Introduction: Rethinking (In)stability in and of Cyberspace

Introduction: Rethinking (In)stability in and of Cyberspace

Robert Chesney, James Shires, and Max Smeets

Many governments and intergovernmental organizations have declared stability to be a central goal of cyber policy. The European Council has called for an "open, stable, peaceful and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply."[1] NATO has recognized cyberspace as a new operational domain, in which it has pledged to maintain stability.[2] The United Kingdom has committed to "promote international security and stability in cyberspace,"[3] while the United States has repeatedly stressed the need to promote "greater predictability and stability in cyberspace."[4]

Stability is by no means an objective only promoted across the Atlantic. In the first drafting stage of the UN Open Ended Working Group (OEWG) on cyber security, China stressed that "the starting point and ultimate goal should be to ensure peace and stability in cyberspace."[5] Equally, India has repeatedly stated that it is committed to a "stable cyberspace environment."[6] The final report of the OEWG, released in March 2021, represents almost 100 states, as well as input from global civil society. It repeatedly emphasizes the triad of peace, security, and stability, as well as the longer formulation of an "open, secure, stable, accessible and peaceful [information and communications technologies] environment."[7]

Some countries have even promoted the establishment of international cyber initiatives specifically focused on stability. The Global Commission on the Stability of Cyberspace (GCSC) was established mainly through the initiative of the Dutch government, following the Global Conference on Cyberspace in The Hague in 2015. The GCSC aims to promote "mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity."[8] Its final report in 2019 recommended

four principles of responsibility, restraint, requirements to act, and respect for human rights, to "ensure the stability of cyberspace."[9]

Stability is thus central to a cluster of terms used normatively in cyber policy to describe those qualities of cyberspace that must be preserved and protected against a wide variety of threats now, and expanded and improved in the future. This is hard to argue against: who wouldn't want cyberspace to be more stable?

Unfortunately – or perhaps intentionally, given the carefully negotiated nature of the quotations above – the meaning of stability in this context, along with its companions in the cluster, remains vague, ambiguous, and contested. Should stability be understood as a thin, technical term, describing the reliability and continuity of the complex layers of technologies that underpin cyberspace? Or, as the GCSC suggests, should it be understood in a "thicker," more substantive way, relating to the potential for war, conflict, and the preservation of individual rights and freedoms? Cyber norms efforts at the UN – and even several consensus reports of the UN Group of Governmental Experts – have highlighted the extent of disagreement between states about what stability includes, what are the most concerning threats to stability, and how to counter them.

Stability is thus a contested concept, with ongoing disputes about its proper use by different actors.[10] Choosing the referent object of stability – who or what is being stabilized – is part of this contest. In some instances, stability is about avoiding escalation between great powers. In other instances, it is about ensuring (authoritarian) regime survival. The stability of cyberspace is also frequently linked to protecting the "core" functionality of the internet or other critical functions of society. The widespread use of the concept of stability in relation to cyberspace obscures the fact that actors are often striving for different end-states, that cyber threats are not objectively given, and that actors mobilize politically in different ways.

Indeed, once we widen the scope of stability from a narrow focus on technical aspects of cyberspace, the normative value of stability as an uncontested good is less clear. Strategic, political, and economic stability (to take a few examples) have all been used historically to justify highly controversial actions, from colonial conquest to threats of nuclear weapons and modern armed interventions, and from repressive authoritarian practices to vastly unequal distribution of resources. In this way, the concept of stability can legitimize power imbalances, inequalities, violence, and injustice, meaning that seeking stability for some often increases instability for others. In other words, insofar as the status quo is problematic, whether from the perspective of those subject to reckless and disruptive cyber operations or those who reject the dominance of

some states in internet governance, so is the concept of stability. We capture this problematic relationship between stability and instability – and their frequent coexistence – in a combined concept of (in)stability.

The purpose of this edited volume is to provide a thorough investigation of cyberspace and (in)stability. It seeks to reconceptualize (in)stability in relation to cyberspace, highlight its various dimensions, and, through this, identify relevant policy measures. It recognizes that the concept of stability as normatively desirable is baked deeply into cyber policy, and it balances this positive orientation toward stability with efforts to probe more critically at its consequences and assumptions. To this end, the volume is guided by a central research question: *How does the (in)stability of cyberspace interact with other kinds of (in)stability in international politics?*

This research question connects cyberspace and international politics in both directions, recognizing that the (in)stability of cyberspace has important consequences for broader strategic, political, economic, and even environmental (in)stability, while these wider (in)stabilities also shape the evolution and development of cyberspace as a complex socio-technical system. All the chapters in this book engage with this central research question, despite their wide range of topics and theoretical approaches. Moreover, while they all incorporate an analytically sophisticated approach to stability, there is, in our view, a productive tension between chapters that treat it more as an achievable goal and those that treat it as an object of critique and revision. This tension is central to the volume's design, and we underline it in this introduction through the concept of (in)stability.

The prominence of stability in cyber policy means that this is an important undertaking, on which thorough and insightful scholarship is urgently required. A quick glance at the news headlines any day underlines the importance of the stable functioning of cyberspace to the everyday lives of individuals around the world – especially during a global pandemic – as well as the myriad threats to and in cyberspace. Only by understanding (in)stability more deeply can we begin to achieve desired forms of (in)stability for cyberspace, and, perhaps more importantly, understand the means by which we wish to do so.

Thinking About Cyberspace and (In)Stability

Academia has hardly helped to conceptualize stability in relation to cyberspace. Only thirty journal articles were published in political science mentioning the concept "cyber stability" between 2005 and 2020, whilst related concepts were more often debated; "cyber resilience" was discussed in 166

articles, "cyber deterrence" in 220 articles, "cyber war" in 982 articles, and "cyber security" in over 5,000 articles.[11] This lack of direct focus on a core policy concept is surprising, but understandable. The other concepts above are all clearly related to stability, and so conceptualizations of stability draw on developments in these other areas. Before detailing the various contributions of this book, we first briefly outline how a richer concept of cyber (in)stability intersects with key aspects of both academic theories and cyber policy, such as resilience, deterrence, conflict, and security, as well as drawing on stability literature outside cyber concerns.

An obvious starting point for discussions of stability and cyberspace is the potential for cyber war or cyber conflict. While these terms have been much discussed – and criticized – in the last two decades, the potential of a cyber "attack" with effects similar to those of conventional arms could clearly impact the stability of the international system (otherwise known as "strategic stability").[12] Cyber capabilities could arguably trigger conflict between great powers, as well as enabling others (for example, smaller states or non-state actors) to enhance their capabilities and leverage. In this way, cyber operations increase risks of systemic instability, as well as potentially making it harder to resolve conflicts through the distorted effects of information operations. The cyber strategy literature predominantly addresses such effects on (in)stability in the international system through the lens of escalation. We devote the first section of the volume to these dynamics (detailed below).

However, systemic (in)stability and cyberspace do not only interact through the potential for cyber operations to have war-like effects. An extensive strand of literature in international relations (IR) has explored the structural stability of different systems, asking for example, whether a "balance" between two superpowers is more stable than a system dominated by a single hegemon.[13] In relation to cyberspace, we are clearly moving from the latter situation (where the internet and many digital technologies were developed, operated, and managed in the United States), to a multipolar cyberspace with several nodes of power: China representing an equal center of gravity to the United States, the European Union representing a node from a regulatory perspective, and India and many African states in terms of user numbers and information and communications technologies (ICT) skills. Thinking about systemic (in)stability and cyberspace requires us to first acknowledge such shifts, and then to parse their consequences for the technical operation – and in the extreme case, balkanization – of the internet, as well as their softer impacts on economic attractiveness, standards-setting, and norm development.

While systemic (in)stability is a clear first and expansive frame for our question, it is far from the only one. The current academic consensus is that cyber

operations are primarily conducted below the threshold of armed conflict,[14] providing new means of covert action and intelligence gathering that collectively help states achieve strategic outcomes.[15] Although cyber operations in the "grey zone" can affect the stability of the system overall, they have more direct consequences for other kinds of stability, such as damaging the political stability of individual states through influence operations, or undermining economic stability through IP theft, fraud, or extortion. It is uncertain whether such cyber operations taking place below the threshold of armed attack can be adequately deterred (much has been written on the applicability of deterrence to this sphere),[16] or whether states should instead engage directly in "persistent" cyber activity, seeking to disrupt activity wherever the adversary maneuvers, reaching a form of stable but largely implicit "agreed competition."[17] What is clear is that here stability and instability are even further intertwined; the gains of one state are often the losses of another, and so such sub-system interactions can clearly benefit from analyses of (in)stability.

As with systemic (in)stability, there are also issues of (in)stability at a subsystem level that are not always related directly to cyber operations. For example, the impact of cyberspace on the political stability of states is another topic with an extensive literature, especially in relation to the role of social media networks in the 2011 Arab Spring protests and many others before and since.[18] For those participating in these protests, the ability to undermine the stability of decades-long authoritarian regimes through online connective action – and extensive offline confrontation – provided a rare opportunity to champion individual rights and freedoms. Conversely, the "digital authoritarian" reaction of such regimes, first improvising and later embedding extensive information controls to subdue and coerce their citizens into compliance, reveals the complex relationship between (in)stability and cyberspace at a national and regional level.[19] The proliferation of advanced targeted surveillance technologies, for example, maintains authoritarian control but violates individual rights and jeopardizes diplomatic relationships.

Finally, we must consider the relationship between cyberspace and (in)stability not just at the level of operations, incidents, and practices – state or non-state, system or sub-system – but also in terms of the structural foundations of how we perceive our world. Throughout history, particular worldviews – racist, sexist, imperial, colonial – have structured political interactions, and it is the (in)stability of these worldviews, their rise and fall, that has shaped the contemporary international system. Equally, stability itself is a signifier with gendered, racial, and colonial implications, which cannot be forgotten in its contemporary application. Cyberspace provides a unique platform for many fringe discourses, while also globalizing dominant ideals and practices through

multimedia products with almost unfathomable reach to billions worldwide. At the most macro level, the stability of human life in an increasingly unstable climate, and the potential for digital technologies to both exacerbate and help ameliorate the climate emergency, underline the centrality of cyberspace for global (in)stability in the most literal sense. We hope that this volume starts a conversation that helps to address these vital issues.

Structure of the Book

The chapters of this book are ordered according to four themes, roughly in line with the unfolding discussion above: escalation, institutions, and infrastructures, with a final section on subaltern and decolonial perspectives on (in) stability in relation to cyberspace. Here, we provide a brief overview of each theme and summary of the chapters' contributions, as well as drawing out connections between them.

Part I Escalation

First, we examine cyberspace and (in)stability in terms of the risks of conducting cyber operations, especially around inadvertent escalation. Inadvertent escalation in the context of cyber operations has at least two different meanings. The first refers to the risk of cyber operations escalating into a major conventional conflict or war. The second refers to cyber espionage operations – or operational activity with defensive aims – ultimately leading to a more severe cyber response from an adversary. This topic has become particularly relevant as many states establish military cyber commands, and as the United States has shifted to a new military strategy of defending forward against adversaries in cyberspace, perceived as more "aggressive" by some observers.

Existing articles considering cyber operations and stability primarily assess states' ability to reduce the risk of inadvertent escalation through deterrence and norms-building measures. For example, Borghard and Lonergan explain how confidence-building measures can foster stability in cyberspace.[20] Geist assesses whether nuclear concepts and thinking on deterrence stability should be imported to the cyber domain, arguing that the United States should create a "strategy of technology", emphasizing "resilience, denial, and offensive capabilities."[21] Donnelly et al. argue that cyber stability can be achieved through a deterrence posture that includes clear communication of credible intention and capability.[22] Overall, the current academic literature largely conceives of cyber stability as a particular condition or state of affairs, whether narrowly as the absence of incentives to conduct (military) cyber operations and develop

an offensive cyber capability, or more broadly as a peaceful and harmonious cyber environment for states to operate in and through.

In Chapter 1, Jason Healey and Robert Jervis introduce the concept of situational cyber stability, suggesting the key question is not "whether" cyber capabilities are escalatory per se, but rather how they are escalatory under certain geopolitical conditions. Their approach to stability is dynamic, rather than static. Healey and Jervis identify four key mechanisms: Pressure Release, Spark, Bring Out the Big Guns, and Escalation Inversion. They note that both optimists – arguing that cyber conflict is not escalatory – and pessimists – arguing that cyber conflict is escalatory – have each touched on parts of these mechanisms. This chapter integrates insights from both perspectives to better understand crisis stability in cyberspace across the range of geopolitical contexts from relative peace to impending war. The chapter also examines the role of surprise in cyber conflict and offers several policy recommendations to reduce the chances of crises escalating.

Healey and Jervis emphasize that certain features of cyber capabilities can create new pathways through which a great-power crisis could escalate into a larger conventional conflict. In Chapter 2, Ben Buchanan and Fiona Cunningham assess one particular pathway for interstate crisis escalation: the use of force in response to adversary hacking operations that are designed to enable high-end cyber attacks. Known as operational preparation of the environment, these kind of hacking operations lay the groundwork for future attacks but are difficult to distinguish from espionage. While some scholars argue that states might respond to the discovery of an intruder with the use of force, others have found little empirical evidence that cyber operations affect interstate conflict dynamics. To assess these competing claims, the authors go further than most in conducting a comparative examination of Chinese and US leadership views, organizational and operational practices for cyber conflict, and the bilateral cyber relationship, drawing on government and policy sources from both countries. Buchanan and Cunningham conclude that the risk of inadvertent escalation due to cyber capabilities in a future Sino-American crisis cannot be dismissed.

In Chapter 3, Jaclyn Kerr explains why the United States was surprised by Russian use of cyber-enabled information operations during the 2016 US presidential elections. She argues that the United States was poorly prepared to anticipate, defend against, or respond to these operations because of a long-developing security dilemma rooted in "domain concept misalignment" – that is, superficially overlapping but significantly different domain conceptualizations – resulting from a distinction in how democratic and non-democratic states conceptualize the scope and nature of the emerging

digital and informational domain of military action. Kerr's findings reveal the importance of conceptual clarity and historical awareness in ensuring effective response and preventing escalation in the future.

Together, these three chapters address different aspects of escalation relating to cyber capabilities. They emphasize how strategic concepts affect the likelihood of escalation, whether in terms of specific doctrine on the risks of cyber operations (Buchanan and Cunningham), or broader ideas about the appropriate boundaries of the cyber domain overall (Kerr). They also highlight the contingency of escalation, teasing apart different mechanisms that lead to opposite outcomes (Healey and Jervis), addressing the consequences of the new US strategy, and exploring the complex relationship between internal bureaucratic divisions and international cyber strategy (Buchanan and Cunningham, Kerr). While these chapters largely focus on the dyadic dynamics of great power escalation, the next section investigates how institutions affect cyber (in)stability in more detail.

Part II Institutions

The accounts of systemic (in)stability above speak directly to long-standing realist traditions of IR thought. However, the more constructivist literature on cyber norms has an equally central relationship with the concept of stability.[23] There is little agreement over what a cyber norm should be (ranging from prescriptive norm lists to more diffuse ideas of tacit bargaining), let alone what norms are appropriate for cyberspace and how such norms can be implemented and enforced. For this reason, we approach this topic from the direction of institutions, noting that IR draws a firm connection between the two concepts, defining institutions as collections of principles, norms, rules, and decision-making procedures. The three chapters in this section examine institutions in both the IR and more vernacular senses: NATO, the US Department of State and the US Department of Defense. All three chapters ask how these institutions incorporate cyberspace into their pre-existing practices, how they adjust or reshape their norms and practices in response, and – crucially – how this re-orientation affects the possibility for cyber norms development more broadly. As Jon Lindsay has observed, cyberspace does not only have institutions, but in a much more fundamental sense cyberspace is itself an institution.[24]

We acknowledge that the choice of institutions in this section is highly skewed: namely, two US government organizations and a transatlantic military alliance dominated by the US. This in part reflects the scholarly networks and production process of the edited volume, with nearly all contributors and

editors working in the US and Europe – sometimes as scholar/practitioners as well as academic "observers." It also reflects our access to and the availability of detailed information about institutional processes in these states, compared to other world regions.[25] Such US- and Euro-centricity is nonetheless an important limitation of this section. We seek to address this limitation in part later in the volume, especially in the section on subaltern and decolonial perspectives, but also recommend readers to see this section as an invitation to engage in wider comparative institutional analyses of (in)stability and cyberspace.

In Chapter 4, Joe Burton and Tim Stevens investigate the implications for strategic stability of NATO's operationalization of the cyber domain. Building upon an historical and theoretical understanding of alliances as stability mechanisms, they determine how NATO's evolving cyber posture – and associated discourses of stability – has been interpreted by its key adversaries, allies, and partners. The scholars thus not only analyze the classic elements of strategic interaction but also NATO's role as a normative actor in global cyber affairs. Overall, this chapter poses questions about how NATO's pursuit of political relevance and operational dominance in the cyber domain shapes and influences strategic stability. In an insightful comment highly pertinent to the devastating war in Ukraine that began toward the end of the writing of this volume, Burton and Stevens note that, for NATO, "Russian actions may have demonstrated [a] sort of stability paradox, wherein efforts to cause instability engender cohesion and collective responses." Such unintended consequences underline the complexity that alliance relationships bring to questions of (in) stability.

In Chapter 5, Emily Goldman examines the role of the US State Department in cyber diplomacy. Goldman begins by noting that American cyber diplomacy has improved but still leaves the United States vulnerable to continuous, state-sponsored cyber aggression that is having strategic effects, even though that aggression never rises to a "significant" level that would elicit an armed response. Goldman argues that the State Department can pivot – without risking armed conflict – from a "reaction-after-the-fact" posture to seizing the initiative from adversaries whose cyberspace campaigns erode US economic competitiveness, reduce military advantages, and weaken political cohesion. Goldman recommends that the US State Department re-examine assumptions about cyber conflict and norm emergence, adopt a competitive mindset, and prioritize efforts tailored for great-power competition. Ultimately, Goldman's conclusion that "restraint in the face of continuous aggression is destabilising because it emboldens aggressors" reveals another paradox of unintended consequences; this time, a reluctance to act diplomatically when faced with a rapidly shifting and institutionally divided policy landscape.

In Chapter 6, Rebecca Slayton observes that cyber competition is about more than technology – it is about the knowledge, skills, and capabilities of a relatively new kind of expert, the cyber warrior. However, the fundamental knowledge, skills, and capabilities needed to defend and attack computer networks are not new. They have been under continual development by computer scientists, in both classified and non-classified contexts, since the late 1960s. Consequently, the question this chapter explores is: how, when, and why did this expertise come to be institutionalized as a kind of warfighting, meriting the authority and resources reserved for a combatant command? Slayton argues that both the process by which military leaders came to appreciate the risks associated with vulnerable computer networks, and the dominant response to those risks, were shaped by military culture as much as they were shaped by technological imperatives. Slayton thus shows that that the role of cyber warriors in influencing the stability of the international order depends as much on how they are imbedded within their national (military) institutions, as their technical prowess.

Together, these chapters tackle the thorny question of how far institutional state or alliance objectives regarding stability contribute to the technical and normative stability of cyberspace more broadly. From Burton and Stevens' analysis of NATO's semi-successful efforts to advocate for improved cyber security defenses across and beyond its membership, to Goldman's dissection of the US State Department's sometimes uncomfortable commitment to norms of openness and interoperability, the relationship between institutions and their broader environment is neither simple nor straightforward. This comes to the fore clearly in Slayton's plea to consider the wider implications – and institutional prestige – of "defensive cyber operations, which stabilize technology for friendly operators." As Slayton argues, "if kinetic operations contribute to international instability, the cyber defenses that enable those operations enable that instability," thereby turning on their head standard assumptions of how offense and defense relate to stability. Such concerns lead us into the third section of the volume, which addresses global infrastructural issues more directly.

Part III Infrastructures

Cyberspace is dependent on multiple overlapping infrastructures, both in Edwards' definition of infrastructures as accumulated relational properties stretching across sectors, and in Starr and Ruhleder's observation that infrastructures are "intended not to be seen."[26] As Ensmenger notes, "technologies become infrastructure only after they are perfected to the point of being rou-

tine . . . we notice them only when they fail."[27] Despite – or, perhaps, due to – this near-invisibility, infrastructures are highly political. What does it mean to "perfect" a technology or a set of technologies? Whose routines do they enable and constrain? And how do they "fail"? These questions all speak to the (in) stability of the infrastructures that underpin cyberspace, and their implications for (in)stability of other kinds of infrastructures.

More specifically, an infrastructural lens connects (in)stability to its close cognate, the concept of resilience. It is widely accepted that cyber security, understood as the defense and protection of digital networks from intrusion and disruption, must be accompanied by cyber resilience in the form of post-incident detection and recovery, enabling targeted entities to return to normal functioning as quickly as possible. A stable infrastructure is a resilient infrastructure, possessing the ability to respond quickly to change, as well as the ability to manage unexpected events in a controlled manner. The two chapters in this section both address infrastructural aspects of (in)stability, highlighting how new technologies and the unexpected or problematic use of these technologies undermines the stability of various infrastructures supporting cyberspace. In the other direction of the relationship – examined throughout this volume – they address how cyberspace as an infrastructure raises questions of international governance more broadly.

In Chapter 7, Mark Raymond examines the rapid emergence and expansion of the Internet of Things (IoT), as it entangles the internet with an array of other issue areas. It thus generates potentially problematic interactions among the legacy internet governance regime, a host of other international regimes, and domestic governance arrangements in highly networked countries. The chapter argues that alongside the rapid diffusion of the internet, we are witnessing the metastasizing of the global cyber regime complex. As a result of this ongoing process, the viability of a variety of international regimes and domestic governance arrangements (and thus the stability of the international system more broadly) will increasingly depend on the efficacy and legitimacy of the global cyber regime complex. The chapter concludes by making the case for treating this regime complex as "critical governance infrastructure" in the international system. Just as electric grids, water systems, and financial systems are systemically important components of modern societies, the global cyber regime complex is rapidly acquiring a singular importance as a condition of possibility for the remainder of the present system of a rules-based global order and global governance; but one that is dangerously fragile. As Raymond astutely concludes, whatever our definition of (in)stability, "a world in which governance is less effective, less legitimate and more contested should be expected to be less stable."

In Chapter 8, Siena Anstis et al. advance a complementary argument by describing how the central characteristics of our evolving communications infrastructure (including devices, protocols, applications, and telecommunications networks) produce mounting insecurities for global civil society. Global civil society depends on a communications infrastructure that is constantly mutating, highly insecure, invasive by design, poorly regulated, and prone to abuse. This ecosystem was not developed with a single well-thought-out design plan, and security has largely been an afterthought. New applications have been thrown on top of legacy systems and then patched backwards haphazardly. In short, the dynamics of "surveillance capitalism, the products and services of the cyber warfare industry, and increasingly aggressive offensive cyber policies yield an insecure structure, contributing to an unstable environment for civil society." It is troubling that there is no single policy, technology, or application that will resolve this dysfunctional environment, and the authors argue that these conditions will almost certainly worsen as the "center of gravity" of cyberspace shifts to China, India, and the Global South.

Together, these two chapters examine the consequences for (in)stability of what Kerr, in this volume, calls the "arbitrary complexity of information systems." Raymond identifies the assemblage nature of cyberspace as a key source of instability, because "the complexity of the global cyber regime complex is itself likely to increase the odds of governance failures of various kinds" – with echoes of Kerr's analysis of competing institutional regimes earlier in the volume. Anstis et al. focus less on the arbitrariness of cyberspace governance, instead seeing unstable complexity as the result of deliberate actions. In doing so, they invert common statist notions of stability, arguing that "what state actors may consider to be beneficial for 'stability' can perversely end up being a threat to civil society." Consequently, for Anstis et al., "stability for civil society necessitates different norms altogether – affirming the ability to exercise human rights without reprisal." The fourth and final section of this volume carries this critique of stability further still.

Part IV Subaltern and Decolonial Perspectives

This section contains two chapters that are central to the project of this book. As is often the case for projects like this, several scholars who participated in the workshops in preparation for this volume were unable to contribute to the final output. However, one particular case stood out, when we asked a colleague to write a chapter on feminist approaches to cyberspace and (in) stability. After much discussion and thought, our colleague pulled out of the project because they could not see a fruitful line of argument between feminist

analyses of cyberspace – of which there are many – and the concept of (in) stability. After initially seeking to argue against the instinctive valorization of stability with which we opened this introduction, especially in a status quo world where violence against women is frequent and, in many situations, normalized, our colleague rejected the concept altogether. This was an important reminder that our choice of analytical frame always has downsides for someone. While we continue to believe that gendered investigations of (in)stability are urgently required – and we invite scholars to contribute their thoughts – we conclude the volume with two chapters that remind readers in other ways to reflect on the assumptions behind their own conceptualization of stability and cyberspace.

In Chapter 9, Mailyn Fidler surveys internet infrastructural developments of the African Union and African states, which occupy a subaltern position in the international system. Her starting point is that analyses of (in)stability must focus as much on capacity as intent, because "even if relative peace and strong desires exist between states, an imbalance in ability to respond can exert a destabilising effect." The chapter challenges the dominant conception that global integration brings stability through technical and regulatory openness, interoperability, and internationality. Instead, the case study analysis in this chapter reveals that global integration can also bring instability through dependence. As Fidler puts it, "For African countries, global integration can bring instability through dependence, and attaining cyber stability can require, at least initially, actions that the global community might view as destabilizing." Furthermore, Fidler argues that African states pursue stability through control of laws and through selectivity in infrastructural investments, both of which cut against typical expectations of subaltern states. In this way, Fidler's chapter surfaces a tension between subaltern states' view of stability and the human rights-focused civil society version advocated by Anstis et al. More specifically, this tension stems from the co-option of human rights discourses for state purposes: "just as Western countries might view an autocracy's views about cyber-openness as a threat to their vision of stability, post-colonial states might view a former coloniser's views of cyber-openness as a threat to theirs."

Finally, in Chapter 10, Densua Mumford applies a decolonial lens to argue that any useful conceptualization of (in)stability in cyberspace will require a critical and intersectional investigation of the Euro-American subject implied in this project, especially what Mumford terms the "transnational techno-elite." While Mumford underscores the downsides of pursuing state stability explored in earlier chapters – noting that "when states try to establish stability for themselves in cyberspace, various societal groups experience more instability" – this chapter takes this critique further. In particular, Mumford argues

that technical proposals designed to make it easier for users to change services or become less reliant on any single platform can usefully "undermine the stability of powerful platforms to the benefit of users." In some cases, the user benefit is precisely the introduction of instability; for example, "for LGBTQ youth, constructing an unstable online identity can be protective." In others, the presumptions of the transnational techno-elite act as "a destabilizing force in the social fabric of [marginalized] communities." Overall, Mumford shows that conceptualizations emerging from a Eurocentric perspective perpetuate coloniality by (de)stabilizing cyberspace in ways that are comfortingly familiar for dominant communities and further silence subaltern communities.

The analysis in this chapter raises some urgent critical questions, which we believe to be an appropriate note on which to conclude this introduction. Whose epistemologies are informing knowledge production and policymaking on (in)stability in cyberspace? On whose terms are such conceptualizations being made? Which knowledges are systematically privileged in these debates and which knowledges are systematically excluded or marginalized? The chapter recognizes that the nascent nature of debates about cyberspace creates an unprecedented opportunity to confront self-defeating practices of coloniality and to instead redefine traditional concepts such as (in)stability from within the epistemologies of subaltern communities across the Global South and North. That is, to be a concept that can be applied usefully to diverse lived experiences in cyberspace, (in)stability must itself incorporate diverse meanings.

Notes

1. European Council, "Declaration by the High Representative on Behalf of the European Union – Call to Promote and Conduct Responsible Behaviour in Cyberspace" (February 2020): https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/
2. NATO, "Warsaw Summit Communiqué": https://ccdcoe.org/uploads/2018/11/NATO-160709-WarsawSummitCommunique.pdf
3. UK Foreign & Commonwealth Office, "Foreign Secretary welcomes first EU sanctions against malicious cyber actors" (July 30, 2020): https://www.gov.uk/government/news/foreign-secretary-welcomes-first-eu-sanctions-against-malicious-cyber-actors
4. The White House, "National Cyber Strategy of the United States of America" (September 2018): https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

5. The White House, "China's Contribution to the Initial Pre-Draft of OEWG Report" (April 2020): https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf
6. Elizabeth Roche, "UNSC: India says Cyber Tools are Used to Target Critical Infra," *Livemint* (June 29, 2021): https://www.livemint.com/news/india/unsc-india-says-cyber-tools-are-used-to-target-critical-infra-11624980216689.html
7. United States General Assembly, "Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report," Conference room Paper (2021, March 10).
8. Global Commission on the Stability of Cyberspace, "The Commission": https://cyberstability.org/about/
9. Global Commission on the Stability of Cyberspace, "Advancing Cyberstability: Final Report": https://cyberstability.org/report/#2-what-is-meant-by-the-stability-of-cyberspace
10. In this way, it mirrors similar developments in the concept of cyber security, which we capture elsewhere as "moral maneuvers." James Shires, *The Politics of Cybersecurity in the Middle East* (London: Hurst, 2021).
11. Over 5,000 articles were published discussing "cyber security" based on a search through JSTOR, a digital library of academic journals, books, and primary sources.
12. This could be deliberate or inadvertent, as is the case for cyber operations against nuclear command and control systems.
13. Arguing that an even distribution of power is more stable see: Hans Morgenthau, *Politics among Nations*, (New York: Alfred Knopf, 1967); John Mearscheimer, "Back to the Future," *International Security* 15, no. 1 (1990): 5–56; William C. Wohlforth, "The Stability of a Unipolar World," *International Security* 24, no. 1 (1999): 5–41. Arguing that preponderance is more stable see: Geoffrey Blainey, *Causes of War* (New York: Free Press, 1973).
14. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* 45, no 4 (2020): https://doi.org/10.1080/01402390.2020.1732354
15. Joshua Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks* (2019, September 16): https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/; Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (2021): 51–90; Robert Chesney and Max Smeets (eds), *Deter, Disrupt, or Deceive? Assessing Cyber Conflict as an Intelligence Contest?* (Georgetown University Press: Forthcoming).

16. Lucas Kello, *The Virtual Weapon and International Order* (Yale: Yale University Press: 2017); also see: Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* 40, no. 1–2 (2017): 92–117; Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly* 77 (2015): 8–15; Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security* 43, no. 3 (Winter, 2016): 44–71.
17. Michael P. Fischerkeller and Richard J. Harknett, "What is Agreed Competition in Cyberspace?," *Lawfare*, February 19, 2019: https://www.lawfareblog.com/what-agreed-competition-cyberspace; James N. Miller and Neal A. Pollard, "Persistent Engagement, Agreed Competition and Deterrence in Cyberspace," *Lawfare*, April 30, 2019: https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace.
18. Gadi Wolfsfeld, Elad Segev, and Tamir Sheafer, "Social Media and the Arab Spring: Politics Comes First," *The International Journal of Press/Politics* 18, no. 2 (2013): 115–137.
19. Shires, *The Politics of Cybersecurity in the Middle East*.
20. Erica D. Borghard and Shawn W. Lonergan, "Confidence Building Measures for the Cyber Domain," *Strategic Studies Quarterly* 12, no. 3 (2018): 10–49.
21. Edward Geist, "Deterrence Stability in the Cyber Age," *Strategic Studies Quarterly* 9, no. 4 (2015): 44–61.
22. Donnelly et al. define cyber stability as "absence of serious hostile cyber actions . . . [between states], where the states have a sufficient common understanding of each other's capabilities and intentions so as to be inclined generally to avoid such actions, likely associated with a common belief that the costs of such conduct would outweigh the benefits"; D. A. Donnelly et al., "A Technical and Policy Toolkit for Cyber Deterrence and Stability," *Journal of Information Warfare* 18, no. 4 (2019): 53–69.
23. Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *The American Journal of International Law* 110, no. 3 (2016): 425–480; Anders Henriksen, "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 2.
24. Jon R. Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Regulation and Governance* 19, no. 6 (2017): 493–514.
25. For comparison, see e.g. Shires, *The Politics of Cybersecurity in the Middle East*.

26. Susan Leigh Star and Karen Ruhleder, "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces," *Information Systems Research* 7, no. 1 (1996): 111–134.
27. Nathan Ensmenger, "The Environmental History of Computing," *Technology and Culture* 59, no. 4 (2018): S7–S33, S14.