p. 140). This perspective has developed alongside an embrace of the role of materials and the agency of 'things' through new materialisms (Bennett, 2010; Dittmer, 2013), such as in feminist work on embodiment (Sharp, 2020). Materiality is, however, crucial to the potential for language and discourse in geopolitics (Anderson, 2018). Therefore, this paper embraces Squire's (2015) call for a focus on more-than-humanism in geopolitics alongside how the materiality and language-practices of computation offer a potential for it to be understood as a geo/political actor.

A critical geopolitics of computation can then be understood as both a study of materiality and language-practice. Computation, I argue, consists of various texts, both representational and not. In *Of Grammatology*, Derrida notes how 'the entire field covered by the cybernetic program will be the field of writing' (2016, p. 9) and that, according to Butler, 'writing … offers a nonanthropocentric way of understanding language by virtue of its distinction from speech' (Butler, 2016, p. xv). Computational texts then may be considered representational if they contain 'human-readable' propositions, such as in software and code, and crucially texts that are not 'readable,' including hardware. This perspective for computation and cybersecurity to be regarded as a series of texts is most eloquently described in Justin Joque's discussions on cyberwar in *Deconstruction Machines* (2018). Thus, how does the material of a binary logic gate, through to the code of a machine learning algorithm, come to be understood as both material and language-practice? This can be understood through both a capacity to materially afford properties (Davis & Chouinard, 2016), such as 'non-readable' propositions such as processing power, and also a language-practice whereby software and code offer a set of 'human-readable' propositions that condition the parameters of possibility as much as the latter can be interpreted as material. As various propositions interact with one another through computation's cognition, new vulnerabilities, for instance, may emerge – or be 'discovered' – that permit a point of entry for malware or in launching a cyber-attack.

This complex array of computational materialities that form contemporary digital, electronic computation then also provide the basis for interaction with other grammars to form ecologies and thus shape geo/politics. Ecologies consist of multiple layers of non/representational texts, which must be read, interpreted, and acted on, alongside a range of other (non-computational) grammars and geo/politics. Parikka understands a computational text to be 'defined by its motion and rest, speeds and slowness, but also its affects, i.e. its relations with other bodies' (2010, p. 124). This then opens up the relation between author(s) and their computational texts to per/form with unknown others in ecologies. For example, when NotPetya encountered the ecologies of Mærsk, the total damage cost in the region of US$300m (World Economic Forum, 2018). Yet, in some 'luck,' one essential computational material in its IT infrastructure (ecology) was able to be recovered: a domain controller, which stores information on who can access a system. Those domain controllers that had been connected to the internal network had all been wiped by NotPetya's grammar. As Greenberg details, however, at 'some point before NotPetya struck, a black-out had knocked [a] Ghanaian machine off-line, and the computer remained disconnected from the network. It thus contained the singular known copy of the company's domain controller data left untouched by the malware – all thanks to a power outage' (2019, p. 194). NotPetya's grammar was unable to actualise at that moment and place as it intersected with other geopolitical formations, such as postcolonial energy infrastructures (MacLean et al, 2016), global shipping, and beyond. Mærsk supports much international trade, which when disrupted has adverse geopolitical consequences. In this case, they were averted by this ecology and associated geopolitics; it also demonstrates how cybersecurity is intimately tied to coloniality, in ways that may be unexpected. Therefore, ecologies are no less important and extend beyond computation, meaning that computational grammars do not just exist in the 'cyber domain' or 'cyberspace' but are always threaded with other materials and ecologies that may at first glance appear banal or be initially dismissed as part of the everyday.

Mærsk's ecologies however still permitted NotPetya's grammar to quickly per/form a destructive act. The reason to linger on such a point is because there is no flat plane to computation – there are multiple human actors and their propositions, computations, ecologies, and their respective grammars at each instance – there is no such 'singular' event (as much as NotPetya may be popularly perceived as such), but instead there is an incessant per/forming. Therefore, one cannot speak solely of *one* grammar as much as the world is not a singular thought or thing. Even one computer is made up of collectives of propositions; streams, big data, multiple software authors, borrowed code routines, and more. Assessing the grammars of cybersecurity and their geopolitics is not one restricted to the study of disassembly (the lowest human-readable code that I analysed at Sophos) nor of a singular malware like NotPetya, but interrogating grammars as a language-practice that can only ever be partially understood

through studying computational cognition, propositions, and ecologies. Studying cybersecurity and geopolitics then requires an appreciation of a terrain that is complex, differentiated, and a fascinating, more-than-human endeavour.

5 | COMPUTATION AS A POLITICAL ACTOR

To further explicate the argument for computation as an explicit geo/political actor rather than agent or tool, I develop N. Katherine Hayles' (2017, 2019) work on non-human cognition and choice, explored elsewhere in geography (Lynch & Del Casino, 2020). According to Hayles, the world is composed of 'cognizers' who read, interpret, and make choices on signs, and those who do not, 'noncognizers.' The former includes plants, humans, and animals, and crucially, computation. For example, during NotPetya's propagation, it was able to read the ecology and, accordingly, interpret this to make a choice, based on its propositions, on whether to *infect* a particular computer. This is different to noncognizers who do not interpret and make choices, such as ocean waves, rocks, and non-computational technologies (that may still afford certain ecological properties). Hayles then distinguishes computation from other forms of technology as it actively reads, interprets, and acts on signs. Thus, computers can create meanings through processes of sign exchange (2019), and in my reading be political actors. This does not mean that computation is on a plane of equivalence to other cognizers, but that its choices are made through alternative signs, alternative forms of language-practice. These choices are not reflexive and cannot be compared to our notions of decision as they are calculative rather than socially informed (Dwyer, 2020), but rather, I argue, provide a foundation for politics – defined as a capacity to read, interpret, and act on signs. Nor does it mean that computation is automatically intelligent. At the 'low' levels of electronic circuitry, choices are barely distinguishable from the material proposition expressed in its hardware arrangement. Alone it would be a noncognizer, but through its performance as a language-practice, reading and interpreting of signs of multiple materials, choices can be made. Humans likewise work in non/representational ways, with choices that are (pre)cognitive, making choices that do not necessarily correspond to popular understandings of the term, where decisions are but one high-level, reflexive, and abstracted form of choice.

As computation becomes increasingly abstracted from hardware (proposition built on proposition), with big data feeding unsupervised machine learning algorithms, a greater range of recursive cognition is possible, with more choices possible. This increases the potential for geo/political action where political actors are those who are choice-makers. I am not claiming that computational choice is new, but that its cognitive abilities have thus far been relatively limited. This means that we have ignored its political potential, as much as it is not like *our* politics either. As Fazi (2019) claims, computation is an *alien thought* as it (re)cognises the world on a different basis to us. That is because its recognition of representational language, for instance, does not follow humanly socially negotiated modes. As much as new materialism has convincingly advocated for more expansive notions of agency for agents as varied as electricity and infrastructures within, and beyond, geography (Whatmore, 2006), it too often blunts an engagement with radical alterity (Jazeel, 2014). Claiming that computation recognises the world – and makes choices – through a calculative rather than an embodied, affectual mode is then also alien in the most radical political form. 'Organicism' (Hui, 2019) has placed technology below 'natural' things, leading to a neglect of computation's capacity to engage in language-practice, yet one still ferociously compared to *our* intelligence through cybernetic informational comparison (Hayles, 1999). These both suggest that computation is less complex and must also be inherently *knowable* due to its foundation on mathematical logic (Fazi, 2020). Grammars do not necessarily correspond to our assessments, recognition, or sense-making, but malware are actors, not simply agents, due to their calculative interpretation of signs, requiring an assessment of how computation has differing forms of (re)cognition that make it alien to our representations, language, and even politics.

6 | A CYBERSECURITY OF GRAMMARS

This paper does not seek to understand language-practice through grammar, but rather understand grammars through language-practice with propositions per/formed by computation. Grammars are not structures, they are teeming full of sign exchanges, interactions that are affective, organic, and non-organic, crafting new forms of geo/politics. This resonates with Bernard Stiegler's (1998) study of grammatisation – a theory and history of writing – where technology becomes an extension of human capability. However, I broaden beyond Stiegler to suggest that computation is not only an extension, but an actor with a distinct more-than-human alien politics. These politics can sometimes be easily rendered negligible amid the 'grander' geopolitics of cybersecurity, but they are quintessential to our modern lives. Malware exhibit some subtlety to these relationships, in how they are still closely tied to the proposition of the hacker. Even here though, through grammars, computation and NotPetya are not tools but more-than-human endeavours. Yet as unsupervised 'deep' machine learning algorithms increase in recursion,

computation's cognitive ability to read, interpret, and act then transforms its capacity to participate and shape geopolitics. This then should be the central focus of developments for 'automated' security, such as in the application of machine learning to cybersecurity in 'Cyber AI' (Buchanan et al., 2020).

Sophisticated hackers could then be understood as co-collaborators. They arrange their propositions for their intended audience with malicious intent (working with computational cognition and anticipated ecologies). When writing malware, they use computational cognition and choice to their advantage. For example, NotPetya's main propagation method was a modified version of the 'mimikatz' hacking tool. This *reads* the ecology of the computer, and associated business networks, *interprets* the signs it reads, in order to identify credentials. These credentials are used to *act* to access another computer using the grammars of other *legitimate* system tools. As the analysts at Sophos noted, NotPetya's propositions had clear omissions in decryption routines, meaning it was impossible to decrypt the MBR and restore the computer. It is possible to understand malware through proposition and to assess some of the representative intentions of the hackers through the lens of conventional critical geopolitics. Yet, this is never the whole story, as how computation and malware come to per/form grammars is always dependent on computational cognition across multiple ecologies. This is a more-than-human, alien, geo/politics.

I thus offer a more-than-human sensibility to cybersecurity and geopolitics, through NotPetya, to situate computation and its various materialities as political actors through grammars. Rather than understanding the geopolitical consequences of NotPetya through collateral damage or unintended effects – grammars enable this to be interpreted and rendered as a political collaboration. Rather than *writing-off* responsibility of hackers and other actors in cybersecurity, geopolitical research requires even more sensitivity to the dangers and risks of computational cognition. We are responsible for propositions, but we do not have explicit control of the geopolitical consequences due to this alien politics. This calls for cybersecurity research to address when and how computational grammars come into actualisation, whom they affect, and how they may perpetuate or transform harms. Those in cybersecurity – including those I witnessed through the autoethnography of malware analysis and detection – are co-collaborators in writing new worlds, making possible that which was not before. Cybersecurity is always dealing with a more-than-human world of language-practice, per/forming grammars. These include intrusions around COVID-19 vaccines, hacking of states through supply chains, conflicts in Ukraine, and the everyday endpoint detection engines protecting our computers. Therefore, new developments that increase computational cognition in cybersecurity must be aware of the doubt introduced (Amoore, 2020) that is inherent in this alien politics, which must not be written-off as the error, bug, or glitch.

Thus, the three strands of grammar – proposition, computational cognition, and ecology – weave together more-than-human relationships between authors and computation in a language-practice that is performative and non/representational. Computation, as a cognizer, exhibits alternative (re)cognition by reading, interpreting, and acting on signs that cannot be wholly opened nor understood. The 2020 compromise of the IT infrastructure business SolarWinds – which provides services to many US government departments (FireEye, 2020) – may raise questions over what grammars were made possible and how ecologies may be adjusted (are outsourced infrastructures desirable, for instance?). There is no resolution to computational cognition and its choices by trying to fit these into representational modes either. Some machine learning algorithms may be able to give 'partial accounts' (Amoore, 2020), but how closely can we hold hackers, or the IT department at Mærsk, responsible for the full geopolitical implications of the grammars of NotPetya? We would be unwise to wholly rely on propositions, but should assess how grammars come to be enacted. As the potential for greater abstraction enabled through machine learning algorithms in both offensive and defensive practice grows, the role, and politics, of cybersecurity will become more complex. Geopolitics is already grappling with these and grammars may offer one path forward that listens when computation 'speaks' back.

ACKNOWLEDGEMENTS

I would like to thank the SFB/TRR138 'Dynamics of Security' collaborative research centre for hosting me as Visiting Fellow in 2019, where this thinking germinated, as well as Nick Robinson, Pip Thornton, and two anonymous reviewers who provided feedback that greatly improved this paper.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

ORCID

Andrew C. Dwyer https://orcid.org/0000-0003-2207-6834

ENDNOTES

[1] The deconstruction of software into its 'assembly,' the lowest human-readable abstraction of code from digital binary.

[2] Names are pseudonyms.

[3] These are known as endpoint protection, or 'anti-virus,' vendors.

[4] 'Backdoor' is a term used when the user or operator of a computer or system is unaware of a 'secret' access route to that computer or system.

[5] EternalBlue is a hacking tool that was released by the 'ShadowBrokers' group, purportedly by Russian state hackers, after this was respectively hacked from the US National Security Agency.

REFERENCES

Amoore, L. (2013) *The politics of possibility: Risk and security beyond probability*. Durham, NC: Duke University Press.

Amoore, L. (2020) *Cloud ethics: Algorithms and the attributes of ourselves and others*. Durham, NC: Duke University Press.

Anderson, B. (2018) Cultural geography II: The force of representations. *Progress in Human Geography*, 43(6), 1120–1132. https://doi.org/10.1177/0309132518761431

Bennett, J. (2010) *Vibrant matter: A political ecology of things*. Durham, NC: Duke University Press.

Buchanan, B., Bansemer, J., Cary, D., Lucas, J. & Musser, M. (2020) *Automating cyber attacks: Hype and reality*. Washington, DC: Center for Security and Emerging Technology. Available from: https://web.archive.org/web/20210317113544/https://cset.georgetown.edu/wp-content/uploads/CSET-Automating-Cyber-Attacks. pdf. [Accessed 17 March, 2021].

Butler, J.P. (2016) Introduction. In J. Derrida *Of grammatology (Trans. Spivak, G.C.)*. Baltimore, MD: Johns Hopkins University Press.

Davis, J.L. & Chouinard, J.B. (2016) Theorizing affordances: From request to refuse. *Bulletin of Science, Technology & Society*, 36(4), 241–248. https://doi.org/10.1177/0270467617714944

Daya, S. (2019) Words and worlds: Textual representation and new materialism. *Cultural Geographies*, 26(3), 361–377. https://doi.org/10.1177/1474474019832356

Derrida, J. (2016) *Of grammatology* (G. C. Spivak, Trans.). Baltimore, MD: Johns Hopkins University Press.

Dittmer, J. (2013) Geopolitical assemblages and complexity. *Progress in Human Geography*, 38(3), 385–401. https://doi.org/10.1177/0309132513501405

Dwyer, A.C. (2020, May 8) *Algorithms don't make decisions!* Available from: https://web.archive.org/web/20210317113728/https://www.digitalsocieties.co.uk/blog/algorithms-dont-make-desicions [Accessed 17th March 2021].

Egloff, F.J. & Wenger, A. (2019) *Public attribution of cyber incidents*. Zürich: CSS Zürich. Retrieved from CSS Zürich website: CSS Analyses in Security Policy No. 244. https://doi.org/10.3929/ethz-b-000340841

Elwood, S. (2020) Digital geographies, feminist relationality, Black and queer code studies: Thriving otherwise. *Progress in Human Geography*, 45(2), 209–228. https://doi.org/10.1177/0309132519899733

Fazi, M.B. (2019) Can a machine think (anything new)? Automation beyond simulation. *AI & Society*, 34(4), 813–824. https://doi.org/10.1007/s00146-018-0821-0

Fazi, M.B. (2020) Beyond human: Deep learning, explainability and representation. *Theory, Culture & Society*, (Online First). 00, 1–23. https://doi.org/10.1177/0263276420966386

FireEye (2020, December 13) *Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with SUNBURST backdoor*. Available from: https://web.archive.org/web/20210312010850/https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html [Accessed 17th March 2021].

Greenberg, A. (2019) *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. New York, NY: Doubleday.

Hayles, N.K. (1999) *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. Chicago, IL: University of Chicago Press.

Hayles, N.K. (2017) *Unthought: The power of the cognitive nonconscious*. Chicago, IL: University of Chicago Press.

Hayles, N.K. (2019) Can computers create meanings? A cyber/bio/semiotic perspective. *Critical Inquiry*, 46(1), 32–55. https://doi.org/10.1086/705303

Hörl, E. (2017) *General ecology: The new ecological paradigm*. London, UK: Bloomsbury Academic.

Hui, Y. (2019) *Recursivity and contingency*. London, UK: Rowman & Littlefield International Ltd.

Jazeel, T. (2014) Subaltern geographies: Geographical knowledge and postcolonial strategy. *Singapore Journal of Tropical Geography*, 35(1), 88–103. https://doi.org/10.1111/sjtg.12053

Joque, J. (2018) *Deconstruction machines: Writing in the age of cyberwar*. Minneapolis, MN: University of Minnesota Press.

Lynch, C.R. & Del Casino, V.J. (2020) Smart spaces, information processing, and the question of intelligence. *Annals of the American Association of Geographers*, 110(2), 382–390. https://doi.org/10.1080/24694452.2019.1617103

MacLean, L.M., Gore, C., Brass, J.N. & Baldwin, E. (2016) Expectations of power: The politics of state-building and access to electricity provision in Ghana and Uganda. *Journal of African Political Economy and Development*, 1(1), 103–134.

Mbembe, A. (2017) *Critique of black reason*. Durham, NC: Duke University Press.

McQuillan, D. (2017) The Anthropocene, resilience and post-colonial computation. *Resilience*, 5(2), 92–109. https://doi.org/10.1080/21693293.2016.1240779

Müller, M. (2008) Reconsidering the concept of discourse for the field of critical geopolitics: Towards discourse as language and practice. *Political Geography*, 27(3), 322–338. https://doi.org/10.1016/j.polgeo.2007.12.003

Noble, S.U. (2018) *Algorithms of oppression: How search engines reinforce racism*. New York, NY: NYU Press.

Parikka, J. (2010) Ethologies of software art: What can a digital body of code do? In: Zepke, S. & O'Sullivan, S. (Eds.) *Deleuze and contemporary art*. Edinburgh, UK: Edinburgh University Press, pp. 116–132.

Sharp, J. (2020) Materials, forensics and feminist geopolitics. *Progress in Human Geography*, (Online First). 00, 1–13. https://doi.org/10.1177/0309132520905653

Sood, K. & Hurley, S. (2017, June 29) *NotPetya technical analysis – A triple threat: File encryption, MFT encryption, credential theft*. Available from: https://web.archive.org/web/20190213211315/https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/ [Accessed 13th February 2019].

Squire, V. (2015) Reshaping critical geopolitics? The materialist challenge. *Review of International Studies*, 41(1), 139–159. https://doi.org/10.1017/S0260210514000102

Stiegler, B. (1998) *Technics and time 1: The fault of epimetheus*. Stanford, CA: Stanford University Press.

Thornton, P. (2017) *Geographies of (con)text: Language and structure in a digital age*. Computational Culture: A Journal of Software Studies, Autumn 2017(6). Available from: http://computationalculture.net/geographies-of-context-language-and-structure-in-a-digital-age/

US Department of Justice. (2020, October 19). *Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace*. Available from: https://web.archive.org/web/20210311183609/https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and [Accessed 17th March 2021].

Whatmore, S. (2006) Materialist returns: Practising cultural geography in and for a more-than-human world. *Cultural Geographies*, 13(4), 600–609. https://doi.org/10.1191/1474474006cgj377oa

Wittgenstein, L. (1969). *On certainty* (G. E. M. Anscombe & G. H. von Wright, Eds.; D. Paul & G. E. M. Anscombe, Trans.). Oxford, UK: Blackwell Publishing.

World Economic Forum. (2018) *Securing a common future in cyberspace [Panel]*. Davos-Klosters, Switzerland: World Economic Forum.

How to cite this article: Dwyer, A. C. (2023). Cybersecurity's grammars: A more-than-human geopolitics of computation. *Area*, 55, 10–17. https://doi.org/10.1111/area.12728