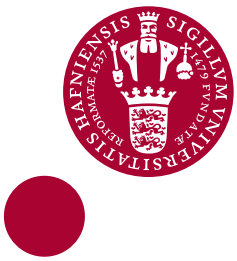

The Ontological Politics of Cyber Security

Emerging Agencies, Actors, Sites and Spaces

Liebetrau, Tobias; Christensen, Kristoffer Kjærgaard

Published in:
European Journal of International Security

DOI:
10.1017/eis.2020.10

Publication date:
2020

European Journal of International Security (2020), page 1 of 19
doi:10.1017/eis.2020.10

EJIS

RESEARCH ARTICLE

The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces

Tobias Liebetrau[1]* and Kristoffer Kjærgaard Christensen[2]

[1]Centre for Military Studies, Department of Political Science, University of Copenhagen, Denmark and [2]Department of Political Science, University of Copenhagen, Denmark
*Corresponding author. Email: tl@ifs.ku.dk

(Received 7 October 2019; revised 27 July 2020; accepted 28 July 2020)

Abstract

In this article, we show how Annemarie Mol's notion of ontological politics helps to open up the research agenda for cyber security in Critical Security Studies. The article hence seeks to further the debate about STS and Critical Security Studies. The article's main claim is that the concept of ontological politics enables an engagement with the complex and transformative dynamics of ICT and the new security actors and practices that shape security politics in the digital age. By examining the virulent attacks executed by the Mirai botnet – one of the world's largest, fiercest, and most enduring botnets – we point to four aspects of cyber security that attention to the ontological politics of cyber security attunes us to: the proliferation and entanglement of security agencies, actors, sites, and spaces. These aspects of cyber security, we argue, are becoming increasingly prominent alongside the development of the Internet of Things (IoT) and 5G network technology. In conclusion, we discuss the wider security theoretical and normative-democratic implications of an engagement with the ontological politics of security by exploring three avenues for additional conversation between ontological politics and Critical Security Studies.

Keywords: Cyber Security; Critical Security Studies; Ontological Politics; Science and Technology Studies; Information and Communication Technology (ICT) and Internet of Things (IoT)

Introduction

Today, news of cyber attacks and various security risks related to information and communication technologies (ICT) are part of the media staple diet.[1] Within Critical Security Studies, attention has lately turned towards how cyber security mould spatial[2], temporal,[3] and functional[4] aspects of security. This article draws on Annemarie Mol's notion of ontological politics[5] to

[1]Undeniably, cyber threats and risks are presented as some of the most pressing security issues confronting contemporary societies. In 2018 the cyber threat was once again ranked among the biggest threats in the World Wide Threat Assessment of the US Intelligence Community (Daniel R. Coats, 'Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community' (Washington, DC: Office of the Director of National Intelligence, 23 May 2017); Along the same lines, President of the European Commission Jean-Claude Juncker stated in his 2017 State of the Union Address that 'Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks.' Jean-Claude Juncker, 'President Jean-Claude Juncker's State of the Union Address 2017', European Commission (13 September 2017).

[2]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.

[3]Tim Stevens, *Cyber Security and the Politics of Time* (Cambridge: Cambridge University Press, 2016).

[4]Madeline Carr, 'Public-private partnerships in national cyber-security strategies', *International Affairs*, 92:1 (2016), pp. 43–62; Kristoffer Kjærgaard Christensen and Tobias Liebetrau, 'A new role for "the public"? Exploring cyber security controversies in the case of WannaCry', *Intelligence and National Security*, 34:3 (2019), pp. 395–408.

[5]Annemarie Mol, 'Ontological politics: A word and some questions', *The Sociological Review*, 47:S1 (1 May 1999), pp. 74–89.

develop an analytical sensitivity that can help us to examine and question these many faces of cyber security and their transformative political effects. We emphasise how studies on cyber security need to take into account the proliferation and entanglement of human and non-human agency and the multiplication of political actors, sites, and spaces of security outside those of traditional state actors and institutions. Attention to the enactment of new security agencies, actors, sites, and spaces are paramount, since the proliferation of ICT fosters diffusion and decentring of security practices.[6] Studying the politics of technologised security 'suggests a powerful need for new conceptual and analytical resources'[7] as well as cyber security research aimed 'at the intersection between the technical and social'.[8] Consequently, we argue, a reliance on state-centrism, human agency, and discourse is not entirely satisfactory for the study of security that have automatic and robotic characteristics, as the subsequent study of the Mirai botnet will show.[9]

The article hence advances Critical Security Studies scholarship on cyber security by arguing that a starting point for engaging with the enactment of cyber security is its ontologically instable socio-material entanglements as well as the opening of security politics that stems from this analytical move. Ontological politics enables us to explore how diverse actors shape contemporary technological security across different sites and spaces. In addition, it enables an empirically driven engagement with how the transformative dynamics of ICT co-constitute cyber security politics by propelling into the limelight the agential qualities of ICT. Rather than politics being eclipsed or erased by the technologisation of security,[10] ontological politics helps us to examine how dynamic socio-material entanglements condition different understandings of what cyber security is and the kind of politics needed to accommodate it. By scrutinising the agencies, actors, sites, and spaces that emerged with the Mirai botnet, it becomes possible to understand how these 'security arrangements'[11] transform cyber security politics by conditioning different kinds of political interferences, controversies, and imaginations.[12] The ontological political sensitivity thereby supports a continuous questioning that can help to spur engagement with otherwise often elusive technological developments and practices of (in)security.

[6]For engagement with the technologisation of security see, for example, Antoine Amicelle, Claudia Aradau, and Jean Jeandesboz, 'Questioning security devices: Performativity, resistance, politics', *Security Dialogue*, 46:4 (2015), pp. 293–306; Ayse Ceyhan, 'Technologization of security: Management of uncertainty and risk in the age of bio metrics', *Surveillance & Society*, 5:2 (2002), pp. 1–22; Lousie Amoore, *The Politics of Possibility: Risk and Security beyond Probability* (Durham, NC and London: Duke University Press, 2013); Claudia Aradau and Tobias Blanke, 'Governing others: Anomaly and the algorithmic subject of security', *European Journal of International Security*, 3:1 (2018), pp. 1–21; Didier Bigo, 'The (in)securitization practices of the three universes of EU border control: Military/navy–border guards/police–database analysts', *Security Dialogue*, 45:3 (2014), pp. 209–25; Jef Huysmans, *Security Unbound: Enacting Democratic Limits* (London and New York: Routledge, Taylor & Francis Group 2014); and Linda Monsees, 'Public relations: Theorizing the contestation of security technology', *Security Dialogue* (2019), pp. 1–16.

[7]Zygmunt Bauman et al., 'After Snowden: Rethinking the impact of surveillance', *International Political Sociology*, 8:2 (2014), p. 124; M. De Goede, 'Afterword: Transversal politics', in X. Guillaume and P. Bilgin (eds), *Handbook of International Political Sociology* (London and New York: Routledge, 2017), pp. 353–65.

[8]Myriam Dunn Cavelty, 'Cybersecurity research meets science and technology studies', *Politics and Governance*, 6:2 (2018), p. 28.

[9]A botnet consists of one or more networks of infected computers/devices. Botnets are often controlled remotely by someone, usually referred to as a 'botherder', to perform specific functions, such as destributed denial-of-service attacks (DDoS attacks), often without the knowledge of the owners of the infected computers/devices.

[10]An argument often associated with security practices that are said to empower bureaucracies and everyday professionals and/or invoke a technocratic security logic. See Amicelle, Aradau, and Jeandesboz, 'Questioning security devices'; Bigo, 'The (in)securitization practices of the three universes of EU border control'; Huysmans, *Security Unbound*; Linda Monsees, *Crypto-politics: Encryption and Democratic Practices in the Digital Era* (London and New York, Routledge, 2020).

[11]Peer Schouten, 'Security as controversy: Reassembling security at Amsterdam airport', *Security Dialogue*, 45:1 (2014), p. 27.

[12]For related observations in Critical Security Studies, see ibid., pp. 23–42; Delf Rothe, 'Seeing like a satellite: Remote sensing and the ontological politics of environmental security', *Security Dialogue*, 48:4 (2017), pp. 334–53 and Stefan Elbe and Gemma Buckland-Merret, 'Entangled security: Science, co-production, and intra-active insecurity', *European Journal of International Security*, 4:2 (2019), pp. 123–41.

Tangential observations have been made in recent advances of the critical cyber security studies literature.[13] Scholars have introduced the vocabulary of Actor-Network-Theory,[14] STS,[15] and assemblage theory[16] to analyse the socio-material creation of cyber security. Thierry Balzacq and Myriam Dunn Cavelty[17] are among the most prominent of these thinkers. They examine the links between cyber-security incidents and politics, via concepts and methodologies borrowed from ANT, and demonstrate how malware (malicious software) and cyber-security incidents unfold in and actively contribute to the enactment of 'three kinds of space (regions, networks and fluids), each activating different types of political interventions'.[18] We expand on their suggested way of researching cyber security by showing how an ontological political approach enables us to study and question how multiple agencies, actors, sites, and space become entangled in 'securitizing process that creates insecurities mainly through dispersing, through continuously associating, reassociating, tweaking and experimenting with materials, procedures, regulations'.[19] The introduction of an ontological political sensitivity should hence be understood as a particular methodological and analytical move that aims at bringing out the political significance of otherwise often scattered and insignificant practices, devices and relations,[20] as the emergence of insecurities is not taken to happen as an individualised and discursive act, but in collective, performative, and relational processes.[21] We thus take ontological politics to be a sensitising term[22] – rather than a consistent and coherent theory – which enables us to approach the relation between the security political and the ontological as one of questioning and thus remaining true to the idea of events and situations as always emerging and constituting in multiple ways.[23] In doing so, we respond to the recent calls for closer engagement between STS and cyber security studies moving forward.[24]

To demonstrate the merits of an engagement with the ontological politics of cyber security, we first discuss the limitations of the current literature on cyber security in Critical Security Studies. Second, we introduce Mol's notion of ontological politics as a way of paying greater attention to the enactment of cyber security in ontologically instable socio-material entanglements as well as the opening of security politics conditioned by this move. Third, by investigating the case of the Mirai botnet[25] we zoom in on how the ontological politics of cyber security sensitises us to the

[13]Already around the turn of the millennium, Ronald Deibert, a central figure in the critical academic study of the intersection between ICT and international relations (including cyber security), forcefully argued for the need to include the role that ICT and its material properties play in shaping these issues when theorising cyber security. However, as Deibert himself moved on to pursue more empirical and problem-oriented work as the Director of the Citizen Lab at the University of Toronto, largely abstaining from theorisation of socio-technical dynamics, eclipsed this line of thinking in the critical literature for a while.

[14]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'.

[15]Cavelty, 'Cybersecurity research meets science and technology studies'; Christensen and Liebetrau, 'A new role for "the public"'.

[16]Jamie Collier, 'Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision', *Politics and Governance*, 6:2 (2018); Stephanie Simon and Marieke de Goede, 'Cybersecurity, bureaucratic vitalism and European emergency', *Theory, Culture and Society*, 32:2 (2015), pp. 79–106.

[17]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'.

[18]Ibid., p. 178; See also the special issue of *Politics and Governance*, 6:2 (2018) on 'Global cybersecurity: new direction in theory and methods'.

[19]Jef Huysmans, 'What's in an act? On security speech acts and little security nothings', *Security Dialogue*, 42:4–5 (2011), p. 377.

[20]Jef Huysmans, 'Democratic curiosity in times of surveillance', *European Journal of International Security*, 1:1 (2016), p. 92.

[21]Schouten, 'Security as controversy', p. 27.

[22]Andrew Barry, 'The translation zone: Between actor-network theory and international relations', *Millennium: Journal of International Studies*, 41:3 (2013), p. 418; Annemarie Mol, 'Actor-network theory: Sensitive terms and enduring tensions', *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, 50:1 (2010), pp. 253–69.

[23]Mikko Joronen and Jouni Häkli, 'Politicizing ontology', *Progress in Human Geography*, 41:5 (2017), pp. 561–79.

[24]Cavelty, 'Cybersecurity research meets science and technology studies', p. 28.

[25]Commonly known as one of the largest and most disruptive distributed denial of service (DDoS) attacks hitherto.

proliferation and entanglement of security agency and the multiplication of actors, sites, and spaces of cyber security. Fourth, and finally, we discuss the wider theoretical and normative-democratic implications of an engagement with the ontological politics of security by laying out three avenues for future conversation between ontological politics and Critical Security Studies.

Extending cyber security beyond national security discourse

Despite its prominence in policy and media discourse, the Critical Security Studies literature on cyber security is still nascent.[26] With a few noticeable exceptions touched upon above, Critical Security Studies scholars have predominantly approached cyber security through the prism of securitisation theory.[27] They have turned away from a focus on how best to manage cyber threats and risks[28] to examine instead the discursive framing of cyber security and the use of metaphors and analogies in such discourses.[29] Thereby they have importantly contributed to a critical engagement with the link between cyber security and national security, as well as the political effects of the particular threat representations.

However, as we show in this section, the focus on securitisation has two important consequences: first, it largely confines cyber security to national security and, second, it subsumes the political role of technology to security discourse. In other words, the critical literature predominantly frames cyber security in terms of continuation of the existing securitisation literature rather than as something that may profoundly challenge and transform our understanding of security politics. While it is generally a good idea to refrain from readily accepting the hype of radical transformation,[30] a narrow confinement of the critical study of cyber security to securitisation theory blinds us to the many cyber security practices that challenge and evade this form of security. First, notwithstanding that it extends cyber security beyond the military domain, the critical literature tends to place cyber security within the realm of national security and give primacy to national security actors. Its basis in securitisation theory brings to the fore the

[26]Tim Stevens, 'Global cybersecurity: New directions in theory and methods', *Politics and Governance*, 6:2 (2018), pp. 1–4.

[27]Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello, 'From "cyberterrorism" to "cyberwar", back and forth: How the United States securitized cyberspace', in Johan Eriksson and Giampiero Giacomello (eds), *International Relations and Security in the Digital Age* (London: Routledge, 2007), pp. 57–82; 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 (2007), pp. 19–36; Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008); Johan Eriksson, 'Cyberplagues, IT, and security: Threat politics in the information age', *Journal of Contingencies and Crisis Management*, 9:4 (2001), pp. 200–10; Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, 53:4 (2009), pp. 1155–75; 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.

[28]The conventional scholarly literature on cyber security tends to be either policy-oriented and problem-solving or centred around conventional debates of power, warfare, and strategic thinking. For examples of the latter, which have emerged out of strategic studies, see, for example, David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: IISS, The International Institute for Strategic Studies, 2011); James P. Farwell and Rafal Rohozinski, 'Stuxnet and the future of cyber war', *Survival*, 53:1 (2011), pp. 23–40; James P. Farwell and Rafal Rohozinski, 'The new reality of cyber war', *Survival*, 54:4 (2012), pp. 107–20; Martin C. Libicki, *Conquest in Cyberspace, National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007); Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: Rand Corporation, 2009); Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015).

[29]David J. Betz and Tim Stevens, 'Analogical reasoning and cyber security', *Security Dialogue*, 44:2 (2013), pp. 147–64; 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; Sean Lawson, 'Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States', *First Monday*, 17:7 (2012).

[30]Laurent Bonelli and Francesco Ragazzi, 'Low-tech security: Files, notes, and memos as technologies of anticipation', *Security Dialogue*, 45:5 (2014), pp. 476–93.

discursive framing of cyber threats and risks as national security issues, which through reference to urgency and survival are placed beyond normal politics and require extraordinary measures. Moreover, it predominantly focuses on statements and practices of government elites.[31] Most of the literature hence examines the securitising moves by changing US administrations; whereas some also include the only partially successful securitisation by the Estonian government of the alleged Russian attack in 2007[32] and even the securitisation of IT by the Swedish 'military-bureaucratic establishment'.[33]

Cavelty challenges the focus on national security elites and calls for 'a broad understanding of cyber-security as discursive practice by a multitude of actors inside and outside of government'.[34] She points to heterogeneous political manifestations of various actors linked to different threat representations. In the end she, nevertheless, returns to the realm of national security and argues that her engagement with such threat representations 'allows for a more nuanced understanding of how cyber-security is presented as a *national security* issue'.[35] Likewise, Lene Hansen and Helen Nissenbaum emphasise the significance of everyday security practices in their grammar of cyber security to highlight how securitising actors may mobilise the experiences of regular people, 'connecting everyday security practices with hyper cascading scenarios'.[36] Yet, the argument is still that this is central to 'move cyber security out of the realm of "corporate security" or "consumer trust" and into the modality of *"proper" national/societal security*'.[37] In sum, cyber security is primarily embedded within state and national security representations. This entails a focus on exceptional security politics as well as the involvement of state agencies and bureaucracies in the production of security.

Second, in the securitisation literature on cyber security the role of ICT and its material properties is largely subsumed to discourse. To be sure, acknowledgments of the importance of both technology and its materiality in shaping the politics of cyber security can be found in the literature. For example, Cavelty stresses that cyber security is 'a type of security that unfolds in and through cyberspace; the making and practice of cyber-security is both constrained and enabled by this environment'.[38] In a similar vein, Ralf Bendrath, Johan Eriksson, and Giampiero Giacomello argue that 'cyberspace is a landscape where every action is only possible because the technical systems provide an artificial environment that is built to allow it. The means of an attack therefore change from system to system, from network to network.'[39] Still this literature predominantly focuses on the discursive constitution or framing of cyber security as an issue of national security. The political status of technology and its materiality is left rather unclear, as primacy is given to the linguistic dimension of cyber security.

This ambiguity in relation to technology and its materiality is also present in Hansen and Nissenbaum's argument that cyber security involves not just the speech act of securitisation, but also that of 'technification':

[31]This critique is indeed also raised against securitisation theory as such. It relates to the critique regarding staticity/fixation that has been raised against the Copenhagen School framework as such. See, for example, Huysmans, 'What's in an act?' and Ulrik Pram Gad and Karen Lund Petersen, 'Concepts of politics in securitization studies', *Security Dialogue*, 42:4–5 (2011), p. 319. In a recent contribution, Lise Philipsen nicely sums up this critique of the theory: 'a specific logic must be used and this must be done from a position of historically contingent authority. The theory is, so to speak, fixed both from the inside (the logic) and the outside (the context)'. See Lise Philipsen, 'Performative securitization: From conditions of success to conditions of possibility', *Journal of International Relations and Development* (2018), pp. 1–25.

[32]Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School'.

[33]Eriksson, 'Cyberplagues, IT, and security'.

[34]Cavelty, 'From cyber-bombs to political fallout', p. 106.

[35]Ibid., p. 118.

[36]Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', p. 1166.

[37]Ibid.

[38]Cavelty, 'From cyber-bombs to political fallout', p. 107.

[39]Bendrath, Eriksson, and Giacomello, 'From "cyberterrorism" to "cyberwar", back and forth', p. 61.

> [Technifications] construct an issue as reliant upon technical, expert knowledge, but … also simultaneously presuppose a politically and normatively neutral agenda that technology serves … Cyber security discourse's simultaneous securitization and technification work to prevent it from being politicized in that is precisely through rational technical discourse that securitization may 'hide' its own political roots.[40]

They point to the importance of not just expertise – which plays a central role in most security practices – but of a particular kind of *technical* expertise. Nevertheless, Hansen and Nissenbaum remain at the level of discourse and thereby subsume the role played by ICT and its material properties to its constitution in discursive practices.[41] By giving the social (discourse) primacy to the technological, they hence, ironically, contribute to downplaying the political role of ICT.

If we make do with the prism of securitisation theory alone, we critically limit what cyber security can be. Indeed, as Balzacq and Cavelty have similarly argued, 'cyber-security is both less and more'[42] than the securitising moves of national security elites. Owing to the dispersed and dynamic nature of digital technologies, much of the politics of cyber security play out among actors and in sites and spaces of security politics that evade traditional forms of national security.[43] These 'multi-faceted relationships cannot be captured by static and often state-centric theories'.[44] Therefore, we need to enable analytical and political purchase to critically engage with these other actors, agencies, sites, and spaces of security politics as well. To emphasise the contingent and relational enactment of insecurities and the transformative role of technology, we ought to attune our analysis to what we, following Annemarie Mol, call the ontological politics of cyber security.[45]

This is also a normative, democratic argument. Knowledge production – academic and otherwise – is as much an intervention in the politics of cyber security as the production of knowledge about it.[46] To contest cyber-security actors and practices and hold them to account, we ought to (also) attend to those that defy the exceptional politics of national security actors and perhaps even fall outside the formal political system as such. Our emphasis on the ontological politics of cyber security, to which we will now turn, opens up our engagement with cyber security by sensitising our analyses to the heterogeneous relations through which insecurities are enacted, as well as their political implications. Following these assumptions, cyber security is taken to be a form of ontological politics, in which the ontological status of phenomena such as botnets or malware – as well as ways of knowing and researching them – is the product of dynamic socio-technical relations unfolding over time – be they in contestation, controversy, or concurrence.

Ontological politics: Towards multiple cyber securities

In calling attention to the ontological politics of cyber security, we draw on insights from Science and Technology Studies (STS). In doing so, we also seek to further strengthen the conversation

[40]Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', pp. 1167–8.

[41]This is further underlined, as Hansen and Nissenbaum state that they break with Ronald Deibert's claims regarding the importance of materiality and technology outside of sole discourse. See Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', p. 1162, fn. 6.

[42]Balzacq and Cavelty, 'A theory of actor-network for cyber-security', p. 179.

[43]For an overview of the engagement with the technologisation of security, see fn. 6.

[44]Collier, 'Cyber security assemblages', p. 15.

[45]Mol, 'Ontological politics'; Annemarie Mol, *The Body Multiple: Ontology in Medical Practice* (Durham, NC and London: Duke University Press, 2002).

[46]Claudia Aradau and Jef Huysmans, 'Critical methods in International Relations: The politics of techniques, devices and acts', *European Journal of International Relations*, 20:3 (2014), pp. 596–619; Christopher Gad, Casper Bruun Jensen, and Brit Ross Winthereik, 'Practical ontology: Words in STS and anthropology', *NatureCulture*, 3:10 (2015), pp. 67–86; Donna J. Haraway, *Simians, Cyborgs and Women: The Reinvention of Nature* (London: Free Association, 1991); Sheila Jasanoff, 'Afterword', in Sheila Jasanoff (ed.), *States of Knowledge: The Co-Production of Social Order* (London: Routledge, 2004), pp. 274–82; John Law, *After Method: Mess in Social Science Research* (London and New York: Routledge, 2004).

between the study of cyber security and current debates in other parts of IR and Critical Security Studies that draw on similar insights from STS to include the relational, technological, and material aspects of contemporary security politics.[47] STS has in recent years experienced what has been called an 'ontological turn'. This 'turn' to ontology in STS has been promoted, exactly to describe and understand how science and technology partake in changing the world materially, socially, technologically, politically, and morally.[48] Indeed, it entails an emphasis on alterity and on interfering with assumptions about the stability of reality. It follows that the purpose of doing research this way is not, as Steve Woolgar and Javier Lezaun note,

> to arrive at a better formulation of the reality of the world, or of the ways in which the world is real, but to interfere with the assumption of a singular, ordered world, and to do so by re-specifying hefty meta-physical questions in mundane settings and in relation to apparently stabilized objects.[49]

This is why we, following Marisol de la Cadena and Marianne Elisabeth Lien, find it more accurate to speak of an 'ontological opening' rather than an 'ontological turn', to signal an openness towards matters that are usually taken for granted rather than a radical turn away from something else.[50]

Hence, attention to the ontological politics of cyber security does not necessarily replace or preclude the analytical utility of, for example, securitisation theory – or, as Balzacq and Cavelty suggest, ANT. Rather, ontological politics should serve as a guiding assumption in analytical strategies for a more experimental engagement with cyber security. That is, we should engage with cyber security as if there are multiple 'cyber securities', so to speak. This move does not involve substantive claims about what the theory or politics cyber security is made up of. Rather, in line with the recent debate on the role of methods in Critical Security Studies, getting at the 'stuff' of the ontological politics of cyber security requires an experimental engagement with empirical practices.[51] This critical analytical sensibility to the dynamic, heterogeneous, and transient assembling of cyber security[52] draws attention to the need for situated and contextual analyses.

Mol's notion of ontological politics draws attention to the ontological open-endedness of cyber security. It thereby enables an engagement with cyber security that, rather than a priori definition of its ontology, focuses on how security itself it at stake when it is brought into being in socio-

[47]Within IR and Critical Security Studies, broadly speaking, similar traits and tendencies can be found in the burgeoning interest in importing insights from Science and Technology Studies (STS), and especially actor-network theory (ANT) and assemblage thinking, as part of what some scholars have called the 'material turn' or 'new materialism'. See, for example, Michele Acuto and Simon Curtis (eds), *Reassembling International Theory: Assemblage Thinking and International Relations* (Basingstoke and New York: Palgrave Pivot, 2014); Claudia Aradau, 'Security that matters: Critical infrastructure and objects of protection', *Security Dialogue*, 41:5 (2010), pp. 491–514; Barry, 'The translation zone'; Christian Bueger, 'Territory, authority, expertise: Global governance and the counter-piracy assemblage', *European Journal of International Relations*, 24:3 (2018), pp. 614–37; Mark B. Salter (ed.), *Making Things International, 1: Circuits and Motion* (Minneapolis and London: University of Minnesota Press, 2015); Mark B. Salter (ed.), *Making Things International, 2: Catalysts and Reactions* (Minneapolis and London: University of Minnesota Press, 2016).

[48]Mol, 'Ontological politics'; Mol, *The Body Multiple*; Noortje Marres, 'Why political ontology must be experimentalized: On eco-show homes as devices of participation', *Social Studies of Science*, 43:3 (2013), pp. 417–43; Brit Ross Winthereik, 'Den ontologiske vending i antropologi og Science and Technology Studies', *STS Encounters: Research Papers from DASTS*, 7:2 (2015), pp. 1–32; Steve Woolgar and Javier Lezaun, 'The wrong bin bag: A turn to ontology in Science and Technology Studies?', *Social Studies of Science*, 43:3 (1 June 2013), pp. 321–40.

[49]Woolgar and Lezaun, 'The wrong bin bag', p. 323.

[50]Marisol de la Cadena, 'The politics of modern politics meets ethnographies of excess through ontological openings', *Cultural Anthropology* (2014); Marianne Elisabeth Lien, *Becoming Salmon* (Oakland: University of California Press, 2015).

[51]Claudia Aradau et al. (eds), *Critical Security Methods: New Frameworks for Analysis* (Abingdon and New York: Routledge, 2015); Marres, 'Why political ontology must be experimentalized'.

[52]Cavelty, 'Cybersecurity research meets science and technology studies'; Christensen and Liebetrau, 'A new role for "the public"'.

material entanglements.[53] In linking ontology with politics, Mol suggests that '*ontology* is not given in the order of things, but that, instead, *ontologies* are brought into being, sustained, or allowed to wither away in common day-to-day, sociomaterial practices'.[54] Consequently, ontologies of cyber securities emerge in process of linking together heterogeneous elements. Cyber securities are always in the making and hence precarious and, potentially, unstable.[55] Hence, cyber security ontologies are mattering through their 'continued enactment and re-enactment in situated practices'.[56]

In other words, rather than a 'matter of fact', cyber security is a 'matter of concern'.[57] When cyber security realities are enacted in socio-material arrangements 'it becomes important to explore the politics of the prevailing realities, the differences and patterns of interference that they make, and which realities we want to live with. This is the salience of 'ontological multiplicity'.[58] That is to say that the ontological status of cyber security is open to contestation; in short, it is political.[59] This focus of analysis points towards examinations pertaining to how cyber security arrangements are assembled and become entangled with politics over time. Concretely, our analysis of the Mirai botnet looks into how relations between human and non-human actors are made, remade, and stabilised over time, as well as how they make a difference to the enactment of security and the conditions of politics.[60]

This has two important implications. First, the reality of security politics is relational; 'to be is to be related'.[61] Importantly, Mol extends these relations beyond the social to include technologies and other material artefacts and non-human entities by emphasising the socio-material nature of practices. This fits well with the study of cyber security in that cyber security does not emerge as a strictly human activity but rather compositions of people and technological and material artefacts.[62] Hence, to paraphrase Langdon Winner, artefacts have politics too.[63] Yet the political role of technologies vary. The relationship between human and non-human elements is not a straightforward one but one of complex and dynamic co-constitution. How the affordances of the various technologies shape and co-produce security politics depends on the devices, practices and relations in question.[64] This is why we need to study specific, empirical instances of how the interplay between various human and non-human elements enact diffuse insecurities and threat images to get at the ontological politics of cyber security.

[53]Schouten, 'Security as controversy'.

[54]Mol, *The Body Multiple*, p. 6

[55]Mol, *The Body Multiple*; John Law, 'Actor Network Theory and material semiotics', in Bryan S. Turner (ed.), *The New Blackwell Companion to Social Theory* (Chichester and Malden, MA: Wiley-Blackwell, 2009), pp. 141–58.

[56]Ingunn Moser, 'Making Alzheimer's disease matter: Enacting, interfering and doing politics of nature', *Geoforum*, 39:1 (2008), p. 99.

[57]Bruno Latour, *Reassembling The Social: An Introduction to Actor-Network-Theory* (Oxford: Oxford University Press, 2005).

[58]Moser, 'Making Alzheimer's disease matter', p. 99.

[59]Andrew Barry, 'The anti-political economy', *Economy and Society*, 31:2 (2002), pp. 268–84; Barry, 'The translation zone', p. 7; Rothe, 'Seeing like a satellite', p. 337; Schouten, 'Security as controversy', p. 37.

[60]Amicelle, Aradau, and Jean Jeandesboz, 'Questioning security devices', p. 297.

[61]Mol, *The Body Multiple*, p. 54.

[62]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'; Ron J. Deibert, *Parchment, Printing, and Hypermedia* (New York: Columbia University Press, 1997); Ron J. Deibert, 'Black Code: Censorship, surveillance, and the militarisation of cyberspace', *Millennium: Journal of International Studies*, 32:3 (2003) pp. 501–30; Wytske van der Wagen and Wolter Pieters, 'From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks', *British Journal of Criminology*, 55:3 (2015), pp. 578–95.

[63]Langdon Winner, 'Do artifacts have politics?', *Daedalus*, 109:1 (1980), pp. 121–36.

[64]Andrew Barry, *Political Machines: Governing a Technological Society* (London and New York: The Athlone Press, 2001); Sheila Jasanoff (ed.), *States of Knowledge: The Co-Production of Social Order* (London: Routledge, 2004); Mareile Kaufmann and Julien Jeandesboz, 'Politics and "the digital": From singularity to specificity', *European Journal of Social Theory* (2016), pp. 1–20.

Second, an emphasis on ontological politics is also an emphasis on the multiplicity of cyber security. When relations are situated in specific, local practices and new relations are continuously forged, it follows that the ontologies of cyber security potentially multiply. Cyber security is hence, ontologically speaking, 'more than one – but less than many'.[65] However, this is not to say that the different realities of cyber security are mutually exclusive; again, we may, for example, very well encounter *both* cyber-security practices that defy traditional national security and exceptional politics *and* practices that take the form of securitisation. Nor is it, however, to say that such realities co-exist side by side as discrete and coherent entities. In fact, we need to accept 'the possibility that heterogeneous elements can hold together *without* actually forming a coherent whole'.[66] Consequently, the different realities may both overlap and interfere with one another in various complex ways. This opens up the space for studying security political controversies.[67] In other words, the ontological politics of cyber security does not imply a competition of different perspectives on cyber security but competing *realities* of cyber security.[68]

In sum, attention to the ontological politics of cyber security points us to the relational, socio-material, and heterogeneous nature of competing realities of cyber security, including the power to perform these realties in given ways and to certain consequences. However, to say that cyber security is multiple is only a first step. It does not, in and of itself, tell us something about the content of the ontological politics of cyber security. Rather, the purpose of turning to the ontological politics is, as argued above, to enable an 'ontological opening" for the engagement with socio-material entanglements by interfering with the assumption of a singular kind of security. This paves the way for different kinds of analyses. It enables us to highlight and juxtapose things that, to paraphrase Mol and Law, 'relate but don't add up'.[69] It reminds us that 'there is no obvious context out there waiting to be revealed, no theory providing the obvious analytical anchor for the material at hand, but instead, endless opportunities for association and juxtaposition, each with the potential for taking the analysis in a new direction'.[70] As we will demonstrate in the following section through an engagement with the case of the Mirai botnet, letting this insight guide our analysis allows for a sensibility towards how cyber security emerge in dynamic socio-technical relations distributed among various agencies, actors, sites and spaces, including the security politics it conditions.

Mirai, Mirai on the wall, who's the least secure of them all?

'We are living in a new era of computing, information, and communication technology, that, as many are saying, pushes forward seamless interaction between humans, nature, and physical objects and is captured within the ecosystems of Internet of Things (IoT).'[71] As a result, we face an increasingly interconnected, interdependent, and interoperable networked world. With the ongoing implementation of 5G network infrastructure and the expansion of the IoT domain into our cars, healthcare devices, (smart) cities and more, the insecurity of smart Internet-connected devices has thus become more concerning than ever.[72] However, the existence

[65]Mol, *The Body Multiple*, p. 55.

[66]John Allen, 'Powerful assemblages?', *Area*, 43:2 (June 2011), p. 154

[67]Monsees, *Crypto-politics*; Schouten, 'Security as controversy'; William Walters, 'Drone strikes, dingpolitik and beyond: Furthering the debate on materiality and security', *Security Dialogue*, 45:2 (2014).

[68]Mol, 'Ontological politics'.

[69]Annemarie Mol and John Law, 'Complexities: An introduction', in John Law and Annemarie Mol (eds), *Complexities: Social Studies of Knowledge Practices* (Durham, NC and London: Duke University Press, 2002), p. 1.

[70]Lien, *Becoming Salmon*, p. 5.

[71]Arafatur Rahman and A. Taufiq Asyhari, 'The emergence of Internet of things (IoT): Connecting anything, anywhere', *Computers*, 8:40 (2019), pp. 1–4; Marie-Helen Maras and Adam Scott Wandt, 'Enabling mass surveillance: Data aggregation in the age of big data and the Internet of Things', *Journal of Cyber Policy*, 4:2 (2019), pp. 160–77.

[72]Pierre-Antoine Vervier and Yun Shen, 'Before toasters rise up: A view into the emerging IoT threat landscape', in M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis (eds), *Research in Attacks, Intrusions, and Defenses* (21st International Symposium, RAID, Heraklion, Crete, September 2018), pp. 556–76.

of botnets exploiting vulnerable, often poorly secured and configured, Internet-facing devices has been known and exploited for many years.

Yet, the Mirai botnet 'took the Internet by storm in 2016 when it overwhelmed several high-profile targets with massive distributed denial-of-service (DDoS) attacks'.[73] The attack caused millions of Internet users to be unable to connect to numerous websites. The attack hereby 'served as an indication of the potential devastating impact that these vulnerable [IoT] devices represent'.[74] More specifically, the Mirai botnet is almost exclusively comprised of thousands (approximately 2,500,000 by the end of October 2016)[75] of insecure IoT devices – that is, ICT-enabled devices such as surveillance cameras, webcams, digital video recorders, routers, and other Internet-embedded devices. In the fall of 2016, the Mirai botnet targeted the prominent cyber security blog Krebs on Security[76] and the French cloud service provider OVH[77] with massive DDoS-attacks. On 12 October 2016, another immense DDoS-attack – targeting the American Internet service provider Dyn. The attack, which authorities firstly feared was the work of a hostile state, turned out to be the work of the Mirai botnet. A number of additional high profile attacks later followed.[78]

The Mirai botnet presents a crucial case to study because the attacks set new precedents for the magnitude and impact of IoT-based DDoS attacks. Considering this, Mirai is not just a sea-changing case; it also seems aptly named, as it translates to 'the future' from Japanese. Moreover, it is a significant case to analyse since its operation and activity informs us about the particular challenges to cyber security studies brought about by the development of 5G infrastructure, IoT and IoT-enabled botnets. However, the Mirai botnet sits unease between the conventional focus on either extraordinary and exceptional politics or everyday bureaucratic expertise practices. The still active Mirai malware, the botnets it has helped create and the attacks these botnets exercise demonstrate a diffusion of cyber-security practices that disperse multiple insecurities. The socio-material assembling of the Mirai botnet creates insecurities both through a series of remarkable events and as a continuing, mundane vulnerability.[79]

Analysing the Mirai botnet, we draw from a diverse set of vantage points including academic analysis, cyber security company reports, media coverage, and statements from public authorities all concerning the composition, evolution, and effect of the Mirai botnet. We take as a starting point that a botnet can be seen 'as a hybrid sociotechnical assemblage of human and nonhuman actors'.[80] In other words, botnets 'are neither fully human nor completely machine driven'.[81] In doing so, we look at the creation and composition of the infrastructure of the Mirai botnet including its connective and collective political effects.[82] In accordance with Mol's notion of ontological politics, this emphasises the need to take into account the complex human-technological dynamics and consider how the agencies and affordances of technological artefacts help insecurities to

[73]Manos Antonakakis et al., 'Understanding the Mirai Botnet', in 'Proceedings of the 26th USENIX Security Symposium', Vancouver, BC, Canada, 16–18 August 2017, pp. 1093–10.

[74]Vervier and Shen, 'Before toasters rise up', p. 556.

[75]McAfee Labs Threats Report (April 2017), p. 31.

[76]Brian Krebs, 'Krebs on security hit with record DDoS', *Krebs on Security*, available at: {https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/} accessed 29 August 2019.

[77]Scott and Spaniel, 'Rise of the Machines: The Dyn Attack Was Just a Practice Run' (2016), p. 4.

[78]At its peak, the Dyn attack generated 1.2 Tbps of traffic, rendering websites such as Amazon, Twitter, and PayPal inaccessible. McAfee Labs Threats Report, p. 2; Kate Conger, 'The Mirai Botnet's Internet takedown opens up a new market for attackers and defenders', *TechCrunch*, available at: {https://techcrunch.com/2016/10/25/the-mirai-botnets-internet-take-down-opens-up-a-new-market-for-attackers-and-defenders/} accessed 29 August 2019.

[79]For an in-depth engagement with security, temporality, and the event, see Tom Lundborg, *Politics of the Event: Time, Movement, Becoming* (Abingdon and New York: Routledge 2012) and Stevens, *Cyber Security and the Politics of Time*.

[80]Marco Deseriis, 'Hacktivism: On the use of botnets in cyberattacks', *Theory, Culture & Society*, 34:4 (2017), pp. 131–52.

[81]van der Wagen and Pieters, 'From cybercrime to cyborg crime', p. 579.

[82]Jane Bennet, *Vibrant Matter: A Political Ecology of Things* (Durham, NC and London: Duke University Press 2009).

emerge and shape the conditions of possibility for cyber security politics.[83] Indeed, we look into the ways in which agential and security political institutional repertoires are simultaneously challenged and reaffirmed by the socio-material assembling of the Mirai botnet. Alongside the broadening of cyber-security agency our analysis, first, shows how the Mirai botnet speaks to the historical position of the nation-state – and with it the international system of states – as the spatio-political fulcrum of security politics.[84] Second, it moves on to explore how this opens up an important discussion on responsibility and accountability across multiple actors and sites of cyber security.

Constructing the botnet: Extending cyber security agencies and spaces

The Mirai malware tells a story of the entanglement of human and non-human agency and the emergence of (un)intended consequences and (un)expected insecurities. A story that shines new light on how cyber security and political agency emerge in a world embedded with IoT devices.[85] Mirai is a malware that turns networked devices into remotely controlled bots that can be used as part of a botnet in large-scale DDoS-attack. The Mirai malware is designed to automatically scan the Internet in order to discover specific IoT devices, infect these, and conscript them into the botnet. Initially, all that the Mirai-infected IoT devices shared was a piece of insecure software. This changed, however, as the Mirai malware was released, creating new relations and networks.

The Mirai botnet self-propagates by exploiting hardcoded administrative credentials present in the relevant IoT devices. The process in which the single IoT device becomes part of the botnet is delegated to the devices themselves and the software embedded into them.[86] These features of the Mirai malware illuminate the role and consequences of (un)intended non-human agency in analysing IoT and DDoS-attacks. The insecure, mundane IoT devices enabled hackers to construct the Mirai botnet. Moreover, the infected IoT devices were transformed by the creation of a command and control function between the IoT entities and the botherder.[87] Through this relation, the botherder became able to draw on the combined force of the Mirai botnet and direct it to a target through various forms of DDoS attacks. The relation between human, device, and technology changed as new IoT entities became part of the networked and semi-automated botnet, whose performances and relationships continuously developed new shapes and effects over time. As an IBM researcher recently put it, 'Mirai malware and its variants are evolving with their operator's intents, delivering a variety of exploits and increasingly aimed against enterprise environments' and continued 'as IoT devices become more common among households and large organizations, Mirai and its variants will continue to evolve to adapt to the changing environments and targets of its choice'.[88] The functionality of the Mirai botnet thus depended on the complex mutual interdependencies concerning the malware and IoT devices ability to operate in an 'autonomous and efficient manner as well as on the efforts and skills of the botherder',[89] which thereby transcend bounded human rationality and a means-end reasoning.

[83]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'; Kaufmann and Jeandesboz, 'Politics and "the digital"'.

[84]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'.

[85]In 2016 approximately 17 billion IoT devices were connected to the Internet. By 2019 that figure has risen to approximately 25 billion. Statista, 'Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions)', available at: {https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/accessed 29 August 2019}.

[86]The Mirai botnet embed a decentralised peer-to-peer architecture that turns every bot into a server that can handle instructions to other bots.

[87]See fn. 9 for definition of botherder.

[88]Tara Seals, 'Mirai botnet sees big 2019 growth, shifts focus to enterprises', *Threatpost*, available at: {https://threatpost.com/mirai-botnet-sees-big-2019-growth-shifts-focus-to-enterprises/146547/} accessed 6 January 2020.

[89]van der Wagen and Pieters, 'From cybercrime to cyborg crime', p. 588.

Consequently, the behaviour of the Mirai botnet cannot solely be backtracked to a human agent, that is, the hacker or botherder. This is not to deny that the botherder played a crucial role in assembling the Mirai botnet, but he/she was not the only actor initiating, building, and developing the botnet. The performance of the botnet is itself a 'dance of agency'[90] in which decision is not that of sovereign, human intentionality, nor non-human, technological determinism. Rather, there is a 'dialectic of resistance and accommodation'[91] in which the intentional actions of the botherder and the agency of malware and devices alter and modify each other. This spurs us to move beyond reductionist and functional technological agency in the singular. The IoT devices in the Mirai botnet express simultaneous modes of engaging with and co-constituting the world. The IoT devices were at the same time, at least, for example, a surveillance camera – partaking in networks with other surveillance cameras, guards, surveilled places, spaces, and people – and part of a malicious Mirai botnet network. As Mol puts it, drawing on Marilyn Strathern, 'being one shapes and informs the other while they are also different … they are partially connected, more than one and less than many'.[92]

In addition, the Mirai botnet is mobile. It is always moving somewhere to some effect, but it is never entirely predictable where this is. Most lately, security researches have shown that 'Mirai is now made up of several different related botnets, which sometimes compete with each other.'[93] At the same time – compared to other botnets that target IoT devices –, Mirai and variants of Mirai were by far the most popular malware to hit enterprise networks in 2018 and the beginning of 2019.[94] This is a prime example of how the delegation of one task to a non-human artefact can enable unintended agency when the artefact enters into new networks comprised of ICT, humans, and infrastructures. The Mirai botnet(s) thus resembles what Jane Bennet has called an assemblage of never fixed blocks but open-ended wholes.[95] Hence, mundane IoT entities containing the specific software targeted by the Mirai malware carried with them a not yet actualised potential to become part of multiple botnets and thereby a potentially transnational political security issue, as the botnets wielded their damaging effects unrestricted by national borders and jurisdictions.

The IP addresses of the infected devices suggest that the geographical performance of the Mirai botnet was extremely effective as the devices were located in over 164 countries.[96] Despite the density being higher in some countries than others,[97] this demonstrates how the Mirai botnet could not be located in a particular physical place of origin. On the one hand, it is ostensibly global in scope given the presence of infected devices in countries across the globe. Yet, on the other hand, it is local if we turn to the vulnerability of the individual device. Hence, the global and the local cannot neatly by separated, but are inherently entangled in the case of Mirai. It is spatio-temporally emergent and makes numerous agencies and realities (in) compatible.

[90]Andrew Pickering, *The Mangle of Practice: Time, Agency, and Science* (Chicago: The University of Chicago Press 1995) and 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.

[91]Pickering, *The Mangle of Practice*, p. 22.

[92]Mol, *The Body Multiple*, pp. 81–2.

[93]Tara Seals, 'Mirai botnet sees big 2019 growth, shifts focus to enterprises', *Threatpost*, available at: {https://threatpost.com/mirai-botnet-sees-big-2019-growth-shifts-focus-to-enterprises/146547/} accessed 6 January 2020.

[94]Tara Seals, 'Mirai botnet sees big 2019 growth, shifts focus to enterprises', *Threatpost*, available at: {https://threatpost.com/mirai-botnet-sees-big-2019-growth-shifts-focus-to-enterprises/146547/} accessed 6 January 2020; Charles DeBeck, 'I can't believe Mirais: Tracking the infamoua IoT malware', *SecurityIntelligence*, available at: {https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/} accessed 6 January 2020

[95]Jane Bennet, 'The agency of assemblages and the North American blackout', *Public Culture*, 17:3 (2005), p. 447.

[96]Scott and Spaniel, 'Rise of the Machines'; McAfee Labs Threats Report.

[97]The highest densities of infected devices were in Vietnam, Brazil, the United States, China, and Mexico. Scott and Spaniel, 'Rise of the Machines'.

This is indicative of a broader point about cyber security. As Simon and de Goede remind us, 'the complex interconnection of cyber-infrastructures forms a vast topological mesh where small events and disruptions can impact relations and elements near and far'.[98] This is not to say that cyber security does away with the relevance of state territories and metrical distances altogether. The Mirai-botnet consists partially of individual insecure material devices situated in particular geographical locations private houses, private companies, public authorities and sovereign territory. Likewise, the aggregation of the spread of infected devices mapped out on countries and regions can be said to 'perform a version of the social in which space is exclusive: there are neat divisions with no overlap based on comfortable geography of well-known political entities'.[99] Political spaces are enacted that are in line with traditional Euclidian space, scale, and metrics. However, the Mirai botnet demonstrates how these traditional spaces are also challenged as the natural spatio-political foundation for our understanding of security, as complex and dynamic socio-technical assemblages, such as the Mirai botnet, enable new potential spaces – and spatialities – of security.

In sum, thinking cyber security through the lens of ontological politics allows us to grasp the associational and operable evolution of the Mirai botnet, as it consists of IoT 'entities with uncertain boundaries, entities that hesitate, quake, and induce perplexity'.[100] Entities, of which 'each one harbors a simultaneous variety of virtual modes of expression and which subset will be actualized at any given moment is not predictable with confidence'.[101] The ontological political lens equips us to better understand and demonstrate how the increasing pervasiveness of IoT and 5G network means that even mundane artefacts – such as a refrigerator, a washing machine, or a child's toy – may be both agents and objects of security, which blur the boundaries between human and non-human agency and co-constitute multiple and overlapping political spaces. These spaces need not be parallel and discrete but may be overlapping, lead to controversies, and/or be folded into each other.[102] To paraphrase Mol and Law, they 'relate but don't add up'.[103] This raises profound questions regarding the sites of cyber security politics and the location of responsibility and accountability, which we will turn to in the next section.

Placing responsibility and assigning accountability across multiple actors and sites of cyber security

A common fear of distributed approaches to agency is that they jeopardise attempts to assign responsibility to people and hold traditional political bodies accountable.[104] In this case, however, the significance of technological agency and the proliferation of security political spaces opens up an important discussion about responsibility and accountability beyond the agency proper to the assemblage of IoT devices itself, as it broadens the range of places to look for sources of harmful effect. In other words, the central role that infected IoT devices play in the Mirai botnet lead to the dispersal of security politics well beyond the traditional arena of (inter)national security and into multiple new sites. Consequently, the case of the Mirai botnet also points to the significance of human actors beyond the conventional sites and institutions related to national security actors.

[98]Simon and de Goede, 'Cybersecurity, bureaucratic vitalism and European emergency', p. 80.

[99]Balzacq and Cavelty, 'A theory of actor-network for cyber-security', p. 188.

[100]Bruno Latour, *Politics of Nature: How to Bring the Sciences into Democracy* (Cambridge, MA: Harvard University Press 2004), p. 75.

[101]Bennett, 'The agency of assemblages and the North American blackout', p. 457.

[102]Law, 'Actor Network Theory and material semiotics'; Mol, 'Ontological politics'.

[103]Mol and Law, 'Complexities', p. 1.

[104]Aradau et al. (eds), *Critical Security Methods*, p. 78; Bennet, 'The agency of assemblages and the North American blackout'; Bennett, *Vibrant Matter*.

The Mirai botnet demonstrates how the traditional tension between the state as either the provider of security or the threat to it[105] is simultaneously reaffirmed and challenged by the spread of ICT. The assembling of the Mirai botnet and the attacks it exercised reveal how human and non-human entanglements enact dispersed and decentred insecurities and threat images. These dispersed and decentred insecurities and threat images emerged together with controversies in multiple sites carried out over political, economic, and technological queries. To understand the political significance of these insecurities and controversies, we place them in larger societal context,[106] specifically by directing attention to how the Mirai case brings to the fore the security politics of particular associations of IoT devices, states, corporate actors, and regular citizens.

Today, most of the ICT infrastructure is privately owned and operated. By knocking down the services of the private DNS provider DYN and the cloud service provider OVH, the Mirai botnet disrupted the Internet services of people across the world for several hours. Corporate security incidents may thus have repercussions far beyond the individual company itself. This aspect of cyber security is becoming progressively more prominent alongside the implementation and development of the Internet of Things (IoT), cloud computing, and 5G-network technology, as the future backbone of our critical infrastructure, including so-called smart cities and self-driving cars. This underscores the importance of the critical issue of the responsibility or the 'responsibilisation'[107] of private companies as partners in security practices, given their role as suppliers of vital elements of our critical information infrastructure.[108] The Mirai attacks demonstrate that deciding who does and does not deserve protection from DDoS-attacks is for private companies to decide. These decisions include considerations concerning protection of and access to societal digital infrastructures. The adequacy and decision-making of private companies is indeed central to the creation of insecurities and the continued operation of an increasing number of functions in contemporary society. If we take this to the extreme private companies may thus in some cases, in the words of Microsoft President and Chief Legal Officer Brad Smith, potentially be 'not only the plane of battle' but 'the world's first responders'.[109]

Another factor that spurred the assembling and spread of the Mirai botnet is the rampant use of insecure default passwords in IoT products. The various IoT manufacturers and the entire production and supply chain of these devices hence become relevant sites of security politics. As technical security research has shown, 'Mirai's ultimate device composition was strongly influenced by the market shares and design decisions of a handful of consumer electronics manufacturers'.[110] Their devices and components were sold downstream to other companies, who then installed them in their products. However, this meant that a wide array of different IoT devices had the same factory-set default usernames and passwords – and in some cases even hard-wired into the components, making them impossible to change – and hence they were easy targets in

[105]See, for example, Huysmans, 'What's in an act?'; R. B. J. Walker, *The Subject of Security in Critical Security Studies: Concepts and Cases*, ed. Keith Krause and Michael C. Williams (Minneapolis: University of Minnesota Press, 1997). Rather, cyber security practices involve 'actors who are different in power and kind (state, corporate, group, individual) and connected nodally through networks rather than hierarchically through states'. James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network*, 2nd edn (New York and London: Routledge, 2009), p. 209.

[106]Andrew Barry, 'Political situations: Knowledge controversies in transnational governance', *Critical Policy Studies*, 6:3 (2012), pp. 324–36.

[107]On responsibilisation see, for example, Karen Lund Petersen, *Corporate Risk and National Security Redefined* (London: Routledge, 2012); Karen Lund Petersen and Vibeke Schou Tjalve, '(Neo)republican security governance? US homeland security and the politics of "shared responsibility"', *International Political Sociology*, 7:1 (2013), pp. 1–18; Tobias Liebetrau, 'EU Cybersecurity Governance: Redefining the Role of the Internal Market (PhD dissertation, University of Copenhagen, 2019).

[108]Carr, 'Public-private partnerships in national cyber-security strategies'; M. D. Cavelty and M. Suter, 'Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, 2:4 (2009), pp. 179–87; Kristoffer K. Christensen and Karen L. Petersen, 'Public-private partnerships on cyber security: A practice of loyalty', *International Affairs*, 93:6 (2017), pp. 1435–52.

[109]Brad Smith, 'The Need for Digital Geneva Convention', Keynote address, RSA Conference, San Francisco, 2017.

[110]Manos Antonakakis et al. 'Understanding the Mirai Botnet', p. 1093.

the efforts to enlarge the Mirai botnet.[111] Private companies are hence central to the shaping of a fragile IoT ecosystem. Arguably, 'the absence of security best practices – established in response to desktop worms and malware over the last two decades – has created an IoT substrate ripe for exploitation'.[112] Research data indicates that 'some of the world's top manufacturers of consumer electronics lacked sufficient security practices to mitigate threats like Mirai'.[113] These manufactures will play a key part in ameliorating IoT vulnerabilities. This shows how private companies are often central actors – and not only when mobilised as partners in national security practices[114] – when it comes to both mitigating and creating cyber vulnerabilities. However, as discussed in the previous section, the assembling of devices spanned territorial borders and legal jurisdictions, exacerbating the challenge of coordinating technical fixes and promulgating security policies. The analysis of the Mirai botnet hence shows that it is compulsory to (re)consider the distribution of security political authority, responsibility, and accountability between states, companies, and citizens.

On that note, cyber security experts, such as Bruce Schneier, have emphasised the need for new forms of government regulation of IoT devices to alleviate the security risks that they currently pose due to poor security settings. In a comment following the initial Mirai attacks Schneier argued that the universe of IoT will largely remain insecure and open to compromise unless and until government steps in and fixes the problem.

> When we have market failures, government is the only solution. The government could impose security regulations on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers, allowing people like Brian Krebs to sue them. Any of these would raise the cost of insecurity and give companies incentives to spend money making their devices secure.[115]

Schneier thereby bring back in the state and reaffirm its position as a provider of security through regulating the market. However, one impediment to such regulation is people's seemingly insatiable demand for new devices to perform a constantly increasing number of tasks in everyday households. Currently, price and functionality generally seem to be prioritised at the expense of security. Yet, even if these priorities switch (and likely only among those who can afford to place security over price), there are already millions of insecure IoT devices in private homes across the globe. Hence, as suggested by both Cavelty and Hansen and Nissenbaum, we also need to take into account the behaviour of regular citizens.[116]

Consumers buttress the increasing supply of so-called 'smart' devices by companies across the private sector. Many of us do so, however, without considering the wider implications – or indeed the necessity – of our refrigerator, our light bulbs, children's toys or even pregnancy tests being

[111]Brian Krebs, 'Naming & shaming web polluters: Xiongmai', *Krebs on Security*, available at: {https://krebsonsecurity.com/2018/10/naming-shaming-web-polluters-xiongmai/} accessed 29 August 2019; Brian Krebs, 'Hacked cameras, DRV's powered today's massive Internet outage', *Krebs on Security*, available at: {https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/} accessed 29 August 2019; Brian Krebs, 'Who makes the IoT things under attack', *Krebs on Security*, available at: {https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/} accessed 29 August 2019.

[112]Manos Antonakakis et al., 'Understanding the Mirai botnet', p. 1094.

[113]Ibid., p. 1100.

[114]Christensen and Petersen, 'Public–private partnerships on cyber security'; Christensen and Liebetrau, 'A new role for "the public"?'; and Kristoffer Kjærgaard Christensen, 'Corporate Zones of Cyber Security' (PhD dissertation, University of Copenhagen, 2018) also explore the role of private companies beyond national security practices

[115]Bruce Schneier, 'We need to save the Internet from the Internet of Things', *Motherboard – Tech by Vice*, available at: {https://motherboard.vice.com/en_us/article/ezpq3m/we-need-to-save-the-internet-from-the-internet-of-things} accessed 29 August 2019.

[116]Cavelty, 'From cyber-bombs to political fallout'; Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School'.

connected to the Internet.[117] We do not wish to dismantle the criticism of manufactures, politician, and political institutional structures. Nor are we advocating a decentralisation that places the entire responsibility on the individual user. Rather, we argue, the analysis of the Mirai botnet enabled by a sensitivity to ontological politics helps us to recognise that we, as societies and individuals, are challenged by having to question and govern that which is not fully visible. That which we cannot comprehend in its entirety. It is, however, paramount that we continuously aim at doing so, since – as the sensitivity to ontological politics suggests – 'the condition of possibilities are not given',[118] but are in the making.

This section has underlined how contestation over the placement and distribution of security political authority, responsibility, and accountability simultaneously reaffirms and moves beyond the formal political arena of the state into multiple new sites, as, for example, the boardrooms of tech companies and private homes across the globe become new potential sites of security politics. Rather than restricting our analyses to formal state-centric security politics, sensitivity to the ontological politics points to how cyber security also may entails various forms of what we with a term from Ulrich Beck may call 'subpolitics' in sites that were previously not considered part of security politics – or even political as such.[119] A sensitivity to ontological politics does not provide political answers or democratic change in and of itself. It does, however, enable a different kind of political and democratic questioning that can help to spur engagement with these otherwise elusive technological developments and practices of (in)security.

Conclusions: Towards ontological politics of security

In this article, we have shown how an engagement with ontological politics enables an analytical opening towards examining the emergence of (in)securities stemming from distributed and multiple socio-material entanglements of political agencies, actors, sites, and spaces. The analysis demonstrated how the construction, maintenance, and workings of the Mirai botnet was made possible by a dynamic assemblage of human actors and a myriad of devices, technologies, and their interrelation. The insistence on the importance of the agency and affordances of devices and technology is not to deny the importance of human intentionality, but rather to demonstrate how it might be less definitive of cyber security outcomes than we tend to think. Paying further attention to the human disability to fully master and control technologies, as well as distributive and multiple security realities is one way to enable a questioning that can help to spur engagement with the increasing importance of vulnerable IoT devices that is soon to be underpinned by 5G digital infrastructure.

This is crucial if we are to engage with the political and democratic difficulties related to cyber security. As the analysis showed, the proliferation and multiplication of entangled political agencies, actors, sites, and spaces makes it harder to contest and engage with security politics – including authority over and responsibility for security – if we restrict our engagement to the traditional arena of (inter)national security. Instead, we need to attend to the various new 'territories of power' that we may otherwise lose sight of.[120] We need to 'find ways of knowing the slipperiness of "units that are not" as they move in and beyond old categories'.[121] This stipulates an ontological political practice that is situated here and now, rather than presenting itself as a theoretical ground

[117]Dan Goodinn, 'Creepy IoT Teddy Bear Leaks >2 million parents' and kids' voice messages', *Ars Technica*, available at: {https://arstechnica.com/information-technology/2017/02/creepy-iot-teddy-bear-leaks-2-million-parents-and-kids-voice-messages/} accessed 29 August 2019; Joanna Stern, 'The connected medicine cabinet: Bluetooth pregnancy test makes debut at CES 2016', *Wall Street Journal*, available at: {https://www.wsj.com/articles/the-connected-medicine-cabinet-bluetooth-pregnancy-test-makes-debut-at-ces-2016-1452045541} accessed 29 August 2019.

[118]Mol, 'Ontological politics', p. 74.

[119]Ulrich Beck, *World Risk Society* (Cambridge: Polity, 1999).

[120]William Walters, *Governmentality: Critical Encounters* (London and New York: Routledge, 2012).

[121]John Law and John Urry, 'Enacting the social', *Economy and Society*, 33:3 (2004), p. 404.

fixed for the purposes of future empirical inquiries. In this sense, the sensitivity enabled by the ontological politics approach emphasises constant inquiry rather than foundational answers provided by a theoretical stance. Yet, one result of thinking in ontologically political terms is that 'every time we make reality claims in social science we are helping to make some social reality or other more or less real'.[122] We thus perceive of our engagement as an ontological opening – a questioning of the conventional reproduction of security – waiting to be engaged with. In conclusion, we therefore suggest three ways forward as to how both cyber security studies and Critical Security Studies more broadly can unfold and question these new territories of security politics and power through further engagement with ontological politics as an analytical frame.

First, the opening towards the ontological politics of cyber security importantly could be extended to a sensitivity to the ontological politics of security as such. It would thus speak to ongoing debates among scholars drawing on different variants of securitisation. A key part of the debate unfolds around the difference between understanding securitisation as depolitisation from either above or below: By the invocation of exceptional and decisionist politics formulated by political elites in the language of existential threat and survival, on the one hand, or securitisation as a matter of incrementally institutionalising and bureaucratising certain issue as a security problem, on the other.[123]

Ontological politics inherits and transforms the theoretical and analytical space opened up by these approaches to securitisation. However, to engage with security in terms of ontological politics means not a priori specifying neither the logic nor the politics of security. The analytical ways forward for security research staked out by the ontological political approach is marked by the way in which politics and (in)security is co-constitutively produced and reproduced in socio-material performances of reality. Which security realities that are enacted matters and that is what the ontological political approach help us to appreciate, analyse, and question. Moreover, it helps us to value the essential possibility of the political invested in ontological openness. The ontological political sensitivity allows us to approach the relation between the security political and the ontological as one of questioning and remaining true to the idea of events and situations as always emerging and constituting in multiple ways.[124]

We do not rule out the possibility that cyber security can be constituted by securitisation or that malware driven cyber incidents perform the three spatial forms suggested by Balzacq and Cavelty.[125] Yet, we suggest to maintain an openness to this: cyber security may (also) potentially (and simultaneously) take the form of, for example, risk management, precaution, or resilience and cyber incidents may enact other topological spatialities. Moreover, the ontological political approach allows us to reconfigure the various securitisation and (de)politisation categories as performative objects of analysis and not stable backdrops of reality or fixed points of departure for analysis. As Mol writes, 'once we start to look carefully at the variety of the objects performed in a practice, we come across complex interferences between those objects'.[126] Hence, ontological politics prompts us to carefully study – not predict – the entanglements of security as relational, processual, and multiple.[127] Thereby enabling us to discern more clearly the various empirical

[122]Ibid., p. 396.

[123]See, for example, D. Bigo, 'The Möbius ribbon of internal and external security(ies)', in M. Albert, D. Jacobson and Y. Lapid (eds), *Identies, Borders, Orders: Rethinking International Relations Theory* (Minneapolis: University of Minnesota Press, 2001), pp. 91–116; CASE Collective, 'Critical Approaches to Security in Europe: A networked manifesto', *Security Dialogue*, 37:4 (2006), pp. 443–87; Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006); Kaufmann and Jeandesboz, 'Politics and "the digital"'; Andrew W. Neal, 'Securitization and risk at the EU border: The origins of FRONTEX', *JCMS: Journal of Common Market Studies*, 47 (2009), pp. 333–56; Ole Wæver, 'Politics, security, theory', *Security Dialogue*, 42:4–5 (2011), pp. 465–80.

[124]Mikko Joronen and Jouni Häkli, 'Politicizing ontology', *Progress in Human Geography*, 41:5 (2017), pp. 561–79.

[125]Balzacq and Cavelty, 'A theory of actor-network for cyber-security'.

[126]Mol, 'Ontological politics', p. 82.

[127]Schouten, 'Security as controversy'; Walters, 'Drone strikes, dingpolitik and beyond'; Rothe, 'Seeing like a satellite'.

enactments and political functions of security – be they in controversy, contestation, or concurrence.

Second, not only does a focus on ontological politics provide analytical purchase to critical studies of security, the argument here is also a normative one. Restricting our engagement with security to securitisation is not politically nor democratically adequate. We realise that central to the delineation of security to the exception in the original formulation of securitisation theory was an argument in favour of liberal and democratic political procedures and against letting the threat-defence logic of security colonise all spheres of society.[128] Historically, this normative argument has been well taken. Nevertheless, following on from our emphasis on the multiplicity and dispersion of cyber security, it is necessary to – in a manner of speaking – turn the normative argument of securitisation theory on its head. That is to say, if we restrict our notion of security to the securitisation of state agents, we run the risk of being blindsided by those practices of security that do not, in and of themselves, amount to high politics or exceptional politics.

This is an oft-cited critique against the Copenhagen School in security studies[129] but it holds particularly true for the critical literature on cyber security, as the critique in this regard is to be directed at most of the limited literature. Engaging with the ontological politics of cyber security critically opens up the study of cyber security and its political implications by also engaging with human and non-human agency, the cyber security practices of non-state actors and the security issues related to ICT that are not readily captured by the categories of 'exceptional' or even 'normal' or 'bureaucratic' politics in the political system. Enhancing conceptual sensitivity could help us move forward, allowing for further engagement with and illustrations of how security issues related to ICT are continuously enacted and contested rather than limited to either the exception or dissipating into normal politics as 'little security nothings'.[130] Thereby, an enhanced conceptual sensitivity might also enable Critical Security scholars to demonstrate the potential of an ontological politics framework to intervene in, disrupt, and open up the political spaces of contestation relating to ICT and security. One potential outcome might be the contestation of the tendency towards technification that Hansen and Nissenbaum rightly point to.[131] An aspiration that is supported by research on the technologisation of security identifying alternative forms of contestation.[132]

Finally, Nortje Marres[133] astutely poses the question if we can 'analyse change as not necessarily coherent and still be demanding of it?'. We believe the answer is yes, and indeed, we should. Not least considering the pervasive, ubiquitous, and ambivalent digital technological development, we face as citizens and societies with the implementation and development of IoT and 5G network technology. A sensibility to the ontological politics of security does not offer intrinsic political or democratic solutions. It does, however, enable diverse ways of engaging with and questioning technological development and potential practices of (in)security. Related to Jef Huysman's 'democratic curiosity',[134] it draws our attention to the contingency and contextuality of these practices. Herein lies a democratic potential. Rather than engaging with these permeating

[128]Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder, CO: Lynne Rienner, 1998); Ole Wæver, 'Securitization and desecuritization', in Ronnie D. Lipschutz (ed.), *On Security* (New York: Columbia University Press, 1995), pp. 46–86.

[129]Huysmans, *The Politics of Insecurity*; Karen Lund Petersen, *Corporate Risk and National Security Redefined* (Abingdon and New York: Routledge, 2012).

[130]Huysmans, 'What's in an act?'.

[131]Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School'.

[132]See, for example, Amicelle, Aradau, and Jean Jeandesboz, 'Questioning security devices'; Huysmans, 'Critical methods in International Relations', ch. 7; Monsees, 'Public relations'.

[133]Noortje Marres, 'On some uses and abuses of topology in the social analysis of technology (or the problem with smart meters)', *Theory, Culture & Society*, 29:4/5 (2012), p. 305.

[134]Jef Huysmans, 'Democratic curiosity in times of surveillance'.

and often opaque security practices wholesale, we should engage with and intervene in them in a more targeted manner. In other words, civil society – be it researchers, interest groups, think tanks, or regular citizens – should indeed be demanding of both state and corporate practices and engage in the shaping and contestation of its multiple ontologies.

Acknowledgements. Earlier versions of this article were presented at several conferences, seminars, and workshops. We wish to express our sincere gratitude to the organisers, participants, and discussants of these events for their encouraging and insightful comments. We also want to thank the anonymous reviewers and the editor.

Kristoffer Kjærgaard Christensen gained his PhD in the Department of Political Science, University of Copenhagen. His research is on the significance of cyber security for contemporary security politics, looking at how cyber security involves new security actors and contributes to creating new political spaces and understandings of security politics and democracy. He now works with cyber security in the Danish Ministry of Health.

Tobias Liebetrau is a postdoc at the Centre for Military Studies, Department of Political Science, University of Copenhagen. His research focuses on the implication of cyber security for contemporary security theory and governance, particularly in the context of the EU. Prior to his position at the university, he worked at the Danish National Centre for Cybersecurity under the Danish Defence Intelligence Service.

Cite this article: Liebetrau, T., Christensen, K. K. 2020. The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security* X: 1–19. https://doi.org/10.1017/eis.2020.10