

The Non-anthropocentric Informational Agents: Codes, Software, and the Logic of Emergence in Cybersecurity

Noran Shafik Fouad

Blavatnik School of Government, University of Oxford, Oxford, UK

Email: noran.fouad@bsg.ox.ac.uk

Orcid: <https://orcid.org/0000-0001-9517-2267>

Abstract

Many theoretical approaches to cybersecurity adopt an anthropocentric conceptualisation of agency; i.e., tying the capacity to act to human subjectivity and disregarding the role of the non-human in co-constructing its own (in)security. This article argues that such approaches are insufficient in capturing the complexities of cyber incidents, particularly those that involve self-perpetuating malware and autonomous cyber attacks that can produce unintentional and unpredictable consequences. Using interdisciplinary insights from the philosophy of information and software studies, the article counters the anthropocentrism in the cybersecurity literature by investigating the agency of syntactic information (i.e., codes/software) in co-producing the logics and politics of cybersecurity. It specifically studies the complexities of codes/software as informational agents, their self-organising capacities, and their autonomous properties to develop an understanding of cybersecurity as *emergent security*. Emergence is introduced in the article as a non-linear security logic that captures the peculiar agential capacities of codes/software and the ways in which they challenge human control and intentionality by co-constructing enmity and by co-producing the subjects and objects of cybersecurity.

Keywords: cybersecurity, information, materiality, non-human agency, emergent security

Biography: Dr Noran Shafik Fouad is a Postdoctoral Research Associate at the Blavatnik School of Government, University of Oxford, where she is conducting public policy research on cybersecurity and working on developing executive education courses on digital governance and cybersecurity. Noran holds a PhD in International Relations from the University of Sussex, in which she examined the socio-political construction of cybersecurity in the U.S.A. through an analysis of the peculiarities and agency of digital information. Prior to her PhD studies, Noran worked as an Assistant Lecturer of Political Science at Cairo University, Egypt, as well as an Academic Assistant and Executive Editor for two academic journals published by the university. Her research generally lies at the intersection of technology, security and governance, and her interests include cybersecurity, critical security studies, securitization, risk theories, philosophy of information, and software studies.

Introduction

Hostile cyber operations have been growing exponentially in both number and sophistication; ranging from those conducted by non-state actors to state-backed cyber attacks. Two of the most high-profile operations in the last few years were the WannaCry ransomware which affected more than 200,000 computers in 150 countries, and NotPetya, considered the costliest cyber attack in history with an estimated loss of 10 billion dollars.¹ In both incidents, a *self-propagating* malicious software (malware) spread itself automatically among information systems, encrypting data on vulnerable computers and demanding ransom payments. As such, both incidents raised scholarly and policy concerns about the unintended consequences of cyber attacks. Although WannaCry was not specifically targeted at the health sector, the National Health Services (NHS) in the UK was significantly hit by it, leading to widespread discussions on the importance and complexities of cybersecurity in healthcare.² On the other hand, NotPetya was not primarily financially motivated; it was allegedly launched by the Russian government in order to disrupt financial, energy, and government institutions in Ukraine.³ As argued by Ciaran Martin, the former head of the UK's National Cyber Security Centre (NCSC): "WannaCry and NotPetya were deliberate attacks, but their impact on the UK and allied countries was accidental. So the two biggest incidents that we faced early on [at the NCSC] were both basically accidents."⁴ These two examples, thus, showcase the significance of *autonomous* cyber attacks that, even if targeted, may spread in

¹ Kaspersky, 'Top 5 Most Notorious Cyberattacks', (6 November 2018), available at: {<https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/>}.

² Jesse M Ehrenfeld, 'Wannacry, Cybersecurity and Health Information Technology: A time to Act', *Journal of Medical Systems*, 41:7 (2017), p.104.

³ For more information on NotPetya, see: Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *WIRED*, (22 August 2018), available at: {<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>} accessed 1 October 2021.

⁴ Ross Kelly, 'Ciaran Martin: Emerging Cyber Threats and Their Unintended Consequences', *DIGIT*, (7 October 2020), available at {<https://digit.fyi/ciaran-martin-ncsc-unintended-consequences-cybersecurity/>} accessed 29 November 2021.

ways that are unpredictable by their initiators, causing haphazard disruption at scale and putting individuals and businesses at the forefront of geopolitical conflicts.⁵

Importantly, these and other examples challenge the anthropocentric theoretical approaches to the study of cybersecurity which tie the capacity to act to human subjectivity and overlook the role of the *non-human* in co-constructing its own (in)security. This anthropocentrism is reflected in the considerable number of literature that approach the socio-political construction of cybersecurity as a function of human discourses and threat representations through linguistic and discursive analysis.⁶ Although these studies generate a conceptually far more sophisticated approach than the overwhelmingly policy-oriented cybersecurity literature, they do not sufficiently capture the non-discursive materiality of cyber incidents that goes beyond human agency and rhetoric. If security is assumed to be discursively constructed, and if discourse is a function of the *human* actor, then the ability to act and influence security ultimately resides in humans. Such an approach is insufficient in studying the complex operations of cyber incidents in which the agency of malware challenges human intentionality and control, and ultimately produces unpredictable and unintended consequences, as in the case of WannaCry and NotPetya. To fill this gap, more

⁵ Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Harvard University Press, 2020), pp.280–90.

⁶ For example: David J. Betz and Tim Stevens, 'Analogical Reasoning and Cyber Security', *Security Dialogue*, 44:2 (2013), pp. 147–164; R. Guy Emerson, 'Limits to a Cyber-Threat', *Contemporary Politics*, 22:2 (2016), pp.178–96; Lee Jarvis, Stuart Macdonald, and Andrew Whiting, 'Analogy and Authority in Cyberterrorism Discourse: An Analysis of Global News Media Coverage', *Global Society*, 30:4 (2016), pp.605–23; Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth: How the United States Securitized Cyberspace', in J. Eriksson and G. Giacomello (eds) *International Relations and Security in the Digital Age*, (Routledge, 2007), pp.57–82; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, CSS studies in security and international relations (London: Routledge, 2008); 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; Johan Eriksson, 'Cyberplagues, IT, and Security: Threat Politics in the Information Age', *Journal of Contingencies and Crisis Management*, 9:4 (2001), pp.200–210; Lene Hansen and Helen Nissenbaum, 'Digital Disaster, Cyber Security, and the Copenhagen School', *International Studies Quarterly*, 53:4 (2009), pp.1155–75.

recent scholarly contributions have shifted from human discourses towards a study of *materiality* in analysing cybersecurity practices.⁷ They investigate the complex configurations of cybersecurity *assemblages* through which cybersecurity is ‘made’,⁸ as well as the performative influences of cyber-incidents as *actants* or political agents per se.⁹

This article contributes to the emerging literature that engages with the materialities of cybersecurity by analysing the agency of *information* in co-producing the logics and politics of cybersecurity. It focuses specifically on codes/software, as syntactic manifestations of information, and conceptualises them as *informational agents* with generative and agential properties that go beyond mere instrumentalization in the construction of cybersecurity. In so doing, the article explores how, even if initially given their agency by humans, codes/software can subsequently change such agency in execution and also lend agential roles back to both humans and material objects. Building upon recent scholarship on the philosophy of information and software studies, the article investigates the complexities of codes/software, their self-organising capacities, and their autonomous properties to develop an understanding of cybersecurity as *emergent security*. Emergence is a key concept in complexity theory and the study of self-organising systems. It illuminates the inherent unpredictability of complex informational systems and the elements of novelty associated with their operations. The article introduces ‘emergence’ as a non-linear logic that captures

⁷ Tim Stevens, *Cyber Security and the Politics of Time* (New York: Cambridge University Press, 2015).

⁸ Jeppe T. Jacobsen, ‘Lacan in the US Cyber Defence: Between Public Discourse and Transgressive Practice’, *Review of International Studies*, 46:5 (2020), pp.613–31; Jamie Collier, ‘Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision’, *Politics and Governance*, 6:2 (2018), pp.13–21; Clare Stevens, ‘Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet’, *Contemporary Security Policy*, 41:1 (2020), pp.129–52; Florian J Egloff and Myriam Dunn Cavelty, ‘Attribution and Knowledge Creation Assemblages in Cybersecurity Politics’, *Journal of Cybersecurity*, 7:1 (2021), pp.1–12.

⁹ 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; Andrew C. Dwyer, ‘Cybersecurity’s Grammars: A More-than-Human Geopolitics of Computation’, *Area*, (2021), pp. 1–18.

the agential capacities of information and the uncertainties they engender in cybersecurity. As will be shown, the *logic of emergence* and *emergent security* challenge the idea of human control in cybersecurity in two ways: by undermining the centrality of human intentionality as a basis for constructing enmity, and by acknowledging the role of codes/software in co-producing the subjects/objects of cybersecurity.

To substantiate these arguments, the article unfolds in three sections. The first section problematises the concept of agency in the theoretical cybersecurity literature, particularly ones that apply discursive and linguistic approaches. It explains the article's contribution to the new materialist and post-humanist debates on the agency of non-human 'things' in critical security studies by arguing that information too - specifically in its syntactic manifestation of codes/software - possess a *distinctive* agency. The second section examines the conceptualisation of agency in technical literature, such as software studies and computer science, to distinguish the agency of codes/software from that of ordinary matter or other non-human things. It goes on to analyse the agential capacities of codes/software, which malware as the ultimate cyber weapon is a prominent example of, and demonstrates elements of autonomy and unpredictability in their operation. Based on an understanding of the peculiar agential capacities of codes/software, the third section conceptualises cybersecurity as emergent security, in which codes/software influence human actancy and agency. It particularly analyses this logic of emergence in light of the construction of enmity and the co-production of subjects and objects in cybersecurity discourses and practices, and explains what this non-human reading does to the politics of cybersecurity.

1. Discourse, materiality, and the non-human in cybersecurity

Technologies and socio-technical structures are often instrumentalised and their agency is reduced to the passive mediation of human subjectivity and the immaterial representation of human desires. They are frequently viewed in utopian terms when they obey human's orders and perform the tasks they are designed for, and in dystopian terms when they do not.¹⁰ In cybersecurity research, this instrumentalisation can be primarily found in studies that employ discursive and linguistic approaches to theorising cybersecurity. A prominent example in this regard is literature that build upon Copenhagen School's securitization theory in studying cybersecurity as a *speech act* or a discourse in which a human securitizing actor presents a threat as *existential* to a particular referent object and thus requiring *emergency measures* to ensure that object's survival.¹¹ Although originally such studies focused on the USA as a case study, more recent contributions are calling for applying securitization theory to cybersecurity in 'the non-West',¹² such as Singapore, Japan, and Egypt.¹³

Related to the cyber securitization literature are a wide range of studies that use a discursive methodology to explore how cybersecurity discourses, utterances, and threat representations are *different* from other sectors. They note that cybersecurity discourses

¹⁰ Michael Schandorf and Athina Karatzogianni, 'Agency in a Posthuman IR: Solving the Problem of Technosocially Mediated Agency', in Erika Cudworth, Stephen Hobden, and Emilian Kavalski (eds), *Posthuman Dialogues in International Relations*, (Routledge, 2018), pp.89–108.

¹¹ Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, Colo: Lynne Rienner Publishers, 1998); Bendrath, Eriksson, and Giacomello, 'From "Cyberterrorism" to "Cyberwar", Back and Forth'; Dunn Cavelty, *Cyber-Security and Threat Politics*; Dunn Cavelty, 'Cyber-Terror—Looming Threat or Phantom Menace?'; Eriksson, 'Cyberplagues, IT, and Security'; Hansen and Nissenbaum, 'Digital Disaster'.

¹² Mark Lacy and Daniel Prince, 'Securitization and the Global Politics of Cybersecurity', *Global Discourse* 8:1 (2018), pp.100–115.

¹³ Paul Kallender and Christopher W. Hughes, 'Japan's Emerging Trajectory as a "Cyber Power": From Securitization to Militarization of Cyberspace', *Journal of Strategic Studies*, 40: 1–2 (2017), pp.118–45; Syed Mohammed Ad'ha Aljunied, 'The Securitization of Cyberspace Governance in Singapore', *Asian Security*, (2019), pp.1–20; Bassant Hassib and Nardine Alnemr, 'Securitizing Cyberspace in Egypt: The Dilemma of Cybersecurity and Democracy', in Scott N. Romaniuk, Mary Manjikian (eds) *Routledge Companion to Global Cyber-Security Strategy* (Routledge, 2021).

operate in the absence of a minimum level of agreement on the nature of threats, and sometimes with no empirical evidence of attacks to justify them. That is why such discourses mostly rely on symbolisations, by drawing comparisons between cyber threats and other conventional ones.¹⁴ Added to this is the biologisation of technology and the use of ‘viruses’ and ‘worms’ metaphors;¹⁵ the spatial analogies of cyber ‘space’;¹⁶ and the use of fear-based hypothetical cyber-doom scenarios.¹⁷ Hansen and Nissenbaum’s theorisation of cybersecurity as a *distinct* security sector by demonstrating its unique ‘security grammars’ is one notable contribution in this regard.¹⁸

All such contributions are important for establishing a dialogue between the relatively new field of cybersecurity and the long-established theories of security, particularly given that, to-date, the majority of cybersecurity literatures remain policy-oriented in nature and tend to be conceptually under-theorised.¹⁹ However, focusing only on speech acts overlooks questions of *materiality* and *agency*. As put by Miller, ‘things that people make, make people’.²⁰ Though technological artefacts are human-made, they are capable of evolving in ways not necessarily envisioned by their creators, and influencing all aspects of human life, including security experiences and practices. The historical rise of information technologies and information sciences have, in fact, long challenged the centrality of human agency and enabled a discussion on the agential capacities of machines and other non-human

¹⁴ Emerson, ‘Limits to a Cyber-Threat’; Jarvis, Macdonald, and Whiting, ‘Analogy and Authority in Cyberterrorism Discourse’.

¹⁵ Myriam Dunn Cavelty, ‘From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse’, *International Studies Review*, 15:1 (2013), pp.105–22.

¹⁶ Betz and Stevens, ‘Analogical Reasoning and Cyber Security’.

¹⁷ Sean Lawson, ‘Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats’, *Journal of Information Technology & Politics*, 10:1 (2013), pp.86–103.

¹⁸ Hansen and Nissenbaum, ‘Digital Disaster’.

¹⁹ Tim Stevens, ‘Global Cybersecurity: New Directions in Theory and Methods’, *Politics and Governance*, 6:2, (2018), p.2.

²⁰ Daniel Miller, ed., *Materiality* (Duke University Press, 2005), p.38.

‘things’. Whilst such debates on technology and agency are becoming more prevalent in other fields of security,²¹ it is not adequately reflected in the study of cybersecurity; i.e., the security of information technology per se and the construction of its logic(s).

There are several material realities regarding the nature of computer disruptions, their effects, and knowledge about them in technical communities that cannot be understood as part of discursive constructions alone.²² This includes, for example, the exponential rise in the number of cyber operations through self-replicating malware that enjoy a considerable level of autonomy in execution, such as the WannaCry and NotPetya examples mentioned earlier. In fact, the very idea of computer viruses and worms – that constitute ‘the cyber weapon’ – is an exemplar of how information systems are capable of deviating from the human intentionality embedded in their design, since they were not initially designed to be used maliciously. Cyber incidents caused by malware are, in turn, major challenges to ideas of control upon which computing technologies were based. As argued by Rid, it is the dystopia of the promises of ‘cybernated’ economies, cyborgs, and cyberspace as a new parallel frontier to reality. Now, control over machines can be taken from humans, systems can be attacked and controlled distantly, and several damages can result in the form of data loss, abuse, denial of services, or even machine damaging.²³

Accordingly, a recent strand of literature has shifted towards a critical engagement with the politics of cybersecurity to unpack its materialities beyond rhetoric and linguistic

²¹ For example: Myriam Dunn Cavelty, Thierry Balzacq, and Sophie-Charlotte Fischer, ‘Killer Robots’ and Preventive Arms Control’, in *Routledge Handbook of Security Studies* (Routledge, 2017), pp.457–68; Mareile Kaufmann, ‘Who Connects the Dots? Agents and Agency in Predictive Policing’, in Marijn Hoijtink and Matthias Leese (eds), *Technology and Agency in International Relations* (Routledge, 2019), pp.141–64; Ian Shaw and Majed Akhter, ‘The Dronification of State Violence’, *Critical Asian Studies*, 46:2 (2014), pp.211–34.

²² Myriam Dunn Cavelty, ‘The Materiality of Cyberthreats: Securitization Logics in Popular Visual Culture’, *Critical Studies on Security*, 7:2, (2019), pp.138–40.

²³ Thomas Rid, *Rise of the Machines: A Cybernetic History* (Scribe Publications Pty Limited, 2016).

representations. They approach cybersecurity as an *assemblage* that comprises a complex configuration of cybersecurity actors and therefore transcends the state-centric focus of linguistic approaches.²⁴ This includes, for example, the various alliances that make complex malware successful, be they conceptual (e.g., ideas about the role of the state or cybersecurity firms), material (e.g., hardware, buildings, and centrifuges), social (e.g., the links between hackers, programmers, and operators), or textual (e.g., news reports and coverage).²⁵ Cybersecurity assemblages can be also seen in analysing attribution as a ‘knowledge creation process’ performed by constantly-shifting networks of actors that establish ‘truths’ about cyber incidents.²⁶ The role of *practices* in co-producing cybersecurity is also highlighted in some literature through, for example, the study of ‘transgressive practices’ by security communities that co-constitute states’ defensive strategies.²⁷

This article contributes to the study of the materialities of cybersecurity by advancing the discussion on *non-human agency*, specifically in relation to the newly-emerging literature that approaches cyber incidents and malware as ‘political actors’,²⁸ capable of co-constructing the ‘space’ in cyberspace²⁹, and therefore co-shaping ‘the conditions of possibility for cybersecurity politics’.³⁰ As such, the article argues that there is more to the limitations of discursive analysis of security than disregarding contextual influences and non-state actors. Specifically, the article criticises the *anthropocentric theorisation of agency* in cybersecurity literature; i.e., tying *the capacity to act* to human subjectivity and disregarding the role of the

²⁴ Collier, ‘Cyber Security Assemblages’.

²⁵ Clare Stevens, ‘Assembling Cybersecurity’.

²⁶ Egloff and Dunn Cavelty, ‘Attribution and Knowledge Creation Assemblages in Cybersecurity Politics’.

²⁷ Jacobsen, ‘Lacan in the US Cyber Defence’.

²⁸ Dwyer, ‘Cybersecurity’s Grammars’.

²⁹ Balzacq and Dunn Cavelty, ‘A Theory of Actor-Network for Cyber-Security’.

³⁰ 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 (2021), pp.25–43,

non-human in co-constructing security. That is to say, analysing the socio-political construction or the 'making' of cybersecurity cannot be sufficiently done if all the subjects of analysis are humans and if non-human things are only considered as 'facilitating conditions' that lie outside the realm of agency.³¹ Capturing the complexities and materialities of cybersecurity necessitates an analysis of information, particularly in its syntactic form of codes/software, not as a mere tool for human actors, but as an *active actant* in its own right.

New materialism and 'information' that matters

"Language matters. Discourse matters. Culture matters. There is an important sense in which the only thing that does not seem to matter anymore is matter." ³²

The idea that non-human entities like information and its syntactic manifestation in codes/software can be *actants* with agential influences on security construction coincides with what is often called 'the material turn', 'non-human turn', 'thing studies', 'posthumanism', or 'new materialism' in social sciences. This so-called turn produced new philosophical paradigms, such as object-oriented ontology,³³ vital materialism,³⁴ agential realism,³⁵ and actor-network theory,³⁶ to challenge the binary division of the world into human subjects and non-human objects. All such contributions share a critical view of the

³¹ Claudia Aradau, 'Security That Matters: Critical Infrastructure and Objects of Protection', *Security Dialogue*, 41:5 (2010), pp.491–514; Mark B. Salter, 'Security Actor-Network Theory: Revitalizing Securitization Theory with Bruno Latour', *Polity* 51:2 (2019), pp.349–64.

³² Karen Barad, 'Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter', *Journal of Women in Culture and Society*, 28:3, (2003), p.803.

³³ Ian Bogost, *Alien Phenomenology, Or, What It's Like to Be a Thing* (University of Minnesota Press, 2012); Levi R. Bryant, *The Democracy of Objects* (Open Humanities Press, 2011); Graham Harman, *Object-Oriented Ontology: A New Theory of Everything* (Penguin UK, 2018).

³⁴ Jane Bennett, 'Systems and Things: On Vital Materialism and Object-Oriented Philosophy', in Richard A. Grusin and Richard Grusin (eds) *The Nonhuman Turn*, (University of Minnesota Press, 2015), pp.223–40.

³⁵ Barad, 'Posthumanist Performativity: Toward an Understanding of How Matter Comes to Matter'; Karen Barad, *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning* (Duke University Press, 2007).

³⁶ Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford University Press, 2005); John Law and Vicky Singleton, 'Object Lessons', *Organization* 12:3 (2005), pp.331–55.

dominant status of the Anthropocene, but differ in the extent to which they move beyond this dominance in articulating the relationship between humans and non-humans.³⁷ They theorise matter as active, politically significant force that has meaning beyond social, political, or economic structures, and has agency that transcends politics of representation. From this lens, the concept of agency in International Relations and Security Studies can be problematised.

In International Relations and Security Studies, the new materialist and post-humanist approaches represent a criticism of the inadequacy of existing ontological and epistemological perspectives to capture the non-human agency, be it that of machines, animals, bacteria, the environment, etc. For many years in the discipline, agency has been tied to the human subject, and the capacity to act has been linked to cognition, intentionality, desires, and decision-making - qualities regarded as exclusive to humans.³⁸ Similarly, despite attempts by critical security studies (CSS) to widen security to include actors other than the state, actancy was still limited to humans and human collectivities. If threats are conceptualised as manifestations of suffering, and if the ability to express such suffering is a function of humans, then security is tangled to human subjectivity.³⁹ However, a strand of research focusing on materiality and non-human agency started to gain momentum in recent

³⁷ Matt McDonald and Audra Mitchell, 'Introduction: Posthuman International Relations', in Clara Eroukmanoff and Matt Harker (eds) *Reflections on the Posthuman in International Relations: The Anthropocene, Security and Ecology* (E-International Relations, 2017).

³⁸ Benjamin Braun, Sebastian Schindler, and Tobias Wille, 'Rethinking Agency in International Relations: Performativity, Performances and Actor-Networks', *Journal of International Relations and Development* 22:4 (2018), pp.787–807.

³⁹ Audra Mitchell, 'Only Human? A Worldly Approach to Security', *Security Dialogue* 45:1 (2014), pp.5–21; Audra Mitchell, 'Dispatches from the Robot Wars; Or, What Is Posthuman Security?', *The Disorder Of Things* (blog), (24 July 2014), available at {<https://thedisorderofthings.com/2014/07/24/dispatches-from-the-robot-wars-or-what-is-posthuman-security/>} accessed 25 November 2021.

years. Examples include analysing the materiality of critical infrastructure,⁴⁰ borders,⁴¹ emotions,⁴² weapons,⁴³ among others.

Indeed, information technologies and the evolution of cybernetics - introduced by Norbert Wiener in the 1940s as the science of control and communication in the animal and the machine - ⁴⁴ had a major impact on the evolution of thinking about human and non-human agency. If approached genealogically, posthumanism can be linked to the Macy Conferences on Cybernetics that took place between 1946-1953.⁴⁵ In these conferences, the human subject was decentralised in relation to other objects, and in particular to *information*.⁴⁶ Cybernetics brought forward an analysis of information as a free-flowing entity among biological and non-biological systems, which opened the way towards blurring the lines between humans and machines. Both humans and machines were seen as autonomous and goal-directed entities; an idea that challenges the humanist subject. As one of its pioneers, Ross Ashby argued that cybernetics is not concerned with “what is this thing?”, but rather asks “*what does it do?*”.⁴⁷

Moreover, with increased digitisation, and the advancements in artificial intelligence (AI) and robotics, the level of control humans maintain over machines began to be largely challenged. Such developments form the basis on which some futuristic trans-humanist approaches in social sciences conceptualise the ‘posthuman’ and problematise ‘human’ as a

⁴⁰ Aradau, ‘Security That Matters’.

⁴¹ Mike Bourne, Heather Johnson, and Debbie Lisle, ‘Laboratizing the Border: The Production, Translation and Anticipation of Security Technologies’, *Security Dialogue* 46:4 (2015), pp.307–25.

⁴² Ty Solomon, ‘Embodiment, Emotions, and Materialism in International Relations’, in Linda Åhäll and Thomas Gregory (ed) *Emotions, Politics and War*, (Routledge, 2015), pp.58–70.

⁴³ Antoine Bousquet, Jairus Grove, and Nisha Shah, ‘Becoming Weapon: An Opening Call to Arms’, *Critical Studies on Security*, 5:1 (2017), pp.1–8.

⁴⁴ Norbert Wiener, *Cybernetics: Or, Control and Communication in the Animal and the Machine* (Wiley & Sons, 1948).

⁴⁵ The Macy conferences were interdisciplinary conferences held in the USA and are sometimes considered the most significant scientific events after WWII. Concepts like ‘information’ and ‘analogue/digital’ were introduced in these conferences as part of regulatory frameworks that can apply to both humans and machines.

⁴⁶ Cary Wolfe, *What Is Posthumanism?* (University of Minnesota Press, 2010), p.xii.

⁴⁷ W. Ross Ashby, *An Introduction to Cybernetics* (Chapman and Hall, 1958), p.1.

category. From their perspective, humans are undergoing a process of evolutionary transformation towards becoming posthuman, i.e., being replaced, outpaced, and outsmarted by the technological non-humans. They contend that technologies are growing autonomously beyond human comprehension or control.⁴⁸ For example, several studies on cyborgs, brain-computer interfaces, and biomedical engineering argue that human body has transformed as a result of ubiquitous technological developments, either through upgrade, enhancement, extension, or invasion.⁴⁹

However, acknowledging the autonomy of technology and machines beyond human subjectivity does not mean they have overtaken agency. Unlike the techno-reductionist views of trans-humanism, the concept of agency can be problematised without resorting to biological, evolutionary, and hypothetical scenarios that assume humans are transforming into something else or being replaced entirely by the non-human. Rather, technology can be approached as one factor among many in breaking the binary division between humans and non-humans. This leads to what is often called a 'flat ontology', in which the traditional separation between the human and the technological non-human is blurred, and thus necessitating a study of *materiality*.⁵⁰

In technology, software, and media studies, the term 'materiality' is used in abundance, though rarely defined. In some instances, physicality is viewed as a defining character of matter, and therefore some studies refrain from using the term 'materiality'

⁴⁸ Elke Schwarz, 'Hybridity and Humility: What of the Human in Posthuman Security?', in Clara Eroukmanoff and Matt Harker (ed), *Reflections on the Posthuman in International Relations: The Anthropocene, Security and Ecology* (E-International Relations, 2017), pp.29–28.

⁴⁹ Carolin Kaltöfen, 'With a Posthuman Touch: International Relations in Dialogue with the Posthuman - A Human Account', in Erika Cudworth, Stephen Hobden, and Emilian Kavalski (eds, *Posthuman Dialogues in International Relations*, (Routledge, 2018), p.42.

⁵⁰ Rosi Braidotti, *The Posthuman* (John Wiley & Sons, 2013).

when they discuss properties of software or data for example, and use words like ‘stuff’ instead.⁵¹ On the other hand, some STS literature use materiality to imply the social conditions that surround the development of technology and scientific discoveries; what could be described as ‘the materiality of practice’. Similarly, in media studies, the materiality of context is discussed in terms of the political economy or geographical considerations of media development, in addition to questions of ownership, control, reach, etc.⁵² Nevertheless, acknowledging the *vitality* of non-human objects led to an increasing focus on materiality as *agency* in studying media infrastructures and digital technologies.⁵³ An example of this approach can be seen in studies that attend to the cultural role of information and ‘digital goods’ and their symbolic weight in material cultures, as well as the study of how information and digital networks are shaping *space*.⁵⁴

This article studies the materiality of cybersecurity by analysing the agency of *information* as an entity that *matters*. Although there is not one single definition for information, it can be generally divided into three categories that speak directly to the field of cybersecurity: syntactic information, in the form of signs, signals, or bits; semantic information, or the meanings conveyed through those bits and signals; and pragmatic information, when those meanings and ideas conveyed are new to someone.⁵⁵ While these multiple categories of information are central to cybersecurity, this article focuses specifically

⁵¹ Paul M. Leonardi, ‘Digital Materiality? How Artifacts Without Matter, Matter’, *First Monday* 15:6–7 (2010).

⁵² Paul Dourish, *The Stuff of Bits: An Essay on the Materialities of Information* (MIT Press, 2017).

⁵³ Lisa Parks and Nicole Starosielski, *Signal Traffic: Critical Studies of Media Infrastructures* (University of Illinois Press, 2015).

⁵⁴ Paul Dourish and Melissa Mazmanian, ‘Media as Material: Information Representations as Material Foundations for Organizational Practice’, in *How Matter Matters: Objects, Artifacts, and Materiality in Organization Studies*, ed. Paul R. Carlile et al. (OUP Oxford, 2013), pp.92–118. p.94

⁵⁵ Terrence W. Deacon, ‘What Is Missing from Theories of Information?’, in Paul Davies and Niels Henrik Gregersen (eds) *Information and the Nature of Reality: From Physics to Metaphysics* (Cambridge University Press, 2010), p.152.

on syntactic information in the form of codes/software because they are considered the ‘centre of gravity in cybersecurity’, as a fundamental quality that distinguishes cyber threats from conventional ones. All cyber threats must go through the syntactic layer to qualify as such; i.e., to originate from code alterations or the use of malicious codes.⁵⁶

In the next sections, to counter the anthropocentrism in the cybersecurity literature, the article gives more weight in the analysis to codes/software, albeit without suggesting that their agency supersedes or replaces human agency. For example, in her introduction to vital materialism, Jane Bennett says:

“I will emphasize, even overemphasize, the agentic contributions of nonhuman forces (operating in nature, in the human body, and in human artifacts) in an attempt to counter the narcissistic reflex of human language and thought. We need to cultivate a bit of anthropomorphism – the idea that human agency has some echoes in nonhuman nature – to counter the narcissism of humans in charge of the world.”⁵⁷

Similarly, the article theorises syntactic information (i.e., codes/software) as generative and productive of the meaning of cybersecurity, alongside humans and in interaction with them, even though it focuses more on codes/software as such. This non-human reading of cybersecurity is done by establishing a dialogue between the newly-emerging fields of the philosophy of information and software studies on one side and critical security studies (CSS) and cybersecurity studies on the other. This dialogue is essential for any attempt to theorise cybersecurity in CSS given the close links that the philosophy of information and software studies have with the sciences and technologies constitutive of the ‘cyber’. As argued by Bellanova, Jacobsen, and Monsees, security studies need to ‘take the trouble’ of transcending disciplinary boundaries in order to understand the role of

⁵⁶ Karsten Friis and Jens Ringsmose (eds), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (London: Routledge, 2016), p.4.

⁵⁷ Jane Bennett, *Vibrant Matter: A Political Ecology of Things* (Duke University Press, 2009).p.xvi

technologies through new frameworks of analysis.⁵⁸ Transcending disciplinary boundaries is particularly important for theorising non-human agency in cybersecurity given that, as argued by Tim Stevens, new materialisms have not sufficiently incorporated ‘information’ as an entity in their ‘conceptual schema’ and therefore did not engage with the important debates in the philosophy of information on the ontology of information in relation to the ‘matter’ that new materialism theorised for.⁵⁹

Additionally, the article takes the argument on the centrality of non-human agency in CSS a step further by delving deeper in the agency of information as a *peculiar* kind of agency. In emphasising the agency of matter, many strands of new materialism and post-humanism include all non-human things in their entirety without distinguishing between the agential capacities they possess. In addition, some approaches adopt a *relational* ontology according to which an object is only *real* if it has an effect on other objects. Latour’s actor-network theory, for example, assumes that there is no force embedded in objects as such beyond their relations with other objects, from which they acquire agency.⁶⁰ Nevertheless, it could be argued that “*all things equally exist, yet they do not exist equally*”.⁶¹ Non-human things are not all of one type and do not exercise the same form of agency.⁶² Further, as noted by Harman, flat ontology should not be an end in itself: it is not enough to reject the position of humans as the centre of ontology. Rather, the analysis should extend to investigating the distinctive features and powers possessed by different non-human entities beyond their

⁵⁸ Rocco Bellanova, Katja Lindskov Jacobsen, and Linda Monsees, ‘Taking the Trouble: Science, Technology and Security Studies’, *Critical Studies on Security*, 8:2 (2020), pp.87–100.

⁵⁹ Tim Stevens, ‘Information Matters: Informational Conflict and the New Materialism’, Paper for presentation at Millennium Annual Conference, ‘Materialism and World Politics’, 20-21 October 2012, London School of Economics, Available at SSRN: <http://dx.doi.org/10.2139/ssrn.2146565>.

⁶⁰ Harman, *Object-Oriented Ontology*.

⁶¹ Ian Bogost, *Alien Phenomenology*, p.11.

⁶² Bryant, *The Democracy of Objects*.

relations with other objects.⁶³ On that basis, the article argues that if all matter in all security sectors have agency, cybersecurity is distinguished by the *peculiar* agency of codes/software as informational agents. That is to say, *all matter matters, but codes/software matter differently* – as will be shown next.

2. An informational account of agency

“It is from this rich and complex ferment of information that the concept of agency emerges.”⁶⁴

The concept of agency has always been central to the theorisation of information, even if not uttered as such. In one of its commonly used definitions, information is conceptualised as ‘the difference that makes a difference’ or the ‘distinction that makes a difference’, in relation to the Latin origin of the word ‘informare’ meaning to ‘shape’ or ‘form’. This definition indicates that information always has a purpose and seeks to achieve a particular change or transformation.⁶⁵ Just like energy heats up matter, information can also be added to matter and change it or give it form and structure.⁶⁶ Therefore, some theorists argue that what distinguishes our planet is the concentration of information intrinsic to its existence. Even if other parts of the universe have more matter or energy than Earth, none has more information.⁶⁷ Consequently, information has a strong relationship with causation. Some studies contend that all causal links are inherently *information*. This is because the idea of

⁶³ Harman, *Object-Oriented Ontology*.

⁶⁴ Paul Davies, *The Demon in the Machine: How Hidden Webs of Information Are Finally Solving the Mystery of Life* (Penguin UK, 2019), p.2.

⁶⁵ Mark Burgin, *Theory of Information: Fundamentality, Diversity and Unification* (World Scientific, 2010), p.102.

⁶⁶ Terrel Ward Bynum, ‘Informational Metaphysics: The Informational Nature of Reality’, in Luciano Floridi (ed) *The Routledge Handbook of Philosophy of Information* (Routledge, 2016), p.207.

⁶⁷ César Hidalgo, *Why Information Grows: The Evolution of Order, from Atoms to Economies* (Penguin UK, 2015), pp.8–9.

causation itself is about transferring a quantity of information between two or more states of a particular system.⁶⁸

This capacity of information to *do* things, be it *order*, *change*, or *causation* is the basis of many informational approaches to cosmology and evolution. According to such approaches, evolution is a complex process of information exchange,⁶⁹ in which information specifies *what* things should do.⁷⁰ They argue that if the question of life is in essence a question of physics, then it is ultimately about information that physical systems possess and the transition in the informational structure of matter.⁷¹ This idea is also connected to Wiener's argument: "Information is information, not matter or energy. No materialism which does not admit this can survive at the present day."⁷² Although it was not clear what Wiener meant by 'information is information', it can be inferred that he regarded information as 'autonomous'; something that has a distinct structure.⁷³

This belief in the ontological primacy of information has echoes in some empirical studies that analyse the transformation of military conflicts in the information age. For instance, Arquilla and Ronfeldt - who wrote the influential paper 'Cyberwar is Coming!'-⁷⁴ view information as 'an essential part of all matter', and that it is as fundamental to the world as matter and energy. Consequently, according to them, information "should be treated as a basic, underlying and overarching dynamic of all theory and practice about warfare in the

⁶⁸ Phyllis Illari and Federica Russo, 'Information and Causality', in Luciano Floridi (ed) *The Routledge Handbook of Philosophy of Information* (Routledge, 2016), pp.235–48.

⁶⁹ James Gleick, *The Information: A History, a Theory, a Flood* (HarperCollins Publishers, 2011), p.12.

⁷⁰ Seth Lloyd, *Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos* (Knopf Doubleday Publishing Group, 2006).

⁷¹ Sara Imari Walker, 'Top-Down Causation and the Rise of Information in the Emergence of Life', *Information* 5:3 (2014), p.425.

⁷² Wiener, *Cybernetics*, p.132.

⁷³ Peter Janich, *What Is Information?* (University of Minnesota Press, 2018), p.4.

⁷⁴ John Arquilla and David Ronfeldt, 'Cyberwar Is Coming!', *Comparative Strategy* 12:2, (1993), pp.141–65.

information-age”.⁷⁵ Similarly, Dunn Cavlety and Brunner argue that information is *the* major source of power both in its material form of computers and infrastructure, and also in the ‘immaterial realm’ of codes. As they put it: “Information becomes a weapon, a myth, a metaphor, a force multiplier, an edge and a trope – and the single most significant military factor”.⁷⁶ Also, in his discussion of ‘network-centric warfare’, Dillon contend that “information is the prime mover in military as in every other aspect of human affairs, the basic constituent of all matter”.⁷⁷

The argument that information has agency, and one that is peculiar when compared with matter or energy, can be made clearer by looking at how ICTs, digital information, and software engineering literatures define the concept of *agency*. As mentioned earlier, many post-humanist literatures derived their main ideas and assumptions about the agency of non-human things from cybernetics. Cybernetics introduced a behaviouristic conceptualisation of agency by focusing on the external, goal-oriented, and purposive behaviour of entities, rather than their internal properties. Alan Turing’s famous paper titled ‘can a machine think?’, published in 1956, posed a question that is still under discussion to this day.⁷⁸ Whether a computer/software has consciousness, can actually think, or even has emotional intelligence remains an open question that reflects the increasingly blurred lines between human and non-human agency in informational settings.⁷⁹

⁷⁵ Ibid, p.154.

⁷⁶ Elgin M Brunner and Myriam Dunn Cavlety, ‘The Formation of In-Formation by the US Military: Articulation and Enactment of Infomantic Threat Imaginaries on the Immaterial Battlefield of Perception’, *Cambridge Review of International Affairs* 22:4 (2009). p. 633.

⁷⁷ Michael Dillon, ‘Network Society, Network-Centric Warfare and the State of Emergency’, *Theory, Culture & Society* 19:4, (2002). pp.72–73.

⁷⁸ A. M. Turing, ‘Can a Machine Think’, *The World of Mathematics* 4 (1956), pp.2099–2123.

⁷⁹ Paul Davies, *The Demon in the Machine*, p.186.

If information in general is the difference that makes a difference, codes/software as the syntactic manifestation of information can be seen as ‘organised array of differences’.⁸⁰ Although not all codes/software can be described as ‘intelligent’ agents in the same manner as AI, they nevertheless remain purposeful. That is why, technical conceptualisation of agency and agents, particularly in the computer science literature, often goes beyond the ability to simply *do* or *act*, towards human-like characteristics that ordinary matter hardly possess. Among the most important of these attributes is *autonomy*. Traditionally, autonomous agency was considered as one characteristic of living beings, through which they maintain their survival. Yet, the evolution of information systems has shown that autonomy cannot be exclusive to living beings or humans. In some computer science literature, autonomous agency is defined as an ‘autocatalytic system’ that can detect, measure, and constrain energy. This demands nuanced intelligent choices, or the ability to choose among various courses of behaviour in a way that is sensitive to the surrounding environment.⁸¹ Autonomous agency thus requires an element of rationality, or the existence of desires on the part of the agent and an ability to act on best interest.

Another agential property is *reactivity*, or the ability of the system to react to its environment, interact with other human and non-human agents, and adapt its behaviour in response. This is also linked to the agent’s *proactivity*, and being able to take initiatives, instead of just reacting to changes in the external environment.⁸² Proactive behaviour is primarily goal-oriented and requires a minimum degree of intelligence that allows the informational agent to understand its internal and external environment, and to adapt its

⁸⁰ Peter Suber, ‘What Is Software?’, *Journal of Speculative Philosophy* 2:2 (1988), pp.89–119.

⁸¹ Anne-Marie Grisogono, ‘How Did Information Emerge?’, in Sara Imari Walker, Paul C. W. Davies, and George F. R. Ellis (eds) *From Matter to Life: Information and Causality* (Cambridge University Press, 2017), pp.86–89.

⁸² Michael Wooldridge and Nicholas R. Jennings, ‘Intelligent Agents: Theory and Practice’, *The Knowledge Engineering Review* 10:2 (1995), pp.115–52.

behaviour based on such knowledge. It should have an inferential capability through which it uses existing knowledge to work on abstract tasks.⁸³ In addition, it should be mobile and able to navigate in different systems and networks flexibly, while possessing human-like traits, such as reliability and trustworthiness. These capabilities, nonetheless, are not necessarily enjoyed by all informational agents with different levels of complexity; the more complex they are, the more of these properties they possess and vice-versa.⁸⁴

The criteria against which the agential capacities of informational agents are measured in these disciplines is one important manifestation of how their agency is fundamentally different from the rest of *things*. For many computer science scholars, a powerful conceptualisation of agency is one in which the properties of informational agents are “conceptualised or implemented using concepts that are more usually applied to humans”.⁸⁵ As summarised by one study: “Agents are unlike other artefacts of society in that they have some level of intelligence, some form of self-initiated, self-determined goals”.⁸⁶ This is one reason why such literature uses the concept of *agents* rather than *objects* in talking about information systems. They see objects as entities that do not have choices of action and cannot make decisions, while *informational agents do and can*.

The agential capacities of codes/software

“...software is somewhat excessive and vexed. It overflows its own context and creates new contexts. In many instances software is so

⁸³ Jeffrey M. Bradshaw, ‘Introduction’, in *Software Agents*, ed. Jeffrey M. Bradshaw (AAAI Press, 1997), 3–48.

⁸⁴ Walter Brenner, Rüdiger Zarnekow, and Hartmut Wittig, *Intelligent Software Agents: Foundations and Applications* (Springer Science & Business Media, 2012), pp.19–34.

⁸⁵ Wooldridge and Jennings, ‘Intelligent Agents’, p.117.

⁸⁶ Donald A. Norman, ‘How Might People Interact with Agents’, in Jeffrey M. Bradshaw (ed) *Software Agents* (AAAI Press, 1997), p.54.

complicated, so distributed and convoluted in architecture that it defeats comparison with any other technical object.”⁸⁷

Studying the actions of codes/software and their operation is ultimately a study of agency. As MacKenzie argues, ‘code is agency-saturated’.⁸⁸ Even if it is primarily a textual entity, code is more than a ‘medium of description’; it is rather a ‘medium of execution’. This executability and inherent causal power of codes/software is a main property that distinguishes their agency from that of other artefacts.⁸⁹ For example, although ‘art-like objects’ usually have a human recipient, it is not necessarily the case for codes/software. Sometimes the recipients of codes/software are other machines or software, which in turn can generate codes.⁹⁰ In cybersecurity, a malicious software (malware) is targeted towards particular vulnerabilities (exploitable coding errors) in the adversary’s system, not humans. Additionally, though they inhabit micro-spaces, codes/software are agents for the ‘automatic production of space’.⁹¹ Malware, as argued by Blazacq and Dunn Cavelty, is capable of co-constructing spatiality by circulating within multiple spaces that cross sovereign boundaries.⁹²

Even if written by humans, once embedded in a digital machine, codes/software start operating automatically, telling that machine what to do or not to do. Here, machines can be considered the ‘final arbiter’ in operating codes, not the human.⁹³ In many tasks, starting from simply logging into the internet, codes/software act autonomously and react to inputs and outputs automatically, often with no direct human intervention.⁹⁴ Machines are

⁸⁷ Adrian MacKenzie, *Cutting Code: Software and Sociality* (New York: Peter Lang Inc., 2006), p.17.

⁸⁸ Ibid, p.16.

⁸⁹ Timothy R. Colburn, ‘Software, Abstraction, and Ontology’, *The Monist* 82:1 (1999), pp.3–19.

⁹⁰ MacKenzie, *Cutting Code*.

⁹¹ Nigel Thrift and Shaun French, ‘The Automatic Production of Space’, *Transactions of the Institute of British Geographers* 27:3 (2002), pp.309–35.

⁹² Balzacq and Dunn Cavelty, ‘A Theory of Actor-Network for Cyber-Security’.

⁹³ Federica Frabetti, *Software Theory: A Cultural and Philosophical Study* (Rowman & Littlefield International, 2015), pp.45–46.

⁹⁴ Rob Kitchin and Martin Dodge, *Code/Space: Software and Everyday Life* (MIT Press, 2011).

now automatically exchanging data, using electronic sensors, updating themselves, producing predictions and warnings, controlling traffic lights, authorising payment cards, opening and closing doors, etc.⁹⁵ As a result, codes/software have become more malleable, flexible, adaptable, and interactive to the outside world than other technologies and ‘material artefacts’.⁹⁶

The relative autonomy of codes/software can sometimes make them unpredictable, and potentially escape the span of human control. Their inherent unpredictability already starts with the way they are produced. Codes/software are not developed by a single person, but are usually engineered within big projects in which many programmers with varying levels of skills and knowledge participate. This process results in a very complex piece of codes/software that no one single programmer can claim they fully understand.⁹⁷ What is more, in most cases, codes/software are engineered through a process of trial and error. They are left to run and have a life of their own, while being tested and improved in the process. For this reason, codes/software are mainly *engineered* rather than *designed*, since they do not always follow what programmers dictate. Programmers almost have an ‘ignorant expertise’ in dealing with codes/software they helped producing.⁹⁸

Hence, although codes/software can be considered a human bid to control the digital, they maintain sovereignty over execution through self-enforceability. Their operation is never linear; they usually incur deviations and self-modification in execution. This is what one author described as ‘code drift’ to explain the many unplanned consequences,

⁹⁵ David Berry, *The Philosophy of Software: Code and Mediation in the Digital Age* (Springer, 2011).

⁹⁶ Jannis Kallinikos, *Governing Through Technology: Information Artefacts and Social Practice* (Springer, 2010).

⁹⁷ Kitchin and Dodge, *Code/Space*.

⁹⁸ Thrift and French, ‘The Automatic Production of Space’.

fluctuations, and transformations that occur in the operation of codes/software.⁹⁹ Added to this, programming is done by standardised, formalised software-enabled languages that facilitate the process of writing code. This involves a lot of abstractions that hide details that may seem unnecessary for the programming process. Although these abstractions make the job of programmers a lot easier, they also reduce their knowledge of and power over the codes they write. As argued by one study, automatic programming “is both an acquisition of greater control and freedom, and a fundamental loss of them”.¹⁰⁰ This is magnified when it comes to ordinary users who normally have no comprehension of internal codes and algorithmic processes beyond the graphical interfaces they interact with. Such interfaces give the human user an illusion of control and an imaginary of a ‘sovereign executive’, when in fact they are perpetuating users’ ignorance.¹⁰¹ As put by Clare Stevens, “Malware and coding are materials that exceed human capacities to sense or understand them, so that they do not present themselves to us in unmediated fashions.”¹⁰²

Acknowledging that agency in informational systems is distributed among humans and non-humans raises an important question: if both humans and codes/software are agential, where is the line of responsibility?¹⁰³ This question primarily challenges the liberal-modernist understanding of humans as the sole agency that establishes causalities based on intentional decision-making.¹⁰⁴ This paradox is starting to gain momentum in cybersecurity practices too, with the increasing use of AI and machine learning. It is estimated that the AI

⁹⁹ Arthur Kroker, *Exits to the Posthuman Future* (John Wiley & Sons, 2014), pp.49–59.

¹⁰⁰ Wendy Hui Kyong Chun, *Programmed Visions: Software and Memory* (MIT Press, 2011), pp.45–46.

¹⁰¹ Ibid.

¹⁰² Stevens, C., ‘Assembling Cybersecurity’, p.131.

¹⁰³ Catherine Adams and Terrie Lynn Thompson, *Researching a Posthuman World: Interviews with Digital Objects* (Springer, 2016).

¹⁰⁴ Marijn Hoijtink and Matthias Leese, ‘How (Not) to Talk About Technology: International Relations and the Question of Agency’, in Marijn Hoijtink and Matthias Leese (eds) *Technology and Agency in International Relations* (Routledge, 2019), p.3.

market in cybersecurity will increase to \$34.8 billion in 2025 from \$1 billion in 2016.¹⁰⁵ AI adds an operational advantage to cybersecurity strategies since it is capable of overcoming the limited cognitive abilities of humans to handle huge amounts of data. Not only is AI growing in use in defence practices; experts also predict that new types of cyber incidents are likely to appear in the future given AI's capability of transcending what humans may consider impractical, such as labour-intensive spear phishing operations.¹⁰⁶ However, the complexity, uncertainty, and lack of transparency associated with anomaly-based AI technologies in cybersecurity raise questions about agency and decision-making between the human and the algorithm.¹⁰⁷ Because AI systems are inherently dynamic, understanding their operation and explaining their outcomes is not an easy task. That is why, when AI systems are attacked, detection becomes difficult, because reverse-engineering their operation to understand whether the outcome of their behaviour is a result of an attack or not is quite challenging.¹⁰⁸ As argued by Tim Stevens, the use of AI in cybersecurity poses a key question: "Where is agency in the new cybersecurity assemblage and who or what makes the decisions that matter?".¹⁰⁹

It is important to note here that the article is not suggesting that it is impossible for humans to unpack the complexity of codes/software or that ordinary users cannot develop an understanding of their behaviour. It also does not deny that codes/software are in fact written by humans and therefore cannot be studied in isolation from what humans wanted them to do. The aim of this section is rather to showcase how the operation of informational

¹⁰⁵ Mariarosaria Taddeo, Tom McCutcheon, and Luciano Floridi, 'Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword', *Nature Machine Intelligence* 1:12 (2019), pp.557–58.

¹⁰⁶ Miles Brundage et al., 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation', *arxiv preprint*, 2018.

¹⁰⁷ Tim Stevens, 'Knowledge in the Grey Zone: Ai and Cybersecurity', *Digital War*, 2020.

¹⁰⁸ Taddeo, McCutcheon, and Floridi, 'Trusting Artificial Intelligence', p.558.

¹⁰⁹ Stevens, 'Knowledge in the Grey Zone', p.168.

systems and codes/software can challenge the idea of an in-control human in ways that other types of non-human things cannot. As such, the agency of codes/software assumed here is not that of intentionality, consciousness, or free will, but rather an agency of *influence*. Even if the previously mentioned code-drifting is a result of a human error in coding, the consequences of this do influence humans in ways they did not necessarily envision or anticipate. The relative autonomy, reactivity, and proactivity of codes/software outlined above is what makes their agency and influence on human and non-human things peculiar.

This agency of codes/software is magnified when they are used maliciously. Malware are special kinds of codes/software. The most peculiar property of viruses and worms is not their maliciousness, because they are not malicious per se, but rather their ability to copy themselves automatically, described as 'self-reproducing automata'.¹¹⁰ Whereas viruses require human action to activate them, like clicking a link or opening a file, worms even have the capacity to self-propagate across devices without this human intervention. Malware are also capable of performing multiple self-preservation techniques to avoid detection and elimination. For example, they can do what is known as stealthing, through which they hide their presence and make it difficult to detect them. This can be done by slowing down their operation or presenting a fake clean image of an infected file to an anti-virus program. Polymorphism is another self-preservation technique by which malware change their base code dynamically every time they run, whilst having the same functionality. A step further to polymorphism is metamorphism, which refers to malware changing their functionality as they propagate across different systems.¹¹¹ In short, malware are inherently active; they are

¹¹⁰ Ibid, pp.173–228.

¹¹¹ Ed Skoudis and Lenny Zeltser, *Malware: Fighting Malicious Code* (Prentice Hall Professional, 2004), pp.64–68.

constantly doing something or spreading somewhere, 'almost like living'.¹¹² The relative unpredictability of malware can defy human control, even if operating through rationally pre-defined codes and algorithms.

Several unintended political and technical consequences that transcend the control of the initiator may result from self-perpetuating malware and self-modifying codes. They can spread to un-targeted systems, they can be discovered due to an error in coding, and they can cause an over-reaction from governments or media that was not initially intended. As Argued by Balzacq and Dunn Cavelty, malware can be approached as mediators with 'transformative agency' that is detached from the initiator's intent. Assuming that objects also enact spaces, malware is co-constitutive of the 'space' in cyberspace, and thus cyber incidents should be analysed within 'the spaces they build themselves' by spreading between devices in completely unplanned ways by their initiators.¹¹³ This argument has far-reaching implications on security and the assumptions of human control imbedded in its logics, as will be explained next.

3. Emergent security: the logic of emergence and human control in cybersecurity

To capture the agential capacities of malware as informational agents in the construction of cybersecurity, the article proposes the *logic of emergence*. Emergence is a key concept in complexity theory, which is also linked to cybernetics, computer science, and chaos theory. The central assumption behind emergence is that a complex system will necessarily produce new, unexpected properties and will end up behaving in an unpredictable way.¹¹⁴ As a result

¹¹²Jussi Parikka, *Digital Contagions: A Media Archaeology of Computer Viruses* (Peter Lang, 2007).

¹¹³ Balzacq and Dunn Cavelty, 'A Theory of Actor-Network for Cyber-Security'.

¹¹⁴ Mark Mason, *Complexity Theory and the Philosophy of Education* (John Wiley & Sons, 2009), pp.32–35.

of interactions among their diverse parts, the properties of such systems will change dynamically in a non-linear process, producing *emergent* rather than *resultant* behaviour. Emergence and non-linearity are characteristics of self-organising and complex adaptive systems, in which outputs cannot be simply predicted based on inputs or analysing the individual parts of the system. The interactions that take place autonomously in these systems lead to emergence.¹¹⁵ This notion of emergence is capable of countering the reductive assumptions of 'ontological individualism' and ideas about humans as the sole agents in the world.¹¹⁶ It is a statement against an in-control human with a full capacity to understand and predict surrounding environments.

Emergence has a number of characteristics that can be employed in theorising cybersecurity as *emergent security*. Firstly, emergence is characterised by *novelty*. New features can appear as a result of dynamic changes, which cannot be simply predicted from existing properties of a system.¹¹⁷ Secondly, emergence is contextual and relational. Emergent properties in every system are unique to its particular context and to its interactions with multiple agents.¹¹⁸ Thirdly, emergent systems are not centralised, and their parts are not necessarily working towards achieving a particular, unified goal. They rather adapt and interact with dynamic changes in their environments, producing emergent results for the entire system.¹¹⁹

¹¹⁵ Antoine Bousquet and Simon Curtis, 'Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations', *Cambridge Review of International Affairs* 24:1 (2011), pp.43–62.

¹¹⁶ Ibid, p.52.

¹¹⁷ Peter A. Corning, 'The Re-Emergence of "Emergence": A Venerable Concept in Search of a Theory', *Complexity* 7:6 (2002), pp.7–18.

¹¹⁸ Mason, *Complexity Theory and the Philosophy of Education*, pp.32–35.

¹¹⁹ Corning, 'The Re-Emergence of "Emergence"', pp.7–18.

Information is entirely connected to the idea of self-organisation, as shown earlier. Information systems are inherently 'self-organising agent-based systems' that act as autonomous agents. They are capable of collecting information and act upon it to pursue a certain set of goals, producing a wide range of future possibilities that cannot be easily predicted.¹²⁰ For that reason, the operation of information technologies and information-processing systems can be only described probabilistically, since it is impossible to accurately predict their future behaviour. Complex, dynamic, and decentralised information systems with emergent behaviour produce complex, dynamic, and decentralised *security* with emergent properties. The elements of autonomy and unpredictability in the operation of codes/software as described earlier generate a logic of emergence in cybersecurity. To be clear, this does not entirely invalidate human control. Rather, it suggests that the construction of security in cybersecurity is not always subject to the sole agency of humans and their intentionality. The elements of novelty, unpredictability, contextuality, and decentralisation associated with emergence can be found in the co-production of enmity and the subjects and objects of cybersecurity, as will be explained in the next two subsections.

The subjects and objects of cyber incidents

Cybersecurity is distinguished by its multi-stakeholder nature. It is co-constituted by every single user of digital technologies, from individual citizens to corporations and governments. However, the identification of the actors of interest in a certain incident and those entitled with taking the necessary measures to counter an ongoing cyber incident or attack is not always pre-defined and can have an emergent nature. Similarly, choosing security *objects* in

¹²⁰ Jeffrey Johnson, 'Can Complexity Help Us Better Understand Risk?', *Risk Management* 8:4 (2006), pp.227–67.

a single incident may not also be entirely controlled by the attacker. The subjects and objects of cybersecurity, together with the resulting consequences of a cyber incident, are co-produced by the agency of malware *in addition to* that of humans.

Firstly, if all software contains bugs (coding errors), a malware is distinct given its ability to self-replicate, which intensifies its potential buggy nature. Bugs are more likely to appear in malware because they do not go through the same testing processes of normal software. Further, since malware does not operate in controlled environments, it becomes difficult to overrule bugs they may contain during propagation, and therefore increasing chances of unintended consequences. Once a malware is deployed, it becomes very difficult for the attacker to maintain control over its propagation or to accurately predict its behaviour. It can always affect unintended systems resulting in varying degrees of damage. Not knowing strictly which systems the malware will propagate to beforehand, in most cases, limits the attacker's ability to test its compatibility with such systems.¹²¹

Secondly, even if propagation is meant to be limited, in practice, that might not be possible, particularly because attacks can hardly be stopped once started. To reach its target faster, the attack needs to spread widely and to propagate fast among non-target systems. A specific algorithm is usually used for target selection, either by simply choosing random IP addresses to infect,¹²² or target neighbouring devices on the same local network as the victim. Once on the target's system, those algorithms can also choose other targets from email address books, DNS server, among other ways.¹²³ This relative independence of malware from

¹²¹ Stephen Cobb and Andrew Lee, 'Malware Is Called Malicious for a Reason: The Risks of Weaponizing Code' (6th International Conference on Cyber Conflict, NATO CCD COE Publications, 2014), pp.71–84.

¹²² IP stands for internet protocol. An IP address is a unique address that identifies a device on the internet or a local network.

¹²³ Kanellis Panagiotis, *Digital Crime and Forensic Science in Cyberspace* (Idea Group Inc (IGI), 2006).

their human initiator is one reason why some scholars criticise the use of cyber attacks by states as a purportedly more ethical choice than military attacks. They argue that unintended and uncontrollable potential implications of cyber attacks on civilian targets make the argument about their ethical use obsolete.¹²⁴ For the same reasons, some argue that collateral damages in cyber attacks are even much higher than military attacks.¹²⁵

There are numerous examples that demonstrate the inaccuracy of cyber targeting, leading to unintended consequences. As mentioned earlier, the NotPetya ransomware of 2017 is thought to have been targeted at companies in Ukraine. However, the target verification mechanisms of the ransomware did not work properly, and it ended up infecting a large number of targets far away from Ukraine and in several parts of Western Europe. Another example is an attack that exploited a vulnerability in a software called CCleaner. Due to an error in coding, the attack ended up infecting targets in Slovakia instead of its initial target: South Korea. But perhaps the most notable example in this regard is Stuxnet worm that, as widely believed now, was designed by the US and the Israeli governments to target the Iranian nuclear centrifuges in 2010. The worm was imbedded on the targeted system initially using a USB stick, before it started propagating. Stuxnet spread to multiple other unintended targets outside Iran, including Germany, China, and even the USA itself. This happened despite the high level of sophistication of this worm, which many believe was designed over many years. It is thought to have included some methods of limitation that developers used to curb its wide proliferation. But these anti-propagation measures and complex design did not stop it from producing unintended consequences. Though it had a

¹²⁴ Neil C. Rowe, 'Ethics and Policies for Cyber Operations', in Ludovica Glorioso and Mariarosaria Taddeo (eds) *Challenges of Civilian Distinction in Cyberwarfare* (Springer, Cham, 2017), pp.40–41.

¹²⁵ Corey Hirsch, 'Collateral Damage Outcomes Are Prominent in Cyber Warfare, Despite Targeting', in Louise Leenen (ed) *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (ACPIL, 2018), pp.281–86.

specific target, it transmitted to more than 100,000 computers in various locations in its original propagation.¹²⁶ The spokesman of Chevron, an American multinational energy corporation that was hit by Stuxnet, reportedly said upon discovering the malware in the company's systems: "I don't think the U.S. government even realized how far it had spread...I think the downside of what they did is going to be far worse than what they actually accomplished".¹²⁷

Hence, it could be argued that although the humans behind cyber incidents can choose which software/hardware vulnerability to exploit, and in turn which private actor would need to issue patches to stop an attack, a lot is left for the agency of malware, and thus, many elements of the cybersecurity environment become *emergent*. As argued by Dwyer, cyber attacks should not be studied as linear relationships between hacker intents and resultant impacts through malware as tools.¹²⁸ Even with the existence of targeting mechanisms, the malware per se co-determines which systems gets infected at the end-users' side during its propagation. By propagating across machines, malware create a network of cybersecurity actors who are then required to take steps to stop the attack, such as updating their systems to apply the necessary patches. In doing so, malware contribute to emergent, contextual actancy in every single incident.

For instance, in 2017, the WannaCry ransomware exploited a vulnerability in Microsoft operating system that allowed for remote execution of a code that encrypts files in the infected systems. The choice of the infected targets depended entirely on the agency of

¹²⁶ Hirsch, 'Collateral Damage Outcomes Are Prominent in Cyber Warfare', p.283.

¹²⁷ Rachael King, 'Stuxnet Infected Chevron's IT Network', *The Wall Street Journal* (blog), 8 November 2012, available at {<https://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrans-it-network/>} accessed 5 November, 2021.

¹²⁸ Dwyer, 'Cybersecurity's Grammars', p.2.

the malware during self-propagation, by scanning unpatched systems and deploying itself. It reportedly infected more than 230,000 systems in 150 countries, among which was the National Health Service (NHS) in the UK.¹²⁹ By infecting its systems, the malware put the NHS under the spotlight as a major cybersecurity actor. Much of the blame was directed towards the entity for not updating its systems to apply the patch issued by Microsoft before the attack.¹³⁰ This has also raised scholarly and policy interest in the importance of cybersecurity for healthcare. Here, the malware not only co-produced actancy, but was also agential in prioritising the health sector as a referent object at the centre of cybersecurity policies.

This does not only apply to big entities, but also to individual users who become influential actors when a particular attack takes place and infects their machines, as well as to other objects. An important example here is the Mirai malware which was designed to target IoT devices and make them part of a botnet (a network of other compromised devices) to launch a distributed denial of service (DDoS) attack in 2016.¹³¹ Millions of users were not able to connect to various websites as a result of this attack. The Mirari botnet, as argued by Liebetrau and Christensen, constituted a 'dance of agency', in which malware constantly moved in ways that were not entirely predictable, transforming mundane IoT entities in 164 countries into bots with damaging effects.¹³²

These agential capacities of syntactic information, thus, undermine the idea of an in-control human securitizing actor who manages cybersecurity environments. It is a

¹²⁹ Charles Cooper, 'WannaCry: Lessons Learned 1 Year Later', *Symantec*, 16 May 2018, available at {<https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later>} accessed 3 November, 2021.

¹³⁰ 'NHS Trusts "at Fault" Over Cyber-Attack', *BBC*, 27 October 2017, available at {<https://www.bbc.com/news/technology-41753022>} accessed 23 November, 2021.

¹³¹ DDoS attacks flood computer servers with requests to stop them from providing services to their intended users.

¹³² Liebetrau and Christensen, 'The Ontological Politics of Cyber Security'.

demonstration of the power of codes/software in co-producing actancy and agency in cybersecurity, which in turn becomes *emergent security*. Furthermore, such agency creates a liability and responsibility dilemma in cybersecurity that resembles the prominent risk theorist Ulrich Beck's argument on the second modernity and its 'highly differentiated division of labour' that results in a 'general complicity' and lack of responsibility in the production of risk. As Beck said, "Everyone is cause and effect, and thus non-cause".¹³³ But this dilemma in cybersecurity is not specifically just a result of modernity. Rather, as argued in this article thus far, it is primarily co-produced by the agency of codes/software.

One implication of conceptualising cybersecurity as *emergent security* is problematising 'active cyber defence' or 'defend forward' cybersecurity strategies by governments. These operations may include non-disruptive practices like hacking adversaries' or allies' information systems and maintaining a presence in such systems for intelligence gathering, or disruptive operations like 'hacking back' to recover stolen data, for instance.¹³⁴ Acknowledging the agency of codes/software and the elements of unpredictability and uncertainty in their operation challenges the idea of human control implicit in such understandings of 'cyber defence'. As shown above, a malware used in targeting a certain system can spread to untargeted ones, even within the geographical location of the initiator, and therefore result in several unintended consequences. That is to say, although some states may conduct cyber intrusions with defensive motives in the background, acknowledging the agency of codes/software illuminates the risks of condoning such operations by labelling them 'defensive'.

¹³³ Ulrich Beck, *Risk Society: Towards a New Modernity* (London: SAGE Publications Ltd, 1992), p.33.

¹³⁴ Jason Healey, 'The Implications of Persistent (and Permanent) Engagement in Cyberspace', *Journal of Cybersecurity* 5:1 (2019); James Pattison, 'From Defence to Offence: The Ethics of Private Cybersecurity', *European Journal of International Security*, 5:2 (2020), pp.233–54.

Enmity and the attribution dilemma

Establishing an enemy in cybersecurity is a complicated process that does not just reflect the agency of humans, but also that of codes/software. Elements of novelty, non-linearity, contextuality, and decentralisation are manifested in constructing enmity in multiple ways. Firstly, the agency of malware conditions the centrality of human intents in constructing cyber threats. This is because hostile intents and aggressors' capabilities are not the only deciding factors for the occurrence and success of a cyber attack. For a cyber attack to take place, a vulnerability has to be identified in the targeted system first; and security vulnerabilities are essentially contextual: they vary across different systems. Besides, the implications of cyber incidents are mainly linked to the level of the target's dependency on information systems. The less cyber dependent the target is, the less effective an attack against it would be, making the impact of such an attack relational too. That is why, it is argued that in cybersecurity, "offensive capacity correlates with defensive vulnerability".¹³⁵ Put differently, human intentionality is not enough to launch a cyber attack.

Secondly, cybersecurity is characterised by a high level of asymmetries between actors and their capabilities that often render any attribution-specific defence strategy insufficient. As argued by one study, "Whereas defenders in the physical domain can reasonably assume that pretty criminals do not have nuclear weapons and that foreign military powers will not rob the local McDonald's, this same categorical logic does not hold true in cyberspace".¹³⁶ That is, attack sophistication is not necessarily an evidence for state-

¹³⁵ S. Schutte, 'Cooperation Beats Deterrence in Cyberwar', *Peace Economics, Peace Science and Public Policy* 18:3 (2012), p.8.

¹³⁶ Jason Rivera and Forrest Hare, 'The Deployment of Attribution Agnostic Cyberdefense Constructs and Internally Based Cyberthreat Countermeasures', in *2014 6th International Conference on Cyber Conflict (CyCon 2014)*, 2014, p.104.

sponsorship. Added to that, determining the cyber capabilities of a certain actor is often more a matter of speculation than knowledge. Unlike military arms, the non-physicality of cyber offensive tools makes them almost unobservable, unquantifiable, and in most cases, unrecognisable before an attack actually takes place.¹³⁷ This, in turn, puts more emphasis on codes/software than human aggressors in immediate cyber defence. It is coding vulnerabilities and exploits used to target them that lie at the core of such defence, even when enmity is more discursively prevalent.¹³⁸

Thirdly, the agential capacities of codes/software challenge attack attribution even further, making it primarily a process driven by profound uncertainties. For instance, malware may take control of a user's computer without their knowledge, creating a network of devices that work together to orchestrate an attack in a way that crosses geographical boundaries. The malware moves between devices across borders, scanning for the targeted vulnerability without consulting the attacker on the devices it affects. This makes it difficult to know if a certain device is acting as a bot or not and to determine who is controlling it, particularly given the irrelevance of geographical proximity as an element of attribution.¹³⁹ This also means that any system can be hijacked by a third party to implant attacks.

Accordingly, attribution is not necessarily part of an immediate response to counter cyber attacks. Although publicly-published reports on attack attribution by the private sector exceed those of governments,¹⁴⁰ it is governments and some think tanks that focus more on

¹³⁷ Schutte, 'Cooperation Beats Deterrence in Cyberwar', p.8.

¹³⁸ This argument particularly refers to passive defence, or defence that happens *after* an incident takes place, in contrast to active defence or what is often called 'defend forward', which takes pre-emptive actions by intruding in the adversaries' systems.

¹³⁹ P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014).

¹⁴⁰ Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* 38, pp.1–2 (2015), p.28.

threat attribution.¹⁴¹ More specifically, intelligence communities are generally more concerned with attributing cyber threats to a particular enemy than private operators and defenders of information systems. This can be seen, for example, in the US government's emphasis on nation-states as a threat source, namely Russia, China, Iran, and North Korea.¹⁴² However, on the practice-level and in immediate responses against a hostile cyber operation, the logic of enmity is not so central. The emergent properties of codes/software condition enmity, particularly in everyday cybersecurity that does not necessarily get publicised.¹⁴³ Thus, the enemy is not just a human attacker or a particular actor; *the enemy also becomes the vulnerability and the malware: codes/software*. This can be seen in the technologies and threat mitigation policies developed for cyber defence which are primarily focused on the tools that adversaries use in hostile cyber operations, rather than determining who this adversary actually is. As argued by a representative of a network security company: "intelligence and law enforcement entities often prioritize attack attribution, while almost no emphasis is placed on attribution by those defending systems".¹⁴⁴

Acknowledging that the immediate adversary in cybersecurity is the vulnerability and the malware, i.e., codes/software as informational agents, calls for prioritising the production of secure-by-design codes over instrumentalising such codes in hacking into other countries'

¹⁴¹ We can differentiate between two types of attribution: *attack* attribution and *threat* attribution. The first is concerned with attacks that have already taken place, while the second is related to ones that have *not* and thus seeks to establish links between the future threat/hazard and a particular source.

¹⁴² Noran Shafik Fouad, 'The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016)', in *Proceedings of the 18th European Conference on Cyber Warfare and Security*, (Academic Conferences and Publishing International Limited, 2019), pp.633-640.

¹⁴³ For examples of every-day and 'mundane' cybersecurity, see: Julia Slupska, 'Safe at Home: Towards a Feminist Critique of Cybersecurity', *St Antony's International Review*, 15:1 (2019), pp. 83–100; Noran Shafik Fouad, 'Securing Higher Education Against Cyber Threats: From an Institutional Risk to a National Policy Challenge', *Journal of Cyber Policy*, 6:2 (2021), pp.137-154.

¹⁴⁴ *Reviewing the Federal Cybersecurity Mission: Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, of the Committee on Homeland Security* (Serial No.111-5), U.S. House of Representatives, 111th Cong. (2009), p.27.

systems as part of defensive strategies. In addition to the above-mentioned active cyber defence strategies, states are increasingly involved in black markets of vulnerabilities and zero-day exploits to build their cyber arsenals. Such practices increase the market price of those vulnerabilities and exploits which may end up in the wrong hands and undermine the long-term security of individual users and their overall trust in technology.¹⁴⁵ On the other hand, software manufacturers rush production processes to get their products into the market fast enough to compete for profits with an intention to ‘fix vulnerabilities later’. They also tend to prioritise functionality over security in software production, leading to a general culture of acceptance of software insecurity.¹⁴⁶ Although perfect cybersecurity does not exist and there will always be *another* bug in every software, shifting the conceptualisation of the adversary in cybersecurity from the human to vulnerabilities and malware (i.e., codes/software) challenges such practices by state and private actors and emphasises the dangers of weaponizing codes in cyber operations that implicitly assume a high level of human controllability.

Conclusion

The article analysed the agential capacities of codes/software as a form of syntactic information, and the implications such agency have on cybersecurity construction. Instead of instrumentalising information technologies or analysing them as a mere capability that influences power relations among actors in international politics, the article focused on the agency of information in and of itself. It interrogated the ontology of codes/software as

¹⁴⁵ Michel Herzog and Jonas Schmid, ‘Who Pays for Zero-Days? Balancing Long-Term Stability in Cyber Space Against Short-Term National Security Benefits’, in Karsten Friis and Jens Ringsmose (eds) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (New York: Routledge, 2016), pp. 97–114.

¹⁴⁶ Jane Chong, ‘Bad Code: Exploring Liability in Software Development’, in *Cyber Insecurity: Navigating the Perils of the Next Information Age*, ed. Richard Harrison, Trey Herr, and Richard J. Danzig (Lanham: Rowman & Littlefield Publishers, 2016), pp.69–86.

informational agents, their intrinsic agential properties, and how they influence the agency of other human and non-human agents in cybersecurity. Such agency, the article argued, cannot be sufficiently studied by focusing on human discourses and linguistic utterances alone, as is the case in many theoretical cybersecurity literatures.

To capture the agency of codes/software as informational agents capable of co-constructing the logics and politics of cybersecurity, the article put more emphasis on codes/software per se, albeit without suggesting that their agency supersedes or replaces that of humans. It explored how codes/software's self-organising, dynamic, and complex nature, as well as their emergent behaviour, often leads to complex, dynamic, and emergent *security*. Conceptualising cybersecurity as *emergent security* illuminates the limitations of human control and intentionality in managing cybersecurity environments, and the ways in which codes/software challenge traditional assumptions of enmity and co-produce the subjects/objects of cybersecurity. As such, a shift towards the logic of emergence is an attempt to distance cybersecurity from the anthropocentric confines of traditional theories of security and to present a non-binary framework in which the agency of human and non-human actors can be studied.

Through this non-human reading, the article contributes to the study of the materialities of cybersecurity beyond contexts and non-state actors, using an interdisciplinary approach that builds upon the philosophy of information and software studies - fields that have direct links to the evolution of the technologies that cybersecurity aims to protect. This is done to challenge perceptions of human control in constructing the security of information systems that evolved in paths humans could not fully envision; that operate in ways they cannot fully predict; and that produce threats they are not able to completely manage.

Further, by emphasising codes/software as *peculiar* non-human entities that differ from the *matter* that new materialism theorised for, the article demonstrated the need for investigating the specificity of the different types of ‘things’ and the different agential capacities they possess, instead of dealing with them as one homogenous category.

Acknowledgements

This article is indebted to conversations with and guidance from Stefan Elbe and Stefanie Ortmann and their generous feedback on my PhD thesis, which this article is part of. I extend my thanks to Tim Stevens and his feedback on some of the arguments made in this article as initially written in my thesis. I am also grateful to the three anonymous reviewers and the editors of RIS for their very helpful and constructive comments.

Funding

This article is based on PhD research funded by the University of Sussex’s Chancellor’s International Research Scholarship.