


RESEARCH ARTICLE

Cybersecurity in practice: The vigilant logic of kill chains and threat construction

Lilly Pijnenburg Muller 

War Studies, King's College London, London, UK
Email: lilly.muller@kcl.ac.uk

(Received 8 February 2023; revised 12 April 2024; accepted 31 May 2024)

Abstract

In this article, I critically examine the 'Cyber Kill Chain', a methodological framework for thought and action that shapes both contemporary cybersecurity practice and the discursive construction of security threats. The history and epistemology of the Cyber Kill Chain provide unique insight into the practice of contemporary cybersecurity, insofar as the Kill Chain provides cybersecurity practitioners with predetermined categories and indicators of threat that shape how threats are conceptualised and understood by defenders and suggests actions to secure against them. Locating the origins of the kill chain concept in US military operational logics, its transformation through the anticipatory inquiries of intelligence, and its automation in computational networks, this article argues that the Cyber Kill Chain is emblematic of a vigilant socio-technical logic of security, where human perception, technical sensing, and automation all respond to and co-produce the (in)security through which political security concerns are articulated. This practice makes politics; it excludes, includes, and shapes what is perceived to be dangerous and not, directly impacting the security constructed. Through a critical reading of the Cyber Kill Chain, this article provides insight into cybersecurity practitioners' epistemic practice and as such contributes to discussions of cybersecurity expertise, threat construction, and the way in which cybersecurity is understood and practised as a global security concern.

Keywords: Cyber Kill Chain; cybersecurity; expertise; methodologies; practice

The Cyber Kill Chain is not just a model. It is a way of thinking.¹

Introduction

Networked digital technology and the broader domain of cyberspace – the composite assemblage of virtual space, communications media, and networked technological infrastructure – are an essential cornerstone of modern societies. The rapid growth of governments', corporations', and citizens' dependence on cyberspace for their daily functioning has left academics and security practitioners alike to wrestle with the possible magnitude and strategic use of cyberspace and the counter-possibilities and means of potential cyberweapons. In these efforts, Security Studies and International Relations (IR) have mostly been limited (for understandable reasons) to publicly attributed cyberattacks, state strategies, or the strategic use of cyberweapons in conflict for their

¹Interview with Hans Christian Petrorius, head of NORCERT, Norway, October 2019.

analyses.² While essential for IR's engagement with cybersecurity, these studies have however not been fully able to engage with 'the complex and transformative dynamics' of cybersecurity and 'the new security actors and practices that shape security politics in the digital age'.³ Some, like Tobias Liebetrau and Kristoffer Christensens, have called for more engagement with the complex and transformative dynamics and security actors that shape cybersecurity politics. In response, growing research in the social sciences has emerged on computer and cybersecurity firms that sheds light on these organisations' role in producing cybersecurity.⁴ Following suit, this article focuses on cybersecurity and threat intelligence organisations to contribute with a cybersecurity practitioner's epistemology to the advancement of Critical Security Studies scholarship on cybersecurity. Cybersecurity and threat intelligence organisations in this article (hereafter cybersecurity organisations) refer to international cybersecurity firms that provide both threat intelligence and security solutions to these identified threats, as well as to government organisations. Cybersecurity organisations are not the sole place where cybersecurity takes place. However, they produce both an understanding of the threat landscape and security measures against it and as such provide an essential missing piece of cybersecurity practice for Critical Security Studies' ability to grapple with cybersecurity as a global security concern.⁵

Engaging with the everyday practice and dynamics within cybersecurity security organisations in this article, I provide grounds to understand what cybersecurity does and how it is informed and thereby support a continuous questioning and engagement with the otherwise-elusive technological developments and practices of cyber (in)security.⁶ Building on the research that identifies the importance of cybersecurity experts⁷ and organisations in shaping cybersecurity,⁸ I draw on theoretical resources afforded by Critical Security Studies and Science and Technology Studies (STS) and set out to question the nature of the everyday processes and practices of cybersecurity making within cybersecurity organisations.⁹ To answer this question, I begin by identifying and analysing the practice bestowed by the Cyber Kill Chain – a widely used methodology that sets out how analysts are to map threat actor behaviour and the corresponding security measures which experts in the field of cybersecurity use to manage future security. The standard industry definition of the Cyber Kill Chain is that it is 'an adaptation of the military's kill chain, which is a step-by-step approach that identifies and stops enemy activity. Originally developed by Lockheed Martin in 2010, the Cyber Kill Chain outlines the various stages of several common cyberattacks and, by extension, the points at which information security teams can prevent, detect or intercept

²Cf. Jon R. Lindsay, 'Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack', *Journal of Cybersecurity*, 1:1 (2015), pp. 53–67; Florian J. Egloff, 'Public attribution of cyber intrusions', *Journal of Cybersecurity*, 6:1 (2020), pp. 1–12; Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, 'A tale of two cybers: How threat reporting by cybersecurity firms systematically underrepresents threats to civil society', *Journal of Information Technology & Politics*, 18:1 (2021), pp. 1–20.

³Tobias Liebetrau and Kristoffer K. Christensen, 'The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces', *European Journal of International Security*, 6:1 (2021), pp. 25–43.

⁴Andrew Whiting, *Constructing Cybersecurity: Power, Expertise, and the Internet Security Industry* (Manchester: Manchester University Press, 2020); 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.

⁵Didier Bigo and Emma McCluskey, 'What is a PARIS approach to (in)securitization? Political Anthropological Research for International Sociology', in Alexandra Gheciu and William C. Wohlforth (eds), *The Oxford Handbook of International Security* (Oxford: Oxford University Press, 2018), pp. 116–30.

⁶Liebetrau and Christensen, 'The ontological politics of cyber security'.

⁷James Shires, 'Enacting expertise: Ritual and risk in cybersecurity', *Politics and Governance*, 6:2 (2018); Rebecca Slayton, 'What is a cyber warrior? The emergence of U.S. military cyber expertise, 1967–2018', *Texas National Security Review*, 4:1 (2021), pp. 61–96.

⁸Whiting, *Constructing Cybersecurity*; Stevens, 'Assembling cybersecurity'.

⁹Bigo and McCluskey, 'What is a PARIS approach to (in)securitization?'.

attackers.¹⁰ While many analysts disagree on the details and the concept, this definition serves as a starting point for this article.

Methodologies offer simplified versions of practice and as such do not force a confrontation with many thorny, real-world application challenges, yet they provide insights into the logic the cybersecurity experts follow. Although we may not be able to gain insight into the specific practice and process of how data is collected, organised, and acted upon, methodologies illustrate the logic that guides how data is collected, organised, and analysed, and the practices that need to be in place to achieve a desired output. Critically engaging with the established methodology, I identify how it bestows a vigilant security logic on cybersecurity which works to detect and mitigate events post facto. The methodology as an apparatus of vigilance structures a particular form of anticipation in an uncertain but potentially dangerous landscape by inscribing a general militarised logic to cybersecurity practice – that is to say, a pattern of reasoning that shapes how threats are identified, how they are understood, and which security measures follow as a result. This practice depends on the continuous integration of new data to detect malicious behaviour and necessitates constant monitoring of networks and input of analysts in order to ensure an updated threat landscape. Where phenomena are seen as unpredictable when taken in themselves or individually, when seen collectively through the Cyber Kill Chain, they are understood to display a constant. This constant directly shapes the security practices that follow and how the threat landscape is understood by constructing a specific imaginary of threat which shapes the security measures taken.

The practice of cybersecurity making in cybersecurity organisations makes politics; it excludes, includes, and conceptualises what is dangerous and not; and it directly impacts the forms of security enacted. Accounting for the epistemic practice of cybersecurity practitioners in these organisations through engaging with their methodologies provides grounds to challenge what is understood as a threat in cyberspace and the security measures that follow. Critically engaging with these knowledge-making practices makes evident that cybersecurity practices are founded on a vigilant security logic that reproduces an always imminent threat. The account not only offers an example of specifically situated and highly illuminating knowledge-making practices but also contributes to efforts to critically examine military and security practices. Following Lucy Suchman's work to challenge 'attempts to make a clean demarcation of enmity within complex relations of affinity and difference',¹¹ I carefully investigate the sites and consequences of the security operations in cybersecurity organisations. Recognising the security apparatus in regenerating the realities that it is trained to see opens up received assumptions and allows for alternative knowledge-making practices.¹²

This article proceeds in three parts. I first set out why the Cyber Kill Chain is an exemplary methodology of cybersecurity practitioners' practice and provide a historical overview of the concept and its origin in military-intelligence thinking. I show how American intelligence and military targeting was appropriated, translated, and applied to cybersecurity globally. In the second part of the article, I identify how the practice of cybersecurity shifted from seeing cybersecurity as a technical solution to a technical problem – one that largely focused on mitigating vulnerabilities from unknown entities – to seeing the practice as one in which threats are rendered legible and knowable and are actively hunted down and neutralised through understanding the social factors that inform malicious actors' behaviour and goals.¹³ With this context in mind, I turn to the operational logic of the Cyber Kill Chain before I demonstrate how knowledge of threats and cybersecurity operations are constructed iteratively through the chain logic, which assumes that the future cannot

¹⁰Crowdstrike, 'What Is the Cyber Kill Chain? Process & Purpose', Crowdstrike, 2022, available at: <https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/>.

¹¹Lucy Suchman, 'Imaginariness of omniscience: Automating intelligence in the US Department of Defense', *Social Studies of Science*, 53:5 (2023), pp. 761–86.

¹²Suchman, 'Imaginariness of omniscience', p. 3.

¹³Fred Kaplan, 'When it comes to cybersecurity, the Biden administration is about to get much more aggressive', *Slate Magazine* (17 January 2023), available at: <https://slate.com/news-and-politics/2023/01/biden-cybersecurity-inglis-neuberger.html>.

be known and thus requires preparation for the inevitable surprise. I lastly account for the way(s) in which cybersecurity organisations operate in a socio-technical manner which is crucial to how threats are understood and security made. This is important for the burgeoning wave in Security Studies literature that focuses on the role machine learning and potentially Artificial Intelligence (AI) has in the field of (cyber)security.¹⁴ While the technology in use changes constantly, the logic that inscribes cybersecurity practice largely stays the same. Critical engagement with methodologies enables questioning of the role of emerging technology in a changing security landscape that goes beyond hypotheticals towards the socio-technical security practices and the consequences that follow.

The subsequent analysis of the Kill Chain and cybersecurity epistemology provided is founded on methodological triangulation.¹⁵ It combines a conceptual analysis of documents – from internal and public reports, training material, methodological literature, research papers, guidebooks, instruction manuals, white papers, policy papers, conference briefs, and public presentations – with empirical research conducted via interviews and informal conversations with developers, cybersecurity analysts, and other security professionals in cyber threat intelligence and security organisations. Specifically, the empirical findings are based upon extensive fieldwork conducted between 2018 and 2023. This includes ethnographic observation from 2018 to 2020 within cybersecurity organisations in Norway, the United States, and the UK. The ethnographic observation was complemented by interviews with public and private actors who are involved in practising cybersecurity in different international and national cybersecurity organisations in Norway, Estonia, the Czech Republic, Italy, the UK, New Zealand, the Netherlands, and the USA. In addition, analyses of public activities, such as industry meetings and webinars, and published reports from the industry are included.

Conceptualising cybersecurity: Methodologies and practice

Cybersecurity is by now a commonly researched topic in Critical Security Studies, within this journal, and beyond. Beginning with Lene Hansen and Helen Nissenbaum's influential argument two decades ago that cybersecurity is the product of a technical computer security discourse combined with securitisation,¹⁶ several scholars have examined the securitisation of cyberspace to shed light on how threats in and from cyberspace are the result of a particular communication to a receptive audience.¹⁷ A now-substantial literature in Critical Security Studies assesses the discourse around cybersecurity, which as Myriam Dunn Cavelty influentially argued, is not reliant on one single speech act but has a complex genealogy.¹⁸ As Balzacq and Dunn Cavelty established in this journal, 'cybersecurity is a type of security that unfolds in and through cyberspace',¹⁹ meaning that the making and practice of cybersecurity is always constrained by its environment, yet the genealogy of cybersecurity relies on actors not always visible in the public discourse.²⁰

¹⁴ Andrew Dwyer, 'Digital', in David Demeritt and Loretta Lees (eds), *Concise Encyclopedia of Human Geography*, (London: Elgar Jason, 2023); Jason Healey, 'The impact of artificial intelligence on cyber offence and defence', *The Strategist*, (2023), available at: {<https://www.aspistrategist.org.au/the-impact-of-artificial-intelligence-on-cyber-offence-and-defence/>}.

¹⁵ Thierry Balzacq, 'The significance of triangulation to Critical Security Studies', *Critical Studies on Security*, 2 (2014), pp. 377–81.

¹⁶ Lene Hansen and Helen Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly*, 53:4 (2009), pp. 1155–75.

¹⁷ Cf. Mike Zajko, 'Canada's cyber security and the changing threat landscape', *Critical Studies on Security*, 3 (2015), pp. 147–61; Robert M. Lee and Thomas Rid, 'OMG Cyber!', *The RUSI Journal*, 159:5 (2014), pp. 4–12; Shires, 'Enacting expertise'.

¹⁸ Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (London: Routledge, 2008).

¹⁹ 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.

²⁰ Myriam Dunn Cavelty, 'From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse', *International Studies Review*, 15 (2013), pp. 105–22.

With cybersecurity as a top priority on national security agendas, important scholarship questions the strategic use of cyber operations, debates the logic of deterrence, and unpacks the wider implications of significant cyberattacks. The relation between the practices of cybersecurity experts and security threat construction however remains largely underexamined. Studies have examined the history of the emergence of cybersecurity expertise²¹ and cybersecurity expertise as a form of knowledge exchange and building.²² Yet the experts who work in the organisations that practise cybersecurity and their role in shaping the field have largely been overlooked.²³ Following Didier Bigo and Emma McCluskey, in this article I engage with the everyday practice of cybersecurity practitioners in making cybersecurity. Understanding cybersecurity as the tension between ‘the processes of (in)security and (in)securitisation’,²⁴ I approach practice as the ‘actual work routines’²⁵ of the practitioners in the cybersecurity organisations. To avoid purely ideational and materialist accounts of practice, I build on Karin Knorr Cetina’s understanding of practice which places attention on the dualisms of agency and structure.²⁶ Attending to the dualism provides the ability to assess the contingency and change in the knowledge–practice dichotomy processes of cybersecurity making through placing focus on the operational instruments that enable and maintain these socio-technical systems, as well as the effects of translating and visualising knowledge. Drawing on the methodologies that guide cybersecurity operations in practice, I specifically concentrate on the several routinised and tested rules and procedures for producing knowledge in these methodologies that structure and enable how threat is thought about and how practitioners are to understand and act within the operational environment.

Embodying and articulating a particular logic, methodologies bring together ontological, epistemological, and practical assumptions that not only provide rules for thought and action but also shape assessments of the necessity, efficacy, and value of their outcomes; that is, they contribute to the discourse of politics. The embodied relationship between threat and its institutionalised conception is fundamental for how threats are understood, how they come to life, and the security practices that follow.²⁷ The everyday practice of cybersecurity professionals is not only shaped by the technology in use but also through concepts and methodologies, and, as we will see, these continuously affect each other in the practice of constructing knowledge of threat and the corresponding security measures. Drawing focus away from the different public knowledge pools that work to define cybersecurity towards how cybersecurity is practised within the organisations that both provide an understanding of the threat landscape and the security against said threat, I challenge how (in)security is understood by focusing on how threats come to life and motivate action and the security measures that follow.²⁸ The implications for scholarship in Critical Security Studies is the ability to understand how a particular form of security has emerged and is emergent. Illuminating the deeply embedded politics in the everyday socio-technical practices of security experts not only allows research to move beyond discussions of securitisation but also provides an

²¹Slayton, ‘What is a cyber warrior?’

²²Shires, ‘Enacting expertise’.

²³Terry Balzacq, Tugba Basara, Didier Bigo, Emmanuel-Pierre Guitte, and Christian Olsson, ‘Security practice’, in R. A. Denmark (ed.), *International Studies Encyclopedia Online* (Blackwell Publishing, 2010); Vincent Pouliot and Jérémie Cornut, ‘Practice theory and the study of diplomacy: A research Agenda’, *Cooperation and Conflict*, 50:3 (2015), pp. 297–315.

²⁴Bigo and McCluskey, ‘What is a PARIS approach to (in)securitization?’.

²⁵Didier 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.

²⁶Karin Knorr Cetina, ‘Objectual practice’, in Theodore R. Schatzki, Karin Knorr Cetina, and Eike von Savigny (eds), *The Practice Turn in Contemporary Theory* (Routledge, 2001), pp. 175–88; Suchman, ‘Imagaries of omniscience’.

²⁷Didier Bigo, ‘Security and immigration: Toward a critique of the governmentality of unease’, *Alternatives: Global, Local, Political*, 27:1 (2002), pp. 63–92.

²⁸Ibid.

alternative way to study the contingent and otherwise often-elusive logics that structure security practice.²⁹

While the concept of the Cyber Kill Chain is not fully equal to situated empirical practice, it nonetheless as a methodology provides insight into how practice is structured and conducted. Methodologies give accounts of security practitioners' paradigmatic worldview and how they operate in the everyday. Though they offer simplified versions of ideas and as such do not force a confrontation with many thorny, real-world application challenges, methodologies provide insights into the logic the organisations follow. Contributing to the methodological agenda for researching opaque security practices, this article builds on critical work in IR-STs that uses methods as methodology.³⁰ We may not always be able to gain insight into the specific process of data analyses, yet methodologies illuminate the importance of the data added, and how models are used to organise data in different ways to achieve desired outputs. Similar to Adrian Mackenzie's observation regarding code, we do not need to reconfigure ourselves into cybersecurity practitioners to examine their practice.³¹ Methodologies bring together ontological, epistemological, and practical assumptions that provide rules not only for thought but for everyday practice and as such allow for engagement with the world making that is taking place.³² With these analyses as background, I turn to what I take to be a core premise that shapes cybersecurity organisation practice, however it is configured, namely, the Cyber Kill Chain. Despite the focus on issues of public-private cooperation in cybersecurity,³³ the closed world of the practitioner rests upon a methodology that both parties share. Powered by the Cyber Kill Chain, the practice of cybersecurity organisations and their use of AI in cybersecurity can, as I elaborate below, be uncovered. In the next section, I provide a historical overview of cybersecurity kill chain methodology as it continues to underwrite the practice of cybersecurity today.

Why the Cyber Kill Chain? A persistent logic that shaped the field of cybersecurity

In 2020, Ben Buchanan and his co-authors argued that 'The kill chain is an established method of conceptualizing cyber operations'³⁴ [which presents] 'a checklist of tasks that attackers work through on their way to their objective.'³⁵ Ten years before, in 2010, Lockheed Martin published the first documented mention of the Cyber Kill Chain in the white paper 'The Cyber Kill Chain: An intelligence-driven computer network defence and risk management strategy'. Since then, the logic it bestows has fundamentally shaped how threat is understood and how cybersecurity is practised. Today, the Cyber Kill Chain is widely used in government and private sector training, as well

²⁹Louise Amoore, Alexander Campolo, Benjamin Jacobsen, and Ludovico Rella, 'Machine learning, meaning making: On reading computer science texts', *Big Data & Society*, 10:1 (2023), available at <https://doi.org/10.1177/20539517231166887>; Claudia Aradau and Tobias Blanke, 'Introduction', *Algorithmic Reason: The New Government of Self and Other* (Oxford: Oxford University press, 2022), pp. 1–20. Suchman, 'Imaginariness of omniscience'.

³⁰Markt Salter, Can E. Mutlu, and Philippe M. Frowd, *Research Methods in Critical Security Studies* (Oxon/ New York: Taylor & Francis, 2023); Marijn Hoijtink, and Matthias Leese, *Technology and Agency in International Relations* (London: Routledge, 2019).

³¹Adrian Mackenzie, *Machine Learners: Archaeology of a Data Practice* (Cambridge, MA: MIT Press, 2017).

³²Claudia Aradau, Jef Huysmans, Andrew Neal and Nadine Voelkner (eds), *Critical Security Methods: New Frameworks for Analysis* (Abingdon: Routledge, 2015); 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; Lilly Muller and Natalie Welfens, '(Not) accessing the castle: Grappling with secrecy in research on security practices', *Secrecy and Society*, 3:1 (2023), pp. 1–44.

³³Madeline Carr, 'Power plays in global internet governance', *Millennium: Journal of International Studies*, 43:2 (2015), pp. 640–59; Lilly Muller, 'Public private cooperation to secure cyberspace', in Karsten Friis and Jens Ringsmose (eds), *Conflict in Cyber Space: Theoretical, Strategic, Legal and Ethical Implications* (London: Routledge, 2016), pp. 56–78.

³⁴Ben Buchanan, John Bansemer, Dakota Cary, Jack Lucas and Micah Musser, 'Automating Cyber Attacks', Center for Security and Emerging Technology, 2020, available at: <https://cset.georgetown.edu/publication/automating-cyber-attacks/>.

³⁵*ibid.*

as structuring how organisations practise threat intelligence collection and security practices.³⁶ A quick Google search shows how both governments and most global cybersecurity firms reference the Cyber Kill Chain in their training material, staff training guides, and threat intelligence reports on cybersecurity.³⁷ Yet, as the head of a European Computer Emergency Response Team (CERT) said in an interview when discussing the Cyber Kill Chain, it is important to remember that ‘The Cyber Kill Chain is not just a model. It is a way of thinking. They [all the versions and models] are all connected, and they are complex systems; cybersecurity is a complex system.’³⁸

Since its inception in 2010, the Cyber Kill Chain has been altered and changed. In 2013, David Bianco, a SANS instructor, published the Pyramid of Pain,³⁹ which covers the different forms of cyber threat intelligence provided by digital forensics and incident response teams after an incident.⁴⁰ Two years later, in 2015, the cybersecurity provider MITRE released ATT&CK: Adversary Tactics, Techniques, and Common Knowledge.⁴¹ This is the current industry standard and the framework most used for understanding and communicating how attacks work. Again, two years later, in 2017, Paul Pols published the Unified Cyber Kill Chain⁴² to overcome some of the divisions in the field. Unifying the different editions, Pols provided what he called an expanded Cyber Kill Chain that united the different divisions in a comprehensive model. All the cybersecurity models differ in how they categorise and structure data and in their focus on different subsets of cybersecurity. However, the Cyber Kill Chain represents an overarching logic of thinking (in)security that all these later methodologies build upon.⁴³ While there are internal discussions in the practitioner community on which models provide better visibility, they are all complementary methodologies.⁴⁴ The methodologies aim to clarify visibility and search functions in data and improve how data is put together with the goal of improving an organisation’s defence. Different organisations have adapted the Cyber Kill Chain to their needs and have added other methodologies in reaction to the growth and development of digital technology. Yet the underlying logic inherent in the Cyber Kill Chain of mapping threat actor behaviour with corresponding security measures has stayed the same and as such provides fruitful grounds to gain insight into the logic of security in operation and the defence measures it bestows. In the next section, I trace the origins of the Cyber Kill Chain in US military thinking and how this way of thinking defence was adapted to cybersecurity.

³⁶The Cyber Kill Chain logic informs both state and private sector cybersecurity organisations and how they understand the threat landscape, which in part enables fundamental cooperation across private sector organisations, as well as civil–military cooperation. While the private sector and state present different threat perspectives of a threat in reports and commentaries (Alexander Bouwman et al., ‘A Different Cup of {TI}? The Added Value of Commercial Threat Intelligence’, www.usenix.org, 2020, available at: <https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman>), this is due to the technological and symbolic specificities of their visibility (Rebecca Slayton and Lilly Pijnenburg Muller, ‘Commodifying threats: Uncertainty in cybersecurity threat intelligence’, *Social Studies of Science* (forthcoming)). The operations are largely informed by the same logic and practice.

³⁷Cf. ‘Digital, Data and Technology (2019) Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts’, UK government cyber security programme. Version 2.0, available at <https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf>; Leonardo Cyber & Security Academy, S2 Threat intelligence slides, Leonardo, 2022, available at <https://cybersecurity.leonardo.com/documents/16277703/0/Information+Superiority+LQ+%28mm09135%29.pdf?t=1695124347619>.

³⁸Interview with Petrorius, 2019.

³⁹David J. Bianco, ‘The Pyramid of Pain: Enterprise detection & response’ (2013), available at: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.

⁴⁰Bianco, ‘The Pyramid of Pain’.

⁴¹MITRE ‘ATT&CK Matrix for Enterprise’, available at: <https://attack.mitre.org/>.

⁴²Paul Pols, ‘The Unified Kill Chain’, available at: <https://unifiedkillchain.com/>.

⁴³While it is outside of the scope of this paper to trace how the cybersecurity community developed the several alterations of the models and the controversies that led to these, the short history of the Cyber Kill Chain offers insight into the general logic of cybersecurity practitioners practice without studying the situated, the general logic of cybersecurity practitioners practice without studying the situated every day practice.

⁴⁴To read more about how models such as the diamond model and MITRE ATTACK build on the Cyber Kill Chain, see <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/>.

Identifying threat with the Cyber Kill Chain

In the early days of cybersecurity in the 1980s,⁴⁵ a general consensus was held within the information security community that viruses operated at random and attacked any vulnerable technology these viruses were programmed to abuse.⁴⁶ Cybersecurity threats to computer networks were understood as self-propagating code created by malicious actors that exploited vulnerabilities in computer networks.⁴⁷ Cybersecurity was as such concerned with patching these vulnerabilities and was essentially understood as a response mechanism, with little to no intelligence – the processes of gathering, analysing, and making useful information about adversaries and adversarial situations – incorporated into the security making. The compromises detected were approached as a fixable flaw – a vulnerability – and cybersecurity was following a technical solution to a technical problem;⁴⁸ responses primarily took place after an intrusion had occurred and been detected. The logic of network defence at the time fostered a promotion of firewalls and antivirus packages that searched for specific signatures – the string of code used by malicious actors to abuse a vulnerability in a system. The security systems designed against compromises mainly focused on mitigating vulnerabilities through patching security flaws, building intrusion detection systems (IDS), more secure code, malware identification, and antivirus software.⁴⁹ As the head of a Cyber Threat Intelligence team explained in an interview, ‘more secure code, malware identification and antivirus software was seen as the solution.’⁵⁰ The importance of more secure code and antiviruses is reflected in the boom of the cybersecurity industry in the early 2000s. This was all to change with the Cybersecurity Kill Chain. While signature-based, the Cyber Kill Chain set out how to incorporate data from previous attacks and intelligence on threat actor behaviour to create an imaginary of how threat actors operated to reach their end goal.

To counter the risk of attack and the cyber threat, vulnerable organisations established Computer Emergency Response Teams (CERTs). These CERTs were established to handle computer security incidents. The first CERT was formed in 1998 by the US Defense Advanced Research Projects Agency, better known as DARPA, and coordinated through Carnegie Mellon University’s Software Engineering Institute (SEI) to research and report on Internet-related security problems. SEI’s CERT Coordination Centre published security information and advisory bulletins which would describe what the code and emails in targeted socially engineered emails looked like. Explaining in detail the code that targeted emails would drop, typically Trojans (a type of malware presented to its victim as legitimate software), which would exfiltrate sensitive information from technological systems, the technical alert bulletins’ goal was to inform technicians what patterns of malicious behaviour to look out for.⁵¹ Once a signature was detected, it could be coded into the firewalls and antiviruses. Signatures detected were understood to be relevant for everyone, and there was little to no comprehension of their origin or goal. The security community’s focus was on the vulnerability side of risk, meaning that cybersecurity meant conducting network defence in the form of firewalls and antivirus software.

⁴⁵ While there are debates regarding when cybersecurity became a field, I start in the 1980s as this is the decade when high-profile attacks increased in frequency. The terms ‘Trojan Horse’ and ‘computer virus’ both made their debut in 1986. Although various people claim to have created the first antivirus program, 1987 marked the beginning of commercial antivirus programs with the release of Anti4us and Flushot Plus. Cf. Finn Brunton, *Spam: A Shadow History of the Internet* (Cambridge, MA: MIT Press, 2013).

⁴⁶ Jussi Parikka, *Digital Contagions: A Media Archaeology of Computer Viruses* (New York: Peter Lang, 2007).

⁴⁷ Brunton, *Spam*.

⁴⁸ Sarandis Mitropoulos, Dimitrios Patsos, and Christos Douligeris, ‘On incident handling and response: A state-of-the-art approach’, *Computers & Security*, 25:5 (2006), pp. 351–70; Eric Hutchins, Michael Cloppert and Rohan Amin, ‘Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains’, Lockheed Martin White paper (2011), available at: {chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf}.

⁴⁹ Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’.

⁵⁰ Interview with head of threat intelligence, European cybersecurity firm, February 2020.

⁵¹ Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’.

Yet, even with these technical solutions in place, intruders evaded the firewall and antivirus capabilities. A growing consensus arose within the cybersecurity community that the current approaches of building signatures, antivirus, and patching were not sufficient to keep systems secure.⁵² Attacks were increasingly understood not as operating at random nor as just attacking anyone that possessed the vulnerability the code was programmed to use. Rather, malicious code was increasingly understood within the community to be targeting specific networks and systems.⁵³ With the recognition that end users were being directly targeted, a realisation grew within the cybersecurity community that cybersecurity was not only a technical solution to a technical problem. Cybersecurity could not just involve building more signatures, antivirus software, and firewalls. Threat intelligence – meaning a broader social understanding of the threat actor, their goals, and their intent – had to be involved, and the Cyber Kill Chain provided the necessary response.

A new way of thinking defence

When the CERT in the Intelligence Driven Defence project at the American aerospace, arms, defence, security, and advanced technologies company Lockheed Martin first published their white paper on the Cyber Kill Chain in 2010,⁵⁴ they did so with the aim not only to mitigate vulnerabilities but also to diminish the threat component in cybersecurity. Presented as a tool to analyse intrusions and drive defensive courses of action through collecting and sorting information on the attacker, the Cyber Kill Chain presented by Lockheed Martin was revolutionary at the time of publication.⁵⁵ To address the potential threat, the model laid out a way to incorporate analysis of adversaries, their capabilities, objectives, doctrine, and limitations (i.e. intelligence) into cybersecurity making.⁵⁶ Importantly, in 2010, the idea of a ‘kill chain’ was not new. Lockheed Martin’s white paper is built on a broader logic prominent within the US military and specifically references the United States Air Force (USAF) use of the kill chain to identify gaps in intelligence, surveillance, and reconnaissance (ISR).⁵⁷ While seen as revolutionary at the time of publication in the cybersecurity practitioner community, the chain way of thinking originated in US military targeting operations that worked to combine kinetic operations with an intelligence cycle.⁵⁸

The white paper describes malicious attacks as having an operational life cycle with sequences of stages that attackers had to accomplish to successfully reach their goal. Stating that ‘intelligence-driven computer network defence is a risk management strategy that addresses the threat component of risk, incorporating analysis of adversaries, their capabilities, objectives, doctrine and limitations’, the paper argued for the necessity of ‘a continuous process, leveraging indicators to

⁵²UK-NISCC, ‘National Infrastructure Security Co-ordination Centre: Targeted Trojan Email Attacks’, CPNI, 2005, available at: {<https://www.cpni.gov.uk/docs/ttea.pdf>}; US-CERT, ‘Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks’, 2005, available at: {<http://www.us-cert.gov/cas/techalerts/TA05-189A.html>}.

⁵³Alex Stamos ‘Aurora Response Recommendations’, Partner Version 1.0 (2010), available at: {https://www.qualys.com/docs/iSEC_Partners_-_Aurora_Response_Recommendations_-_Public_-_QUALYS.pdf}.

⁵⁴Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’.

⁵⁵The Lockheed Martin Cyber Kill Chain did not erupt in a vacuum. The Cyber Kill Chain was seen as pioneering at the time of the white paper publication. While security company Mandiant proposed ‘the exploitation life cycle’ in the same year, which also mapped out the phases of a cyberattack, the Mandiant model, however, did not map the courses of defensive action and was based on post-compromise actions (Mandiant, ‘M-Trends: The Advanced Persistent Threat’ January 2010, available at: {<http://www.mandiant.com/products/services/m-trends>}, Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’). The move of detections and mitigations to earlier phases of the intrusion kill chain was seen as essential for building defence against APTs.

⁵⁶Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’, p. 1.

⁵⁷John A. Tirpak, ‘Find, fix, track, target, engage, assess’, *Air Force Magazine*, 83 (2000), pp. 24–9, available at: {<http://www.airforcemagazine.com/MagazineArchive/Pages/2000/July%202000/0700find.asp> x.}. Cited in Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’.

⁵⁸Air Force Doctrine Publication 3–60, ‘Targeting’, available at: {https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf}.

discover new activity with yet more indicators to leverage.⁵⁹ The paper claimed to give a new understanding of the intrusions themselves. Attacks are described not as singular events, but rather as phased progressions, and the intrusion kill chain model would enable practitioners to analyse intrusions and drive their defensive courses of action. Providing a methodology for how to understand the steps of a targeted attack, the white paper claims to give analysts the ability to monitor and build response plans, thereby ‘killing’ the threat before it reaches its end goal.

The Cyber Kill Chain aimed to make threat actors visible and enable the creation of security measures against them. Operating out of an understanding that malicious actors can break into other network systems and operate without being detected, the basic premise of the Cyber Kill Chain was that by providing a methodology that groups together indicators of compromise detected, and combining this with intelligence, security actors can build, and hence more easily categorise, threat actor profiles. With these profiles, cybersecurity organisations could find malicious actors in networks before they were able to reach their targeted goal. By setting out threat actors’ steps and a methodology to build threat actor profiles, the Cyber Kill Chain produced a specific understanding of threat and the threat landscape driven by intelligence feedback loops that allow for continuous incorporation of exploitations detected and analysis of data collected.

Where network defence and early CERTs would previously build signatures of formerly detected attacks, the Cyber Kill Chain enabled an understanding of the structure of a cyberattack. It outlined how the malicious actors were likely to attack and with what measures, altering the logic of cybersecurity thinking.⁶⁰ As the methodology became integrated into the CERT process, it shifted how analysts and operators in CERTs understood and dealt with the data they processed, and following that how the threat landscape was portrayed. The analytical framework upon which Lockheed Martin based the Kill Chain was a product of their close ties with, and also an intuitive way of framing for, the security community. That many of the early analysts that worked in these CERTs had previously worked with or had close ties to the American military likely helped add credibility and legitimacy to the Kill Chain.

The ‘Kill Chain’ way of thinking

Originally designed for and adopted by the US Foreign Internal Defence missions in Latin America in the 1980s, the Kill Chain logic stems from targeting methodologies developed to counter the perceived communist threat.⁶¹ With the Global War on Terror (GWOT) and the wars in Iraq and Afghanistan, targeting as a military logic grew extensively in support of so-called Full Spectrum Operations (a combination of offence, defence, stability, and civil support missions), primarily, but not exclusively, by special operations forces (SOF).⁶² The authors of the Cyber Kill Chain white paper explicitly draw on the military concept of targeting, which, based on the assumption of an existing, although elusive threat – the terrorist – asks the defenders to go out offensively to ‘the root’ of a problem or threat. The ability to identify, locate, and target enemy forces through performing intelligence exploitation and analysis of captured enemy material and resources made the logic of targeting especially attractive.⁶³ The core premise of fusing operations and intelligence functions into a symbiotic relationship was seen as a game changer for the field of cybersecurity.

In the 2010 white paper, the authors draw on and use references from both US military targeting and kill chain methodologies to justify and explain the utility of the Cyber Kill Chain, stating that the applicability of wider ‘lessons learned’ from ‘the antiterrorism planning process for military installations ... identifies principles to help commanders determine the best ways to protect

⁵⁹ Ibid.

⁶⁰ Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’.

⁶¹ Jimmy A. Gomez, ‘The targeting process: D3A and F3EAD’, *Small Wars Journal* (2018), available at: <https://smallwarsjournal.com/blog/journal/docs-temp/816-gomez.pdf>.

⁶² Anders Nese, ‘Improving Security Posture by Learning from Intrusions’, *Norwegian University of Science and Technology Department of Information Security and Communication Technology* (2018).

⁶³ Gomez, ‘The targeting process’.

themselves'.⁶⁴ Presented as a phase-based model in seven steps, the Cyber Kill Chain is meant to enable an ability to capture the intent and capability of malicious actors. Riddled with US military references and phrases, the white paper describes how 'phase-based models have also been used for antiterrorism planning' and that 'the United States Army[s] ... seven-step process ... [that] serves as a baseline to assess the intent and capability of terrorist organisations' is applicable to the cyber domain.⁶⁵ The white paper as such not only constructs legitimacy for the Cyber Kill Chain based on the broader models used in counterterrorism, it also enables a militarised understanding of enemy in cyberspace which pushes cybersecurity's focuses beyond vulnerabilities. Using the Cyber Kill Chain, the threats in and from cyberspace become identified as similar to other 'on the ground' threats in military operations. Through the incorporation of military logics and language, the white paper actively shifts the practice of cybersecurity from being a reaction to vulnerability to a proactive defence.

Drawing an equivalence between cyber threats and terrorists, and between threats and anti-terrorism planning, the white paper promises the ability to detect and mitigate cyberattacks. Through coordinated intelligence and defence and drawing explicit links to existing frameworks for kinetic attacks and applying them to cybersecurity, Hutchins, Cloppert, and Amin argue that malicious actors can be stopped before they reach their end goal to prevent them conducting a cyberattack. Identifying the series of steps an adversary must complete in order to achieve its objectives in a cyberattack, namely Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control (C2), Actions, and Objectives, the Cyber Kill Chain promotes an understanding of cybersecurity as a continuous process where indicators represent not just singular events but rather a phased progression. This understanding of cybersecurity means leveraging the ability to discover new activities and a new understanding of the intrusions as targeted and defeatable before it reaches its end goal.⁶⁶ The framework builds an understanding of the structure of a cyberattack that simultaneously allows for the visualisation of the larger threat landscape where different threat actors have different intents and operation patterns.

The introduction of the Cyber Kill Chain altered cybersecurity from being reactive (vulnerability patching) to proactively practising security against a more diverse targeted threat. In addition to patching and searching for vulnerabilities, the cybersecurity operators could now stop attackers before they reached their end goal of destruction and even proactively hunt them down through the continuous searching for, collection, and interpretation of data.⁶⁷ Through the creation of a signature of how a threat actor operates and their intent, the Cyber Kill Chain allowed organisations to make risk calculations as to the chances of a malicious actor attacking a certain system while also guiding defenders as to how to stop the attackers when detected. Instead of building all defences to protect against all threat actors, cybersecurity became targeted.⁶⁸ This move took place within a broader shift in global security practice, where a move to risk and pre-emption produced a security practice that focuses on 'interoperability, emergence, flexibility and analytical foresight' to bridge the perceived gaps of security spaces and the temporal bridges between present and possible futures.⁶⁹ The materialisation of anticipation logic in cybersecurity was as such entangled in 'the making' of cyber (in)security as a modern global security concern,⁷⁰ yet it differs from the pre-emptive logic of security governance.⁷¹

⁶⁴Hutchins, Cloppert, and Amin, 'Intelligence-Driven Computer Network Defense'.

⁶⁵United States Army Training and Doctrine Command (2007) in Hutchins, Cloppert, and Amin, 'Intelligence-Driven Computer Network Defense', p. 2.

⁶⁶Hutchins, Cloppert, and Amin, 'Intelligence-Driven Computer Network Defense', p. 3.

⁶⁷'Cyber Command PAO, CYBER 101: Defend Forward and Persistent Engagement' (2022), available at: <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>.

⁶⁸Erik Reichborn-Kjennerud, *The World According to Military Targeting* (Cambridge, MA: MIT Press, 2025).

⁶⁹Marieke de Goede, Stephanie Simon, and Marijn Hoijsink, 'Performing preemption', *Security Dialogue*, 45:5 (2014), pp. 411–22.

⁷⁰Ibid.

⁷¹Ibid.

Since its debut in cybersecurity practice, the Cyber Kill Chain has gone through several rounds of alterations. Garter, Mandiant, FireEye, and others, even Lockheed Martin itself, have criticised, expanded, altered, and adapted the framework.⁷² In response to the growth of cybersecurity as a field, different organisations and practitioners adapted the steps to their needs and added other methodologies as they saw fit. Factors that have promoted these shifts are, amongst others, the criticism of the original focus on perimeter security (systems like firewalls and browser isolation systems) and a limited ability in malware prevention.⁷³ The several adaptations and expansions have led to internal discussions within the information security community as to what version of the model holds best.⁷⁴ Yet the underlying logic inherent in mapping threat actor behaviour in stages to evaluate the accurate security response inherent in the Cyber Kill Chain has stayed the same.⁷⁵ The later models and methodologies developed, the Diamond Model or ATT&CK, help categorise indicators in different ways. They all however have the same goal and intent of enemy construction and following guiding security practice. When in the next section I unravel the Cyber Kill Chain, I do not refer solely to the paper published by Lockheed Martin, but to the logic it reflects and the insights it provides into cybersecurity practice. Having established the historical roots of the Cyber Kill Chain, I next trace the anticipation of enemy operations through the Cyber Kill Chain, the practice of incident response, and the building of indicators of compromise, signatures, and threat classification, and I examine the way in which the Cyber Kill Chain shapes how threat actors become known and acted upon.

The Cyber Kill Chain: From planning to attack to delivery

The Cyber Kill Chain sets out how to methodologically collect intelligence on malicious behaviour to allow for the anticipation and prediction of enemy operations. Across several operational phases, the methodology describes indicators of malicious behaviour, and how to use these indicators to locate malicious actors; collects intelligence; and captures target material (in the form of the traces left and/or found by the malicious behaviour in systems).⁷⁶ The inputting of indicators of malicious behaviour found in data into this methodological framework creates a specific understanding of cyberattacks and attackers. By laying out attackers' steps in stages, the Cyber Kill Chain creates a threat picture of the enemy and sets out steps security practitioners take to predict, protect, or handle what was previously unknown.

In the phases of intrusion of the Cyber Kill Chain, the first stage is *Reconnaissance*. In this stage, the malicious actor plans, observes, and assesses the target outside-in to identify which aspect of the network the attacker is to target and which tactics to use.⁷⁷ The intruder, having selected its target

⁷²While some of the alternative and additional models combine several of the seven 'original' steps into a command and control, or C2 stages (C&C), others divide these stages into actions and objectives. Others, like the Diamond Model or the Pyramid of Pain, combine lateral movement and privilege escalation into an exploration stage and combine intrusion and exploitation into a 'point of entry' stage. Cf. Giora Engel, 'Deconstructing the Cyber Kill Chain', *Dark Reading* (2014), available at: <https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/>.

⁷³Marc Laliberte, 'A twist on the Cyber Kill Chain: Defending against a JavaScript malware attack', *Dark Reading* (2016), available at: <https://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/>.

⁷⁴To read more about how models such as the Diamond Model and MITRE ATT&CK build on the Cyber Kill Chain, see <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/>.

⁷⁵Cf. Francesco Maria Ferazza, 'Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: A comparison of cyber intrusion analysis models', *Technical Report RHUL-ISG-2022-5*, available at: <chrome-extension://efaidnbnmnibpcjgclcfldfmkaj/https://www.royalholloway.ac.uk/media/20188/techreport-2022-5.pdf.pdf>.

⁷⁶Critique and engagement with this way of security thinking is broadly discussed in Critical Security Studies. Cf. Claudia Aradau and Jef Huysmans, 'Critical methods in International Relations: The politics of techniques, devices and acts', *European Journal of International Relations*, 20:3 (2013), pp: 596–619; Claudia Aradau and Tobias Blanke, 'The (Big) Data-security assemblage: Knowledge and critique', *Big Data & Society*, 2:2 (2015), available at: <https://doi.org/10.1177/2053951715609066>; Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction* (London: Routledge, 2020).

⁷⁷Hutchins, Cloppert, and Amin, 'Intelligence-Driven Computer Network Defense', p. 5.

and researched it, attempts to identify vulnerabilities in the target network. This initial information gathering can take the form of studying targets through sites, such as their public websites, following their employees on social media, and using other types of public information. Technical tactics such as scanning ports for vulnerabilities, services, and applications to exploit can also be used. This is all conducted to find the best entry point to access their target. In the second stage, *Intrusion/Weaponisation*, the adversary prepares the attack by analysing the data collected. Once the adversary has determined which methods to use and which malware or security vulnerabilities to leverage to create remote access, malware (often referred to as ‘the weapon’ in the industry) – such as a virus or worm – is tailored to one or more of the vulnerabilities discovered within the target networks in the first stage. When this is decided, the attack enters the third stage, *Delivery*. Here, the intruder ‘transmits the weapon to target’; they transfer the chosen malware to the victim, generally via email attachments, websites, or USB drives.⁷⁸

At the fourth stage, the attack can first be noticed within a network by a cybersecurity practitioner: *Exploitation*. Here, the vulnerabilities are used to deliver the malware code onto the system. Using the vulnerability detected in stage 1, the malware code built or decided upon in stage 2 is delivered into the system. When the malware is delivered, the malware program code is triggered, taking action on the target network to exploit the vulnerability detected in the second stage. In the fifth stage, *Installation*, the malware is installed. This means that the single system is infected, and the malicious activity has the potential to spread rapidly. Once installed, infections hide their existence from security devices through a variety of methods, including tampering with security processes in order to maintain access for an extended period of time. In the sixth stage, *Command and Control (C2)*, the malware is executed, enabling the intruder to have ‘hands on the keyboard’.⁷⁹ In this phase, persistent access to the target network and ‘lateral movement’ takes place, which means that the attackers can in theory move laterally to other systems and accounts without being detected to gain more leverage. Examples of C2 can be higher permissions, more data, or greater access to systems. Lastly, in the seventh and last stage, *Action*, the intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom. In order to successfully pull off the attack, they might cover their tracks through laying false trails, compromising data, and clearing logs to confuse and/or slow down any forensics team.⁸⁰

By setting out the steps malicious actors use to reach their goal, the Cyber Kill Chain structures how indicators of threat actor behaviour are built. The idea to structure threat actor behaviour into a chain guides analysts’ practice in their steps to detect malicious actors after a possible malicious indicator is detected. For example, if abnormal behaviour is detected in the first step of the Kill Chain, the corresponding aim of the defender is to observe and determine whether an attacker is poking around in the system to collect information. If so, focus is placed on preventing information disclosure and unauthorised access. If an intruder is however detected in the form of a compromised server (stage 5), the analysts’ first steps will be to isolate and stop the spread of the compromise (stage 6). Suggesting where the malicious behaviour which is detected in a network sits or where it is ‘down the chain’ guides the analyst as to where to look in a network to assess the damage and contain it. Similarly, where abnormal behaviour is detected in the chain informs how analysts determine the likely motivations and rationales for the attack: for example, if malicious behaviour is detected in a server rather than on an endpoint, this suggests that the malicious actor is seeking to maintain access to wider systems rather than exploiting a single target and then severing its command and control. The chain in this way shapes how indicators are interpreted,

⁷⁸ Ibid.

⁷⁹ Ibid.

⁸⁰ For different descriptions, cf. Digital, Data and Technology (2019) *Cyber Threat Intelligence in Government*; Leonardo Institute, *Incident response e IOC*, Leonardo cyber and Security academy, Day 1, student guide slides, 2022; Leonardo Cyber & Security Academy; Cyber Security Program, ‘Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts’. V.2.0, TLP_white, UK government, available at: <https://chrome-extension://efaidnbmnncnqpdjccglcfldmckaj/https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf>.

which indicators are searched for, how indicators are found, and lastly how these indicators are organised. After identifying malicious behaviour, the next step for analysts is to isolate it, protect the asset, detect the incident, respond, and recover.

Anticipating and predicting enemy operations: A vigilant intelligence logic

Cybersecurity practitioners' work hinges on the ability to map the threat landscape and the actors that operate within the networks that digital systems are connected to. In their efforts to detect malicious behaviour, cybersecurity practitioners collect as much data as possible from previous attacks to map the patterns of behaviour and malicious code in use. However, simultaneously malicious actors change the order of code and patterns of operation to make themselves harder to detect. The Cyber Kill Chain provides a structure for the data collected and informs how data is gathered from previous breaches and incidents to create an image of threat. Where risk management 'involves the creation of a common space of calculation through which planners can predict the likelihood of future events', cybersecurity as a form of vigilance, in contrast, 'assumes that the future cannot be known and that one must therefore be prepared for surprise.'⁸¹ Cybersecurity practitioners' goal is first to detect, not to predict events. Analysts practise vigilance through intelligence feedback loops, a process referred to as 'cyber threat intelligence', where the data from incidents and the analyses of the data shapes the prescribed security measures. Using the Cyber Kill Chain, analysts translate malicious patterns, abnormal behaviour, and indicators of threat identified into knowable and actionable intelligence within specific standardised layouts.⁸² Once set in a structure, other analysts can use the indicators found to locate similar behaviour. The cyclical and iterative structure of the Cyber Kill Chain methodology makes it, and those who use it, a self-propagating and seemingly indispensable resource, ensuring a market for the providers of the security measures delivered.

The Cyber Kill Chain sets out steps to guide analysts as to where and how to organise indicators detected of anomalous behaviour and potential threats. The organisation of indicators of compromise is the interoperable descriptions of previously identified behaviour or similar patterns identified and associated with malicious operations. Organising indicators of compromise helps detect patterns similar to previously detected malicious behaviour. Structuring the indicators after the methodology enables analysts to turn the detected indicators into threat knowledge. For example, if a customer of a cybersecurity organisation is hit by a multitude of emails that want the user to go to a page that is already registered as serving malicious codes, a signature is created that triggers on this type of traffic for all of the other customers. When talking about 'files and websites', malicious indicators could be the code itself, corresponding to a known bad file, which could be an IP address or domain name embedded in the code that is known to be malicious (maybe used by the malware to communicate with the command and control [C2] server). Importantly, signatures are not one specific thing; they can vary and stem from different sources, but they are intended to represent pre-identified known security threats in that they are signatures built on previously detected attacks. Indeed, despite aspirations for drawing generalisable signatures from specific attacks and contexts, when discussing signature detection with threat intelligence teams what is defined as a signature is debatable. A signature can be a series of actions and commands executed by the file when it is launched and is known to be at least suspicious. This could for example be a PDF that, when opened, runs a Python command and downloads a file from the Internet. A signature can

⁸¹ Andrew Lakoff, 'Real-time biopolitics: The actuary and the sentinel in global public health', *Economy and Society*, 44:1 (2015), pp. 40–59.

⁸² MITRE (n.d.). MITRE ATT&CKTM. [online] Mitre.org, available at: {<https://attack.mitre.org/>}; Dicken, 'A New Cyber Kill Chain Mnemonic', 2022, available at: {https://medium.com/@Jamie_Dicken/a-new-cyber-kill-chain-mnemonic-c0e9908db114}.

also be a portion of the code itself in which static malware analysis can reveal code routines that are very specific and known to be used by a specific threat actor. Who or what is identifying an indicator, and which signature becomes identified, holds politics and is socio-technically shaped.

While what defines a signature can vary, they are generally conceptualised as indicators of compromise: unique data points that verify the presence of malware or the exploitation of a service.⁸³ Indicators of compromise can be inferred, for example, from multiple failed credential authorisations from a user that is not defined as the main user of a system, traffic to a known IP that has previously been used to feed malware to a system, faulty logins, or traffic from a known malicious IP address. Indicators of compromise can be the presence of a certain file (name, hash sum, etc.), a specific process, logline in Domain Name Systems (DNS) request records, or specific network events. When indicators of compromise are detected several times in systems, a pattern is created which groups them together, and a threat (actor) is built.⁸⁴ Through providing a set methodology to organise indicators of compromise and combine them with threat intelligence, the Cyber Kill Chain provides analysts and defenders with a system to build an agglomeration of the different factors and ‘fingerprints’, which leads to the ability to name threat actors. For example, when Neel Mehta from the Google Threat Analysis Group (TAG) announced the attribution of the cyberattack WannaCry to Lazarus (an advanced persistent threat [APT] group), he did so with a tweet where he pointed at two very particular sections of codes, one in WannaCry and another one in a malware that was known to be from Lazarus, which were specific and the same in both samples.⁸⁵ Other analysts could then choose to use the specific algorithms to look for these codes, referring to ‘code similarity’, which means similar patterns, to detect if they had been exposed to the WannaCry attack. Mehta thus shared a signature that other analysts then used to search for similarities in their systems.

The Cyber Kill Chain is instrumental in shaping how threat indicators are identified and located, and how potential threat actors are targeted. Providing a supposed understanding of attacker practices, the Cyber Kill Chain logic informs the range of security measures that follow. The Cyber Kill Chain is presented to analysts as an instrument that allows them to think like the attacker⁸⁶ and permits them to trace the steps a malicious actor has taken based on where malicious behaviour is found in a network system.⁸⁷ For example, if a sort of delivery exploitation installation is detected, the Cyber Kill Chain guides analysts to look at the installation from an attacker perspective and shifts their attention to the next likely step of the attacker: command and control, as such leaving out other sorts of lateral movement within a network. By setting out the next steps to look out for, the many possibilities in a network, and how to stop the attacker in their path, ideally before reaching their end goal, the Cyber Kill Chain informs how the incident responder acts and reacts.⁸⁸ The methodology shapes how responders approach the incident, how they work to stop an incident,

⁸³Understanding Indicators of Compromise (IR108), CISA (2023), available at: <https://www.cisa.gov/news-events/events/understanding-indicators-compromise-ir108>.

⁸⁴Cf. Cybersecurity and Infrastructure Security Agency (CISA), ‘Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways’ (29 February 2024), available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b>.

⁸⁵Pierlugi Paganini, ‘Security experts link WannaCry ransomware to Lazarus group’, *Security Affairs* (16 May 2017), available at: <https://securityaffairs.co/wordpress/59139/apt/wannacry-ransomware-lazarus-group.html>.

⁸⁶Lauren Barraco, ‘Defend like an attacker: Applying the Cyber Kill Chain’, ATT Cybersecurity blog (2014), available at: <https://cybersecurity.att.com/blogs/security-essentials/defend-like-an-attacker-applying-the-cyber-kill-chain>.

⁸⁷Cf. Cyber Kill Chain. Lockheed Martin (2023), available at: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>; ENISA, Understanding the Increase in Supply Chain Security Attacks (2021), available at: <https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>; CISA, Federal Government Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems (November 2021 Cybersecurity and Infrastructure Security Agency) TLP: White, available at: chrome-extension://efaidnbmnfnkpiehdjffpihkpnkplhkpgohpjklpcjpcglcfindmkaj/https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

⁸⁸Ibid.

and the order of which data is collected post-incident. The Cyber Kill Chain demands practitioners introject a vigilant logic of pervasive threat and normalise ‘maliciousness’, making the practitioner an extension of the Cyber Kill Chain. The choices of action become predetermined by the Cyber Kill Chain, which limits and shapes the analyst space within the security assemblage.

When an intrusion into a network is discovered, analysts follow the most likely steps taken by the malicious actor to discover how far into a network they have come before they secondly trace lateral movements in the network to deny any further unauthorised attacker access to other systems. For example, a defender can stop or reroute outbound traffic away from the attacker by counterattacking the Command and Control (C2) pathways of the attackers. By contrast, if a malicious actor is inside the defender’s systems and has already started their infiltration process, the Cyber Kill Chain framework leads analysts to focus their efforts on containing the segmentation. When malicious behaviour is detected, the way the methodology sequentially processes the categorisation of attack and attacker leads analysts and defenders to make particular choices in practising cybersecurity which shape both how the threat is understood and the security measures taken in response. While the analysts choose what to fill into the model and not, they are shaped by the institutional norms and the imposition of this logic on their daily routine, and the routine reflects the security logic that informs their practice. The work that takes place to establish patterns of behaviour is continuous and experimental, with the dualism of (infra)structure and agency shaping the knowledge–practice dichotomy.⁸⁹

The Cyber Kill Chain perpetuates a governance apparatus where every potential threat actor is also a potential source of intelligence that generates intelligence on new potential threats. Structuring what data is searched for and how the data is organised, the Cyber Kill Chain shapes how the threat landscape is understood through a vigilant security logic. The way intelligence is coordinated and defence practised draws explicitly on existing frameworks for kinetic attacks, which perpetrate a practice that works to stop malicious actors before they reach their end goal.⁹⁰ While the threat in cyberspace holds similar descriptions to catastrophes in Aradau and Van Munster, being ‘unknown’ and ‘deemed potentially catastrophic, requiring security interventions at the earliest possible stage’,⁹¹ the logic of cybersecurity does not accept that the threat landscape is unknowable or that it cannot be specified.⁹² Rather, the cybersecurity practitioners work to organise attacker data to foresee the attacker’s next steps. Cybersecurity is thus not guided by a logic of (statistical) risks, nor is it about evaluating the chances of attack; rather, it implements an ongoing system of vigilance, detection, and preparedness for events whose likelihood is incalculable but nevertheless deemed probable and whose political and economic consequences can be detrimental.⁹³

The ongoing system of vigilance perpetuates the need for surveillance to obtain continuous new data, monitoring, and defence. To detect malicious behaviour in networks, the integration of new data is key. The Cyber Kill Chain is based on feedback loops where the continuous detection, incorporation, and analysis of data from detected breaches and attacks keeps the process iterative. This cyclical process necessitates constant monitoring of networks and input of analysts in order to ensure an updated threat landscape. The logic practised holds similarities to Foucault’s earlier reflection on society and defence where phenomena are seen as unpredictable when taken in themselves or individually, but when seen collectively they ‘display constants that are easy, or at least possible, to establish.’⁹⁴ The logic of vigilance in cybersecurity does not unfold in a pre-emptive

⁸⁹ Knorr Cetina K. Laboratory studies: the cultural approach to the Study of Science, in Jasanoff S (ed), *Handbook of Science and Technology Studies* (Los Angeles: Sage Publications, 1995), pp. 832.

⁹⁰ Hutchins, Cloppert, and Amin, ‘Intelligence-Driven Computer Network Defense’, p. 3.

⁹¹ Claudia Aradau and Rens Van Munster, *Politics of Catastrophe* (Oxford: Routledge, 2011).

⁹² Brian Massumi, ‘Potential politics and the primacy of preemption’, *Theory and Event*, 10:2 (2007), available at: {<https://dx.doi.org/10.1353/tae.2007.0066>}.

⁹³ Lakoff, ‘Real-time biopolitics’, p. 56.

⁹⁴ Michel Foucault, ‘*Society Must Be Defended: Lectures at the College de France, 1975–1976* (New York: Pantheon, 2003), p. 243.

manner by hindering harm or breaches before their occurrence.⁹⁵ Rather, cybersecurity is a vigilant monitoring logic that works to detect and mitigate events post facto. As an apparatus of vigilance, the Cyber Kill Chain structures a particular form of anticipation in an uncertain but potentially dangerous landscape. The practitioners' work to identify the series of steps an adversary must complete to achieve its objectives in a cyberattack is shaped by the Cyber Kill Chain, which informs how data is collected and analysed to make threats become known, presented, and understood. Promoting a security practice where indicators do not just represent singular events but rather a phased progression, the Cyber Kill Chain shapes how threats emerge and the analytical foresight that is meant to 'bridge the perceived gaps of security spaces and the temporal bridges between present and possible futures'. The methodology and infrastructures in use form how cybersecurity is practised, how data is structured, and how knowledge is produced, validated, and maintained.

Threat actors and with it the threat landscape are presented by industry experts as continuously changing, in both their tactics and patterns.⁹⁶ Security is then sold as the ability to detect patterns and create early-warning systems.⁹⁷ Infrastructure systems are promoted to detect future threats and put measures in place that can mitigate their occurrence. Among these tools are devices that alert analysts to suspicious patterns and events and trigger mechanisms that direct the attention of analysts. This form of cybersecurity is practised in two ways: signatures and anomalies. While signatures are created through mapping threat actor practice over time and across networks, anomalies are indicators that stand out from patterns of standard computer operations. These anomalies cannot be mapped, only anticipated and prepared for. To identify either signatures or anomalies means continuous surveillance of networks. Mapping malicious actors' operations as an active threat actor 'out there' constructs a specific view of malicious behaviour which continuously needs new data to secure against an unpredictable threat. The Cyber Kill Chain informs how threat and malicious actors are visualised through informing the correlations that are created between attacks, which actively builds an imaginary of the threat actors.⁹⁸ Bestowing a vigilant security practice on the work to anticipate and predict enemy operations, the Cyber Kill Chain (infra)structure creates a specific form of threat actor and practice. The vigilant security logic produces a specific form of threat which materialises as the 'doomsday cyberattack' it is described to hinder. This produced understanding of threat becomes transferred to the increased automation of AI security systems, wherein enmity becomes automated.⁹⁹ Not only do cyberattacks become automated through the Cyber Kill Chain,¹⁰⁰ enmity itself becomes predetermined and automated.

The challenge in the promise of automated security

The identification of indicators of threat is not just the result of technological progression or linear trajectories, nor simply the product of methodology, an overarching logic, legal construct, or politics in a set context. Rather, these practices are the result of ongoing configurations of discourses, practices, and technologies emergent from and within their interplay and shaped by the infrastructure of the cybersecurity organisations. The Cyber Kill Chain (infra)structure of surveillance necessitates a continuous collection, deciphering, and analysis of data. In practice, this means that, if starting at collection, when a breach is detected in a company an incident response team from a CERT is sent to the physical location or virtually to obtain the data. The data collected goes through evaluation before the network is cleaned and the breach is contained. When the data is collected, it is deciphered and analysed before it is integrated into the existing database organisations have

⁹⁵Lakoff, 'Real-time biopolitics.'

⁹⁶Katy Allan, 'The threat landscape is constantly changing,' *Cybermagazine.com* (12 October 2023), available at: <https://cybermagazine.com/articles/the-threat-landscape-is-constantly-changing>.

⁹⁷Michael Powell 'Detecting abnormal cyber behavior before a cyberattack,' *NIST* (5 March 2021), available at: <https://www.nist.gov/blogs/manufacturing-innovation-blog/detecting-abnormal-cyber-behavior-cyberattack>.

⁹⁸Suchman (2023).

⁹⁹Healey, 'The impact of artificial intelligence.'

¹⁰⁰Buchanan et al., 'Automating Cyber Attacks.'

of previous breaches. The new threat data collected is subsequently added to the internal database where it can be combined with data from other cyber threat intelligence firms and sometimes shared with other organisations or on platforms.¹⁰¹ Together, this data is used to build a picture of the threat actors and landscape to plan and direct security measures while guiding the practice and collection of new intelligence gathered in future incident responses.

When conducting incident responses, every analyst has their own ‘toolbox’ of software codes and programs they prefer to use. Built over time, the tools used impact how an analyst conducts incident response and become their trademark of sorts. The experience of having worked with certain cases and incidents is evaluated as essential in the ability to deal with new cases if they have similar traits. Similar to Donald MacKenzie and Graham Spinardi’s observation regarding the importance of tacit knowledge – knowledge that is possessed but not easily expressed – in building nuclear weapons, knowledge of threat intelligence is embodied in people, equations, and diagrams.¹⁰² Analysts, often with pride, proclaim how the unique tools and codes that they built themselves allow them to conduct specialised incident response.¹⁰³ How software is built and combined depends on the coders and specialists. While the analyst who conducts incident response follows the broader instructions of containing data post-breach, as mirrored in the Cyber Kill Chain, each individual uses the software and tools they are comfortable with. What one analyst might find crucial and worth taking note of, another practitioner might not choose to include. The work to collect and use intelligence, and the combination in which it is done, impacts the nature of an incident, how it is detected and contained, and the speed at which this happens. How the results are disseminated depends on the combination of software used to conduct analyses and the tacit knowledge of the analyst digesting the data. Yet the practice of collecting and analysing data to pre-empt future attacks is the same across cybersecurity organisations in that it follows the logic that data collection from breaches detected enables the stopping of future attacks.¹⁰⁴

The expertise of the analyst and their ‘toolbox’ shape how malicious actors are detected and analysed. While analysts underscore the importance of human agency, what technology is used in this process is equally important, making the process of threat detection inherently relational between the human and technology, neither functioning without the other in detecting the malicious behaviour. Each cybersecurity practitioner varies in how they search for data and how they structure data to create knowledge of malicious behaviour in the everyday.¹⁰⁵ While working with the same logic of collecting data from incident responses to understand the malicious behaviour, which techniques are used to build and analyse and make cyber threat intelligence depends on the analyst who detects the indicator and how they add this data into the data system for processing and analyses. As a cyber threat intelligence analyst explained, ‘data has to be analysed and combined with intelligence, or knowledge, by putting it into context and making it actionable for defence purposes’.¹⁰⁶

A tension is produced in the Kill Chain’s promise of a world that is predictable and uniform enough for machine learning to usefully engage with and the non-linear knowledge production of machine learning. Neither threat data nor machine learning is this uniform. The ability to gain knowledge about enemy capability depends upon and is impacted by the combination of tools,

¹⁰¹CISA (2021), Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.

¹⁰²Donald MacKenzie and Graham Spinardi, ‘Tacit knowledge, weapons design, and the uninvention of nuclear weapons’, *American Journal of Sociology*, 101:1 (1995), pp. 44–99.

¹⁰³Cf. Marco Ramilli Web Corner (n.d.), available at: <https://marcoramilli.com/>; Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, ‘Computer security incident handling guide’, *Computer Security Incident Handling Guide*, 2:2 (2012), pp. 1–47.

¹⁰⁴Cichonski et al., ‘Computer security incident handling guide’; ENISA (2021) Understanding the Increase in Supply Chain Security Attacks; CISA (2021) Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.

¹⁰⁵Siri Bromander, Lilly Muller, Martin Eian, and Audun Jøsang, Examining the Known Truths of Cyber Threat Intelligence - the case of STIX. In Proceedings of the 15th International Conference on Cyber Warfare and Security (ICWS 2020), pp. 493–XII.

¹⁰⁶Interview with Head of Research and Development, European cybersecurity firm, Europe, October 2019.

methods, and sources used to acquire the data after a breach, as well as by the in-built social knowledge and experience of the technician collecting the data. How technologies are used and how they are put together by the engineers and analysts who collect, organise, and digest the data shapes the intelligence produced. Each analyst's tacit knowledge impacts how incident response is conducted. This variation of practice and technology shapes how the threat picture is both presented and communicated. While the particularity of how data is structured and the analytical techniques used to collect and make intelligence differ internally between security organisations, the goal is to organise the data and feed it back into security practices. While variations exist, the methodology behind these practices is broadly consistent following the logic of the Cyber Kill Chain, where the findings in one stage of the intelligence loop feed into the next steps taken to collect data and pre-empt potential enemies.¹⁰⁷ Knowledge of malicious behaviour and actors is relational, contingent, and changes in the knowledge–practice dichotomy. The knowledge produced and patterns of malicious behaviour detected in these processes are inscribed into the technology used and developed, which in turn impacts the daily operations and operationalisation of cybersecurity. The logic of the Cyber Kill Chain informs the infrastructure that enables and maintains the socio-technical systems, as well as translating and visualising knowledge. The cybersecurity practitioners informed by the Cyber Kill Chain inform what data goes into the methodology and structure.

While cyber(in)security is a continuous experimental practice that works to build new security measures to both detect the enemy and find patterns of behaviour, the logic of the Cyber Kill Chain informs the logic of this practice. Cybersecurity is not a process that is a product of a 'macro-political rationality'; it is socio-technical, built through cybersecurity analyst practice. Cybersecurity is a continuous experimental practice that works to build new security measures to both hunt the enemy and find patterns of behaviour that enable the hunting of the enemy. The instruments that enable and maintain these systems affect, translate, and visualise a specific knowledge of threat which shapes how cybersecurity practitioners use data to predict future enemy behaviour.

Cybersecurity practitioners understand malicious actors as discoverable and knowable through data, where their action cannot be halted but contained and their impact reduced. With digital technologies' expansion, a high degree of automation and standardisation is built into security and response systems to stop malicious actions before damage has been caused.¹⁰⁸ A priority within the information security community is to enable the integration of all the stages of detection and defence into high-speed response platforms that can detect and block attacks as early as possible. In practice, this means that the searches for indicators of compromise become automated, while the search for the unknown becomes the focus of defence. In tandem with the automatisation of these processes, the literature on cybersecurity questions the consequence of this automation for security;¹⁰⁹ however, less attention has been given to the automation of enmity. The automated security practices are based on previously detected threats with the Cyber Kill Chain (infra)structure informing the automation. While the technology in use – the information sources and consequently the ways in which data is collected, presented, and used – changes continuously, the overarching logic that informs what data is collected and looked for stays the same. The automatisation of cybersecurity in practice is neither as new or revolutionary as the justificatory discourse of security professionals and many academics critical of emerging technology and security suggest.¹¹⁰ Continuous developments in technology create new modes and sites of cybersecurity practice,¹¹¹ yet these developments do not change the operational logic.

¹⁰⁷ENISA (2021) Understanding the Increase in Supply Chain Security Attacks; CISA (2021) Federal Government Cybersecurity Incident & Vulnerability Response Playbooks.

¹⁰⁸Tim Stevens, 'Knowledge in the grey zone: AI and cybersecurity', *Digital War*, 1:1 (2020), pp. 164–70.

¹⁰⁹Buchanan et al., 'Automating Cyber Attacks'.

¹¹⁰Ben Buchanan and Andrew Imbrie, *The New Fire: War, Peace, and Democracy in the Age of AI* (Cambridge, MA: MIT Press, 2022).

¹¹¹*Ibid.*

Knowledge of threat is socio-technically constructed in the interaction between analysts, the tools employed, and the institutional methodologies used to build knowledge. The logics that inform security practices, the relationship between epistemological convictions and practices, and the epistemic infrastructures they rest on enable visibility of the practice that takes place between actors and the infrastructures and as such facilitate the ability to question the knowledge produced, validated, and maintained of threat and security and the possible role of automation therein. More research is needed on the automation of the continuous and experimental work that takes place to build new security measures to both hunt the enemy and find patterns of behaviour.

Conclusion

I have here focused on the practice of cybersecurity making. Through critical engagement with the Cyber Kill Chain, this article has shown how the methodology informs cybersecurity practitioners' practice and subsequently offered insight into how cybersecurity practitioners think, practise, and work in the everyday. Rather than focusing attention on certain people speaking on behalf of the state or private sector about what threats in and from cyberspace are and what the necessary security measures are to entail, the unravelling of the Cyber Kill Chain has shown how the work to detect malicious behaviour and secure against attacks is continuous and iterative. Cybersecurity politics is not solely located in cyber weapons or in when and how a cyberattack is attributed; the everyday socio-technical making of cybersecurity holds politics in its ability to shape how and what becomes understood as a threat in cyberspace and, following that, how cybersecurity is practised as a modern security concern. The relational practice that takes place between actors and the infrastructures produced validates and maintains knowledge of threat and security. This practice makes politics; it excludes, includes, and conceptualises what is and is not dangerous, directly impacting the forms of security that are enacted.

Examining the 'making of' cybersecurity, this article has challenged the credibility of who and what is understood as a threat in cyberspace. By contributing to the critical examination and theorisation of cybersecurity in Critical Security Studies with an empirical contribution of how security unfolds within the cybersecurity organisation environment, cybersecurity is placed within the larger debates of Critical Security Studies and Science and Technology Studies. Questioning how cyber incidents become known, what constitutes a threat, and how these condition global security practices, this article has made visible the relationship between epistemological convictions, practices, and the epistemic infrastructures they rest on. Uncovering the continuous production of cybersecurity and how it may be changing expands the explanatory factors involved in understanding cybersecurity as a modern security challenge. The Cyber Kill Chain vigilant intelligence logic shapes the efforts of cybersecurity organisations to maintain and secure cyberspace. By identifying and recognising the security apparatus in regenerating the realities that it is trained to see, the ground is laid to reconfigure how threat and enemy are produced and the assumptions made of the potential consequences of security operations that are automated.

The findings in this article have several implications for the area of International Relations and Science and Technology Studies. First, it expands Critical Security Studies' engagement with expertise and practice in cybersecurity, by contributing to the practice-based understanding of knowledge of cyber (in)security through its provision and analyses of the everyday practice of security actors. By using methodologies to research security practices that can be hard to get access to, the article has secondly contributed to discussions on how to research 'closed worlds of knowledge'.¹¹² With the lack of access to everyday situated security practices,¹¹³ methodologies, handbooks, and white papers can serve as insightful tools to examine security practitioners' routinised security practices. Methodologies contain several tested rules and procedures for producing

¹¹²Suchman, 'Imaginarities of omniscience'; Dider Bigo, 'Shared secrecy in a digital age and a transnational world', *Intelligence and National Security*, 34: 3 (2019), pp. 379–94.

¹¹³Muller and Welfens, '(Not) accessing the castle'.

knowledge that structure and enable how threat is thought about, the operational environment, and how practitioners act within it. Critically examining methodologies and practice opens new possibilities for the study of security issues that are not easily accessible. Thirdly, contributing to the now substantial critical literature on cybersecurity within this journal and beyond with empirical research on the process of (in)security and (in)securitisation, the article has contributed to shifting focus away from the different knowledge pools that work to define cybersecurity towards the practice of the everyday making. States' and private sectors' current understanding of cybersecurity hangs to a considerable degree on the routinised practices of identifying, assessing, and acting on threats. Opening up the act of translating the complexities of the world into technical problems that can be rendered actionable and made into meaningful action, the article has uncovered a politics in cybersecurity practice. The relationship between threat and the institutionalised manifestation thereof is key for how (in)security is understood, for how threat comes to life, and the security practices that follow.¹¹⁴ The practice of making cybersecurity is deeply relational and takes place between actors, technology, and the infrastructures by which knowledge is produced, validated, and maintained. Attending to the dualism, future research is needed that assesses the contingency and change in the knowledge–practice dichotomy processes of cybersecurity making, as well as the security effects of translating and visualising knowledge of the operational environment through the Kill Chain and future automation of enmity.

Acknowledgements. Thank you to the five anonymous reviewers for their generous and insightful comments. Earlier versions of this paper have been presented at the 'State of the Art of Cybersecurity and Cyberconflict Research Conference', organised by the Center for Security Studies, ETH Zurich, Switzerland, 2018 and the EWIS 2019 Workshop, 'Global Reconfigurations of Science, Technology, and Security', Krakow, 2019. Thank you to all participants for their generous comments and encouragement. A special thank you to Erik Reichborn-Kjennerud for his work on the Kill Chain and many comments on drafts of this paper through the years. Thank you to Tim Stevens and Myriam Caveltly Dunn for your comments and conversations on this research project. Rebecca Slayton and Suman Seth have been generous and encouraging with comments on later drafts, for which I am truly grateful.

Funding statement. This research was supported by U.S. National Science Foundation Grant #1553069, LISS DTP, the Norwegian Fulbright Foundation, and the Norwegian Research Council of Norway Grant # 325297.

Lilly Pijnenburg Muller is a post-doctoral Fellow in War Studies, King's College London. This article was written during her Fulbright post-doctoral fellowship in Science and Technology Studies at Cornell University. She is the author of several articles on cybersecurity, expertise, knowledge production, and (in)security.

¹¹⁴Bigo, 'Security and immigration.'