Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision

Collier, Jamie

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Collier, J. (2018). Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision. *Politics and Governance*, *6*(2), 13-21. https://doi.org/10.17645/pag.v6i2.1324

COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 13–21
DOI: 10.17645/pag.v6i2.1324

Article

Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision

Jamie Collier [1,2]

[1] Department of Politics and International Relations, University of Oxford, Oxford, OX1 3UQ, UK;
E-Mail: jamie.collier@cybersecurity.ox.ac.uk
[2] Centre for Doctoral Training in Cyber Security, University of Oxford, Oxford, OX1 3PR, UK

Submitted: 23 December 2017 | Accepted: 28 February 2018 | Published: 11 June 2018

Abstract
In the context of globalisation and privatisation, an emerging body of literature has applied the concept of an 'assemblage' to international relations and security studies. This article will argue that an assemblage framework provides the best means for understanding the complex configuration of cyber security actors, given that contemporary cyber security practices do not conform to the traditional public-private and global-local distinctions used in security studies and International Relations literature. With the configuration of cyber security actors, and the relationships between them in constant flux, an assemblage framework provides a means for understanding the contested, dynamic and diachronic nature of contemporary cyber security provision. While the concept of security assemblages is favoured in this article, the process and context in which the term has traditionally been used cannot be blindly imposed on the issue of cyber security. This article will therefore propose a different model of how cyber security assemblages have developed and explain the implications this has on contemporary security dynamics.

Keywords
assemblages; cyber security; private security; state power

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

Cyber security is provided by a complex configuration of actors and institutions (Choucri, 2012). Non-state and non-traditional actors sit at the forefront of contemporary cyber security challenges: multinational corporations, hacktivist groups, intergovernmental organisations, and volunteer networks all provide (or threaten) security in some important way. Whether it be the historically prominent role of private actors in the development and growth of cyber-related industries, or the low barriers to entry, non-traditional actors have developed meaningful capabilities (Nye, 2011, pp. 113–151). As this phenomenon has emerged, the traditional distinctions used to capture international politics are becoming hazy: the lines between what is public and private, between what is global and local, are waning. If the Weberian notion of the state, whereby states possess a monopoly on the legitimate use of force and defence, has ever existed, its application to cyber security is increasingly limited. Cyber security, therefore, requires refreshed thinking.

The proliferation of security actors leads to important questions for international politics. The fragmentation of security provision has meant that states cannot take their traditional standing as the primary security provider in the international system for granted. Government actors may find not only their capabilities, but also their legitimacy as a security actor fundamentally questioned. The flight of power away from state structures has produced what Lucas Kello calls a 'sovereignty gap' where private sector firms and individuals can no longer take their government's ability to protect them for granted as they might have done in the face of other threats (Kello, 2017, pp. 160–162). Cyber security is of-

ten provided by a network of actors. Here, existing International Relations (IR) theories, concepts and paradigms provide useful tools in understanding the emerging models of security provision and their implications for international politics. Current academic literature has already addressed many of the relationships between actors that are central to cyber security provision, including public-private partnerships, (Carr, 2016; Dunn Cavelty, 2015; Dunn Cavelty & Suter, 2009) the role of civilian-led groups (Ottis, 2012; Sheldon & McReynolds, 2015; Suciu, 2015; Toomesaar & Ottis, 2010) and states' use of proxies (Collier, 2017; Maurer, 2015, 2018; Rattray & Healey, 2011; Schmitt & Vihul, 2014).

The diffuse model of security provision observed in many cyber security contexts lends itself naturally to theories and concepts that accommodate actors other than the state. This is not particularly novel or controversial within IR literature. Concepts such as actor-network theory and the military-industrial complex have helped to articulate such a world view where state institutions work alongside other actors (Balzacq & Dunn Cavelty, 2016). These concepts would therefore represent a natural home of sorts within the IR tradition for understanding contemporary cyber security provision.

Yet, the challenges associated with interpreting and understanding cyber security provision go beyond just the proliferation of security actors. The emergence of various cyber security actors has led to significant disruption that requires further consideration. Various actors compete for power and ownership of cyber security issues. First-order questions of what aspects of cyber security are 'public' or 'private' are still being contested and defined (Egloff, 2017). The incentive structures of different security actors often clash rather than converge (Carr, 2016). As state actors further develop, processes of securitisation often follow (Hansen & Nissenbaum, 2009). As defence institutions become increasingly interested in cyber security, the issue becomes further militarised, creating an atmosphere of insecurity and tension in the international system (Dunn Cavelty, 2012).

Further, the implications of such a proliferation of security actors cannot necessarily be captured with uniform theories and trends. In truth, various simultaneous and yet seemingly contradictory trends coexist, often unhappily. States are simultaneously undermining and being undermined by private actors. Private actors may compete against states while working directly with them in separate contexts. For example, whilst Apple has publicly challenged the UK governments stance on encryption and privacy (Hern, 2015), the US technology firm also works alongside the UK intelligence community with the UK signals intelligence agency, Government Communications Headquarters (GCHQ), providing Apple with information about vulnerabilities in their products (Cox, 2016).

Given the above, simply acknowledging the proliferation of security actors is not enough. Studying its implications, however, represents the altogether more interesting question. An emerging body of literature that applies the concept of an 'assemblage' to IR and security studies provides a useful first step. The security assemblage concept is one able to articulate the empirical realities and ongoing challenges of contemporary cyber security challenges. Section two proceeds to define the term and discuss how it relates to cyber security. Section three then develops this concept further by suggesting how the formation of cyber security actors and structures is different to the contexts in which the concept of a security assemblage has typically been deployed. Section four then presents concluding arguments and considers the practical applications of the assemblage term.

2. Cyber Security Assemblages

Refreshed thinking is required to better understand the provision of cyber security and the configuration of cyber security actors. Here, the term cyber security is defined as the security of the environment formed by physical and non-physical components and characterised by the use of computers and other networked devices. Cyber security actors, by definition, provide security in some capacity. Yet this does not mean that all actors strive to achieve a single, unitary concept of security. The prevalence of private actors means that cyber security is often provided by actors who prioritise other commercial objectives over security. Encryption disputes between the US government and technology firms show that different actors have altogether different motivations.

This makes the study of the different cyber security providers, and how they interact with one another essential. The concept of global cyber security assemblages provides a conceptual anchor that provides a means for further understanding these issues. The term provides a more appropriate concept for understanding contemporary cyber security contexts when compared to more traditional frameworks. The security assemblage term refers to new hybrid structures that are often simultaneously public and private, global and local. The use of the term is part of an emerging body of scholarship within IR literature that seeks to empirically assess complex structures where a range of different global and local, public and private security agents, interact, cooperate and compete to produce new institutions, practices and forms of security governance that cannot be captured neatly though the boundaries of nation states (Abrahamsen & Williams, 2011; Williams, 2016).

The assemblage concept therefore moves away from the traditional centre of the nation-state to multi-layered, networked configurations that are able to accommodate a range of entities including (inter)governmental, para-governmental, nongovernmental, and private organisations (Voelkner, 2013). The boundaries of an assemblage can be drawn in alternative ways to the traditional contours of national borders. They can be drawn to examine the provision of security within a territory but can also be used to examine security or

governance contexts that are inherently international. The issue of internet governance, for example, comprises a global assemblage of actors, albeit one dominated by US actors (Carr, 2014). Perhaps the most defining characteristic of the assemblage concept is therefore an accommodation of the forces of globalisation and a scepticism of rigid borders and distinctions. Of course, much of the above relates closely to other terms including actor network theory; indeed, the difference between the terms is one of emphasis, rather than kind (Acuto & Curtis, 2014) with the similarities and differences between the two concepts discussed in greater detail elsewhere (Acuto & Curtis, 2014; Müller & Schurr, 2016).

For the purposes of understanding cyber security provision, it is the notion of assembly and disassembly—where actors relinquish, transfer and develop capacities and functions—that is central to the added value of the assemblage concept. As security functions emerge and are captured by either public or private actors, actors assemble greater capabilities and responsibilities. As private actors increasingly take on strategic, ethical, and foreign-policy alignment issues that were previously outside their purview, they are assembling into more political actors. Conversely, as aspects of cyber security are increasingly regulated and managed by states, other aspects of private actors' capabilities and responsibilities are disassembling. Contemporary cyber security practices are replete with these instances of assembly and disassembly. Assemblage thinking therefore pays attention to the instability of security networks. While cyber security is provided by a vast array of actors, assemblage thinking also highlights the contestation related to the roles and responsibilities of security actors. In light of emerging and shifting actors, the point is not to demonstrate that states are stronger or weaker. Rather, the intention is to examine the complex configuration of actors that maintain contingent and multifaceted relationships with each other (relationships that cannot be captured by static and often state-centric theories). Cyber security is replete with global and local, public and private agents whose relationships are deeply competitive as well as cooperative, conflictual, and at times coordinated. While the concept of a security assemblage has been applied to cyber security in previous literature (Stevens, 2012, 2016, pp. 181–186), the argument for why and how the concept should be used and applied to cyber security remains underdeveloped—an imbalance this article hopes to correct.

These hybrid structures are clearly observed through contemporary examples with the cyber security of critical national infrastructure (CNI) in the UK a case in point. The vast majority of CNI is owned and managed by corporations—itself a broad church that includes a variety of actor types including not-for-profit community owned private limited firms, regional and UK-based firms, multinational firms (National Grid operates in both the US and UK for example, probing traditional global-local distinctions) and state-owned or quasi-state owned firms (the now approved Hinkley Point nuclear plant will be owned and managed by a combination of French-state majority owned EDF energy and Chinese state-owned China General Nuclear Power Corporation) (Ward, Pickard, & Stothard, 2016). As a collective, these corporations cannot neatly be categorised as 'private' given the variety of entities including the presence of both partially and fully state-owned entities. Corporations provide cyber security alongside a range of government departments, including GCHQ and its subsidiary, the National Cyber Security Centre (NCSC); the Cabinet Office, the various government departments that are largely responsible for infrastructure related to their department and related institutions such as the Centre for the Protection of National Infrastructure (Collier, 2016). All of these government entities have their own identities, agendas and motivations—a reality that means that 'the government' is not necessarily a coherent entity at all. Adding to the plethora of actors are various international organisations and multilateral bodies. Various actors work together within this cyber security assemblage, often in unusual ways. With Chinese-based firm Huawei providing communication equipment for CNI organisations, GCHQ employees will routinely monitor, take apart and inspect the equipment supplied (due to security concerns) at a centre that is itself funded by Huawei (Rifkind, 2013; Rosenzweig, 2013).

An assemblage approach also considers the normative agendas behind the traditional categories and distinctions used in IR literature. Pursuing assemblage thinking means paying attention to the relationships between a variety of actors and the forces that impel them to act in the way they do (Lisle, 2013). The process of assemblage formation is not neutral but deeply political. Different actors have clashing views on what aspects of cyber security should be 'public' or 'private' as well as where the boundaries of these distinctions lie. Returning to the UK example, the UK 2016 Cyber Security Strategy declared that market based solutions to cyber security have 'not produced the required pace and scale of change', meaning that 'Government has to lead the way and intervene more directly by bringing its influence and resources to bear' in a move that overtly seeks to increase the government's cyber security purview (HM Government, 2016). On the other hand, governments have also sought to relinquish both their authority and responsibility of cyber security issues within other contexts in order to avoid the backlash of security failings (Carr, 2016). This is also observed in recent US encryption disputes that reflect broader political disagreements about the agency afforded to different actors. Law enforcement organisations' interests in accessing intelligence on devices clash with technology firms who instead seek to protect their customers' data from government access, (albeit while simultaneously selling user data to other businesses and using it themselves for the purposes of targeted advertisements). Various government entities compete with each other for ownership of cyber secu-

rity and the tax revenue that accompanies the issue. Alternative visions of cyber security are proposed within such intra-governmental competition—the issue may be framed through a military, business or criminal prism depending on the government entity that seeks to capture the issue. These tensions are mirrored at the international level where various multilateral organisations compete for relevance on the issue including the North Atlantic Treaty Organization (NATO); the United Nations (UN) through the Group of Governmental Experts on Information Security; The European Union Agency for Network and Information Security (ENISA); the International Telecommunication Union (ITU); etc. It is this notion of contestation that further distinguishes an assemblage approach from other theoretical lenses that merely acknowledge the importance of units other than states or the increasingly blurry lines that exist between different types of actors.

3. The Cyber Security Assemblage Process

The arguments and theoretical developments of previous assemblage literature provides a rich intellectual backdrop in which the concept of a global cyber security assemblage can be developed. Assemblage thinking owes its intellectual roots to Gilles Deleuze and Felix Guattari's book that developed an ontology that includes assemblages as a core entity in light of the development of a number of concepts, including 'open systems, complexity, emerging and non-linear dynamics' in the global system (Deleuze & Guattari, 1987). For Deleuze and Guattari, an assemblage is a number of disparate and heterogeneous elements convoked together into a single discernible formation that displays some form of consistency and regularity while remaining open to transformative change, either through the addition or subtraction of elements, or the reorganisation of the relations between elements (Deleuze & Guattari, 1987). Manuel DeLanda subsequently developed the concept to develop a comprehensive theory of assemblages that challenges existing social analyses—often focused at either the individual or societal level (DeLanda, 2002, 2006, 2010).

Assemblages were subsequently considered in an IR and security studies context. Saskia Sassen has pushed back against the focus of globalisation literature on the withdrawal from the state in areas such as the economy as it often ignores the way states actively participate in setting up new structures. In short, globalisation is not a matter of outside private forcers eroding state power and sovereignty; instead, it is a process entwined with a restructuring of institutions and power relations through practices such as privatisation and regulation. Sassen used the assemblage term to articulate how globalisation has led to a new world order that challenges state-centric ontologies. The assemblage process described by Sassen involves three steps. First, a process of state disassembly occurs with traditional state functions taken up by private actors. This first shift therefore involves the transformation of the national state through the denationalisation or privatisation of national authorities and policy agendas (Sassen, 2008). Second, private actors develop new capacities that allow them to act at a global level. For Sassen, this primarily came through a new normative capacity, where private power is increasingly recognised as legitimate and accepted in the international system (Sassen, 2008). Third, a process of reassembly occurs where new actors and capabilities become part of global assemblages that are embedded in national settings but operate at a global scale (Sassen, 2008; Williams, 2016).

Although state-centric ontologies may no longer be coherent for Sassen in the context of globalisation and privatisation, they do at least represent an appropriate starting point in her analysis. States certainly played a decisive role in the formation of cyberspace. Yet, it is not the case that a process of state disassembly has occurred, where many cyber security functions that were once the purview of states have now been taken up by private actors. Instead, many cyber security functions have emerged over time as the internet and networked technologies have become increasingly integral to society. From a theoretical perspective, this means that while security assemblages provide an ideal lens for examining cyber security issues, Sassen's three-part assemblage process does not represent an accurate representation of the development of cyber security actors. Cyber security provision represents a curious counter-example to the ongoing trend of states outsourcing security and military functions to the private sector. In these other areas of security, traditional state functions are increasingly outsourced to contractors (McFate, 2014; Mumford, 2013; Singer, 2008). In a cyber security context, by contrast, states have, if anything, expanded their security role and acquired new functions—often challenging private sector governance in the process. It must therefore be acknowledged that the formation of cyber security assemblages contain their own idiosyncrasies.

Rather than Sassen's three-shift account, a five-shift process of assemblage formation is a more appropriate representation of the formation of assemblages in a cyber security context and is outlined below. Note, rather than to provide a comprehensive history of events, the objective here is to explain how various actors have developed and come together in the context of cyber security. The five shifts outlined below are therefore overlapping and not necessarily perfectly linear. Moreover, with 'cyber' such a broad catch-all term that in fact comprises a number of separate processes (including encryption disputes, disinformation campaigns, and internet governance), clearly not all issues that sit within the concept have developed in the same way (Shires & Smeets, 2017). The following five shifts therefore represent a broad generalisation, rather than a precise account of specific cyber security issues.

3.1. One: Development of Underpinning Technologies

The starting point for contemporary cyber security challenges does not begin with a coherent Weberian state model. To understand the starting point of contemporary cyber security challenges, it is necessary to understand the development of the two key technologies that underpin it: computers and computer networks.

It is difficult to confidently declare when the first computer was built, given the range of classifications. The reality is that a gradual process of incremental technological developments eventually led to the computers used today. For example, the first programmable computer was created by German Konrad Zuse in his parents' living room between 1936 and 1938; the Turing Machine, which became the foundation for theories about computing and computers, was first proposed by Alan Turing in 1936; and the Electronic Numerical Integrator and Calculator, which was the first electronic computer used for general purposes, was invented by John Presper Eckert and John Mauchly at the University of Pennsylvania in 1946.

The emergence of computer networks has a more coherent history. The first paper on switching theory was published in 1961 and by the late 1960s, plans of the ARPANET were being developed. By 1969, a Network Measurement Center at UCLA was selected to be the first node on the ARPANET and the first host computer was connected. Further design choices that have shaped the internet in its current form continued to be made into the 1970s.

For both the creation of computers and the internet, a number of actors were integral. Indeed, the starting point of computers and computer networks was an assemblage of different actors in its own right: academia was at the forefront in many of the decisive developments, yet both states and private sector firms also played vital roles.

3.2. Two: Development of the Private Sector

While initially an academic and military pursuit, commercial incentives drove the subsequent development of computers and computer networks. As APRANET was decommissioned in 1990, the obvious market opportunities of the technology led to an influx of private sector firms who were willing to invest significantly in research and development. This was seen most clearly in the US, where several US computer manufacturers, software vendors and internet service providers began to develop capabilities at a global level. Firms such as IBM, Microsoft and Apple grew rapidly during this shift.

These private developments have grown cyberspace exponentially, making it an integral part of society. With this growth, cyber security has become an increasingly important issue. With many of today's cyber security concerns emerging as a result of the private sector driven growth of networks, it is private actors, who have often been at the forefront of cyber security challenges.

Through their growth, private actors have also taken on a greater political role. Microsoft, for example, has created an international diplomacy team that participates actively in international fora in order to lobby the technology firm's perspective to policymakers from around the world. Google has likewise become involved in various political issues, ranging from protecting the identities of protestors (Halliday, 2012), to developing sophisticated measures to steer potential ISIS recruits away from the terrorist cell (Greenberg, 2016). Yet, whilst political, ethical and security challenges are thrust upon private actors, this does not mean they are always embraced or anticipated. Social media platforms, for example, have come under increasing criticism for failing to deal with disinformation campaigns. While many private actors are undoubtedly now political actors in a cyber security context, this does not, however, mean that they are necessarily competent in such a capacity.

3.3. Three: State Realisation

Although states played an integral role in the formation of the internet and the development of networks, governments on the whole have responded slowly to the cyber security challenges that have emerged as the private sector-led growth of cyberspace has developed since the 1990s (with certain military and intelligence agencies an exception). As computers and networks have become increasingly integral to modern life, states have gradually woken up to the importance of developing their own cyber security capabilities and are starting to invest significantly in the issue. The variety of government objectives has naturally led to divergence in the sort of developments that states have invested in. Authoritarian regimes have developed technology and infrastructure that prevents dissent and political protest (Deibert, 2013). Conversely, Western democracies have invested heavily in cyber security programs: the UK Government has significantly increased its cyber security spending to £1.9 billion in the period 2016–2021 (HM Government, 2016) while The Pentagon has requested $34.7 billion in cyber security funding between 2017 and 2021 (Capaccio, 2016).

3.4. Four: Emerging Hybridity and Contestation

Computers and computer networks, have always comprised an assemblage of actors that includes academia, governments, private sector firms and advocacy groups. These assemblages have become increasingly complex over time with a marked increase in the number of actors involved. The result is the emergence of increasingly hybrid structures—assemblages that embed a range of actors and transcend traditional global-local and public-private distinctions. For example, information sharing partnerships also exist with active participation from both corporations and government entities (NCSC, 2016). Such security arrangements are neither clearly public

or private security but instead an amalgamation of the two—one captured more coherently through an assemblage lens. The network of computer emergency response teams (CERT) also collaborate through the Forum of Incident Response and Security Teams (FIRST) network that combines national and international as well as public and private CERTS. At a more active level, hacker groups will assist and work with government actors in conducting offensive activities. Although these activities are often state-directed, hacker groups also operate independently—often representing a government's interests without explicit instruction or direction from government actors (Suciu, 2015). Such relationships have been presented as state-proxy relationships (Maurer, 2018) that, by definition, imply a certain binary relationship between two actors. However, an assemblage framework that accommodates what are often looser hybrid structures and naturally affords a greater agency to non-state actors provides a more coherent concept for capturing this empirical reality.

As these cyber security assemblages have grown and become more complex, they have also represented an increasing source of tension. Security assemblages are not necessarily harmonious or stable structures. Assemblages are often marked by competition and struggles for power and influence with different actors appealing to conflicting visions of what should be 'public' and 'private'. The history of cyber security related issues is replete with examples of these tensions. The state is a key protagonist in the vast majority of these disputes, becoming increasingly assertive and willing to challenge established private sector norms. The growth in their capabilities has therefore proved a notable source of tension and instability.

3.5. Five: Generativity

If the previous shift described the further development and growth of hybrid structures, comprised of a range of pre-existing actors, then the process of generativity points to the emergence of altogether new actors and processes.

Generativity, first espoused by Jonathan Zittrain, refers to the way in which the malleable nature of digital technologies (such as the internet) allows them to serve a variety of purposes, potentially providing a platform for innovation that may not have even been foreseen by their creators (Zittrain, 2006). Most computers are designed to be able to run software that is not written by the computer manufacturer or operating system publisher, thereby enabling a computer to be used for a range of processes that it was not initially designed for. For example, while Twitter was launched in 2006, computers built before this time would nevertheless be able to run the service provided they had an internet connection and internet browser.

The generative process goes beyond adaptations to hardware and software: it also leads to the emergence of altogether new actors and processes. The outbreak of the WannaCry ransomware worm provides a clear example of these other forms of generativity. Take a moment to consider the strange trajectory of events which led up to the WannaCry ransomware outbreak. First, the US National Security Agency (NSA) developed a number of exploit tools to be used for intelligence gathering and offensive cyber operations (Burgess, 2017). These vulnerabilities were then leaked by The Shadow Brokers (whose identity and intentions remain unverified) (Goodin, 2017), before going on to being used as part of the WannaCry ransomware deployed by North Korea (Volz, 2017). Here, a number of previously separate processes have become embedded: the NSA's development of cyber tools for intelligence gathering and offensive cyber operations led to both the development of a group that leaked these tools before a separate global breakout of ransomware.

Taking the response to malware for example, hardware and software vendors initially tried to protect their own products and services. Yet, it did not take long for an anti-virus industry to form (McAleavey, 2011). The assemblage of actors and processes involved with malware has expanded further still, including white-hat hackers, bug bounties and crypto-markets that illegally sell malware tools. Some of these emerging actors and processes will have further knock-on effects: the emergence of online illegal malware market will create new government police and cybercrime units. Cybersecurity is replete with examples of these sort of generative cascades that creates unstable processes where the implications of an emerging technology, in terms of its impact on the development and emergence of both actors and processes, is highly uncertain.

This five-shift model of security assemblage has implications for security provision today. While states were involved since the beginning of cyber security assemblage processes, they have significantly developed their political role and capabilities in the last decade. Throughout the emergence and development of cyber security assemblages, private actors have therefore enjoyed a significant degree of agency. The more recent further emergence of government actors therefore explains many of the tensions observed today. Whether it is encryption disputes, the increasing regulation of cyber security issues, or the knowledge of vulnerabilities that government actors withhold, states increasingly challenge, disrupt and often undermine the norms and practices that have previously been established amongst private actors. Government actors often 'argue through the past' (Stevens, 2016) evoking, for example, historical analogies regarding their previous ability to access the data of criminals and terrorist suspects through wiretaps in an attempt to make normative claims and justify why they should be able to access encrypted data. Here, states play on their broadly-perceived legitimacy within other security issues in the past to justify an expanded role in the context of cyber security in the future. As private ac-

tors have developed with relatively minimal state involvement since the 1990s, as the state now enters this space further, their previous lack of involvement makes their increasingly active role and their legitimacy as a security actor controversial and increasingly contested.

The diachronic nature of cyber security assemblages is therefore critical. The above analysis highlights the dynamic and highly unstable nature of cyber security assemblages. This constant to-and-froing of cyber security providers, as their power, roles and responsibilities shift, stands as a perennial feature in the development of cyber security assemblages. It remains unclear what aspects of cyber security will eventually be 'public' or 'private'. These contestations are therefore largely unresolved. Flat analyses of cyber security that neglect these ongoing processes therefore miss crucial components regarding the nature of contemporary security provision.

4. Conclusion

This article has introduced a framework for how the assemblage concept can be applied to cyber security. Yet specific cyber security issues have their own unique features—the dynamics of a US encryption assemblage are rather different to an international internet governance assemblage for example. Moving forward, the concept has greater utility when applied to specific case studies. Here, it can be used to examine the issues outlined above, with focus on how security actors interact and with consideration towards power relations, incentive structures and the practices that embed actors together.

The cyber security assemblage concept goes beyond merely recognising the importance of non-state actors or the interdependence between different actors. Crucially, the concept unearths and captures processes that are essential to contemporary cyber security challenges—the current disputes over what should be 'public' and 'private', the presence of contradictory trends as different security actors cooperate and compete with each other simultaneously, a consideration of the diachronic nature of cyber security provision, and the emerging hybridity of cyber security practices that cannot be neatly accommodated within traditional theoretical paradigms.

Thinking with assemblages is useful for understanding the security implications of particular configurations of actors. Discussions of cyber security have become lopsided. Analysis within security studies literature has focused primarily on issues including attribution, deterrence, and offence-defence balance with the dynamics between security actors often neglected. Yet, when considering the relationships between actors—the extent to which mutual understandings of 'public' and 'private' are settled or disputed, or whether there are clashing incentives between actors—these are issues that have fundamental implications towards the nature of security.

Whilst the arguments within this article are largely theoretical, the benefits of an assemblage approach also lie in its practical application. In a security environment where issues such as the use of contractors and diverse supply-chains present security concerns, understanding the network of security actors and how actors relate to one another is important. Thinking with assemblages can be used to understand shifts in actor's capabilities. As public and private actors seek to expand their remit, the assemblage framework provides a lens for capturing processes such as securitisation that present very real threats to individuals. Viewing the growth of private sector actors through an assemblage paradigm brings attention to the nascent challenges they face. As technology firms expand, their purview has increased exponentially as they are confronted with strategic, ethical and foreign-policy alignment challenges. Here, an assemblage approach brings attention to the profoundly political nature of many of these private firms.

There may also be useful comparative insights. Cyber security assemblages, however they are drawn, contrast starkly within different contexts. This provides insight into the different strategic challenges each government faces. Taking the US for example, the incentive structures of private actors often run contrary to the interests of the US government in relation to issues including encryption. A US cyber security assemblage is therefore characterised largely by disputes and friction between public and private actors. A Chinese cyber security assemblage, by contrast, contains a much greater level of harmony between different security actors. Such a comparison, therefore helps policymakers understand the challenges they face, and crucially the relative characteristics of the assemblages that they operate in.

Often underestimated, challenges related to security provision are critical to cyber security. The configuration of security actors, and how actors relate to one another, have fundamental implications for the nature of cyber security. The discipline of IR has much to offer in developing a fuller understanding of these issues. Thinking with assemblages provides a promising framework for advancing such an endeavour.

Acknowledgements

The author is grateful to the thoughts and comments provided by Nazli Choucri, Lucas Kello and Lucie Kadlekova. The author would also like to thank the three anonymous reviewers who engaged with an earlier draft of the article.

Conflict of Interests

The author declares no conflict of interests.

References

Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state*. Cambridge: Cambridge University Press.

Acuto, M., & Curtis, S. (2014). Assemblage thinking

and international relations. In M. Acuto & S. Curtis (Eds.), *Reassembling international theory: Assemblage thinking and international relations* (pp. 1–15). London: Palgrave Macmillan.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber security. *European Journal of International Security*, *1*(2), 176–198.

Burgess, M. (2017). Everything you need to know about EternalBlue—The NSA exploit linked to Petya. *Wired*. Retrieved from http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch

Capaccio, A. (2016). Pentagon seeks $35 billion to beef up cybersecurity over 5 years. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/articles/2016-02-29/pentagon-seeks-35-billion-to-beef-up-cybersecurity-over-5-years

Carr, M. (2014). Power plays in global internet governance. *Millennium*, *43*(2), 640–659.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Collier, J. (2016). Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. In M. Taddeo & L. Glorioso (Eds.), *Ethics and policies for cyber operations* (pp. 187–212). Cham: Springer.

Collier, J. (2017). Proxy actors in the cyber domain: Implications for state strategy. *St Antony's International Review*, *13*(1), 25–47.

Cox, J. (2016). GCHQ Has disclosed over 20 vulnerabilities this year, including ones in iOS. *Motherboard*. Retireved from http://motherboard.vice.com/read/gchq-vulnerabilities-mozilla-apple

Deibert, R. J. (2013). *Black code: Inside the battle for cyberspace*. Toronto: McClelland & Stewart.

DeLanda, M. (2002). *Intensive science and virtual philosophy*. London: Continuum.

DeLanda, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. London: Continuum.

DeLanda, M. (2010). *Deleuze: History and science*. New York, NY: Atropos.

Deleuze, G., & Guattari, F. (1987). *A thousand plateaus: Capitalism and schizophrenia*. London: University of Minnesota Press.

Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th international conference on cyber conflict* (pp. 141–153). Tallinn: NATO CCDCOE.

Dunn Cavelty, M. (2015). Cyber-security and private actors. In R. Abrahamsen & A. Leande (Eds.), *Routledge handbook of private security studies* (pp. 65–71). Abingdon: Routledge.

Dunn Cavelty, M., & Suter, M. (2009). Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179–187.

Egloff, F. (2017). Cybersecurity and the age of privateering. In G. Perkovich & A. E. Levite (Eds.), *Understanding cyber conflict: Fourteen analogies* (pp. 231–247). Washington DC: Georgetown University Press.

Goodin, D. (2017). NSA-leaking shadow brokers just dumped its most damaging release yet. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet

Greenberg, A. (2016). Google's clever plan to stop aspiring ISIS recruits. *Wired*. Retrieved from https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits

Halliday, J. (2012). Google introduces face-blurring to protect protesters on YouTube. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2012/jul/19/face-blurring-technology-youtube-protestors

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Hern, A. (2015). Apple calls on UK government to scale back snoopers charter. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/dec/21/apple-uk-government-snoopers-charter-investigatory-powers-bill

HM Government. (2016). *National cyber security strategy 2016–2021*. London: HM Government.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT: Yale University Press.

Lisle, D. (2013). Energising the international. In M. Acuto & S. Curtis (Eds.), *Reassembling international theory* (pp. 67–74). London: Palgrave Macmillan.

Maurer, T. (2015). Cyber proxies and the crisis in Ukraine. In K Geers (Ed.), *Cyber war in perspective: Russian aggression against Ukraine* (pp. 79–86). Tallinn: NATO CCDCOE.

Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press.

McAleavey, K. (2011). The birth of the antivirus industry. *Infosec Island*. Retrieved from http://www.infosecisland.com/blogview/15068-The-Birth-of-the-Antivirus-Industry.html

McFate, S. (2014). *The modern mercenary*. New York, NY: Oxford University Press.

Müller, M., & Schurr, C. (2016). Assemblage thinking and actor-network theory: Conjunctions, disjunctions, cross-fertilisations. *Transactions*, *41*(3), 217–229.

Mumford, A. (2013). *Proxy warfare*. Cambridge: Polity.

National Cyber Security Centre. (2016). *Cyber security information sharing partnership (CISP)*. Retrieved from https://www.ncsc.gov.uk/cisp

Nye, J. S., Jr. (2011). *The future of power*. New York, NY: PublicAffairs.

Ottis, R. (2012). *Lessons identified in the development of volunteer cyber defence units in Estonia and Latvia*. Tallinn: NATO CCDCOE.

Rattray, G. J., & Healey, J. (2011). Non-state actors and cyber conflict. In K. M. Lord & T. Sharp (Eds.), *Americas cyber future security and prosperity in the information age* (pp. 65–86). Washington, DC: Center for a New American Security.

Rifkind, M. (Ed.). (2013). *Foreign involvement in the critical national infrastructure: The implications for national security*. London: Intelligence and Security Committee.

Rosenzweig, P. (2013). The United Kingdom and Huawei. *Lawfare*. Retrieved from https://www.lawfareblog.com/united-kingdom-and-huawei

Sassen, S. (2008). *Territory, authority and rights: From medieval to global assemblages*. Princeton, NJ: Princeton University Press.

Schmitt, M. N., & Vihul, L. (2014). Proxy wars in cyberspace: The evolving international law of attribution. *Fletcher Security Review*, *1*(2), 53–72.

Sheldon, R., & McReynolds, J. (2015). Civil-military integration and cybersecurity: A study of Chinese information warfare militias. In J. R Lindsay, T. M. Cheung, & D. S. Reveron (Eds.), *China and cyber security* (pp. 188–222). New York, NY: Oxford University Press.

Shires, J., & Smeets, M. (2017). The word cyber now means everything—And nothing at all. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2017/12/01/the_word_cyber_has_lost_all_meaning.html

Singer, P. W. (2008). *Corporate warriors: The rise of the privatized military industry*. Ithaca, NY: Cornell University Press.

Stevens, T. (2012). Norms, epistemic communities and the global cyber security assemblage. *E-International Relations*. Retrieved from http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage

Stevens, T. (2016). *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Suciu, P. (2015). How hackers work like a PAC. *Fortune*. Retrieved from http://fortune.com/2015/08/31/how-hackers-work-like-a-pac

Toomesaar, K., & Ottis, R. (2010). From pitchforks to laptops: Volunteers in cyber conflicts. In C. Czosseck & K. Podins (Eds.), *Conference on cyber conflict* (pp. 97–109). Tallinn: NATO CCDCOE.

Voelkner, N. (2013). Tracing human security assemblages. In M. B. Salter & C. E. Mutlu (Eds.), *Research methods in critical security studies* (pp. 203–206). Abingdon: Routledge.

Volz, D. (2017). U.S. blames North Korea for 'WannaCry' cyber attack. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

Ward, A., Pickard, J., & Stothard, M. (2016). Hinkley go-ahead after 'national security' safeguards. *Financial Times*. Retrieved from https://www.ft.com/content/0cde26b6-7b66-11e6-b837-eb4b4333ee43

Williams, M. C. (2016). Global security assemblages. In R. Abrahamsen & A. Leande (Eds.), *Routledge handbook of private security studies* (pp. 131–139). Abingdon: Routledge.

Zittrain, J. (2006). The generative internet. *Harvard Law Review*, *119*(7), 1974–2040.

About the Author

Jamie Collier is a Cyber Security DPhil Candidate based at the Department of Politics and International Relations, and the Centre for Doctoral Training in Cyber Security, University of Oxford. Within Oxford, Jamie is a Research Affiliate with the Centre for Technology and Global Affairs, and a Research Associate with the Changing Character of War Programme. Jamie was based in the US as a Cyber Security Fulbright Scholar at the Massachusetts Institute of Technology during 2017. Jamie also works with Oxford Analytica on cyber security issues and has previous work experience with the NATO Cooperative Cyber Defence Centre of Excellence and PwC India.