THEME SECTION

Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interactions

James Shires, Harvard Kennedy School

Abstract

Cybersecurity can be defined as the prevention and mitigation of malicious interference with digital devices and networks. This broad definition leaves crucial questions unanswered, including the question of how prevention and mitigation take place, the question of against what or whom cybersecurity is directed, and the question of scope: whether the digital devices and networks belong to individuals, organisations, certain states, or even the entire world. These questions bedevil cybersecurity research, as both scholars and practitioners move deftly between them according to their priorities and audiences. This article addresses this issue by providing a general theoretical framework for thinking about cybersecurity in international politics. The article identifies three conceptions of cybersecurity. The first is ***national cybersecurity****, where the networks to be protected are primarily those within a state's territorial boundaries; the most concerning malicious actors are primarily other states, and the means involved are the traditional tools of international statecraft, including diplomacy, laws, intelligence, and military force. In the second,* ***commercial cybersecurity****, the networks to be protected are those of profit-making organisations, which may be sub- or trans-national; malicious actors are any that affect the function and purpose of the organisation, usually framed in financial terms; and the means involved centre around calculations of risk, liability, incident prevention, and reputation management. In the third,* ***individual cybersecurity****, the devices and networks to be protected are those owned by the individual; malicious actors are those that would infiltrate those devices to cause harm to the individual or their possessions; and means involved are the improvement of privacy rights, awareness, and communications security. The article concludes that only by understanding both family resemblances and family arguments between these three conceptions can we establish dialogues between the various communities working on urgent cybersecurity problems.*

James Shires, "Family Resemblance or Family Argument? Three Perspectives on Cyber Security and Their Interactions," *St Antony's International Review* 15. no. 1 (2019): 18-36.

Cybersecurity can be defined as the prevention and mitigation of malicious interference with digital devices and networks. Although no definition captures all aspects of what could be termed cybersecurity (for example, this definition specifically excludes non-malicious or accidental events), this definition highlights the core concerns of many policy and academic communities.[1] Within this broad definition, scholars have identified several distinct perspectives, with two common threads.

The first is a distinction between national or state-based cybersecurity and what Ronald Deibert calls 'human-centred' cybersecurity.[2] Although Deibert is not the only proponent of the latter view, his work represents perhaps the most sustained attempt to distinguish the cybersecurity of individuals from the cybersecurity of the states in which those individuals reside. Unlike other political science and international relations literature that focuses on cybersecurity issues within and between states, Deibert forcefully argues for a reorientation of cybersecurity towards a cosmopolitan understanding based on liberal personhood and human rights.

The second thread also begins with national cybersecurity but contrasts it instead with what I term 'commercial' cybersecurity: the approach to cybersecurity taken by profit-motivated organisations seeking efficient means of maximising investment and protecting assets. This approach is characterised by calculative methods of risk management, seeking to quantify and then integrate cybersecurity risks into existing corporate structures and use economic solutions such as insurance, auditing, and outsourcing. Again, many scholars have written about the difficulties inherent in aligning national and commercial perspectives on cybersecurity, notably in Madeline Carr's account of public-private partnerships in the UK.[3]

These two threads are rarely woven together. Although Deibert recognises the importance of private companies for both national and individual cybersecurity—including through ethical imperatives and reputation-motivated corporate social responsibility—their cybersecurity risk management practices are not a major theme of his work. Similarly, while Carr elsewhere locates state approaches to cybersecurity within a wider human rights framework,[4] this is not emphasised in her work on public-private dynamics.

In contrast, this article focuses on the interaction between all three perspectives on cybersecurity, identifying both contradictory and complementary elements of this interaction. These complex

relationships bedevil cybersecurity research, as both scholars and practitioners move deftly between the three perspectives according to their priorities and audiences. This article argues that only by understanding both family resemblances and family arguments between these three perspectives can we establish dialogues between different communities working on urgent cybersecurity problems.

The term 'family resemblance' is drawn from Wittgenstein's work on foundational concepts in analytic philosophy.[5] Wittgenstein argues that different uses of the same word (e.g., 'cybersecurity') do not necessarily need a common core of meaning, an approach diverging from much positivist social science.[6] Instead, uses bear merely a family resemblance, with similar characteristics between most particular instances, but enough flexibility that some have no overlap whatsoever. This flexibility is partly why scholars have argued that 'cyber' fits Walter Gallie's definition of an 'essentially contested concept.'[7]

Wittgenstein's concept of 'family resemblance' also seeks to pinpoint an instinctive aspect of conceptual similarity: knowing that two things are alike (like brother and sister) without necessarily knowing why. This ability stems from immersion in a broader form of life and set of shared practices; in this case, the set of shared practices known as cybersecurity expertise.[8] For this article, the most relevant implication of a practice-based view is that the three perspectives analysed here are not different theoretical levels of cybersecurity, organised hierarchically according to scope from individual to commercial, and then to national. Instead, they are different practical worldviews, each incorporating universal and particular value judgments and factual claims. In this conceptual family, there is no suggestion that one perspective is more foundational than the others.

The National Perspective

For the purposes of national cybersecurity, the emergent geography of the internet—as information flowing around the globe according to technical protocols deciding the most efficient path for individual packets of data—is forced into an older statist geography, with territorial boundaries determining possession and jurisdiction.[9] Many scholars frame state perspectives on national cybersecurity as fitting into two broad camps, with non-Western perspectives focusing more on information flows than network protection.[10] The situation is in fact far more complicated, with almost as many versions of national cybersecurity as there are states.[11] Consequently, despite many differences between states

in cybersecurity, this section seeks to identify their common elements in contrast to commercial and individual cybersecurity.

All states attempt, in different ways, to reconcile global internet communications with national borders. This distinction is not purely between physical geography for states and sociotechnical construction for the Internet. On one hand, the contours of the Internet, its chokepoints and highways, are shaped by numerous physical factors. On the other, state borders are themselves defined socially, through prior ideas of nationhood and political community, and technologically, based on evolving means of cartography and communication.[12] This joint social and technological construction is equally important for 'neutral' territories, such as space and international waters (crucial for the satellites and cables that enable internet communication). National cybersecurity interprets cyberspace from the state perspective, seeing servers, networks, and users as located within one or another territory, and flows of information as crossing state boundaries, transiting from one jurisdiction to another.[13] Consequently, the primary objects of protection are networks—and information, organisations, and functions reliant on those networks—within a state's borders.[14]

National cybersecurity privileges some malicious actors over others. Although scholars have argued for an overall diffusion of power from state to non-state actors as part of the growth in digital technologies and Internet communication, national cybersecurity sees other states as the key threats.[15] This is partly a matter of resources: adversarial states have the capability to build far more sophisticated forms of malicious software, and mount more sustained campaigns against digital infrastructure, than non-state actors such as terrorist groups.[16] However, sophistication is not always equated with success, and non-state groups could have a large—if brief—impact on state functions. The deeper reason for states seeing other states as the main threat is a shared belief that the state system is the basic dynamic of cybersecurity politics, echoing older critiques of realism as being a more accurate description of what statesmen believe than how the international system functions.[17] Cybersecurity is seen by academics and policymakers in terms of hegemony and great power competition, as what Fiona Adamson calls 'methodological nationalism' pushes even nuanced analyses of state cyberattacks towards questions of hegemonic control of the internet.[18] This theoretical predisposition is matched by bureaucratic inertia: existing national security leaders and organisations, imbued with a culture of state threats, find it easier to justify their actions and competition for resources by appealing to the threat of familiar

adversaries.[19]

National cybersecurity also seeks to *influence* cybersecurity through the application of existing tools of statecraft. The long-running debate over the possibility of cyber-deterrence is a good example of this, as nuclear analogies have been dissected to locate similarities and differences for cyber 'weapons.'[20] Similarly, scholars have concluded that coercive action more broadly is difficult if not impossible 'in cyberspace,' conceived as a distinct military domain.[21] However, existing tools of statecraft are not limited to the coercive approaches of deterrence or compellence: states have proved equally adept at using international law (in the Tallinn Manual on the rules of armed conflict), bilateral and international diplomacy (in US-China agreements on cybercrime and the ongoing, bifurcating (in the UN Group of Governmental Experts [GGE] in cybersecurity), and infrastructural power, such as standard setting and technical control.[22] Finally, intelligence agencies have been the historical locus of cyber power for most states, meaning that cybersecurity practices are fundamentally structured in terms of intelligence collection and analysis as much as, if not more than, through military doctrine.

The overall theme of this approach has been characterised by scholars in similar ways. For Lucas Kello, it forms a domain of 'unpeace,' where relations are conflictual yet do not meet widely accepted definitions of war.[23] For Richard Harknett, cybersecurity is a matter of "persistent engagement *under the threshold* of armed conflict."[24] Persistent engagement—forming the basis for the first US Department of Defense cyber strategy that moves away from deterrence—is nonetheless strategically motivated and competitive.[25] In this view, it may be desirable to act directly against an adversary's digital presence (for example, by conducting coordinated information campaigns or digital sabotage), rather than coercing another actor through threat of 'cyber-force,' or shaping their desires through normative convergence.

While these scholars argue that new understandings of cyber power are therefore required, their suggestions bear a surprising resemblance to existing critical theories of power, where persuasion and what Foucault calls 'governmentality'—seeking control of conduct, rather than direct influence—are the primary means of influence.[26] They also echo Foucault's view of power as 'capillary,' with Harknett explicitly suggesting that the US military should embed itself in adversary networks wherever possible, seeking small and frequent forms of influence. Consequently, critical theories—where even peacetime is seen as competitive and adversarial in many ways—could be a useful alternative way to understand the 'under-the-threshold' character of state actions

taken in the name of national cybersecurity.

Justin Joque takes this argument further by suggesting that what he calls "cyberwar," as conducted by states, can be understood as a type of 'deconstruction' in the Derridean sense.[27] Joque argues that while Derridean deconstruction seeks to destabilise binaries of fixed meaning in natural language texts (including that of author/reader), malicious cyber activity destabilises the logical flow of programming language texts from the intended purpose of a program to its execution. By doing so, it inserts another intention (author) into the system. While Joque's conclusions on the political potential of such destabilisation are beyond the scope of this article, his provocative contribution to conceptions of national cybersecurity is that this interruption is ultimately self-defeating. By revealing the fragility of digital critical infrastructure, what he calls the 'war machine' of the state (its intelligence and military apparatus) undermines its claims to reliable action both in and outside its borders.

Importantly, this is not merely the repetition—in a different theoretical vocabulary—of the trade-off between secretly discovering and retaining vulnerabilities for offensive action, and communicating those vulnerabilities widely to secure networks. That trade-off is well illustrated by the development of the US Vulnerabilities Equities Process (VEP) in the context of the 2017 release of zero-day exploits from US intelligence agencies by adversarial hackers associated with Russia.[28] Joque's argument goes deeper: it suggests that the logic of strategic military action in general is undermined by the increasing prevalence and exploitation of digital vulnerabilities in military and critical networks, casting doubt on the potential for force (cyber or otherwise) to achieve strategic gains rather than descend into chaos. In other words, cyberwar becomes action in the absence of strategy not through lack of creativity or vision, but because strategising itself is undermined by a position of unpredictable vulnerability.

In sum, despite the significant differences between different conceptions of cybersecurity in different states and regions, there remains a common perspective that can be identified as national cybersecurity based on similar understandings of power, territory, and technology. This perspective views the object and means of cybersecurity through a territorial lens, closely associated with military and intelligence capabilities. While for some scholars this association leads to new areas of non-war competition, for others it begins to dissolve the classical foundations of military strategy.

The Commercial Perspective

Commercial cybersecurity treats organisations rather than states as the main reference point for cybersecurity. Organisations can be theorised in several ways, from thin interpretations as sets of formal and informal contracts between individuals to much thicker understandings of the organisation as a Bourdieusian field, complete with its own taken-for-granted practices (doxa) and structures of symbolic capital.[29] These thicker interpretations highlight the fact that, although economic calculations are the basis for commercial cybersecurity, there are many other factors at play. For example, organisational cultures and individual reputations may mean that specific cybersecurity initiatives are embraced or resisted.

In this section, I use corporations (public and private companies) as the prime examples of organisations. Although they are nominally subject to the laws of the state in which they are headquartered, contemporary capitalist structures mean that many organisations—from small start-ups to massive multinationals—are able to proactively shape their relationships to states, including tax structures, headquarters, and legal requirements, in ways that give them the greatest financial advantage and decision-making flexibility. Organisations are thus both sub- and trans-national: sub- because they lack the 'hard' power of states, but trans- because their networks stretch across state borders.[30]

Commercial cybersecurity is fundamentally structured in terms of risk management. Organisations, as economic entities, seek the most efficient means of maximising investment and protecting assets.[31] Cybersecurity risks—once they have emerged into an organisation's consciousness from back office IT functions—are therefore framed as risks to profit (in this way, they can be accidental as well as malicious, although such events are outside the scope of this article). The usual organisational response to these risks is to quantify and integrate cybersecurity risks into existing corporate structures: for example, by appointing a Chief Information Security Officer as a board or near-board level post. However, cybersecurity risks are not easily quantified, partly due to their intangible consequences outside a clear profit impact (e.g., reputational damage) and partly due to difficulties in predicting large scale events such as data breaches.

The profit motive means that cybersecurity is also an opportunity. As well as the growth of a new industry specialising in protective solutions, organisations seek ways to govern and exploit cybersecurity risks through insurance, auditing, and outsourcing.

This evolution can be theoretically understood as a productive risk *dispositif,* which colonises ever further geographically and into the future, endlessly expanding because there are always residual risks.[32] In cybersecurity, organisational focus has moved from the network perimeter, to key assets, to endpoints, to cloud storage and supply chains, and so on in an infinite logic where once one risk has been commodified and mitigated, another is identified.

However, commercial cybersecurity is not strictly limited to profit-making organisations. Non-profit entities, government agencies, and international organisations can also adopt a commercial perspective insofar as they see cybersecurity as a question of economic investment and risk. Their very different purposes (for example, civil society organisations often promote individual cybersecurity, while international organisations create norms and institutions adjudicating between national concerns) mean that commercial cybersecurity overlaps with these other perspectives.[33]

How does commercial cybersecurity relate to national cybersecurity? We can use the framework of family resemblances and arguments to illuminate two contrasting aspects of this relationship. First, there are family resemblances between commercial and national cybersecurity, as states are dependent on private sector organisations in many aspects of cybersecurity. In defensive arenas, states contract companies to manage and protect their networks. They also use companies to supply 'offensive' tools, seeking to break into others' networks in conjunction with military or intelligence services.[34] These companies are integrated into the state very tightly, with individuals moving between the two regularly. More widely, the state controls the economic rationale and operating environment for these companies, creating what has been called a 'cyber-military-industrial complex.'[35]

There is also a family resemblance in the professional practices of cybersecurity experts in both commercial and national settings. The growing industry providing 'threat intelligence' to organisations claims to function in a similar manner to traditional national security intelligence analysis, with a revolving door between the two. In both environments, threat intelligence analysts track the tools, tactics, and procedures (TTPs) and indicators of compromise that could be used to mitigate future incidents. They also perform 'attribution,' finding links between a specific actor and past incident, or, as Thomas Rid and Ben Buchanan put it, asking the question, "who did it?"[36]

However, different parts of the industry diverge in their attribution practices. Some companies, especially in the US, explicitly name a familiar roll call of adversarial state actors, sometimes on a very

speculative basis.[37] For others, revealing the identity of malicious actors is less of a concern than tracking the evolution of a 'campaign' or grouping them into broad categories (hacktivist, cybercriminal, etc.). In many cases, traditional identification (name and/or nationality) is not required for these purposes. Furthermore, attribution is rarely relevant for incident response. For example, in one of the most economically damaging recent cyberattacks, the 2017 malware called NotPetya that temporarily halted operations of shipping company Maersk, the technical characteristics of the malware were crucial for its attribution: it was designed to look like ransomware built for profit, but was later attributed by the US and other states to the Russian military.[38] However, this attribution was extremely low priority for Maersk and other affected organisations seeking to limit their economic losses, as what mattered was understanding how the malware functioned, rather than who made it.[39] Overall, as Myriam Cavelty concludes in her comprehensive mapping of cyber-threat representations, "it is neither natural nor inevitable that cybersecurity should be presented in terms of power-struggles, war-fighting, and military action."[40] This family resemblance is instead the result of sustained shared practices and congruent purposes.

Outside the role of economically-motivated organisations in the national security apparatus, the mammoth social media and advertising companies that constitute the basis of most individuals' experience of the Internet worldwide generate more of a family argument than family resemblance. Especially after the Snowden disclosures, such companies have sought to portray themselves as opposed to national security overreach, and even engage in 'diplomatic' lobbying to this end.[41] They also portray technological developments, such as end-to-end encryption, as a way to avoid government pressure to disclose information.[42] Nonetheless, these companies are often seen by governments as elements of 'national power' due to their worldwide prestige and economic weight, as well as specific contributions to intelligence collection.[43]

Although the US has so far been the locus of most of these internet giants (and the lack of a similar 'regional champion' for the EU has been taken as evidence of its weakness), Chinese companies are beginning to adopt a similar role, encountering the same advantages of national champions in terms of market access and state support, and similar disadvantages in terms of distrust from other states.[44] The repeated attempts by the UK to navigate between US security pressure and perceived economic benefits by closely scrutinising the source code of Huawei systems demonstrate this contradictory dynamic. For international

behemoths like Huawei and the US internet giants, the concept of commercial cybersecurity at times aligns and at other times contradicts that of national cybersecurity.[45]

A family argument also exists between national and commercial cybersecurity in the domestic, as well as international, sphere. Even in the best case scenario where states and private companies seek the same thing—for example, defence against agreed adversaries, calculated in a risk management framework for profit—commercial and national perspectives diverge in three main ways. First, there is a tension in perceived power dynamics: corporations see that states hold much information to which they do not have access, while states see corporations as quietly benefiting from their unappreciated protection. In the US, this is exacerbated by an East Coast/West Coast split, where an entrepreneurial Silicon Valley culture that imagines the almost total absence of government has been characterised by Stanford academics as a national security threat.[46] Second, when states seek to encourage information sharing—the most basic level of cybersecurity cooperation—between companies, they encounter reluctance due to fear of losing a competitive advantage or sharing damaging or IP-protected information.[47] The exceptions are where trust networks develop and there are sufficient shared incentives and resources: for example, through sector-based Information Sharing and Analysis Centres (ISACs).

The third and final difficulty in this partnership is the tendency for organisations to 'hack back,' leading to both escalation dynamics and risks of confusion.[48] Although the extent of the hack-back phenomenon is unclear, some participants have provided detailed accounts of their experiences to media outlets.[49]

In sum, as a conception of cybersecurity grounded in economic risks, organisations view cybersecurity risks in a similar way to other corporate challenges and seek to mitigate them using standard management and economic methods. Economic competition provides opportunities for greater protection—and supports the cybersecurity industry itself—but also spreads vulnerabilities due to disincentives to cooperate. This creates a family resemblance with the state-based competition of national cybersecurity, leading to similarities in overall focus and everyday practices. However, other areas of interaction create the more conflictual dynamics of a family argument, where although some organisations fit closely within the national perspective, others seek to distance themselves to build a global business.

Several scholars have put forward an alternative concept of human-centred cybersecurity to both national and commercial perspectives. A key proponent of this approach is Ron Deibert, director of the Citizen Lab, a non-profit organisation based at the University of Toronto which uses interdisciplinary methods to investigate cyber threats to civil society. In his academic work, Deibert has explicitly tied human-centred cybersecurity to a broader movement in security studies to address issues of 'human security,' to see what are usually cast as questions of national or international security as threats to individuals.[50] Theories of human security usually articulate these threats in reference to international human rights. The human rights on which the Citizen Lab focus are first, freedom from torture, mistreatment, or arbitrary detention in connection to spyware facilitating such actions; and second, freedom of expression in connection to censorship and filtering, both directly and as an indirect 'chilling effect' of known censorship. The right to privacy and related data protection issues are also a central aspect of the Lab's work. There are of course other human rights, including rights of development, political participation, and non-discrimination, that are on the cusp of becoming cybersecurity issues due to factors such as the influence of social media on political opinions, the manipulation of targeted advertisements, and the free or subsidised provision of essential services in exchange for personal data. Overall, human-centred cybersecurity can adapt with the expansion of cybersecurity itself, keeping individual rights at the core of its protective mission.

An individual perspective also interrogates the effect of digital technologies on existing forms of violence against vulnerable individuals. Current research suggests that internet-connected devices, especially those designed for domestic convenience or security purposes, enable new forms of domestic abuse.[51] This argument is analogous to the logic by which Citizen Lab argues that spyware enables mistreatment, in that these technologies provide information to the rights violator that is then used to facilitate or justify rights violations. However, the association between 'Internet of Things' (IoT) devices and domestic abuse also functions in a more psychological sense, as the awareness of sensors gives victims a feeling of helplessness and being under constant surveillance. This psychological effect takes individual cybersecurity in a different direction, moving away from violent physical effects linked to information technologies and towards non-physical forms of violence: psychological, cultural, and

structural.[52] Following trends in human security more broadly, individual cybersecurity highlights the differential impact of cybersecurity threats on specific groups, especially gender and ethnic minorities or vulnerable immigrants. For example, the extent to which migrants in Europe rely on their smartphones throughout the migration process enables governments to collate metadata about their travel history and contacts, which could be used to justify deportation.[53]

The relationships between individual cybersecurity and national and commercial cybersecurity include both family resemblances and family arguments. The family resemblance between individual and national cybersecurity is so close that at some points they converge completely. States are the main guarantors of individual rights, and so unless a state can function competently, including providing basic critical infrastructure and both a domestic and foreign-facing security apparatus, individual cybersecurity is automatically imperilled.

In the other direction, liberal political theory promotes a view of personhood where the existence of a private sphere is the basis for the constitution and articulation of individual identity itself. Without a protected private space for individual flourishing, there are no meaningful individual identities for the state to protect.[54] Consequently, national cybersecurity depends on individual cybersecurity just as much as the other way around. This symbiotic relationship is, of course, based on a liberal conception of both individuals and states, and the central role of individual cybersecurity in national cybersecurity depends on the extent to which other viable conceptions of personhood exist.

However, this convergence of individual and national cybersecurity overlooks an important family argument: the fact that states are just as often threats to a wide range of individual rights both within their borders and outside them—in this case, mainly freedom of expression and privacy. As the extensive debate following the 2013 Snowden disclosures revealed, many citizens in the home states of the 'Five Eyes' intelligence partnership (the US, UK, Canada, Australia, and New Zealand) felt that the extent of mass surveillance (or bulk data collection) by intelligence agencies breached their rights to privacy.[55] This was the case even if such surveillance was intended to protect them from mutually agreed threats, such as terrorism. In many states where the surveillance apparatus is more closely connected to repressive security practices both online (censorship and filtering) and offline (detention and mistreatment), national and individual cybersecurity can become almost entirely opposed. Overall, rather than simplifying the relationship between individual and national cybersecurity as a

binary trade-off between security and freedom in all cases, the framework of family resemblances and arguments provides space for the points of agreement and tension between these concepts to exist simultaneously.

Individual cybersecurity also bears a family resemblance to commercial cybersecurity. Individual rights can fit easily into profit-motivated attempts to secure corporate data from state access. A good example of this alignment is Apple's refusal to unlock an iPhone used in a mass shooting for the US Federal Bureau of Investigation (FBI).[56] As Apple's business model has less to lose from a more restrictive data provision model than its competitors, its refusal to allow FBI access was useful public relations material, cementing the company's privacy-conscious reputation in the minds of consumers. Of course, commercial entities like Apple do not present these actions as economically motivated, instead highlighting their self-perception as ethically capable actors with duties and responsibilities to individuals, rather than merely profit-making entities. This view has been bolstered by international organisations, as the UN's 2011 Guiding Principles on Business and Human Rights highlights how companies have a duty to both avoid directly causing rights violations and participating in areas where rights violations are expected.[57] Some specific actions, such as Microsoft's Tech Accord, cited in the previous section, and Google's withdrawal from the Chinese search market in 2010, seem to support this view.

However, human rights justifications for economically-motivated action are hostage to a future when these motives diverge.[58] Although this is not yet the case with Apple, Google has begun to reconsider its position in China, and is building a censored version of its search engine for the Chinese market.[59] A more intense argument between individual and commercial cybersecurity emerges when private companies more directly enable, rather than simply comply with, repressive state practices. Citizen Lab's work investigating states' use of commercially-developed spyware against journalists, activists, and dissidents worldwide, from Mexico to Saudi Arabia, highlights how various surveillance systems (sometimes even branded as their 'most advanced form of cybersecurity')[60] restrict civil society and reduce the individual cybersecurity on which it depends.

There seems no easy route to put an end to this family argument and reconcile individual cybersecurity with its commercial cousin. As indicated by the response of these surveillance suppliers to accusations of human rights violations, the creation of 'ethical committees' and review boards are often no more than reputation-saving attempts to placate influential

backers, rather than a genuine commitment to avoiding misuse.61 Social media companies perform similar damage limitation exercises when they conduct internal investigations and create oversight bodies: for example, Facebook's PR tactics have come under scrutiny following alleged Russian interference surrounding the US Presidential election.[62] Overall, although individual and commercial perspectives on cybersecurity occasionally overlap, this resemblance is contingent on individual decision-makers and the convergence of different motivations. From a global perspective, family arguments are just as common, and more concerning in the long run.

Finally, there is a wider contradiction between individual and commercial cybersecurity due to structural features of the software market that encourage speed and innovation at the expense of secure systems. In contrast to other critical infrastructure sectors, national regulators avoid making software producers liable for negative consequences due to software vulnerabilities, and so it is unclear where liability lies for human rights violations. Unfortunately, it is not obvious that the solution is to strengthen human rights law by making software producers liable, as companies have proven adept at using human rights law to their advantage in disputes with both individuals and states in other sectors.63 Although a full treatment of these deeper structural contradictions is beyond the scope of this article, market assumptions about acceptable software creation and data collection practices create a broader environment termed by some scholars as 'surveillance capitalism,' in which narrower clashes occur.[64]

Conclusion

This article has sought to lay out three different perspectives of cybersecurity: national, commercial, and individual. In each case, it has connected these perspectives with wider bodies of political science and sociological and philosophical thought; theories of interstate conflict, both realist and critical; organisation studies and risk management; and human security and liberal individualism. While cybersecurity scholars recognise the existence of these different perspectives, and commonly bring them together in pairs, none consider all three equally. This article does so and explicitly analyses their interaction—the areas where they complement each other, leading at some points to merging, as well as the areas where they conflict, most starkly leading to the object of protection for one being exactly the threat for the other.

I have argued throughout that these different perspectives

can usefully be analysed within a conceptual framework of family resemblances and family arguments. Overall, there is a family resemblance at work: there is no common core to these three perspectives, but certain elements are borrowed and shared among them. As I explore throughout the body of this article, family arguments also persist between these rich and productive worldviews, and so cybersecurity continues to be contested between these three perspectives. The framework of family resemblances and arguments cautions against an exclusionary approach that focuses on one perspective instead of the others. Rather, it suggests that different communities working on separate but urgent cybersecurity problems should consciously explore areas in which their work resembles that of other communities to better understand their different concerns. Putting these three perspectives in direct conversation is thus not merely a reflective analytical exercise, but also an active intervention in cybersecurity politics; by doing so, I seek to reorient cybersecurity debates towards a more inclusive, and more optimistic, digital future.

Notes

1 A comprehensive list is contained in New America Foundation, "Global Cyber Definitions Database," accessed April 25, 2019, http://cyberdefinitions.newamerica.org/. For further discussion, see James Shires and Max Smeets, "What Do We Talk About When We Talk About 'Cyber'?" Working Paper, accessed February 8, 2017, https://papers.ssrn.com/abstract=2860839.

2 Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," Ethics & International Affairs 32, no. 4 (ed 2018): 411–24.

3 Madeline Carr, "Public–Private Partnerships in National Cyber-Security Strategies," International Affairs 92, no. 1 (January 1, 2016): 43–62.

4 Madeline Carr, "Internet Freedom, Human Rights and Power," Australian Journal of International Affairs 67, no. 5 (November 1, 2013): 621–37.

5 Ludwig Wittgenstein, Philosophical Investigations: The German Text, with a Revised English Translation (Malden, MA: Wiley-Blackwell, 2001).

6 Patrick Thaddeus Jackson, The Conduct of Inquiry in International Relations: Philosophy of Science and Its Implications for the Study of World Politics (London, New York: Routledge, 2010).

7 Shires and Smeets, "What Do We Talk About When We Talk About 'Cyber'?" Working Paper, accessed February 8, 2017, https://papers.ssrn.com/abstract=2860839.

8 James Shires, "Enacting Expertise: Ritual and Risk in Cybersecurity," Politics and Governance 6, no. 2 (2018).

9 I do not attempt to disentangle the concepts of nation and state in this section,

which would artificially treat them as largely synonymous.

10 Forrest Hare, "The Cyber Threat to National Security: Why Can't We Agree?" in Conference on Cyber Conflict: Proceedings 2010, ed. Christian Czosseck and Karl Podins (Tallinn: CCDCOE Publications, 2010), 211–26; Keir Giles and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in 2013 5th International Conference on Cyber Conflict, ed. K Podins, J Stinissen, and M Maybaum (Tallinn: CCDCOE Publications, 2013).

11 James Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States," War on the Rocks (blog), October 12, 2018, accessed May 17, 2019, https://perma.cc/L4CL-2B8A.

12 Jordan Branch, The Cartographic State: Maps, Territory, and the Origins of Sovereignty (New York: Cambridge University Press, 2014).

13 Nazli Choucri, Cyberpolitics in International Relations (Cambridge, MA: The MIT Press, 2012); Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace," American Foreign Policy Interests 36, no. 5 (September 3, 2014): 322–31; Paul Cornish, "Governing Cyberspace through Constructive Ambiguity," Survival 57, no. 3 (May 4, 2015): 153–76.

14 This is just as much the case for non-Western states like Russia, who seek to manage a national internet, as it is for the US or Europe.

15 Joseph S. Nye, The Future of Power (New York: PublicAffairs, 2011).

16 Maura Conway, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism," in Cyberterrorism: Understanding, Assessment, and Response, ed. Lee Jarvis, TM Chen, and Stuart Macdonald (New York: Springer, 2014), 103–22.

17 Richard K. Ashley, "The Poverty of Neorealism," International Organization 38, no. 2 (1984): 225–86.

18 Fiona B. Adamson, "Spaces of Global Security: Beyond Methodological Nationalism," Journal of Global Security Studies 1, no. 1 (February 1, 2016): 19–35; Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?," Journal of Global Security Studies 2, no. 3 (July 1, 2017): 184–203.

19 Fred Kaplan, Dark Territory: The Secret History of Cyber War (New York: Simon & Schuster, 2017).

20 Joseph S. Nye, "Nuclear Lessons for Cyber Security?," Strategic Studies Quarterly 5, no. 4 (2011): 18; Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (January 1, 2017): 44–71; Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," Journal of Strategic Studies 42, no. 1–2 (February 16, 2017): 1–28.

21 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," Security Studies 26, no. 3 (July 3, 2017): 452–81.

22 Eneken Tikk-Ringas, "International Cyber Norms Dialogue as an Exercise of Normative Power," Georgetown Journal of International Affairs 17, no. 3 (2017): 47–59; Shawn M. Powers and Michael Jablonski, The Real Cyber War: The Political Economy of Internet Freedom (Urbana: University of Illinois Press, 2015); Madeline Carr, "Power Plays in Global Internet Governance," Millennium 43, no. 2 (January 1, 2015): 640–59.

23 Lucas Kello, The Virtual Weapon and International Order (New Haven: Yale University Press, 2017).

24 Richard J. Harknett and Joseph S. Nye, "Is Deterrence Possible in Cyberspace?" International Security 42, no. 2 (November 1, 2017): 196–99; Michael P. Fischerkeller and Richard J. Harknett, "Deterrence Is Not a Credible Strategy for Cyberspace," Orbis 61, no. 3 (January 1, 2017): 381–93.

25 "Summary: Department of Defense Cyber Strategy 2018," US Department of Defense, accessed April 25 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

26 Graham Burchell, Colin Gordon, and Peter Miller, eds., The Foucault Effect: Studies in Governmentality (Chicago: University of Chicago Press, 1991); Mitchell M. Dean, Governmentality: Power And Rule In Modern Society, Second edition (London ; Thousand Oaks, Calif: Sage Publications Ltd, 2009).

27 Justin Joque, Deconstruction Machines: Writing in the Age of Cyberwar (Minneapolis: University Of Minnesota Press, 2018).

28 Riana Pfefferkorn, "Security Risks of Government Hacking," The Center for Internet and Society (Stanford University, September 2018).

29 Mustafa Emirbayer and Victoria Johnson, "Bourdieu and Organizational Analysis," Theory and Society 37, no. 1 (2008): 1–44.

30 Although for a more nuanced view on the role of corporations in the exercise of military power, see Rita Abrahamsen and Anna Leander, eds., Routledge Handbook of Private Security Studies (London; New York: Routledge, 2015); Rita Abrahamsen and Michael C. Williams, Security Beyond the State: Private Security in International Politics (Cambridge; New York: Cambridge University Press, 2010).

31 Robert Deuchars, The International Political Economy Of Risk: Rationalism, Calculation And Power (Aldershot, England; Burlington, Vermont: Ashgate, 2004).

32 Michael Power, The Risk Management of Everything: Rethinking the Politics of Uncertainty (London: Demos, 2004); Claudia Aradau and Rens Van Munster, "Governing Terrorism Through Risk: Taking Precautions, (Un)Knowing the Future," European Journal of International Relations 13, no. 1 (March 1, 2007): 89–115.

33 I thank an anonymous reviewer for this point.

34 Herbert Lin, "Governance of Information Technology and Cyber Weapons," in Governance of Dual-Use Technologies: Theory and Practice, ed. Elisa D. Harris (Cambridge, Massachusetts: American Academy of Arts and Science, 2016), 112–57.

35 Ronald J. Deibert and Rafal Rohozinski, "The New Cyber Military-Industrial Complex," The Globe and Mail, March 28, 2011, accessed May 17, 2019, https://perma.cc/PJL9-AKGU; Martin Stabe, Steve Bernard, and Marissa Oberlander, "The New Cyber-Industrial Complex," Financial Times, October 10, 2011.

36 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," Journal of Strategic Studies 38, no. 1–2 (January 2, 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

37 Brian Krebs, "Blowing the Whistle on Bad Attribution," Krebs on Security (blog), August 2017, accessed May 17, 2019, https://perma.cc/NS2B-Q6KT.
38 Ellen Nakashima, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," Washington Post, January 12, 2018, accessed May 17, 2019, https://perma.cc/U26X-K9RN.
39 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, August 22, 2018, accessed May 17, 2019, https://perma.cc/6EGM-TDWQ.
40 Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," International Studies Review 15, no. 1 (March 1, 2013): 105–22, 119.
41 Robert Gorwa and Anton Peez, "Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord," December 11, 2018; Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs," Journal of Cyber Policy 3, no. 1 (April 27, 2018): 1–16.
42 "Information for Law Enforcement Authorities," WhatsApp FAQ, accessed April 2, 2019, https://perma.cc/KSY6-F46P.
43 Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," International Political Sociology 8, no. 2 (June 1, 2014): 121–44.
44 Daisuke Wakabayashi and Alan Rappeport, "Huawei C.F.O. Is Arrested in Canada for Extradition to the U.S.," The New York Times, December 10, 2018, accessed May 17, 2019, https://perma.cc/CUL8-UECR.
45 Huawei Cyber Security Evaluation Centre, "Oversight Board Annual Report 2019" (London: HCSEC, March 2019).
46 Amy Zegart and Kevin Childs, "The Divide Between Silicon Valley and Washington Is a National-Security Threat," The Atlantic, December 13, 2018, accessed May 17, 2019, https://perma.cc/F5NA-4PR5.
47 Elaine M. Sedenberg and Dierdre K. Mulligan, "Public Health as a Model for Cybersecurity Information Sharing," Berkeley Technology Law Journal 30, no. 3 (2016): 1687–1740.
48 Herbert Lin and Amy Zegart, eds., Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations (Washington D.C.,Brookings Institution Press, 2019).
49 Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," The New Yorker, April 30, 2018, accessed May 17, 2019, https://perma.cc/X7S8-DQSJ.
50 Ronald J. Deibert, "Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace," Canadian Defence and Foreign Affairs Institute (August 2012); Ron J. Deibert, Black Code: Inside the Battle for Cyberspace (Plattsburgh, NY: Signal Books, 2013); Deibert, "Toward a Human-Centric Approach to Cybersecurity."
51 Phoebe Braithwaite, "Smart Home Tech Is Being Turned into a Tool for Domestic Abuse," Wired UK, July 22, 2018, accessed May 17, 2019, https://perma.cc/QDJ2-ZKPL.
52 Laura Shepherd, Gender, Violence and Security: Discourse as Practice (Zed

Books Ltd., 2013); Anita R. Gohdes, "Studying the Internet and Violent Conflict," Conflict Management and Peace Science, October 25, 2017.

53 Morgan Meaker, "Europe Is Using Smartphone Data as a Weapon to Deport Refugees," Wired UK, July 2, 2018, accessed May 17, 2019, https://perma.cc/79FC-FWV4.

54 Daniel H. Deudney, Bounding Power: Republican Security Theory from the Polis to the Global Village (Princeton, N.J: Princeton University Press, 2008).

55 'Bulk data collection' is the term used by the intelligence agencies themselves. Individuals around the world also felt violated; however, in many dominant strands of political theory states have less (sometimes no) responsibility towards individuals not within their domestic political community.

56 Susan Landau, "Revelations on the FBI's Unlocking of the San Bernardino IPhone: Maybe the Future Isn't Going Dark After All," Lawfare, March 30, 2018, accessed May 17, 2019, https://perma.cc/R3WA-FPDM.

57 "Guiding Principles on Business and Human Rights," United Nations, (HR/PUB/11/04, 2011).

58 Gary Elijah Dann and Neil Haddow, "Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China's Internet," Journal of Business Ethics 79, no. 3 (May 1, 2008): 219–34.

59 Ryan Gallagher, "Google Plans to Launch Censored Search Engine in China, Leaked Documents Reveal," The Intercept (blog), August 1, 2018, accessed May 17, 2019, https://perma.cc/6MN8-TBAP.

0 Simone Margaritelli, "How the United Arab Emirates Intelligence Tried to Hire Me to Spy on Its People," Evilsocket (blog), July 27, 2016, accessed May 17, 2019, https://perma.cc/EDD3-Y9RZ.

61 Miles Kenyon, "Open Letter to Francisco Partners: Continued Misuse of NSO Group's Pegasus Technology," The Citizen Lab, November 1, 2018, accessed May 17, 2019, https://perma.cc/F3X9-BN28.

62 Sheera Frenkel et al., "Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis," The New York Times, January 29, 2019, accessed May 17, 2019, https://perma.cc/6HR9-VFQ8.

63 Sarah L. Steele et al., "The Role of Public Law-Based Litigation in Tobacco Companies' Strategies in High-Income, FCTC Ratifying Countries, 2004–14," Journal of Public Health 38, no. 3 (September 17, 2016): 516–21.

64 Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power (Profile Books, 2019).