

LETTER FROM OUR MANAGING EDITOR.....	3
--------------------------------------	---

EDITORIAL INTRODUCTIONS.....	4
------------------------------	---

WHOSE SECURITY IS CYBERSECURITY? AUTHORITY, RESPONSIBILITY AND POWER IN CYBERSPACE

Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interaction	18
<i>James Shires</i>	

The Politics of Cybersecurity: Balancing Different Roles of the State.....	37
<i>Myriam Dunn Cavelty and Florian J. Egloff</i>	

Conceptualizing Active Cyber Defence in Cyber Operations: <i>Quo Vadis</i> , Switzerland?	58
<i>Bastien Wanner and Solange Ghernaouti</i>	

Safe at Home: Towards a Feminist Critique of Cybersecurity	83
<i>Julia Slupska</i>	

Internet, Social Media and Conflict Studies: Can Greater Interdisciplinarity Solve the Analytical Deadlocks in Cybersecurity Research?.....	101
<i>H. Akin Ünver</i>	

FEATURE INTERVIEW: Ms.Stephanie Snyder.....	125
---	-----

GENERAL SECTION

Implications of Migration for the Contemporary State: Paradoxes of Conventional Statehood in Liberal World Order	133
<i>Hassan Fiaz</i>	

China, the Belt and Road Initiative, and the Hambantota Port Project.....	153
<i>Shantanu Roy-Chaudhury</i>	

The Chinese Triad Trials: Political-Criminal Cooperation and Legitimate Economic Investment as Modern Trends in Organized Crime in Asia.....	165
<i>Brody Weinrich</i>	

The Durability of Peace: Examining Factors in Peace Agreements in the Aftermath of the Salvadoran Civil War.....	183
<i>Joshua S. Ebiner</i>	

Book Reviews.....	199
-------------------	-----

LETTER FROM OUR MANAGING EDITOR

3

Oxford, May 2019

Dear Reader,

Welcome to the May 2019 issue of the St Antony's International Review (STAIR).

Many of the most salient contemporary challenges to international security and governance are defined by the attributes of cyberspace. The cyber domain, according to existing research, is fundamentally transforming key characteristics of international relations as an academic discipline as well as an every-day reality. This issue of STAIR, entitled 'Whose Security is Cybersecurity?', seeks to contribute to a burgeoning body of literature by focusing on three factors underpinning the dynamics of international affairs in cyberspace: authority, responsibility, and power. In so doing, it gathers contributions that elaborate on the persistent challenges facing states, private companies, and individuals in navigating the cyber threat landscape as well as a regulatory framework defined by ever-ambiguous divides between the regulators and the regulated.

The feature interview with Stephanie Snyder, Commercial Strategy Leader for Cyber Solutions at the risk management company Aon, further reflects on these issues as well as the challenges pertaining cyber risk management in the private sector. The interview hopes to provide a practitioner's perspective from the field to complement the academic, theoretical, and conceptual debates presented by contributors to this special issue. It includes valuable insights and recommendations for young professionals aspiring to make a contribution in the cybersecurity field.

True to STAIR's tradition, this issue presents contributions of established academics and emerging scholars from various academic backgrounds. At STAIR, we are confident that scholarly and expert knowledge can play a positive role in society, and we see our search for excellence in sourcing and publishing articles as part of that role.

I would like to offer my personal gratitude for the hard work of the entire STAIR editorial team in preparing this issue, as well as for the guidance of our senior member, Kalypso Nicolaïdis. I would also like to thank all members of the STAIR Advisory Board, St. Antony's College, and the Department of Politics and International Relations for supporting STAIR.

I sincerely hope you enjoy this issue of STAIR.

Best wishes,

Linda Slapakova
Managing Editor

EDITORIAL INTRODUCTIONS

I. Theme Section Introduction

Kirstie Bosman, Taylor Grossman, Huu Phu Gia Nguyen

II. General Section Introduction

Aleksei Opacic, Carina Uchida, Sophie Vériter

III. Book Review Introduction

Jan Tomek

I. Theme Section

A Field Facing Challenges

Cybersecurity scholarship appears to face more challenges than most academic fields. First, the field is inherently interdisciplinary, spreading across a range of academic areas with distinct vocabularies, value propositions, and incentive structures. Because political scientists often lack in-depth technical know-how, assessments by these academics regarding the risk of cyber threats, or actors' security in cyberspace, vary widely. Some argue that cybersecurity is an over-hyped threat,¹ while others focus their research on cyber war as an imminent reality.²

At the same time, technologists frequently neglect the political and social dimensions of cybersecurity. These deep tensions create challenges for politicians and policymakers attempting to develop coherent norms of behaviour and protective policies in cyberspace. Should states pursue active defense (also known as 'hacking back')? Do states have a "duty to hack" when they can achieve their military objectives through cyber operations, instead of pursuing kinetic alternatives?³ In short, the disjunct between the expertise needed to understand the technical, social, and political aspects of cybersecurity creates inherent tensions within the field.

The second, and related, challenge facing the field of cybersecurity is the distinct lag between research and policy. The production of academic scholarship is not well equipped to deal with the high-speed development of digital technologies; industry innovation continues to outpace academics' abilities to analyse and interpret new developments. Politicians and lawmakers also struggle to keep up with the fast-paced nature of the digital era.

Law has often trailed behind technological advances; in the era of Moore's law, this gap has only widened. Proactive cyber regulations are difficult to build, as policymakers do not know what cyberspace will look like in five or ten years' time. And yet, policy-

makers cannot fall back on ‘standard operating procedures,’ lest they find themselves completely ill-equipped to deal with future risks and challenges in this area. Thus, most lawmakers and politicians are left uncertain not only of what the relevant threats in cyberspace are, but also of what to do about them.

Finally, more than other domains of international relations, cyberspace entails the coordination of a cacophony of actors that do not conform to traditional ‘levels of analysis’ or geographic bounds. From online banking to social media, and GPS to advanced medical treatment, digital technology has become embedded in the fabric of private and social life, connecting individuals all over the globe. Domestic and multinational companies are key actors in cyberspace. The private sector was the main developer of information technologies and thus has shaped their trajectory.⁴ Indeed, much of the physical infrastructure through which the Internet operates remains privately owned.⁵

Private-sector companies face competing incentives, and the competitive nature of ‘start-up’ culture does not generally reward the security-minded. Indeed, most new IT companies focus their early efforts on growing exponentially; thoughtful cybersecurity is often an expensive and time-consuming endeavour that does not lead to many early customers. Older companies also face the challenge of updating legacy systems, leading them to develop quick fixes instead of employing a more powerful security-by-design frameworks.

Simultaneously, governments face both the challenge of regulating this space, and the burden of securing their own infrastructure from external threats. Cyberspace is a convenient site for ‘bad actors’ to shield their true identity, making regulation and prosecution inherently difficult enterprises. States like the US face threats from adversarial nations and non-state actors alike. In short, the plethora of actors in cyberspace confounds traditional ways of studying international interactions and exacerbates the challenges of collective action in creating stable norms and regulatory practices.

Whose Security is Cybersecurity?

These challenges are likely to persist. The starting question of this theme section in this edition of STAIR, ‘Whose Security is Cybersecurity?’, has conceptual, practical, and normative elements. Who or what is insecure? How are they made insecure? Equally, there is a practical element: who is *actually* securing cyberspace? Finally, there is a significant and foundational normative element: who or what *should* be responsible for the provision of cybersecu-

rity? Or, more broadly: how *ought* we secure cyberspace?

These strands of debate have all too frequently remained siloed from one another. Political scientists who study norms consider the *ought*, while others focus on who and how. Meanwhile, policymakers and industry leaders are faced with the day-to-day challenges arising in cyberspace, and the shifting threat landscape. This edition of STAIR intends to move this debate forward by recognising the importance of integrating these separate questions into one coherent discipline. Before addressing the concepts of ‘security’ and the ‘cyber domain,’ upon which these discussions rest, we briefly elaborate on the two components of the question, ‘whose security is cybersecurity?’

First, who (or what) needs protecting, and from who or what do they need protecting? The conventional subjects of cybersecurity are understood to be systems, networks, and infrastructures, together comprising what is called cyberspace. Most scholars refer to the direct subject of cybersecurity as “the technical plane comprising machines and networks whose uniform feature is manipulability by code.”⁶ Yet, cyberspace is also a fundamentally human-centric realm. This issue of STAIR aims to push beyond these technical understandings and re-focus on the human. While individuals occupy a central place in cyberspace, the socio-political consequences of change in digital technologies remain under-examined. System security does not always coincide with human security. The focus on the technical over the human appears to be a feature of Western cybersecurity studies; recent scholarship has begun to examine non-Western cybersecurity narratives, which often approach these questions and trade-offs quite differently.⁷ Moving beyond the conventional focus on malware, espionage, and cyberattacks, this body of literature suggests adopting a wider lens, stressing the importance of human security. Digital technology is deeply entangled with individuals in ways that go beyond traditional understandings of inter-state and inter-governmental interactions. Thus, a human-centrist approach crucially requires a widening of the traditional domain of who/what is considered to be threatened in cyberspace.

Second, who/what is doing the protecting, and how? These questions tug at the nature of the private-public sector relationship in regulating cyberspace. States have become increasingly involved in shaping the trajectory of cybersecurity, from investing directly in new security technologies, to instituting requirements for the private sector regarding data storage and IT security. The recent proliferation of legislation and regulation at the international, national, and local levels has complicated questions of authority,⁸ as such legislation often obfuscates who is in charge of

what facet of protection. By redefining what cybersecurity encompasses, this issue of STAIR also seeks to provide a timely understanding of the (potentially limited) role of nation-states.

On the other hand, private sector actors are undergoing a rigorous process of re-defining their roles as cybersecurity providers, facing backlash from both consumers and regulators alike. Unicorn companies like Facebook are increasingly held responsible not only for data regulation, but also for actions that have political implications.⁹ Digital technology is deeply entangled in individuals' everyday lives, inflating companies' degrees of influence. Governments are concurrently increasing security demands on companies, including instituting new data protection laws (such as GDPR or California's 'Internet of Things' laws) and providing new guidelines for robust cybersecurity.¹⁰ At the same time, tech companies are urging governments to improve their legislation on cybersecurity and data protection, as many emerging issues lie beyond the capability of private firms.¹¹ In sum, the division of responsibility between the public and private sectors for securing cyberspace is often unclear. Questions of authority in cyberspace continue to be a source of contention. How can we overcome the growing challenges of coordinating regulatory cybersecurity practice on a global scale, especially as digital technology becomes increasingly integrated into our everyday lives? This issue seeks to explore this challenge and broaden the debate regarding the allocation of responsibility in cyberspace.

Conceptual Debates: Security and the Cyber Domain

Cybersecurity implicitly engages with the debate about what constitutes 'security.' Traditional Security Studies (TSS) take states to be the primary actors in international relations and the referent objects of security. Broadly speaking, despite a great deal of internal variation, TSS assume states are unitary rational actors seeking to maximise security in an anarchic international system, where 'security' is usually understood in material terms and, for realists, to be zero sum.¹² Thus, the referent objects are states, the threats are other states, and these threats are assessed in terms of relative (material) power.

More recently, the literature has undergone both a broadening and a deepening of understandings of security. These developments have reflected normative shifts regarding whose security ought to matter, as well as what 'counts' as a security issue. In 1983, Buzan introduced a broader, "sectoral approach" to security, outlining five major sectors: military, political, economic, social, and environmental. In the 1990s, understandings of security

deepened, focusing on referent objects traditionally ‘below’ the state. For instance, Buzan et al argue that society is the correct referent object of security, as being human entails being part of specific social groups.¹³ Critics point out, however, that this cannot account for the insecurities faced by social outcasts or (minority) groups facing systematic discrimination.¹⁴ This intuition—that ‘security’ does not make sense without reference to individual human beings—is expressed by Booth and McSweeney, kick-starting a move to Critical Security Studies (CSS), which came to dominate the discourse on security in the years following the Cold War.¹⁵

The literature on CSS quickly fuelled a move towards a new way of thinking about security: human security. The notion of human security made its first appearance in a 1994 UNDP Report, which emphasised the need to protect individuals, and the responsibilities of the international community to do so. Human security is grounded on the notion that every individual has a right to basic human needs and broadens the concept beyond Buzan’s sectors to include health, personal, and community security. Thus, the referent objects of security are individual humans, and the threats can be anything from hunger and disease to repression, gender inequality, and domestic abuse. In sum, the question ‘what is security?’ is at least as normative as it is conceptual, and crucial to answering the question, ‘whose security is cybersecurity?’

The term ‘cyber’ also sits on an axis of perpetual debate. Some academics favour a narrow interpretations of ‘cyberspace,’ while others lean toward a more inclusive and wide-ranging definitions. For instance, Clarke and Knake (2010) define cyberspace as “all computer systems and networks in existence, including air-gapped systems.”¹⁶ Kello (2017) similarly understands cyberspace as the “technical plane” of networks and machines within which the “virtual weapon” (computer code) can operate, and thus defines cybersecurity as measures to protect this plane from hostile action.¹⁷ However, unlike traditional technical scholars, Kello includes a *social and political plane* of ‘cyber’ interaction, which he calls the “cyber domain.”¹⁸

In US policy-making circles, the perennial joke is that ‘cyber’ is simply the term used to describe a computer that has entered the District of Columbia.¹⁹ These definitional arguments are theoretically situated, but can also have wide-ranging practical implications. How do we delineate the kinetic from the virtual? These debates impact how we structure and regulate borders and peripheries, as they cross from the concrete to the electronic.

Where does this leave cybersecurity studies? Cybersecurity literature inherently engages with these definitional debates, even if not explicitly. Scholars have often attempted to offset this potential problem by drawing precise and neat terminological borders around cyberspace and the field of cybersecurity. They have imported frameworks—often from war studies, international security studies, or economics—and, with a few minor adjustments, finagled the cybersecurity debate so that it fits into an already existing scaffolding.

Much of the early cybersecurity scholarship employed nuclear strategy as a starting point for a comparative understanding of cyberweapons.²⁰ More recent scholarship has likened cybersecurity and the proliferation of breaches and attacks to the use of sanctions, particularly in the context of the threat of ‘cyberwar.’ Analogical reasoning continues to permeate more contemporary scholarship.²¹ These comparative frameworks have both fuelled some scholars to conclude that a ‘cyber Pearl Harbour’ is imminent,²² while simultaneously leading other prominent thinkers to conclude that ‘cyberwar’ is a practical impossibility.²³ Many of these arguments hinge on a very narrow definition of ‘cyberwar,’ thus neglecting some of the more interesting and ambiguous questions in cyber-enabled conflict.

These analogies have helped to underscore important similarities and differences between cyber and other security threats. Analogical conceptual frameworks have also helped make cybersecurity more practicable and approachable.²⁴ However, this method of comparative framing can also prove theoretically and practically limiting. Even when scholars use analogies to highlight differences, these methodological choices can circumscribe our understandings of how cybersecurity shapes our world. The literature on cyber-attacks often narrows its scope to only include attacks that cause direct physical harm, allowing many thinkers to ignore a range of other grey areas in this space.²⁵ Analogical thinking constrains our analysis; older frameworks often fray or crack when they are applied to cyberspace, leaving many theorists to focus on these moments of divergence, rather than widening and complicating their picture of cyberspace.

Introduction to the Articles in This Issue

This theme section, entitled ‘Whose Security is Cybersecurity?’, intends to press beyond the analogical and definitional in-fighting that too often plagues cybersecurity studies. While

remaining grounded in conceptual questions, the articles in this theme section push past the theory-policy deadlocks in the field to discuss what policy informed by these debates might, and should, look like.

James Shires directly addresses this issue's main question by offering three conceptions of cybersecurity, each reflecting one of the three main subjects of cybersecurity: national, commercial, and individual. The article first elaborates on typology, arguing that, depending on the framework and scope of the matter at hand, these concepts suggest a diverse set of subjects to be protected and potential offenders. Shires explores where national, commercial, and individual cybersecurity compliment and conflict with each other, delineating their similarities and differences. This typology is particularly helpful in systemising ongoing works of cybersecurity and understanding the fundamental sources of conflict among them. By providing a theoretical framework for present-day cybersecurity debates, Shires' piece can act as a foundation for transdisciplinary scholarly efforts to establish a common linguistic mode in order to work towards "a more inclusive, and more optimistic, digital future" (Shires, p.32.).

Myriam Dunn Cavelty and Florian J. Egloff examine one specific facet of cybersecurity: the novel and evolving role of the state. Specifically, they focus on liberal democratic states and how they manage national cybersecurity. Cavelty and Egloff argue that extensive interactions between states, businesses, and society in shaping cybersecurity policy require states to negotiate interests and maintain flexibility in the roles that they adopt. The authors depart from traditional understandings of the role of the state as a security actor in international relations, broadening the debate by discussing an array of increasingly complex roles that the state embodies in the cyber domain, from security guarantor to threat actor. This constitutes a comprehensive examination of the historical development of the roles of the state in these capacities, laying the groundwork for future researchers. In sum, Cavelty and Egloff provide a timely analysis that captures the increasingly ambiguous role(s) of the state in cybersecurity policy.

Bastien Wanner and Solange Ghernaouti address an important aspect of national cybersecurity strategies: active cyber defence. They argue that the increasing complexity of cyberattacks has prompted states to take active measures to secure their systems and networks. The piece juxtaposes the concept of active cyber defence with both passive defensive and offensive measures, providing empirical observations of American, French, and Swiss active cyber defence policies. Specifically, Wanner and Ghernaouti hone in on the US and France as examples that demonstrate the

innovative edge of active cyber defence capabilities. Next, Wanner and Ghernaouti analyse Switzerland as a case study that raises key questions in state policy development of active defense. Wanner and Ghernaouti offer several recommendations, including: “[T]he armed forces need to adapt their operational availability to allow timely provision of defensive measures to private-sector operators. This will require re-evaluation of modes of communication and cooperation between the armed forces, civilian agencies and critical infrastructure operators” (Wanner and Ghernaouti, p.78).

Employing a critical approach to the central question of this section, ‘whose security is cybersecurity?’, Julia Slupska draws on feminist literature to examine individual cybersecurity through the example of smart home security devices. She argues that the ways in which traditional cybersecurity discussions have reinforced public/private binaries have neglected individualised threats facilitated by digital technology, particularly gendered insecurities such as gendered abuse facilitated by digital technology in the form of ‘revenge porn’ or intimate partner violence (IPV). As such, Slupska proposes an understanding of cybersecurity as measures “designed to protect against threats mediated by digital technology” (Slupska, p.84). Her feminist approach focuses on individual humans, rather than simply machines or information, as the referent objects of cybersecurity, and urges researchers to consider the ways in which social structures, particularly gendered ones, can operate through information architecture to threaten individuals. Reviewing forty smart home security analysis papers, Slupska finds that the IPV threat model is largely ignored, a fact which underlines the importance of critical studies of information architecture. In her definition of cybersecurity, Slupska pushes past traditional public/private binaries to include socially-contingent threats perpetrated through digital technology. This new analytical framework opens the doors for a wave of critical cybersecurity studies to address previously understudied practical and policy challenges in this new metaphorical ‘space’ of interaction.

Addressing current challenges to studying cybersecurity, H. Akin Ünver offers an account of how digital conflict studies is emerging as an increasingly useful tool for cybersecurity research projects. Ünver observes that existing scholarship suffers from a serious lack of data and empirical testing, which risks populating the discipline with mere conjectures and untested theories. Through integrating Internet and social media research tools, he argues, digital conflict studies can be a useful framework for cybersecurity scholarship in IR to adopt to address the short-term methodological and conceptual deadlocks it faces. Ünver concludes by calling for more rigorous data collection, asserting that scholars

need to hold cybersecurity research to higher standards in order to generate more effective dialogue among academic communities to address theoretical and practical issues. Cybersecurity scholarship promises interdisciplinary productivity; Ünver argues that digital conflict studies research projects and standards are necessary for fulfilling that promise.

Finally, this issue of STAIR explores the shifting role of the private sector in a feature interview with Stephanie Snyder, SVP and Commercial Strategy Leader for Cyber Solutions at Aon. Snyder deals with many of the practical implications of an ever-changing landscape of cybersecurity policy—from the difficulties of adhering to the GDPR in Europe, to the challenge of keeping up with new federal and state legal frameworks in the US. Managing cybersecurity is not simply a matter of a conceptual debate: for many companies, the digital revolution has meant importing an entirely new paradigm for securing customer data, protecting proprietary technology, and defending internal and external communications. Companies are scrambling to stay one step ahead of rogue criminals and nation-states alike. Additionally, the private sector faces a continual shortage of expertise in this field. Snyder touches on several of the major challenges companies face in cyberspace, providing insights into how to better prepare for proliferating insecurities in cyberspace.

II. General Section

To accompany the selected articles of this STAIR issue's thematic section, the General Section typically features pieces from a wide variety of disciplines. The May 2019 issue includes original contributions about migration in the liberal world order, China's growing economic engagement in the Asia-Pacific region, organised crime in China and the Salvadoran Civil War of 1979-1992.

In the opening article, Hassan Fiaz challenges orthodox international relations theory, which views the modern state as an autonomous, authoritative entity, by exploring the competing and oftentimes contradictory forces the state must navigate in the context of migration politics. Fiaz draws on a number of case studies about issues ranging from national identity to economic development in far-reaching contexts in order to analyse states' responses to these economic and political forces. He draws these cases together to demonstrate the interrelated implications of migration for each of the major components of statehood – territory, a distinct population, and sovereign capacity – emphasising in particular their malleability and mutability.

In the next piece, Shantanu Roy-Chaudhury looks at the growing geoeconomic importance of the Asia-Pacific region and China's increasing economic engagements in this realm, which are being boosted by the Belt and Road Initiative. This article particularly examines China's expanding presence in Sri Lanka, focussing on the Hambantota Port project, the largest Chinese-run project in Sri Lanka, which Roy-Chaudhury argues is a major national security concern for India. The author argues that growing Chinese investments will negatively impact Sri Lanka in the long run.

In a separate piece, Brody Weinrich argues that substantial economic growth in East Asian economies, particularly China, have been accompanied by the evolution of transnational organised crime. While organised crime has been a long staple of China's black economy, the twentieth century saw new versions of criminal groups increasingly involving themselves in politics given, what Weinrich argues, is a functional use to the state and politicians. Focusing on the Shanghai Green Gangs and Hong Kong-based triads, Weinrich argues that it is the political dimensions of triad activity which cemented their role as key players in the regional transnational crime often seen today.

Joshua Ebner evaluates the conditions and variables that impact the non-proliferation of negotiation completion through the case of the Salvadoran Civil War (1979-1992). From information failures to credible security guarantees, the author extrapolates upon the complex interaction of international and domestic conditions that influence the enforcement of peace agreements and outbreak of civil war. The probability for the durability of peace is therefore evaluated under the increasing occurrence of intra-state conflict in the current international political arena.

We hope that the General Section of this issue will serve as a valuable addition to the contributions presented in the Theme Section on cybersecurity, offering additional insights on the changing dynamics of world politics.

III. Book Reviews

It is a pleasure to introduce this edition's book review section. Highly relevant in relation to this edition's theme, all five reviewers cover publications centred on cybersecurity in all of its diversity, while simultaneously managing to strike the right balance between technical competency and accessibility. Samuel Forsythe, a doctoral research student at the Peace Research Institute Frankfurt and Goethe University and graduate of Philosophy and War Studies at King's College London, reviews Lucas Kello's *The Virtual*

Weapon and International Order. Authored by one of the world's leading International Relations (IR) scholars currently working on cybersecurity, the book skilfully extrapolates well-known IR-specific theoretical concepts to the cyber-realm. As Forsythe is quick to point out, Kello's propensity to coin new terminology, rather than repurposing old IR terms is a double edged sword, the author's insistence on combating 'strawman arguments' being the sole other not-unambiguously-positive aspect of the *Virtual Weapon*.

Anisa Kassamali, an alumna of SOAS and a trainee solicitor, contributes to STAIR for the second time in a row. She examines *The People Vs Tech: How the Internet Is Killing Democracy (and How We Save It)* by Jamie Bartlett, a publication aiming to reach the broadest audience out of all books reviewed here, which she assesses it on its own considerable merits. The publication's author argues that some of the more predictable effects of information technologies are also some of the biggest threats to democracy, ranging from internet users' gradual loss of civil attachment or responsibility to the negative socio-political effects of mass-scale job loss resulting from automation. While Bartlett's book being novel and well-argued overall, the reviewer highlights the latter's failure to touch upon the structural reasons behind current corporate behaviour that promises to only continue exacerbating this challenge.

Claudine Tinsman, a doctoral (DPhil) researcher in Cyber Security at University of Oxford, reviews *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* by Bruce Schneier. The latter is also on the more pessimistic side of extrapolations of current cybersecurity trends. Tinsman highlights the author's admonition of how modern technology will only render large-scale cyberattacks more disruptive and potentially lethal. She also adeptly points out how the book decries governments' reluctance to tackle these dangers, currently preferring surveillance over tackling structural vulnerabilities of said cyber-technology. While lauding the book on a whole, especially the author's policy recommendations and his example of the European Union as a pioneer in setting safer technological standards, Tinsman would like to see a deeper exploration of how political considerations prevent even further progress.

Rachel Hirshman, a master's student at Stanford University studying Management, Science, and Engineering, reviews *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* by Ben Buchanan. The key IR concept of the 'security dilemma' gets exported to the cyber-realm here, rendering miscalculation and escalation ever more likely. Hirshman points out how attribution of

a given cyberattack to a specific state actor becomes more complex in case of automation, in addition to bemoaning the narrow definition of ‘state actor’ espoused by Buchanan. Finally, James Sullivan, an alumnus of Duke University currently pursuing a Master of Liberal Arts in IR at Harvard University, reviews the edited volume *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Campaigns of disinformation and attempts of large-scale voter manipulation are an extremely topical issue, but as the reviewer explains, technology and propaganda have always tended to go hand in hand. Much like Schneier and Buchanan, the authors of this edited volume provide policy recommendations and anticipate the issues of automation and attribution. Sullivan finishes his review concluding how the old days of unrestricted access to the internet and near-perfect anonymity online have likely ended. Overall, the reader of this issue can look forward to a compelling collection of reviews of an equally compelling selection of relevant recent literature on cybersecurity.

Notes

Erik Gartzke, “The Myth of Cyberwar,” *International Security* 38, no. 2 (2013): 41–73; Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.

James P. Farwell and Rafal Rohozinski, “The New Reality of Cyber War,” *Survival* 54, no. 4 (2012): 107–20.

Duncan B. Hollis, “Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?” in *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein (Oxford: Oxford University Press, 2015).

Jungbae An and In Tae Yoo, “Internet Governance Regimes by Epistemic Community,” *Global Governance* 25, no. 1 (2019): 123–48; Milton Mueller, *Network and States: The Global Politics of Internet Governance* (London: MIT Press, 2010); Dmitry Epstein, “The Making of Institutions of Information Governance: The Case of the Internet Governance Forum,” *Journal of Information Technology* 28, no. 2 (2013): 137–49.

For example, see Joseph S. Nye Jr, “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* 5, no. 4 (2011): 28. He reflects the common knowledge that most of the Internet and its infrastructure are privately owned.

Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017).

Jon R. Lindsay, “The Impact of China on Cybersecurity: Fiction and Friction,” *International Security* 39, no. 3 (2015): 7–47.

Ronald Deibert and OpenNet Initiative, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (London: MIT Press, 2010); Ronald Deibert and

International Development Research Centre (Canada), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (London: MIT Press, 2012); An and Yoo, "Internet Governance Regimes by Epistemic Community."

Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford University Press, 2018).

Facebook is always a great example. For government holding tech companies to higher standards, see for example: Kevin Roose and Cecilia Kang, "Mark Zuckerberg Testifies on Facebook Before Skeptical Lawmakers," *The New York Times*, April 10, 2018, accessed May 18, 2019, <https://www.nytimes.com/2018/04/10/us/politics/zuckerberg-facebook-senate-hearing.html>; For tech companies increasingly allocating resources for cybersecurity, see for example: Lee Mathews, "Facebook May Buy A Cybersecurity Company To Prevent Another Major Hack," *Forbes*, October 22, 2018, <https://www.forbes.com/sites/leemathews/2018/10/22/facebook-buy-cybersecurity-firm/#1674fc2851fc>

Mark Zuckerberg, "Mark Zuckerberg: The Internet Needs New Rules. Let's Start in These Four Areas," *The Washington Post*, March 30, 2019, accessed May 19, 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.66a118c0ee9c.

Steve Smith, "The Contested Concept of Security," in *Critical Security Studies and World Politics*, ed. Ken Booth (London: Lynne Rienner, 2004), 30–32.

Barry Buzan, Jaap de Wilde, and Ole Wæver, *Security: A New Framework for Analysis* (London: Lynne Rienner, 1998).

Bill McSweeney, *Security, Identity and Interests: A Sociology of International Relations* (Cambridge: Cambridge University Press, 1999).

Ken Booth, "Security and Emancipation*," *Review of International Studies* 17, no. 4 (1991): 313–26; McSweeney, *Security, Identity and Interests: A Sociology of International Relations*.

Richard A. Clarke and Robert Knake, *Cyberwar: The Next Threat to National Security & What to Do About It* (New York: Ecco, 2010), 69.

Kello, *The Virtual Weapon and International Order*, 46.

Kello, 46.

See the following for examples of the overuse of the term cyber: Danny Yadron and Jeniffer Valentino-DeVries, "This Article Was Written With the Help of a 'Cyber' Machine," *The Wall Street Journal*, March 4, 2015, accessed May 18, 2019, https://www.wsj.com/articles/is-the-prefix-cyber-overused-1425427767?fbclid=IwAR0IWcJH1xKgTgJjFTlwQ1Hx_XvYc9jk-pADcVaD2jPomKhCW2WVJq-iKMnw; Andrew Futter, "'Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies," *Journal of Cyber Policy* 3, no. 2 (2018): 201–16; Brian Feldman, "Cyber' Is Here to Stay," *Intelligencer*, September 27, 2016, accessed May 18, 2019, http://nymag.com/intelligencer/2016/09/cyber-is-here-to-stay.html?fbclid=IwAR3mbXVdKMEiiTZp_Gr5i1khZJf2wwpeC8In6Parz-D33EAwwBx6VZkwlstM.

Jason Healey, "Healey: Cyber Deterrence Is Working," *Atlantic Council*, July 30, 2014, accessed May 18, 2019, <https://www.atlanticcouncil.org/news/in-the>

news/healey-cyber-deterrence-is-working.

George Perkovich and Ariel E. Levite, eds., *Understanding Cyber Conflict: Fourteen Analogies* (Washington, D.C.: Georgetown University Press, 2017).

Clarke and Knake, *Cyberwar*; Lisa Daniel, "Panetta: Intelligence Community Needs to Predict Uprisings," *American Forces Press Service*, February 11, 2011, accessed May 18, 2019, <https://archive.defense.gov/news/newsarticle.aspx?id=62790>; Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair*, March 2011, accessed May 18, 2019, <https://www.vanityfair.com/news/2011/03/stuxnet-201104>

Rid, "Cyber War Will Not Take Place."

Martha Finnemore and Duncan B. Hollis, "Constructin Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 425–79.

Larry May, "The Nature of War and the Idea of 'Cyberwar,'" in *Cyber War: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Claire Finkelstein (Oxford: Oxford University Press, 2015).

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

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.

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 Cavelti 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).

THE POLITICS OF CYBERSECURITY: BALANCING DIFFERENT ROLES OF THE STATE

Myriam Dunn Cavelty and Florian J. Egloff,
Center for Security Studies, ETH Zürich

Abstract

*In liberal democratic countries, the role of the state in cybersecurity is a politically contested space. We investigate that role along three dimensions: the first is **theoretical** and we look at existing cybersecurity literature, showing that international affairs literature is almost exclusively highlighting the role of the state as a security actor. We argue that this view is too narrow and risks limiting the discussion to only a few aspects of what cybersecurity entails. The second is **empirical** and we analyse policy development, showing the diversity of the roles the state imagines for itself. The state occupies six different roles in cybersecurity: (1) security guarantor, (2) legislator and regulator, (3) supporter and representative of the whole of society, (4) security partner, (5) knowledge generator and distributor, and (6) threat actor. The third dimension is **normative** and we investigate what the role of the state should be. To do that, we outline three main areas of tension between the state, the economy, and society in which cybersecurity policies are situated. Diverse coalitions of interests, spanning across the three social fields, support or challenge the six roles. Thus, two types of questions occupy the centre stage of cybersecurity policy: a question regarding the boundaries of responsibility (i.e., where does the responsibility of the state, economic, and societal actors start and end?) and a question regarding the concrete assumption of responsibilities (i.e., which means is an actor allowed to use to assume the responsibilities of his/her roles?). In sum, our conceptualisation enhances the understanding of cybersecurity as a diverse and crosscutting policy field. The result is a more comprehensive understanding of different roles of the state, which will help researchers with finding innovative research questions in the future.*

Introduction

What is cybersecurity? What seems like a simple question is at the heart of the political challenge this issue has become. Exemplified in the difficulties many state actors confess to have when it comes to agreeing on official definitions,¹ cybersecurity is notoriously hard to pin down and is contested politically in both national and international arenas. In explaining the reasons for this contestation, we will advance a better understanding of what cybersecurity has become and will highlight the diverse roles of "the state" that have emerged.²

Myriam Dunn Cavelty and Florian J. Egloff, "The Politics of Cybersecurity: Balancing Different Roles of the State." *St Antony's International Review* 15 no.1 (2019):37-57.

One reason for the difficulty in defining cybersecurity to the satisfaction of different stakeholders is the continuing evolution of the concept. Not so long ago, cybersecurity – or rather, its predecessor concepts, such as critical information infrastructure protection or information security – used to be an issue primarily discussed in expert circles as a technical or risk management problem. Now it has become a national security issue dealt with in the highest government circles, not least due to a marked increase in strategically motivated state activity in cyberspace, which is itself a side effect of current geopolitical tensions.³ High-level cyberincidents not only affect individuals or single businesses, but also are seen as a threat to states, societies, and economies. Consequently, states are reviewing their own offensive and defensive capacities and are consolidating their strategic planning regarding the use of cyberspace.⁴

However, cybersecurity is not only moving upwards in political agendas worldwide: parallel to the advancing digitalisation, which is reflected in the increasing computerisation and automation of processes in business and society, cybersecurity is also expanding as a problem area to a multitude of additional policy domains not traditionally within the narrow purview of security. Cybersecurity has become a new focal point for education and training of the cybersecurity workforce, makes an appearance as capacity building in development cooperation, has been linked to a new type of diplomacy in foreign policy, appears as cybermediation in conflict management, and, definitely not least, is considered an important business sector or, more generally, the backbone for economic viability in a digitalising world.⁵ Thus, cybersecurity is at the same time becoming more important, more diverse, and more diffused.

These developments raise pertinent questions for research that we explore in this article: How should cybersecurity be understood to do justice to its current and future conceptualisation in policy debates and political practice? Given its diversity, what roles and responsibilities do different actors have for which aspects of the complex problem? And which contestations between different actors structure the cybersecurity policy field?

To highlight the political governance aspects of the issue, we put ‘the state’ at the centre of this investigation. Using bibliographical data, a comparison of policy documents, and country-related policy papers from an ongoing research project as our main empirical basis,⁶ we show which different political functions the state is expected to perform in cybersecurity and which political and social problems arise as a result.⁷ On the one hand, the article undertakes a conceptual sharpening by showing empirically what

cybersecurity is from the state perspective. On the other, this article argues that cybersecurity must be understood in its multiple facets and as a cross-cutting policy field in which political trade-offs are necessary.

The roles of the state in cybersecurity can be investigated in at least three dimensions. A first dimension is *theoretical*. In what ways does the existing literature theorise the role of the state? A second dimension is *empirical*. It encompasses questions such as: What role does the state play in building cybersecurity as national security (both active and passive)? What other roles do states play today? What kind of institutions are there that deal with cybersecurity? What are their tasks? How do they work? What impact does the special way cybersecurity looks today have on societal security? The third dimension is *normative* and investigates the question of what the role of the state should occupy. We consider all three dimensions to be important and therefore dedicate a section to each of them.

In the first section on the theory, we focus on existing definitions of cybersecurity as well as on the literature on cybersecurity politics. We note that the cybersecurity literature in international relations and political science more generally looks at its topic almost exclusively as an international security problem. This, we argue, is too narrow. National cybersecurity strategies illustrate that cybersecurity touches a multitude of issues in different policy areas. In the second section, we therefore highlight manifold roles of the state, partly desired by the state itself and partly demanded from outside. We situate cybersecurity concerns as emerging from three areas of tension between state, economy, and society. This, we show, leads to political conflicts inside and outside the state on several levels, due to the varied interests of different stakeholder groups.

We conclude that cybersecurity policy encompasses problems in these three areas of tension that can only constructively be dealt with if different interests are understood and consciously balanced. Such a policy finds a balance between the thematic alliances existing in societies, the different departments of the state, and the various interest groups of the economy. Different visions of the role of the state are therefore reflected to varying degrees in the three areas of tension. Such an understanding provides a solid foundation for making strategic decisions, negotiating policy guidelines, and further researching the changing roles of the state around cybersecurity.

Given that cybersecurity is an empirically dynamic and fundamentally interdisciplinary issue, doing justice to the literature is not a banal undertaking. First, ‘cybersecurity’ is a relatively new term, coming into existence only around the year 2000.⁸ Second, with origins in the computer sciences, cybersecurity has different meanings for different research communities. To get a better understanding of how the literature treats ‘the state,’ we first attempt to get an ‘objective’ overview that extends beyond our own disciplinary bias through using two of the most prominent scientific databases, World of Science (WoS) and Scopus.⁹ Second, we dig deeper into the most cited articles¹⁰ to identify the different roles of the state that make an appearance in the literature on an abstract level. Last, we look at how international relations literature has treated the subject to identify the most pertinent gaps.

Cybersecurity research across disciplines

The two prominent scientific databases, World of Science (WoS) and Scopus, show that from 2012 to 2014, the quantity of scientific output on ‘cybersecurity’ almost doubled. In both databases, computer science tops the list of research areas with a very high percentage (WoS: 72 percent / Scopus: 61 percent), followed by engineering on the second rank (WoS: 36 percent / Scopus: 40 percent).¹¹ All the top ten cited articles in both databases focus on smart grids and/or SCADA (Supervisory Control and Data Acquisition) systems, a category of software used in many industrial processes to control equipment and conditions. Though the larger backdrop of insecurity resonates with the national security narrative, the technical view on cybersecurity is predominant, with little to no interest to understand the threat context. The main aim of research is to develop better cyber incident prevention, protection, and detection capabilities on the one hand, and more ‘resilient’ systems and infrastructures, signifying timely recovery of functionality if under duress due to an attack, on the other. The role of the state is of very little to no interest in this literature.

Bibliographical data further reveals that social science research on cybersecurity issues is marginalised in comparison to research in the technical sciences. Scopus has ‘social sciences’ as a lump category in third place, with 18 percent, whereas WoS lists 31 percent of its cybersecurity records in the same category. There are two main focal points in top-cited research in the social sciences: the first is an interest in organisational and managerial aspects of cybersecurity, like ‘information sharing’ between state

and private actors¹² or the combination of technology with human and organisational factors.¹³ The state, argues the general opinion in the literature, is incapable of providing the public good of security on its own, since an overly intrusive market intervention is a flawed and undesirable option. This opinion is based on the observation that what the state aims to protect due to national security considerations is also the foundation of the competitiveness and prosperity of a nation.¹⁴ Hence, the state is treated as an important actor, while simultaneously there is much emphasis on the necessity to take into consideration the preferences of other actors.

The second focal point, fitting squarely into the 'international relations' sub-category, is the analysis of cyberwar and other threat forms. This literature aims to understand cybersecurity as a political phenomenon more generally, and specifically to understand how cybertechnologies change conflict dynamics, thus influencing the overall security in the international system. Before there were enough real-world cases to study, cybersecurity publications in this category focused primarily on cyberwar, especially the rhetorical hyperbole about it¹⁵ or how best to fight wars in cyberspace.¹⁶ Only more recently, traditional conflict research has started to look at the effect of cybertechnologies as tools in foreign policy and conflict using quantitative methods.¹⁷ This type of research asks how and to what degree cyberspace as a domain of warfare influences (inter alia) coercion, offence-defence theory, and deterrence.

The focus is on how cybertechnologies become tools for disruption and insecurity in the hands of political actors, and how this relates to the type of security tied closely to political borders and 'states.' Because a link is established to the abstract notion of 'national security,' states are the actors called upon to re-establish control over the use of cybertechnologies through international norms, yet are also the actors mainly responsible for creating more insecurity.¹⁸

The role of the state in the literature

Computer scientists and engineers' reasons to study cybersecurity are driven by the aim to make technical systems more secure. The type of security that is sought is a combination of the three IT-security goals: integrity, availability, and confidentiality of a resource.¹⁹ 'Cybersecurity governance' is the concept used to reach this type of security, a risk management approach based on continuous monitoring, measurement, and control of relevant processes.²⁰ The key concept here is 'regulation,' which comprises

various governance tools, such as industry standards, national laws, or international agreements, with the prime aim being to establish 'trust' and stability of expectations among different actors.²¹

Technically-oriented cybersecurity research tends to focus little if at all on the role of the state, given its decidedly different focus. However, as soon as we move towards questions of information sharing and other organisational measures that are usually treated in the social science literature, the state makes an appearance in its multifaceted capacity as a governor. According to governance theory, *governance* becomes important when political power is highly fragmented. Fragmentation of political power can occur through decentralisation when government tasks and authority are delegated downwards (localisation), upwards (supranationalisation), or sideways (privatisation).²² Fragmentation also takes place inside the government itself through ever-increasing functional differentiation of the administration.²³ Increasingly, performing tasks requires highly specific expert knowledge. The increasing division of labour, a hallmark of modern societies, blurs the lines between the public and the private sector. Many tasks that were previously performed by the state are now handled by specialised companies.

The network approach to governance therefore assumes that modern societies require new forms of public administration.²⁴ In this literature, the assumption is that the government can no longer simply issue instructions and monitor their implementation, but must also shape the framework conditions in such a way that cooperation operates smoothly even without constant oversight. Public administration thus becomes a team sport where persuasion, negotiation, and mutual trust are more important than control and regulation.²⁵ Thus, public services are provided by a plethora of independent, self-regulating, and self-organising networks. The role of the state in this type of literature is diverse. Depending on the research focus, the state and its bureaucratic entities is *security guarantor*, *legislator and regulator*, or *security partner*.

In the literature associated with international relations, there is a simpler view of the state. Predominantly, the use of cyberspace for strategic and military aims reinforces the neo-realist conception of interstate security in an anarchical system. In this system, states are 'black boxed' (they can all be treated as comparable units), and it is the balance of power which compels them to act in specific ways. Cyber offensive means are abstract instruments of power which can be used to threaten objects and services of value to the state and society (in peacetime and during conflict), and the question to be answered is whether they have a desired

effect in a particular context. Given this conception, states are also the actors called upon to re-establish control over the misuse of cyberspace through international norms, often by looking to lessons from previous security issues and solutions, like nuclear deterrence or arms control. In their roles as *security guarantors*, states act to maximise power or security, or to minimise threats. When they are considered enemies by other states, state actors emerge as *threats*.

There is an additional role in the literature, mainly to be found in the literature that applies the Copenhagen School's securitisation theory to cybersecurity.²⁶ *Securitisation* signifies the sum of the representation of a fact, a person, or a development as a danger for the military, political, economic, ecological, and/or social security of a collective and the acceptance of this representation by the respective political addressee.²⁷ The successful securitisation of a topic justifies the use of all available means, including those outside the normal political rules of the game. Therefore, a strongly mobilising discursive justification for this extraordinary situation must be made in the political process. This happens above all in the narrative representation of great danger threatening the state or society.

Here, the role of the state and its bureaucracies is problematised rather than looked at instrumentally. Securitisation theory deals with a type of security that is discursively tied to the highest possible political stakes: the existential threats to the survival of the state and its society. The invocation of security sets in motion a securitisation process that has the power to lift the issue out of the 'normal' (desirable) political sphere, so that the associated threat can be dealt with swiftly and with all necessary means.²⁸ Measured against an ideal of 'normal politics,' security is suspect.²⁹ Hence, numerous scholars have foregrounded the normative implications of securitisation processes and called for opposing or reversing the process in order to return to 'normal politics' instead.³⁰ In this type of literature, the state and its representatives are *securitisers*, which, in certain contexts, can again amount to being a *threat* to other states and to society more broadly.

Historical Development of Cybersecurity Policy

In what ways does this view contrast with what we can learn from the evolution of the policy field? In this section, we will look at the 'evolutionary history' of cybersecurity into a political and security problem to show that 'the state' had (and has) different roles driven by various factors over the years. This creates the historical embedding of the discourse on which functions the state

can, may, and wants to fulfil.

Telling the cybersecurity story from its inception means telling a strongly American-dominated story. Indeed, due to historical, political, social, and economic factors, the United States has shaped a large part of the information revolution in its early stages.³¹ In particular—and importantly for the current debate about cybersecurity—the United States was at the forefront of developing specific ways of understanding both the benefits and the risks of the emerging information age.³² When other countries began to think about the information age and politics, especially the needs of critical information infrastructure protection in the late 1990s, a lot of the policy concepts and threat perceptions were adopted from the United States, at least in their broad strokes. If we talk about the role of the state in what follows, we therefore claim some generalisability to other states, knowing that a detailed empirical analysis of different policies would unearth many country-specific details.³³

More, better, more?

In the 1980s, the cyber threat was still regarded as primarily affecting government networks and the debate was fixed on cyber-espionage. Only in the later 1990s can a qualitative change in threat perception be observed. More and more (American) documents have made a connection between computers (or information infrastructures) and so-called critical infrastructures, with specific effects on the debate.³⁴ They are described as critical because a failure or substantial impairment of these organisations and institutions could have dramatic consequences for society. The implementation of all these infrastructures with IT is a rapidly progressing trend.

In the second half of the 2000s, two developments in cyber aggression began to emerge: the first (already mentioned) is a shift of focus away from theoretical ‘doomsday’ scenarios towards the reality of cyber aggression in conflict situations affecting both state and non-state actors. The reason for this shift is the ‘normalisation’ of cyber conflicts below the war threshold as a constant accompaniment to political conflicts. The second is more attention to targeted attacks. On the one hand, we have an increase in so-called ‘mega hacks’—successful penetration into prominent economic or political targets. On the other hand, the focus of the political debate is now on so-called *Advanced Persistent Threats* (APTs)—capable actors, who use cyber means to achieve specific, persistent goals. Both mega hacks and APTs are a sign of the professionalisation of attackers and attacks, such as the Bundestag

hack. Together, they refer to the increasingly direct and indirect roles that states play in cyber aggression.

But even though much has been reported about state-orchestrated cyber operations in the media in recent years, high-level attacks with considerable impact are still relatively rare. The exceptions confirm the rule: prominent examples are the attacks on Saudi Aramco in 2012, against the electricity network in Ukraine in 2015 and 2016, as well as the global infections by WannaCry and NotPetya in 2017. Cyber means were used mainly for disruptive actions and destabilisation of the political environment, but rarely for destruction, due to the difficulties of achieving clearly controllable effects, and due to the prevailing strategic restraint of states. More unspectacularly, the vast majority of cyber incidents that companies and individuals face on a daily basis do not make headlines. They are simply too banal to gain media attention.

The relative ordinariness of cyber life leads to the fact that the probability of an anticipated cyber catastrophe must be proven in the political process. For this to work, the risk of such an event's occurrence—always relying on anecdotes and events of the present as 'near misses' and to illustrate 'what could have been'—is presented as imminent. Following the logic of these mobilisation attempts, quasi-apocalyptic 'worst-case' scenarios are used, which are associated with a gigantic extent of damage. In combination, this means that the main threat is no longer the actual risk of the catastrophe, but rather non-action in the present. And last, but not least, the 'logical' reaction to this kind of danger representation is the reflex-like call, 'the state is not doing enough for cyber security!' But what can 'the state' do at all? In the following sub-chapters we look at solutions and problems.

Military perception of danger ...

Originally, there was a sensitisation to a new threat posed by the reorientation of security policy following the collapse of the Soviet Union, when the US began to focus more on non-state actors who could pose a threat to American citizens through terrorist attacks. It was significant and disturbing that the 'new opponent' could no longer be clearly identified. Consequently, uncertainty assessments increasingly assumed the potential danger of the means, which could be available to potential opponents of the US, as well as a focus on one's own vulnerabilities.

In the first half of the 1990s, US government documents began to contain a growing number of warnings that national security was increasingly threatened by possible cyberattacks on power plants, banks, air traffic control, or armed forces.³⁵ In the

cybersecurity debate, hacking is seen not only as an activity that can be used by technically qualified individuals for minor offences, but also as a *modus operandi* for well-organised groups of actors with political intentions, such as terrorist organisations or states. Although most hackers may lack the motivation to use their knowledge to cause serious economic or social harm, government experts feared that people with these skills and low motivation could be made to act as cyber mercenaries incentivised by large sums of money.

Increasing warnings that national security is threatened by possible cyberattacks on critical facilities coincided with growing concerns about the vulnerability of US forces. Initially, the discussion about the *revolution in military affairs* and the computerisation of the armed forces was characterised by great euphoria. From the mid-1990s onwards, however, greater attention was also paid to possible risks. The formulation of strategies and doctrines, which no longer aim only at the enemy's forces, but also directly at their information flows, brought into focus the comparatively high vulnerability of the electronically strongly networked US troops. The further the discussion about attacks on the information systems of possible opponents progressed, the more intensively the possible dangers to one's own military and civil data networks were addressed.

... and civilian 'solution' approaches

Due to the strongly military nature of the debate, the US Department of Defense's responsibility for threatening the critical information and communications infrastructure seemed clear. However, the difficulties in dealing with threats that were no longer territorially limited and could no longer be identified by any identifiable actors quickly raised fundamental questions about the division of competences and legal regulations, as well as political and technical strategies of a new security policy. There were difficulties in identifying the perpetrators (attribution). Assigning blame based on *cui bono* logic (stands for 'whose benefit?') alone, however, is not a legitimate basis for political or police action. In an attribution determination, the scenario of an operation under false flag (an operation in which a third party pretends to be another actor) must always be evaluated.³⁶ Uncertainties about the possibilities and limits of attribution help state actors credibly deny their existence, so that they can officially distance themselves from attacks at any time.³⁷

While the doctrine for information warfare was further developed in the military area,³⁸ in the civilian area other actors tried

to get a grip on the vulnerability of society as a whole due to its dependence on inherently insecure information infrastructures. In 1995, the US *Presidential Commission on Critical Infrastructure Protection* (PCCIP) was established to produce a comprehensive report on the security of all US infrastructure systems. The main focus was on the still largely unknown threats from cyberspace. The PCCIP should assess these risks, develop defensive measures, and contribute to clarifying the institutional and legal reform needed. All relevant agencies were represented in the Commission, no longer just the security policy apparatus. In addition, the private infrastructure owners were also included. This approach assumed that, in the case of critical infrastructure protection, security policy could no longer be an exclusive task of the state, but required a sharing of responsibility, in particular, with the private sector.³⁹ The final report of the PCCIP laid the foundations for the ways in which critical infrastructures and critical information infrastructures are protected worldwide today.⁴⁰

Thanks in part to the revelations by former US National Security Agency employee Edward Snowden, we now know that intelligence services are probably the most important players when it comes to the strategic use of cyberspace. Precisely because of the focus on spectacular ‘cyber war’ scenarios, which could clearly be situated in the area of military operations, research has long overlooked how the practices in this community shaped strategic behavioural norms in cyberspace over many years. It is particularly important for the following explanations that intelligence services exploit (non-public) security gaps in common operating systems to exploit numerous strategically opportune locations of the Internet infrastructure for various purposes. Their accesses and implants can be used for numerous purposes (surveillance, espionage, disruptive actions, etc.) and can theoretically be activated at any time if they remain unknown to the victim. Such infected machines reduce the security of the entire system, and there is no guarantee that these gaps will not be detected and exploited by another party, such as other intelligence agencies, criminal hackers, or other politically motivated actors. The security of the entire Internet is thus deliberately—or for strategic reasons—endangered. Thus, the paradoxical situation arises that state actors are directly responsible for indirectly endangering the very same national security for which they are responsible.⁴¹

Role of the State in Cybersecurity Policy

Historically, we see a development of the roles of the state coinciding with three phases in cybersecurity policy. In a first role,

the state appears as the owner of endangered networks (*owner*). In a second role, the state appears as the actor who must solve the problem in terms of security policy (*problem owner*). Third and finally, the state or individual units within the state appear as the originator of the problem (*originator of the problem*). Importantly, this development is additive: new roles are assumed, whilst old ones remain, thereby increasing the complexity of the cybersecurity policy field. This development is shown schematically in Table 1.

Stage	Problem areas	Role of the state
1980s	• 'Hacking' is recognised as a problem in the political public due to different incidents • The main concern is the prevention of classified data being stolen from government and government-related networks • The solutions were mainly related to the state as the 'owner' of these networks and this information	owner
1990s	• Increasingly networked systems and commercialisation of the Internet lead to a bigger collective problem that concerns broader parts of society and the economy • Critical infrastructures become a focal point (from 1995 onwards) • Appeals are made to the state from public and private actors to improve the security of these systems and of the collective	owner problem owner
2000s	• The quantity of, quality of, and attention given to 'targeted attacks' increases • States (and intelligence services) are much more active as actors • States appear responsible for the situation becoming 'worse' • A cyber 'arms race' develops	owner problem owner originator of the problem

Table 1. Historical Roles of the State

As we saw in the previous section, the literature in international affairs focuses most strongly on the third and most recent role. However, cybersecurity policy documents from a variety of states display a much bigger empirical diversity.⁴² Through these, cybersecurity reveals itself as a typical cross-cutting issue, which requires cooperation between a wide variety of actors. Actors are not only drawn from a variety of public authorities, but also from business and civil society.

It is a truism that the state alone cannot ensure an increase of cybersecurity, not least because many crucial networks are in private hands. Cybersecurity is also to a large extent the responsibility of every individual and every company. Not only is industry (also including small and medium-sized enterprises) particularly

affected by cybercrime and espionage; most critical infrastructures are also privately owned, so the state cannot guarantee their protection against cyberattacks. In addition, the broad range of necessary countermeasures includes many elements that cannot be designed or implemented by the state alone.

A rundown of all the roles given to the state reveals the following. First, the state is to secure its own civil and military networks against all forms of cyber conflict by technical and other means. In this role, the state acts as *guarantor and protector* of the central state institutions.

The state has other roles in its function as *legislator and regulator*. On the one hand, it creates the necessary legal basis to clarify its hierarchical function vis-à-vis society and the economy. It does this, for example, in the fight against cyber crime or in the regulation of critical infrastructures (those whose disruption could seriously harm society). On the other hand, it also creates the legal framework to regulate the tension between citizens and businesses. This happens, among other things, with safety regulations in product certifications, or in the legislation on manufacturers' liability for products with digital components. How and to what extent this role is exercised varies and depends on the historically developed relationship between the economy and the state.⁴³

Since actors in cyberspace often operate internationally, the international dimension, especially around criminal law cooperation, is also of great importance. State institutions act as *supporters/representatives of society* by advocating for international frameworks that are conducive to both the respective economy and civil society.

In addition to its role as a regulator, in the field of critical infrastructures the state also plays the *role of a partner*. Many Western countries are trying to provide more protection through so-called public-private partnerships. Most of these take place in voluntary cooperation between industry and the state, particularly in the area of information exchange. The partnerships are based on the insight that, apart from a complete nationalisation or a completely private security architecture of critical infrastructures, national security issues in the cybersecurity area can only be addressed jointly.

Raising awareness on cyber issues among the general public is also a major policy endeavour. The state often plays the role of a *knowledge creator and disseminator*, in which it wants to be perceived as a trustworthy source of information. Whether or not this will succeed depends on the relationship of trust that has developed historically between different groups in society and state institutions, in some cases in very different ways. In this function,

the state acts as a *securitiser* by using its position of trust to disseminate a certain representation of danger.

The relationship of trust is also an important component of *the role of the state as the originator of more cyber-in-security*. The state, in the context of its intelligence activities, also acts as a threat to some; this dimension is not new, but it is particularly accentuated through the rapid technical advancement witnessed over the past ten years. Domestically, this can be the case, for example, in the defence against terrorism and espionage, but also in the prevention of violent political extremism. In some societies, a history of the misuse of these competences for unjustified state interference in civil rights reinforces the perception of the state as a danger. In addition, political and economic espionage emanating from foreign states reinforces the perception of states as sources of danger. In this role, state action is thus declared a problem; the state becomes the originator of the problem—it becomes the *securitised*.⁴⁴

Three Areas of Tension Between the State, Economy, and Society

A satisfactory level of cybersecurity can only be achieved by government, business, and society together. However, the sub-groups within these sectors often have different interests. This gives rise to at least three areas of tension in which every cybersecurity policy should be consciously positioned. Where cybersecurity policy is prescribed on these axes and where it moves to is the result of complex negotiation processes that are strongly dependent on individual events and related perceptions of danger (see Figure 1).

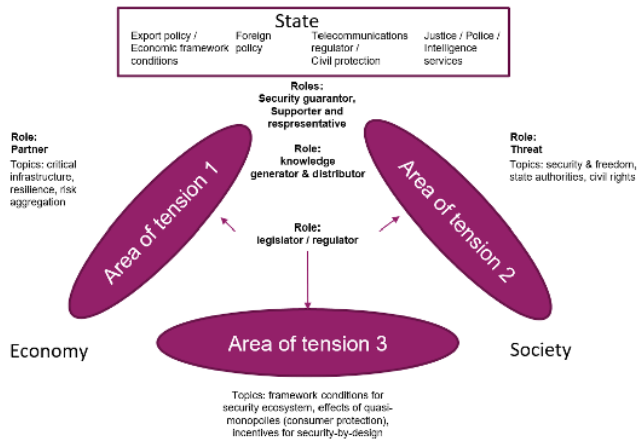


Figure 1. The three areas of tension in cybersecurity policy (own graphic)

In the first area of tension between the state and the economy, it is necessary to formulate a policy for securing critical infrastructures that absorb the negative consequences of liberalisation, privatisation, and globalisation from the point of view of security policy without preventing their positive effects. In this area of tension, the state is concerned with the dependence on economic action and the resulting resilience of society. How can trust be created between business and government? Where must the state intervene in order to prevent risk aggregations and contagion effects that pose a threat to society? Finding answers to these questions takes place in this area of tension and is an important part of the cybersecurity policy process.

In the second area of tension between the state and citizen, it is necessary to find the politically desired balance between more security and more freedom in the digital space. Additional police or intelligence powers often come into conflict with civil rights: specifically, the basic right to informational self-determination or anonymity on the Internet. When cyberthreats are discussed in depth, people tend to forget that, despite increased attention and calls for more and better protection, cybersecurity is just one of many complex intersectoral issues that the state has to address today. The harm caused by past cyber incidents may not be high enough (or may not be experienced as directly) to make substantially higher costs and cuts in civil rights acceptable. Rather, the harm perceived in other issues (such as terrorism) serves as legitimisation to make cuts in the political discourse in cybersecurity issues (e.g., the encryption policy debate).

In the third area of conflict between citizens and business, it is necessary to set the framework conditions for the development of a successful security ecosystem. How can the market, which is also confronted with the problem of quasi-monopolies, be regulated in such a way that an optimal balance between safety and functionality is achieved? How can incentives for more safety obligations be created for service providers? How can users be sensitised to the fact that they no longer put more functionality before thinking about safety? How can the (global) legal framework conditions for activities in virtual space be harmonised to counteract the danger of loopholes and the priority of cheap solutions?

What is taken for granted by economic and civil society actors also applies to the roles of the state: it assumes a multitude of roles. It is therefore not surprising that in many cybersecurity policy issues, the state represents a wide variety of interests at the same time. Consequently, thematic alliances are formed between different departments of the state with different interest groups of the economy and society. Each of these different politi-

cal groups represents a different vision of the role of the state in the issue at hand.

In democracies, such role conflicts are dealt with at the political level and can be approached systematically. For example, while the state has, for the purpose of an effective criminal prosecution and modern intelligence capabilities, an interest in the use of vulnerabilities for surveillance, it also has an interest in the greatest possible use of secure technologies and their use by business and society. In some states, this conflict of objectives is managed politically in an institutionalised vulnerability management process. Among other things, the public interest in secure platforms is contrasted with the public interest in the effectiveness of law enforcement. The recognition of the legitimacy of the multiple roles of the state helps to structure this consideration in an institutionally meaningful way and to recognise that decisions in this area take on an intrinsic political dimension.

Conclusion

In this article, we have explained the main features of cybersecurity policy through an investigation of its depiction in the literature and an analysis of policy documents. Our analysis shows that cybersecurity policy is diverse and necessarily includes state, economic, and societal actors. The variety of different countries in the historically evolved constellations of state, economy, and society determine the possibilities and limits of state roles, and political conflict about these roles.

The recognition of the diversity of government action is a solid foundation for developing strategic options, which then can lead to an overall strategy. An overall strategy for cybersecurity policy should create clear relationships as to how the various goals are weighed against each other, and should clearly identify the goal the state fulfils in its various roles. From a strategic point of view, role conflicts can be analysed in advance and included in political processes. This enables basic strategic decisions to be made (e.g., in the area of offensive powers of private actors), but also a strategic management of role conflicts (e.g., in the area of vulnerability management).

Even if the results look dissimilar in different countries, the areas of tension in which cybersecurity policy takes place remain the same. Cybersecurity policy revolves mainly around defining the various roles of the state in cybersecurity (and through so doing also those of semi- and non-state actors).⁴⁵ It should be noted that such clarifications, in a rapidly changing technological and political environment, are always temporary and subject to politi-

cal scrutiny and shifts of power. Changing social and political coalitions are reflected in new political decisions, which are discernible in several generations of cybersecurity strategies.

While the topics of political interaction are similar in different countries, the concrete manifestation of different roles depends on the strength of the different interest groups and the historically evolved distribution of roles and relationships of trust between the actors. Topics include questions of the limits of responsibility (i.e., where does the responsibility of the state, the economic, and societal actors begin and end?) and questions of the concrete assumption of this responsibility (i.e., which means may which actor use to fulfil their role?). As shown in this article, the answers to both questions are the results of multi-faceted political cybersecurity processes. As a structuring element, we have proposed that the political debates be divided into three areas of tension and six roles. This enables a more systematic analysis of political conflicts in the field of cybersecurity.

*Acknowledgments: The authors thank Jasper Frei for his excellent research assistance for this article

Notes

1 Robert S. Dewar, ed., "National Cybersecurity and Cyberdefense Policy Snapshots," Center for Security Studies (CSS) Collection 1 (2018), ETH Zurich, accessed February 5, 2019, <https://www.research-collection.ethz.ch/handle/20.500.11850/314596>.

2 The use of the "black box" term "state" is chosen deliberately, as this corresponds to the usage of language in international relations. See Sean Fleming, "Artificial Persons and Attributed Actions: How to Interpret Action-Sentences About States," *European Journal of International Relations* 23, no. 4 (2017): 930-50.

3 See, for example, the deterioration of relations between Russia and the West and the associated increase in cyber activities between the two: [Marie Baezner and Patrice Robin, "Cyber-conflict between the United States of America and Russia," *CSS Cyber Defence Hotspot Analysis* 2 (2017): 1-28.]

4 Cyberspace is understood here as the totality of all computers and network components (including the entire Internet, but also separate networks) and associated content. See Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 17.

5 Robert S. Dewar, "The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern," in *Challenges and Critiques of the EU Internal Security Strategy*, ed. Maria O'Neill and Ken Swinton

(Newcastle upon Tyne: Cambridge Scholars Publishing, 2017), 113-48.

6 The reports are available on the website of the Center for Security Studies, ETH Zürich, "Risk and Resilience Reports": <http://www.css.ethz.ch/en/publications/risk-and-resilience-reports.html>.

7 The conceptualisation of this article concerns only liberal democracies, since this political model enables different, contested roles of the state, and makes the debate about it possible in the first place.

8 Rossouw von Solms and Johan van Niekerk, "From information security to cyber security," *Computers & Security* 38 (2013): 97-102.

9 Important: Because the content in the databases is expanded constantly, the findings have to be taken with a grain of salt, or rather, with some scepticism. However, we believe that the numbers and observations can serve as indicators of trends. On the technicalities: searches were done for 'cybersecurity' OR 'cyber-security' OR 'cyber security' because the databases distinguish between the different spellings. For better comparability, searches were done for 'article title, abstract, and keywords' (rather than 'all fields') in Scopus, to match the category 'topic' in WoS, which contains title, abstract, and keywords. Searches in WoS were done in All Databases and not only in the Web of Science™ Core Collection. In general, the high competition between the two providers leads to improvements in the services offered, and therefore, to frequent changes in the database content. For example, Scopus has actively tried to reduce the negative bias towards the Social Sciences and the Arts and Humanities through the inclusion of more books in the last few years. Also, both databases have continually increased their coverage of non-English language content. See Philippe Mongeon and Adèle Paul-Hus, "The journal coverage of Web of Science and Scopus: a comparative analysis," *Scientometrics*, 106(1) (2016): 213-228; Jie Li, Judie F. Burnham, Trey Lemley and Robert M. Britton, "Analysis: Comparison of Web of Science, Scopus, SciFinder, and Google Scholar," *Journal of Electronic Resources in Medical Libraries* 7, no. 3 (2010): 196-217.

10 The ranking of articles in both databases is done via citation-count.

11 Multiple categories per entry are allowed.

12 The top-cited paper in both databases in this category is Esther Gal-Or and Anindya Ghose, "The Economic Incentives for Sharing Security Information," *Information Systems Research* 16, no. 2 (2005): 186-208.

13 Cf. Iván Arce, "The Weakest Link Revisited," *IEEE Security & Privacy* 1, no. 2 (2003): 72-76.

14 Myriam Dunn Cavelty and Manuel Suter, "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2(4) 2009: 179-187; also Dan Assaf, "Models of Critical Information Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 1 (2008): 6-14.

15 Exemplary: Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5-32; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics*, 10, no. 1 (2013): 86-103.

- 16 Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.
- 17 Exemplary: Brandon Valeriano and Ryan C. Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-11," *Journal of Peace Research* 51, no. 3 (2014): 347-60.
- 18 For a historical overview see: Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013); Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012): 781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.
- 19 Exemplary: Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed, (Indianapolis, IN: Wiley, 2008).
- 20 Pauline Bowen, Joan Hash, and Mark Wilson, *Special Publication 800-100 Information Security Handbook: A Guide for Managers* (Gaithersburg: National Institute of Standards and Technology (NIST), 2006), 6.
- 21 Laurin B. Weissinger, *Modelling Trust and Trust-Building among IT-Security Professionals: How do practitioners find out whom to work with?* *Lecture Notes in Computer Science*, 10292 (2017), 557-566.
- 22 Elke Krahmann, "Conceptualizing Security Governance," *Cooperation and Conflict* 38 (2003): 6-26.
- 23 Mark Bevir and R.A.W. Rhodes, *A Decentered Theory of Governance: Rational Choice, Institutionalism, and Interpretation*, Working Papers of the Institute of Governmental Studies, Number 10, (Berkeley, 2001).
- 24 Guy Peters and John Pierre, "Governance Without Government? Rethinking Public Administration," *Journal of Public Administration Research and Theory* 18 (1998): 223-43.
- 25 Lester M. Salamon, "The Tools Approach and the New Governance: Conclusion and Implications," in *The Tools of Government: A Guide to the New Governance*, ed. Lester M. Salamon (Oxford: Oxford University Press, 2002), 600-10.
- 26 Johan Eriksson, "Cyberplagues, 'IT, and Security: Threat Politics in the Information Age," *Journal of Contingencies and Crisis Management* 9, no. 4 (2001): 211-22; Dunn Cavelty, "U.S. Efforts; Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber-Security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155-75; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (2013): 86-103. Also, with focus on metaphors, David Barnard-Wills and Debi Ashenden, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk," *Space and Culture* 15, no. 2 (2012): 110-23; David J. Betz and Tim Stevens, "Analogical Reasoning and Cybersecurity," *Security Dialogue* 44, no. 2 (2013): 147-64; Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15, no. 1 (2013): 105-22.
- 27 Barry Buzan, Ole Waever, and Jaap De Wilde, *Security: A New Framework for*

Analysis (Boulder, CO: Lynne Rienner, 1998).

28 Ole Wæver, "Securitization and Desecuritization," in *On Security*, ed. Ronnie D. Lipschutz (New York/Chichester: Columbia University Press, 1995): 46-86; Jef Huysmans, "The Jargon of Exception - On Schmitt, Agamben and the Absence of Political Society," *International Political Sociology* 2, no. 2, (2008): 165-83; Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (Boulder: Rienner, 1998).

29 Lene Hansen, "Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it," *Review of International Studies* 38, no. 3 (2012): 525-46; 528.

30 See for example Claudia Aradau, "Security and the democratic scene: Desecuritization and emancipation," *Journal of International Relations and Development* 7, no. 4 (2004): 388-413; Hansen, "Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply it"; Jef Huysmans, "The Question of the Limit: Desecuritisation and the Aesthetics of Horror in Political Realism," *Millennium - Journal of International Studies* 27, no. 3 (1998): 569-89; Philippe Bourbeau and Juha A. Vuori, "Security, Resilience and Desecuritization: Multidirectional Moves and Dynamics," *Critical Studies on Security* 3, no. 3, (2015): 253-68.

31 On the particular U.S. development, see Dunn Cavelty, *U.S. Efforts*; Jason Healey, *A fierce domain: conflict in cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013); Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27 (5) (2012): 781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.

32 Dunn Cavelty, *U.S. Efforts*.

33 Myriam Dunn Cavelty, *Cybersecurity in Switzerland*, Springer Briefs in Cybersecurity. (Cham: Springer International Publishing, 2014).

34 Dunn Cavelty, *U.S. Efforts*.

35 Ralf Bendrath, "Elektronisches Pearl Harbor Oder Computerkriminalität? Die Reformulierung Der Sicherheitspolitik in Zeiten Globaler Datennetze," *Sicherheit und Frieden (S+F) / Security and Peace* 18, no. 2 (2000): 135-44; Michael Warner, "Cybersecurity: A Pre-history," *Intelligence and National Security* 27, no. 5 (2012): 781-99, accessed on April 2, 2019, doi: 10.1080/02684527.2012.708530.

36 Timo Steffens, *Auf Der Spur Der Hacker: Wie Man Die Täter Hinter Der Computer-Spionage Enttarnt* (Berlin: Springer Vieweg, 2018), 127-137 (*On The Trail of the Hackers: How to Expose Offenders Behind Computer Espionage*). For more on attribution, see Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no.1-2 (2015): 4-37.

37 Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no.1 (2010): 12, 15-32, Even though such distancing is not always plausible, see Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (2018): 477-494.

38 Myriam Dunn Cavelty, "Cyberwar," in *The Ashgate Research Companion to Modern Warfare*, ed. George Kassimeris and John Buckley (Ashgate, 2010), 123-

144.

39 Dunn Cavelty and Suter, *Silver Bullet*, 179-87.

40 President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, 1997). Accessed May 17, 2019. <https://www.documentcloud.org/documents/2800106-Documents-02-President-s-Commission-on-Critical.html>

41 For the strategic impetus that drives this behaviour, see Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (Oxford: Oxford University Press, 2017).

42 Dewar, *National Cybersecurity and Cyberdefense Policy Snapshots*.

43 Peter A. Hall and David Soskice, *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford: Oxford University Press, 2001).

44 Developing this view and beyond, see Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," *Ethics & International Affairs* 32, no. 4 (2018): 411-24, accessed April 2, 2019, doi: 10.1017/S0892679418000618.

45 Florian J. Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates" (PhD diss., University of Oxford, 2018).

CONCEPTUALIZING ACTIVE CYBER DEFENCE IN CYBER OPERATIONS: QUO VADIS, SWITZERLAND?

Bastien Wanner and Solange Ghernaouti,
University of Lausanne, Faculty of Business and Economics (HEC
Lausanne), Department of Information Systems

Abstract

Increasing numbers of sophisticated, destabilising, and malicious cyber activities have prompted many states to add active cyber defence measures to their national defence arsenals. While these include passive security measures, many also include active elements (i.e., measures conducted outside of the defended systems and networks to halt ongoing cyber attacks). This article outlines the various definitions of active cyber defence, inter alia by describing their characteristics and typologies. In addition to describing the expected effects of these measures, it highlights their advantages, disadvantages, and limitations. Furthermore, as cyber operations originate from military doctrines, it describes, analyses, and compares two national cyber defence policies: those of the US and France. They are selected as good examples to guide Switzerland's current reflections on active cyber defence. Against this background, by delineating the relevant Swiss political and legal frameworks, this article depicts Switzerland's approach to active cyber defence. It concludes with recommendations for Switzerland concerning cyber defence capabilities, keeping in mind Swiss particularities.

Introduction

Threats originating from the use of information and communication technologies (ICT) have long been a source of major concern for states. In the early days of widespread Internet use (i.e., the early 1990s) these activities were mainly limited to criminals employing digital devices for financial gain or simple vandalism. Today, states must fight not only cyber criminality, but also sophisticated cyber operations designed to disrupt and destabilise entire societies and economies.

In response, states have started developing national cyber strategies that increase their cyber resilience and mitigate their cyber risks. Until recently, cyber defence focused mainly either on passively shielding vulnerable assets or on making them more resilient. As the number, sophistication, and disruptiveness of attacks continued to increase, states began to add active defence

Bastien Wanner and Solange Ghernaouti, "Conceptualizing Active Cyber Defense in Cyber Operations: Quo Vadis, Switzerland?," *St Antony's International Review* 15. no. 1 (2019): 58-82.

measures. These were designed not to prevent unauthorised access and disruption, but to halt attacks at their source. The most recent step which several states have taken is to develop national cyber defence policies and adopt a dynamic stance in defending their digital environments. As the level of secrecy surrounding offensive cyber capabilities remains high, the exact number of states who possess them remains unknown. However, some estimates suggest that the number of countries in possession of offensive cyber capabilities ranges from thirty to fifty.¹

This article will focus on clarifying the somewhat nebulous concept of active cyber defence approaches, particularly as it relates to the Swiss context. In addition to defining key terminology, it will provide descriptive analyses of the most common characteristics and typologies captured in the literature. We posit in our article that active cyber defence and offensive capabilities are not the same. The risks that emerge with the usage of active cyber defence go beyond the scope of this paper and will not be discussed. For the purpose of this article, we will focus on active cyber defence in the context of states' military strategies. Moreover, as Switzerland lacks a military cyber defence strategy and doctrine, this article intends to draw inspiration from existing examples. Therefore, we will delineate and present the US and French cyber defence strategies and military doctrines as possible frameworks upon which to design and conduct cyber operations. In doing so, we will also provide an analytical view of the two approaches' commonalities and differences.

Finally, we will discuss the case of Switzerland's intentions and attitudes regarding active cyber defence. After describing the Swiss cyber defence policy and the legal frameworks that guide and allow the use of active cyber defence capabilities, the paper critically reviews the Swiss stance. After considering the unusual characteristics of the Swiss national defence system, it concludes with recommendations to begin developing active cyber defence.

Active Cyber Defence: Definitions and Concepts

Ensuring the resilience of today's ICT requires going beyond purely technological protective measures. In addition to preparing for, withstanding, and recovering rapidly from disruptions,² states have started developing active capabilities to increase their defensive cyber postures. The move from purely protective measures towards more active defensive stances constitutes an emerging development and legitimate yet not always uncontroversial step states have also undertaken in the cyber environment.³ Thus, cyber defence and the state are intrinsically linked, as security and

defence are exclusively state prerogatives and this also applies to cyberspace. In cyberspace, states defend themselves by both defensive and offensive cyber operations. Moreover, these operations can have either passive or active components. The current literature contains no commonly accepted definition of active cyber defence.

Terminology of Active Cyber Defence

In the literature, the terms ‘active computer network defence’⁴ and ‘internet hack back’⁵ were first mentioned in the early 2000s. ‘Active computer network defence’ usually refers to military operations conducted by states. Nevertheless, active cyber defence can also be executed by private entities. By the same token, ‘hack back’ is one component of broader active cyber defence applied by both state and non-state actors. Since then, many more terms, such as ‘strike back,’⁶ ‘active response,’⁷ and ‘cyber weapon’⁸ have emerged, sowing confusion and misunderstanding around the concept of active cyber defence. No universally recognised glossary clearly defines the terminology used in cybersecurity to qualify a defensive action in cyberspace. Nevertheless, since 2010, ‘active cyber defence’ has prevailed in the literature as a broadly used, politically established, and less technically connoted generic signifier.

Definitions of Active Cyber Defence

In 2011 the US Department of Defense (DOD) released its ‘Strategy for Operating in Cyberspace,’⁹ which included the first state-level definition of active cyber defence. According to this strategy, active cyber defence is the “synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.”¹⁰ Three years later, the UK’s Ministry of Defence (MOD) released their Cyber Primer, a guiding document of the UK’s defence cyber program which explores the fundamentals of cyber and its relevance for defence. However, it was the Primer’s second edition, issued in 2016, which proposed the following definition for active cyber defence: “[a]ctivities that target hostile offensive cyber operations in order to preserve our freedom of manoeuvre within cyberspace.”¹¹ Concurrently, the Tallinn Manual of NATO’s Cooperative Cyber Defence Centre of Excellence (CCD COE) offered its own definition: a “proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber

counter-operation against the source.”¹²

The US and the CCD COE definitions emphasise the importance of timely, coordinated execution of active cyber defensive operations, that is, the appropriate measures need to be synchronised in real-time and may even be conducted proactively. It is crucial to specify that, in this context, proactive defence implies taking the initiative (from a militaristic point of view) rather than reacting to a potentially crippling attack. The distinction between preemptive and preventive military action can be defined in terms of the planned operation's imminence: “Preemption is the taking of military action against a target when there is incontrovertible evidence that the target is about to initiate a military attack. Prevention is the taking of military action against a target when it is believed that an attack by the target, while not imminent, is inevitable, and when delay in attacking would involve greater risk.”¹³

In parallel to states providing definitions, various scholars have developed language relating to active cyber defence. In line with the CCD COE, Ducheine and van Haaster argue that “proactive measures are launched to defend against malicious cyber activities or cyber attacks.”¹⁴ Denning and Strawser's article on the topic compares cyber defence to air defence, in that “active cyber defense is a direct defensive action taken to destroy, nullify or reduce the effectiveness of cyber threats against friendly forces and assets.”¹⁵ On the other hand, Dewar posits that, as a security paradigm, active cyber defence is “an approach to achieving cybersecurity predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities including action in those entities' home networks.”¹⁶ More congruent with the UK MOD definition, Iasiello defines active cyber defence as a “range of offensive damaging or destructive actions such as counterhacking, that engage an adversary during or promptly after an initial cyberattack. Active cyber defence does not include nonviolent actions such as diplomatic or economic sanctions. Examples include counterhacking and technical countermeasures with weaponised payloads.”¹⁷ Finally, Rosenzweig distils the principle down to “actors may hack back at the hackers who are attacking them.”¹⁸

While we acknowledge the value and validity of the above-mentioned definitions, we consider the definitions proposed by the CCD COE and Ducheine and van Haaster incomplete, as they address only a single aspect of active cyber defence. Additionally, as both use ‘proactive’ and ‘preemptive’ interchangeably, they understate the significance of time. Realistically, active cyber defence is

unlikely to be applied before the launch of a malicious cyber activity. By outlining an effect-based approach, the impacts of which include destroying, nullifying, or even simply reducing the attacker's offensive capacities, Denning and Strawser propose the most complete and holistic definition. Rosenzweig's concept of real-time response complements this approach.

In addition to these definitions, we believe that active cyber defence constitutes a range of cyber operations that assume real-time responses and an effect-based approach. Despite all protective measures, the likelihood of being attacked remains high. Therefore, we consider that real-time offensive responses ought to be part of a broader array of cyber options designed to defend against a cyber attack. Moreover, due to the complexity of the systems involved, active cyber defence measures should not be limited to computer operations, but also be accompanied by coordinated legal and political actions. Therefore, any cyber action needs to be proactively coordinated and tailored to available legal and political capacities.

While active cyber defence involves offensive cyber capability, the two concepts are not synonymous. Smeets and Lin agree that offensive cyber capability is "a capability designed to access a computer system or network to damage or harm living or material entities."¹⁹ This added to Lin's earlier proposal of active cyber defence as a "hostile action against a computer system or network"²⁰ that can take two forms: destructive (cyber attack) or non-destructive (cyber exploitation). Rattray and Healey argue that offensive operations are analogous to either Computer Network Attack (CNA) or Computer Network Exploitation (CNE),²¹ while Williams frames the ultimate aim of all offensive cyber operations as attempts to "project power in and through cyberspace."²²

Characteristics of Active Cyber Defence

Few studies have systematically characterised the concept of active cyber defence. The few articles that have attempted to characterise active cyber defence remain imprecise and vague. According to Dewar, for example, cyber defence includes three main traits: first, the use of specific tools to counteract the immediate effects of a cyber attack in victim networks, such as shutting down a command and control server; second, the development of capacities to engage directly with the perpetrators in their networks; and third, direct or indirect interaction with the adversary.²³ Similarly, the concept provided by Kello has three main elements: defensive purpose, out-of-perimeter location, and tactical flexibility.²⁴ Defensive purpose is the aim "to enhance the security of the defend-

er's assets: to deny proactively but not to penalise the attacker."²⁵ Out-of-perimeter location encompasses the capacity to launch active defensive measures outside one's home domain (i.e., in adversarial or neutral domains). Tactical flexibility denotes a range or combination of actions ranging from intelligence collection to disruption (including destruction) of attackers' assets.

According to Denning, four characteristics distinguish active cyber defence: scope of effects, degree of cooperation, types of effects, and degree of automation.²⁶ The scope of effects can be either internal (with effects limited to the defended network) or external (with effects reaching beyond that network). The degree of cooperation can be cooperative, wherein the action is performed on a system with the knowledge and consent of the system owner or, it can be non-cooperative, wherein the action is performed on a system without the knowledge and the consent of the system owner. There are four types of effects: sharing, or action that distributes threat information; collecting, or action to acquire more information about the threat; blocking, or action that stops activity deemed hostile; and preemptive, or action that neutralises or eliminates a source used in the attack. Finally, the degree of automation pertains to the degree of human involvement; defensive measures can be executed either automatically or manually.

Considering the above-described features, we posit that active cyber defence is a combination of all of the above features. However, the core element that makes this concept active is the fact that the defensive action takes place outside the perimeter of the defenders' network, hardware, and software. In other words, all actions targeting the adversary's ICT infrastructures or third party's digital premises, for the purpose of ceasing the ongoing cyber attack, are active cyber defence. Needless to say, states are more likely to use such measures to stop attacks originating from abroad. While states could technically use active cyber defence measures to halt cyber attacks from within, they can opt for other instruments in accordance with domestic laws. Therefore, cyber active defence is a capability most likely to be applied in an international context. All measures need to focus on the attacker's tools and the infrastructure used to conduct malicious acts. Inevitably, conducting such operations of active cyber defence will route third party territory.

Another key aspect of active cyber defence is its disruptive nature. It is impossible to counteract an ongoing cyber attack without partially or totally disabling the attacker's capacities (i.e., hardware and software). Therefore, given the strong possibility of collateral damage, it should be initiated only in situations where no other defensive options are feasible. Consequently, appropriate

use of such active measures will require all manners of relevant information. Ongoing intelligence collection can help identify and understand potential attack vectors, thereby increasing preventive, protective, and reactive capacities. Ideally, regardless of the geographic origin of an attack, effective intelligence collection will help identify and target its true source. Therefore, based on the information presented in this section and in accordance with Denning's classification system, we suggest that, to achieve maximum effect, active cyber defence has to comprise a combination of external, non-cooperative, preemptive, and semi-manual actions.

Expected Effects of the Use of Active Cyber Defence

As discussed in this article, high-level cybersecurity is not only a means to ensure the resilience of computer systems and networks, but also a desired end state. With that in mind, the first step towards achieving it is to establish and maintain a basic level of cyber protection. At the national level, this begins with passive measures in domestic cyberspace, such as patching vulnerabilities, monitoring systems, mitigating risks and, wherever possible, investigating suspicious or malicious activities. These protective measures are performed by information security officers and units, such as security operations centres (SOCs) and computer emergency response teams (CERTs). However, when the systems and networks are targeted by an advanced cyber attack with a strong disruptive capability, more sophisticated defensive measures, such as computer network defence (CND), are needed: first, to halt the attack and, second, to prevent it from spreading into networked systems.

As noted above, defensive measures fall into two categories. The first is designed to defend systems and networks by reinforcing internal security measures. They function by concentrating cyber protection via additional security layers. For example, they may reroute traffic, deploy diagnostic tools on the affected network, and actively track whoever has penetrated their system. Still, however dynamic these defensive measures may be, as they are executed within the defended ICT infrastructure, they are not classed, according to Kello's notion, as active measures.²⁷ Furthermore, apart from blocking attacks and impeding attackers, these internal measures have no particularly disruptive intent.

The second class of defensive action is active cyber defence measures. Because of their strong disruptive characteristics, these are applied as a last resort. If reinforcement of protective barriers has either failed or is likely to fail, it is necessary to address the perpetrators in a way that will render them unable to continue

or conduct further attacks. The objective of an active measure is to disrupt the attack at its source. This may mean destroying the command and control servers, closing off the attack vectors, creating disorder in the attack plan, or otherwise disorienting the perpetrators. It is important to stress that the defender's objective is not to annihilate or eradicate the attacker by totally damaging their infrastructure or other resources. The focus is simply to stop the attack and inhibit the attacker from launching other attacks.

Against this background, rules of engagement for active cyber operations are crucial. Any active defence measure must be fully compliant with both existing international law and domestic legal frameworks. The defender should bear in mind that the state in which the target entity is located could interpret and respond to any such measure executed within their territory as a violation of the UN Charter's prohibition of the use of force.²⁸ As a defensive measure, it must also be proportional to the attack and minimise collateral damage. Finally, it must comply with the principle of necessity (i.e., all reasonable less aggressive means must have been tried and failed).

Still, even assuming that an active defensive measure is the only appropriate response, the question remains of how to measure its success. The answer might seem trivial: if the attack stops or the attackers are blocked, the measure was successful. Nevertheless, any use of active cyber defence measures can lead to an escalation of tension, which can, in turn, lead to a tit-for-tat rationale. In addition, active cyber defence measures could have another non-negligible effect, such as deterring potential future cyber attacks. If a nation is known to have a strong cyber defence posture, one could assume that it would serve as a deterrent. This may be the main reason why more nations, *inter alia* Belgium, Denmark, Germany, and the Netherlands, have published their active cyber defence doctrines.²⁹

One absolute necessity before launching an active cyber defence measure is thorough information gathering, as false flag attacks have exacerbated the difficulty of attribution. This is all the more important when the purpose of a measure is to disrupt the source of a cyber attack. The defender requires a view of the attack that is both precise and panoramic, specifying, for example, the weapons it employs, its vectors, targets, and intrusion paths. Therefore, to shape an effective response, the defender needs to analyse every relevant characteristic of the attack.

For the military operators conducting an active defence, determining what is relevant demands a distinction between technical characterisation and attribution. The first case involves an attack's technical characteristics (e.g., vector, indicator of compro-

mise, and malware). The second involves fully attributing the attack (i.e., identifying its authors, their nationalities, affiliations, and motives via technical, legal, and political analyses).

In fact, as attribution is ultimately a sovereign political decision,³⁰ timely defence measures cannot depend on whether an attack can be traced to specific perpetrators. The operators' task is to respond to the attack by targeting the computer system from which it originates. Fulfilment of that task depends completely on a clear and precise technical characterisation.

Active Cyber Defence in Military Doctrines

As the principles of active cyber defence originate from military doctrines, the following section provides a descriptive analysis of US and French national approaches to defining and utilising their military capabilities. While several states have well-developed stances that include active cyber defence, our analysis is limited to the US and France. We have chosen the US model mainly because the US armed forces are at the forefront of cyber defence developments and present some of the most advanced policies regarding it. They are in this advanced position because they were affected more than a decade ago by severe breaches, including the 2008 cyberattack targeting the US Central Command, leading to the creation of the US Cyber Command. Moreover, the US is one among few nations who are open and transparent about their cyber defence doctrines. We have selected France for similar reasons. Like the US, France also experienced high intensity cyberattacks approximately a decade ago. Consequently, they have created structures (e.g., cyber commands), policies, and doctrines to address these threats. The common denominators of the two mentioned countries are threat exposure, state practice, and the articulated willingness to use cyber offensive measures as a defensive strategy. Additionally, both countries have been transparent about their cyber defence posture and rely on strong industrial partnerships to develop and deploy these tools.

United States Department of Defense: Cyber Defence Doctrine

In June 2018, the United States Department of Defense released an updated cyberspace operations doctrine in Joint Publication 3-12 Cyberspace Operations.³¹ According to this doctrine, cyberspace operations are composed of three main missions: Department of Defense Information Network (DODIN) Operations, Defensive Cyber Operations (DCOs), and Offensive Cyber Operations (OCOs). While the actions and capabilities necessary

to conduct these cyberspace missions can overlap, one important distinctive feature which differentiates these missions is the objective or intention of the commanding authority.

Pursuant to this doctrine, DODIN's missions are to secure, configure, operate, extend, maintain, and sustain cyberspace pertaining to the DOD, with the aim of ensuring the triad confidentiality, availability, and integrity of all related information systems. These actions are designed to increase the security of information and communication technologies, regardless of the types of threats they face. Thus, DODIN is network-focused and threat agnostic.

The second category of cyberspace operations is DCO missions. These are conducted to defend US cyberspace, focussing particularly on assets critical to the success of military operations. In a military context, these critical assets are called key terrains, as they generate a marked advantage for the combatant who controls them.³² In order to ensure the freedom of manoeuvre in cyberspace, DCO missions are designed to defeat malicious activities that have bypassed or breached DODIN's protective measures. Unlike DODIN operations, DCOs consider the nature of the threats faced and are applied to fulfil individual objectives. Thus, DCOs are threat specific and mission-focused.

This category of defensive operations is further split into two subcategories: Internal Defensive Measures (DCO-IDMs) and Response Actions (DCO-RAs). As the name implies, the first are conducted within the defender's own digital environment to re-establish the security of an attacked system. If necessary to eliminate the identified threat, the actions conducted during internal defensive measures can take on a proactive and even aggressive form of threat hunting, as well as active internal reaction. Comprising the second subcategory, DCO-RAs fulfil defensive missions in neutral or foreign cyberspace without the permission of the targeted systems' and networks' operators. While these response actions have a disruptive purpose and may even physically damage or destroy their targeted systems, the main purpose of DCO-RAs is to stop or block attacks before they reach key cyber terrains.

To receive authorisation to initiate a DCO-RA, two conditions must be satisfied. First, an attack must be either ongoing or imminent. Second, the attack must be attributed beyond reasonable doubt. Response actions must include clear military order and limited scope, have measurable objectives, and adhere to rules of engagement (ROEs). Finally, OCO missions are intended to project power in and through cyberspace. They exclusively target adversaries in cyberspace in order to disturb weapons systems, command and control processes, logistic nodes, high-value targets,

etc. All missions conducted outside of a state's own cyberspace, with an intention other than defending its own digital environment, are considered offensive cyber operations. As noted above, the defining characteristic of cyber operation types is intention. Each cyber mission includes a combination of four forms of possible action: cyberspace security, cyberspace defence, cyberspace exploitation, and cyberspace attack. Each of these actions is defined by its intended effect.

Cyberspace security actions are conducted within protected cyberspace to prevent breaches to the confidentiality, integrity, and availability triad. They are primarily taken during DODIN missions with the goal of reducing or eliminating vulnerabilities. Furthermore, cyberspace defence actions are also executed within protected cyberspace; however, their aim is to defeat threats that might or have already breached cyberspace security measures. They include detection, characterisation, elimination, or mitigation of threats, malware, or unauthorised activities. They also include reconstructive functions: once a threat is neutralised, they restore a secure configuration to the system. Finally, cyberspace exploitation actions include all actions necessary to enable future military operations, including information collection to gain intelligence. Exploitation actions include mapping cyberspace to support situational awareness, discovering vulnerabilities, and enabling target development. They also provide opportunities to manoeuvre within adversaries' networks and to take favourable positions therein (e.g., gaining and maintaining access to systems, networks or nodes of military value).

Like all OCOs and DCO-RAs, exploitation actions are conducted in adversarial or neutral cyberspace. However, as they do not alter or disturb the environment in which they are deployed, they do not generate the effects of cyberspace attacks; on the contrary, they tend to be clandestine and operate in the shadows. In contrast, cyberspace attack actions aim at degrading, disrupting, or destroying adversaries' assets. They may also manipulate information to create a false understanding that leads to physical denial effects. As appealing as obfuscating an action might be, the effects will eventually become apparent to the victim. In cases of manipulation, the effects will remain unnoticed until the denial takes effect.

In September 2018, the US DOD released another update of its Cyber Strategy, reaffirming the DOD's will to fight and win battles in all its operating spheres, including cyberspace. To achieve this objective, however, the updated policy introduced the concept of 'defend forward.' In this case, the aim is to proactively and persistently halt, disrupt, or degrade any cyberspace operations

targeting the US as closely as possible to their sources and before they reach national networks. In addition, DOD operations will “seek to pre-empt, defeat or deter malicious cyber activities targeting the critical infrastructure that could cause a significant cyber incident.”³³

This represents a significant shift in direction regarding the use of offensive cyber capabilities in foreign networks with neither the consent nor the permission of the networks' owners. It needs to be viewed in relation to another line of effort of the US strategy, which is to “build a more lethal joint force”³⁴ by developing more innovative and effective automated cyber capabilities. Our interpretation of the ‘defend forward’ concept is that, as completely as possible, the US hopes first to occupy key cyber terrain then to use the advantage this affords it to search and confront any perceived threat to their protected infrastructure.

French Ministry of Armed Forces: Cyber Defence Doctrine

With France's release of its Strategic Review of Cyber Defence in February 2018, the French published a cyber defence doctrine proposing six categories of French cyber defence missions: prevention, anticipation, protection, detection, attribution, and reaction.³⁵ Then, in January 2019, the Ministry of the Armed Forces went public with their “ministerial policy on defensive computer warfare”³⁶ and “public elements of the military doctrine on offensive computer warfare.”³⁷

The defence doctrine outlined the overall objective of defensive cyber operations—which the doctrine refers to as ‘defensibility’—including the defence of military systems and attenuation of vulnerabilities. On the one hand, this acknowledged that the risk of cyber attack needs to be considered and the consequences to the targeted organisations analysed. On the other, its premise that the ability to act and react is a precondition to conducting any actions in cyberspace suggests that the final goal of defensive cyber operations is to preserve the defenders' freedom of action. That is, the aim of responding to a cyber attack is to prevent the disruption of social and economic activities.

Accordingly, defensive cyber operations cover three main missions: anticipation, detection, and reaction to threats or attacks, all of which are designed to be conducted in neutral or adversarial cyberspace. Defensive cyber operations are to fulfil missions of prevention, protection, and attribution in France's own cyberspace, thus contributing to the cyber resilience of its armed forces. Naturally, offensive cyber operations would involve the use of cyber weapons. In compliance with international law, these

would be designed to alter the confidentiality, integrity, or availability of data within the adversary's system. Destabilisation of the adversary would result from effects on their cyberspace's physical, logical, or social layers.

France's offensive cyber operations have three objectives: evaluate the military capabilities of the adversary, then reduce or neutralise those capabilities, possibly by distorting the adversary's perceptions or analytical outcomes. As for offensive cyber capabilities, the French doctrine lays out a sequence of three roles: intelligence gathering (monitor adversaries, allowing characterisation and attribution of their systems), defence (identify the attacker, riposte them in cyberspace in case of intrusion, and ultimately neutralise an attack), and action (counter misinformation and disrupt adverse military capabilities).

The US and France: Descriptive Analysis

One striking observation is that both the US and France neither explicitly mention nor use the term active cyber defence in their respective doctrines. In our view, the US DCO-RA is one good example of an active cyber defence measure. In the French case, defensive cyber operations conducted in neutral or adversarial cyberspace in order to anticipate, detect, or react to attacks are clearly active cyber defence. One area of commonality between the US and France is both countries' tendency to lead by example in developing more active cyber defence capabilities. Both clearly understand the need for defensive capacities in all operational domains, including cyberspace, and both have prioritised the development of related tools and measures to promote active stances on cybersecurity. What is more, both have grouped their cyber defence capabilities in three incremental categories: protection, defence, and attack.

However, the main difference between these two countries is their declaration as to how and when they are prepared to deploy these capacities. Regarding the Americans, their 'defend forward' and 'persistent engagement' policies indicate an intention to tackle any relevant threat at its source, which will require them to be virtually 'omnipresent.' This means that these cyber defence actions are active in nature, as they are inevitably conducted out of their own cyber perimeter and with a clearly disruptive purpose. The main value this approach adds is that of 'proactively engaging' and 'persistently contesting malicious cyber activities.' Rather than waiting for an attack, the US armed forces will constantly be scanning the horizon to identify and eradicate potential problems before they pose a threat. One example is the US Cyber Command

attack against a Russian troll factory which was allegedly spreading misinformation during the 2018 mid-term elections.

The French, on the other hand, have only declared that they have cyber weapons and are willing to use them if necessary—a more reactive application of their means. Despite their high degree of transparency, though, it remains unclear as to what weapons make up their actual cyber arsenal and how they intend to use them. Habitually high levels of defence secrecy remain a major challenge for most states. This is all the more important because, to date, very few countries have reported their deployment of an active cyber capability.

Active Cyber Defence: Swiss Case Study

The following section outlines the Swiss policy regarding active cyber defence. To do so it will first delineate the relevant political and legal frameworks, from which it will distil a definition of the concept at hand. After a brief analysis of active cyber defence as it pertains to the Swiss context, it will conclude with general recommendations on the topic.

Alongside ICTs' many advantages and opportunities, serious threats have arisen. In early 2010, the Swiss Federal Council declared its political will to promote the development of strategic programmes that would protect the country against cyber risks. In June 2012, the Swiss government adopted the first 'National strategy for the protection of Switzerland against cyber risks (NCS).'³⁸ Therein, the roles and responsibilities of the Swiss administration are described. The Federal Department of Finance (FDF) has the overall responsibility for the development and implementation of the NCS. However, having opted for a decentralised approach, each of the Federal Departments has a leading role in implementing the measures. With regard to the protection of critical infrastructures, Switzerland pursues a self-regulatory approach. This means that the operators of critical infrastructures are responsible for their own cybersecurity. Nevertheless, the Reporting and Analysis Centre for Information Assurance (MELANI), jointly operated by the Federal Department of Defence, Civil Protection and Sports (DDPS), and the FDF, supports the critical infrastructures operators in a subsidiary manner. Involving a "continuity and crisis management sphere of action," this strategy's Measure 14 addresses active cyber defence measures: "In the event of a specific threat, active measures are foreseen for identifying the perpetrators and their intentions, as well as for investigating the perpetrators' abilities and compromising their infrastructure."³⁹

A year later, in May 2013, an implementation plan described

the results to be achieved with regard to prevention, response, continuity and crisis management, and support processes. In the Response section, Measure 14 outlined the principles of active cyber defence as “active measures to identify the perpetrator and possible impairment of its infrastructures in the event of a specific threat.” To summarise Measure 14’s content, if the Federal Intelligence Service (FIS) of the DDPS can identify the perpetrator(s) of a cyber attack, it should forward whatever relevant information is legally permissible to the Office of the Attorney General, which will then decide whether to initiate criminal investigations. In cases where prosecution is either inappropriate or impossible, an alternative would be to deploy an active countermeasure.

The following paragraphs describe the roles and responsibilities of the Federal Intelligence Services regarding active cyber defence of Switzerland’s critical infrastructures. The question of legality required special legislation. Accordingly, on September 1, 2017, the enactment of the Intelligence Services Act (IntSA)⁴⁰ provided a corresponding legal framework.⁴¹ Article 37 of IntSA allows the Federal Intelligence Service (FIS) to infiltrate systems and networks located abroad if they are used to attack critical infrastructures located in Switzerland. Two cumulative conditions regulate the FIS’s mandate to infiltrate systems and networks. First, these systems and networks have to be located abroad. Second, the targeted systems and networks have to be used to attack critical infrastructures located in Switzerland. If these conditions are met, the FIS has the right to disrupt, impede, and slow down the access to information.

Alongside the Intelligence Services Act, the Swiss Federal Council also adopted the Intelligence Services ordinance,⁴² which specifies more precise criteria for the use of active cyber defence measures. Article 24 of the ordinance demands that, prior to infiltrating computer systems and networks abroad, the FIS must send a formal request to the Swiss Defence Minister indicating six essential points: the legal field of activity, the type of information sought, the potential third parties, the period in which the measure will be used, the concerned computer systems and networks, and, finally, the proposed measure’s necessity, proportionality, and risks.

Article 25 states that the FIS can collect information in the domain of cyber threat exploration and critical infrastructure protection, with the objectives first to clarify the nature of the engagement, including the origin and technical characteristics of the cyber attack’s means, then to implement effective cyber defence measures. In 2016, the DDPS was the target of a cyber attack campaign that led to the development of an Action Plan for Cyber

Defence (APCD),⁴³ which was implemented in 2017. Responding to cyberspace threats perceived by the DDPS, the APCD identifies protective and reactive tasks and illustrates the Federal Department of Defence's existing legal framework for passive and active cyber defence.

The Armed Forces offer another line of defence. Normally, they are responsible for the defence of their own ICT systems and infrastructures; however, in peacetime, they can also be authorised to launch active cyber defence countermeasures. This capacity articulates the principle that, as in its other spheres of operation, in the event of a conflict, the Swiss Armed Forces should be capable of conducting actions in cyberspace (in accordance with international humanitarian law) against hostile ICT systems and infrastructures.

Since the DDPS attack in 2016, the Swiss Armed Forces have reorganised their structures in a program called 'Upgrading of the Armed Forces (UAF)'. In January 2018, a new Armed Forces Act (ArmA)⁴⁴ officially implemented the new structure. Among other points, its Article 100, 'Military Security,' lists the tasks the Armed Forces should perform in the domain of cyber defence. This article states that, in the event that their computer systems and networks are attacked, they are authorised to take the necessary defensive measures. These may include breaking into any computer systems and networks used to carry out the cyber attacks and disrupting, impeding, or slowing down their access to information.

In 2018, the Federal Council also reviewed the national strategy for the protection of Switzerland against cyber risks, leading to the adoption, in April, of an updated 2018–2022 edition.⁴⁵ In addition to specifying the roles played by the Armed Forces, the current strategy helps ensure their operational readiness in cyberspace. Measure 23, 'Capability for implementing active measures in cyberspace under the IntSA and ArMA,' explicitly states these capacities: The DDPS (FIS and Armed Forces) has sufficient qualitative and quantitative competencies and capacities to disrupt, prevent, or slow down attacks on critical infrastructures where necessary. These measures are used in accordance with the legal requirements of the IntSA and ArMA.

With the IntSA's legal framework clearly defined, the ArMA was reinforced through the Ordinance on Military Cyber Defence,⁴⁶ adopted in March 2019. This ordinance's underlying rationale is that it is only applicable in reaction to a cyber attack. In the event of an attack against the Armed Forces' computer systems, it governs the measures to be taken in cyberspace for purposes of self-protection or self-defence. Like the Intelligence Services Ordinance, the Ordinance on Military Cyber Defence lists

the conditions under which active cyber defence actions are to be authorised, namely the purpose of the action, the period during which the action will be conducted, the systems and networks concerned, the maximal amount of penetration, the proof of legality (notably its proportionality), as well as the risks related to a specific action.

Finally, it defines the relevant roles and responsibilities. Accordingly, the military cyber defence falls under the Armed Forces Command Support Organisation (AFCSO), which in turn is also the technical service provider of the FIS. The AFCSO has the capability to execute active cyber defence actions, while the Chief of the Armed Forces has the authority to give the order for such actions, and final approval must come from the defence minister.

Discussion

As used in the cited Swiss legislation, the definitions of ‘perturb’ and ‘impede’ differ from those provided by dictionaries. In a defence context, their denotations are very precise, leaving little latitude for interpretation. According to the general Swiss military doctrine,⁴⁷ ‘perturb’ means “hinder the adversary’s manoeuvre and if possible inflict losses;” and ‘impede’ means “ensure that an adversary cannot reach or take over a determined portion of terrain.” Regarding a third term used alongside these, ‘slow down’ has no specific military meaning and standard usage applies.

However, as the statutes employing these three terms have only recently come into force in the cyber realm, no state-wide guidelines yet define their meanings or usage. In the context of cyber defence, “inflicting losses [to the adversary]” more or less matches the US concept of physical damage or destruction of systems resulting from the application of active cyber defence capabilities. However, as no precise meanings are yet available from the Swiss Department of Defence, the use of these newly introduced terms merits caution until more in-depth analyses have been performed.

One plausible explanation for the lack of clear prescriptions regarding these terms’ use is the lack of an explicit Swiss cyber defence doctrine. While the Swiss government has adopted a National Cyber Security (NCS) strategy, leading to the Department of Defence’s formulation of an Action Plan for Cyber Defence (APCD), what remains to be developed is a military doctrine on cyberspace operations. Ideally, this doctrine would define the roles and responsibilities of the armed forces in cyberspace and, particularly, the scope and intended uses of active cyber defence and its related procedures. In developing a military doctrine which

should encompass active cyber defence, there are a few Swiss particularities that need to be considered.

One particularity of the Swiss armed forces is that they are a conscription army. As the vast majority of armed forces members are reservists, making it a 'militia army,' its permanent full-time staff is comprised of a small nucleus of military professionals. Therefore, most adopted cyber strategy documents have been focused on providing this small professional staff with the competencies, authorities, and resources necessary to protect the Department of Defence from cyber attacks.

A natural and logical step would be to develop a military doctrine designed specifically for Switzerland's militia army. From our perspective, as many reservists are private sector IT professionals, they embody a rich, untapped potential. It would be highly beneficial to identify the most motivated and knowledgeable reservists for cyber defence force positions. With this in mind, Switzerland could draw inspiration from the Estonian Defence League's Cyber Unit.⁴⁸ The purpose of this league is to empower the readiness of the Estonian society to defend its independence and constitutional order. At the core of this league is 'free will and self-initiative.' The Estonian initiative could serve as a reference for Switzerland, since the participants contribute to this purpose on a purely voluntary basis.

Against this background, promoting recruitment would require development of specific and targeted curricula for cyber defence force reservists. This would include the possibility to go from rank-and-file positions to professional careers as commissioned officers. With respect to active cyber defence, the required skills to plan and conduct such operations would require specific training and exercises in order to build the necessary expertise. Therefore, the DDPS need to develop a chain of command to plan and conduct cyberoperations, including active cyber defence. One step in this direction is the recently developed cyber-training course available to new recruits.

The lack of critical mass of full-time staff and reservists also affects another task of the armed forces: according to Measure 24 of the NCS 2018–2022, they must ensure operational readiness across all situations in cyberspace and exert their role of subsidiarity in support of the civilian authorities.⁴⁹ However, this principle of subsidiarity entails certain challenges for the Swiss armed forces. First, no clear boundaries delineate civilian from military domains, since military environments are highly dependent on civilian infrastructures. Thus, strong collaboration is required between all relevant agencies of the Swiss Federal Administration. Moreover, the relations and interactions between the military and

providers of critical infrastructures (e.g., telecommunications and energy) are strategically important, not least due to the Armed Forces' dependency on these services. Thus, well-orchestrated interaction and collaboration—both between the administration's civil and military agencies and between the Armed Forces and the providers of critical infrastructures—will be a key determinant for the successful management of cyber risks. Second, the Swiss national approach to cyber risks lacks institutionalised collaboration between the stakeholders noted above. In fact, even though the NCS 2018–2022 acknowledges the subsidiary role of the Swiss Armed Forces, the principle of subsidiarity in the cyber domain remains only vaguely defined. The doctrine would need to first define what the subsidiary role encompasses, even more so if the use of active cyber defence measures is foreseen, as this notion demands a concrete definition. Furthermore, the doctrine to be developed will first need to depict the status quo of the military's capabilities at hand in cyberspace, not only to defend military networks and systems, but also to support federal agencies and critical infrastructure providers. The question is: what types of skills and services can the Swiss armed forces provide to the responsible national authorities and operators of critical infrastructure? To what extent, if any, can the Swiss armed forces contribute to the effective handling of a major cyber incident that disrupts vital services on a national level (e.g., communication and transportation systems)?

In our view, the Swiss armed forces have not yet acknowledged the potential benefits of active cyber defence. Until now, the related policies have focused primarily on cyber protection in a technical sense, such as ICT security. Moreover, all other domains of operations (land, air, sea, and space) have long recognised the digitalisation of the battlefield as a major consideration affecting all operations.

Therefore, as the armed forces perceive cyber capabilities as enablers for traditional warfare—which is true—they prioritise cyber protection over active defence. However, their current stance fails to acknowledge the vital additional principle that military actions in cyberspace produce valuable opportunities for modern armed forces in relation to emerging threats. Therefore, we argue that active cyber defence needs to be fully integrated into military operations planning. One important step is to widen the scope of cyber defensive measures to include active components. This will pave the way for active cyber defence missions.

Lastly, active cyber defence is based largely on thorough intelligence gathering regarding the source of an attack. Because of the disruptive nature of active cyber defence, the characterisation

(and possibly attribution of the attack's origin) is a criterion that has to be met with the highest level of confidence (i.e., beyond reasonable doubt). Consequently, with respect to the principle of proportionality and necessity, cyber rules of engagement need to be developed and established as a *sine qua non* standard.

Conclusion

In this paper, we have attempted to contribute to a greater understanding concerning the concept of active cyber defence. This includes outlining various definitions provided in the literature. Even though no formally accepted definitions were available, we noted general agreements on the following features of cyber defence: defensive purpose, real-time response, out of the defended perimeter, and disruptive effect.

One further commonality apparent in the existing literature is the understanding that active cyber defence does not equal offensive cyber operations. While the main purpose of active cyber defence is to cease an ongoing cyber attack, thereby maintaining the defender's freedom of manoeuvre in cyberspace, offensive cyber operations seek to project power in and through cyberspace, and may include no defensive function.

Current approaches to cyber operations have been established through a combination of cyber defence policy and military doctrine. While many countries have defined roles, responsibilities, and procedures for the execution of cyberspace operations, the US and France are at the forefront of cyber defence doctrine development. The US armed forces have established a framework upon which they categorise all conceivable cyberspace defence operations into three groups: protective, defensive, and offensive missions. Recently, they updated their policy to signal their willingness to 'persistently engage' and undertake 'forward defence,' making it the most active known national cyber defence stance.

In parallel, France has developed one of the most advanced European cyber doctrines. Similar to the US, France uses a cyber warfare triad of protection, defence, and offence. One particularity of France's position, though, is its public claim that they have developed cyber weapons and are willing to operationalise them as they would other weapons systems.

The Swiss case studied in this paper shows that the Swiss have followed the trend, shaped by the US and France, as they have recognised the importance of active cyber defence measures. Therefore, even as a neutral country, Switzerland has developed a political and legal framework for the use of these means.

However, until now, this remains mainly a political declara-

tion, as a considerable gap exists between strategy and implementation. According to our analysis, the armed forces have not yet fully integrated cyber defence principles into military operations. This is because, in our view, many Swiss leaders still think and plan in terms of the four conventional operational domains—land, sea, air, and space—leading them to treat cyber defence purely as a protective means to enable traditional military missions. This type of thinking obscures not only the threats and opportunities that accompany active cyber capabilities, but the strengths they offer in any military mission.

In order to begin to tap the potential of active cyber defence, we recommend the following steps. First, all involved parties need to understand that the notion of cyber defence goes beyond purely protective measures. According to our analysis, traditional ICT protective measures are insufficient to address sophisticated threats, especially coordinated adversarial cyber operations. Therefore, it is imperative to operationalise active cyber capabilities at all levels of war, from strategic to tactical. Second, to overcome the current lack of skilled personnel conversant in both cyber and conventional defence language, it will be necessary to explore alternative recruitment models. One possible path would be to consider reservist staff. The Swiss ‘militia’ army provides an important advantage available in few other countries: the armed forces can benefit from the cyber skills conscripted soldiers have learned and practised in their personal and professional lives. Third, as the use of force in cyberspace is a unique state prerogative, the use of active cyber defence of essential assets has to be placed, in a subsidiary manner, at the disposal of operators of critical infrastructures. Thus, the armed forces need to adapt their operational availability to allow timely provision of defensive measures to private sector operators. This will require re-evaluation of modes of communication and cooperation between the armed forces, civilian agencies, and critical infrastructure operators. Finally, while we recognise the importance of integrating active cyber defence in cyber operations, we are also aware that this development is not without its risks. The most obvious of these is the fact that states’ increasing need to develop active cyber capabilities will spur an arms race in cyberspace thereby exacerbating the security dilemma.⁵⁰

- 1 James Andrew Lewis and Götz Neuneck, "The Cyber Index: International Security Trends and Realities," Geneva and New York: United Nations Institute for Disarmament Research, 2013, 3.
- 2 "Presidential Policy Directive – Critical Infrastructure Security and Resilience," White House, February 12, 2013, accessed January 6, 2019, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.
- 3 See also Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," (paper presented at the 4th International Conference on Cyber Conflict, 2012) and Bruce Schneier, "Militarizing Cyberspace Will Do More Harm Than Good," Irish Times, November 29, 2012, accessed January 14, 2019, https://www.schneier.com/essays/archives/2012/11/militarizing_cybersp.html.
- 4 Eric J. Holdaway, "Active Computer Network Defense: An Assessment" (research report, Air Command and Staff College, U.S. Air University, 2001).
- 5 Vikas Jayawal, William Yurcik, and David Doss, "Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism?" Proceedings of the International Symposium on Technology and Society: Social Implications of Information and Communication Technology, 2002, 380–386.
- 6 Dorothy E. Denning, "The Ethics of Cyber Conflict." In Luciano Floridi and Mariarosaria Taddeo (eds.), *The Handbook of Information and Computer Ethics*, (Cham: Springer Verlag, 2008), 408.
- 7 Ibid. Denning, "The Ethics of Cyber Conflict," 408.
- 8 Solange Ghernaouti, *Cyber Power: Crime, Conflict and Security in Cyberspace*, (Lausanne: EPFL Press, 2013).
- 9 United States Department of Defense (US DOD), Department of Defense Strategy for Operating in Cyberspace, 2011. Accessed January 7, 2019, <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.
- 10 Ibid., 7.
- 11 United Kingdom Ministry of Defence (UK MOD), 2016. *Cyber Primer*, 2nd ed., accessed January 8, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf.
- 12 Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge: Cambridge University Press, 2013), 257.
- 13 Joe Barnes and Richard J. Stoll, *Preemptive and Preventive War: A Preliminary Taxonomy*, (Houston: James A. Baker III Institute for Public Policy at Rice University, 2007), 7.
- 14 Paul Ducheine and Jelle van Haaster, "Fighting Power, Power, Targeting and Cyber Operations," (paper presented at the 6th International Conference on Cyber Conflict, 2014), 304.
- 15 Dorothy Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain." In George Perkovich and Ariel E. Levite (eds.),

Understanding Cyber Conflict: Fourteen Analogies, (Washington: Georgetown University Press, 2017), 194.

16 Robert S. Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence," (paper presented at the 6th International Conference on Cyber Conflict, 2014), 10.

17 Emilio Iasiello, "Hacking Back: Not the Right Solution," *Parameters* 44, no. 3 (2014): 106.

18 Paul Rosenzweig, "International Law and Private Actor Active cyber defensive measures," *Stanford Journal of International Law* 50 (2014): 103.

19 Max Smeets and Herbert S. Lin, "Offensive Cyber Capabilities: To What Ends?" (paper presented at the 10th International Conference on Cyber Conflict, 2018), 58.

20 Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010): 63.

21 National Research Council, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in *Proceedings of a Workshop on Detering Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington: National Academies Press, 2010.), 77–97.

22 Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* 73, no. 2 (2014): 12–19.

23 Robert S. Dewar, "Active Cyber Defense," *CSS Cyber Defence Trend Analysis* no. 1 (2017).

24 Lucas Kello, "Private-Sector Cyberweapons: Strategic and Other Consequences," *SSRN Electronic Journal* (2016), <http://dx.doi.org/10.2139/ssrn.2836196>.

25 Kello, "Private-Sector Cyberweapons: Strategic and Other Consequences," 4.

26 Dorothy E. Denning, "Framework and Principles for Active Cyber Defense," *Computers & Security* 40 (2014): 108–113.

27 Kello, "Private-Sector Cyberweapons: Strategic and Other Consequences," 7.

28 United Nations, *Charter of the United Nations*. San Francisco, United States, 1945. Article 2(4).

29 For the complete list, consult the following NATO Cooperative Cyber Defence Centre of Excellence webpage: <https://ccdcoe.org/library/strategy-and-governance/>.

30 Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37.

31 United States Department of Defense (US DOD), *Cyberspace Operations*. Joint Publication 3-12 (JP 3-12), 2018, accessed January 11, 2019, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

32 David Raymond et al., "Key Terrain in Cyberspace: Seeking the High Ground," (paper presented at the 6th International Conference on Cyber Conflict, 2014), 287–300.

33 United States Department of Defense (US DOD), *Summary Department of Defense Cyber Strategy*, 2018. Accessed January 11, 2019, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMA-

RY_FINAL.PDF.

34 Ibid., 4.

35 France Secretariat-General for National Defence and Security, *Revue Stratégique de Cyberdéfense*, 2018, accessed January 14, 2019, <http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense>.

36 France Ministry of Armed Forces, *Politique ministérielle de lutte informatique défensive*, 2019, accessed January 25, 2019. <https://www.defense.gouv.fr/content/download/551563/9394730/Politique%20minist%C3%A9rielle%20de%20lutte%20informatique%20DEFENSIVE.pdf>

37 France Ministry of Armed Forces, *Éléments publics de doctrine militaire de lutte informatique offensive*, 2019, accessed January 25, 2019, <https://www.defense.gouv.fr/content/download/551555/9394645/EI%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf>.

38 Switzerland Federal Council, *National strategy for the protection of Switzerland against cyber risks (NCS)*, 2012, accessed December 22, 2018, https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html.

39 Ibid., 40.

40 Switzerland Federal Assembly, *Loi fédérale sur le renseignement (LRens)*, 2017, accessed December 23, 2018, <https://www.admin.ch/opc/fr/classified-compilation/20120872/index.html>.

41 Switzerland Federal IT Steering Unit (FITSU), *National Strategy for the Protection of Switzerland against Cyber Risks – NCS implementation plan 19*, 2013, accessed December 22, 2018, https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie-2012/umsetzungsplan-ncs-2012.html.

42 Switzerland Federal Council, *Ordonnance sur le renseignement (ORens)*, 2017, accessed December 23, 2018, <https://www.admin.ch/opc/fr/classified-compilation/20162430/index.html>.

43 Switzerland Federal Department of Defence, Civil Protection and Sport, *Action Plan for Cyber Defence (APCD)*, 2018, accessed December 22, 2018, <https://www.vbs.admin.ch/fr/defense/protection-cyberattaques.detail.document.html/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.html>.

44 Switzerland Federal Assembly, *Loi fédérale sur l'armée et l'administration militaire (LAAM)*, 2018, accessed December 23, 2018, <https://www.admin.ch/opc/fr/classified-compilation/19950010/index.html>.

45 Switzerland Federal IT Steering Unit (FITSU), *National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022*, 2018, accessed December 22, 2018, https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html.

46 Switzerland Federal Council, *Ordonnance sur la cyberdéfense militaire (OC-Mil)*, 2019, accessed February 2, 2019, <https://www.admin.ch/opc/fr/classified-compilation/20182319/index.html>.

47 Switzerland Armed Forces, *Begriffe Führungsreglemente der Armee*, 2004,

accessed August 1, 2017, [https://https://www.lmsvbs.admin.ch](https://www.lmsvbs.admin.ch)

48 “Estonian Defence League’s Cyber Unit (EDL CU),” Estonian Defence League (Kaitseliit), accessed February 4, 2019, <http://www.kaitseliit.ee/en/cyber-unit>.

49 Switzerland Federal IT Steering Unit (FITSU). 2018. National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022, accessed December 22, 2018, https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html.

50 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (Oxford: Oxford University Press, 2016).

SAFE AT HOME: TOWARDS A FEMINIST CRITIQUE OF CYBERSECURITY

Julia Slupska, University of Oxford

Abstract

Feminist theorists of international relations (IR) have long argued that binaries of public/private reinforce the subsidiary status given to gendered insecurities, so that these security problems are 'individualised' and taken out of the public and political domain. This article argues that the emerging field of cybersecurity risks recreating these dynamics by omitting or dismissing gendered technologically-facilitated abuse such as 'revenge porn' and intimate partner violence (IPV). I present a review of forty smart home security analysis papers to show the threat model of IPV is almost entirely absent in this literature. I conclude by outlining some suggestions for cybersecurity research and design, and reaffirming the importance of critical studies of information architecture to the modern study of IR.

*And so you're back
From outer space
I just walked in to find you here
with that sad look upon your face*

*I should have changed that stupid lock,
I should have made you leave your key
If I'd known for just one second
you'd be back to bother me*

- I Will Survive (Gloria Gaynor)

The ease of changing locks after a break-up—and the design of homes and domestic architecture more broadly—could have once been seen as a private matter, far from the concern of international relations (IR) and security scholars. However, the global spread of information technologies means that information architectures designed in one part of the world mediate the lives of people worldwide both in the workplace and in 'private' spaces like the home. For example, 'smart home' technology allows users to

Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity,"
St Antony's International Review 15. no. 1 (2019): 83-100.

control their home from an interface, adjusting temperature, unlocking doors, controlling lights, or viewing security cameras. The smart home market is growing rapidly and is forecast to comprise nearly 1.3 billion devices by 2022.¹ Therefore, lack of diversity and failures of imagination among designers, theorists and practitioners of cybersecurity have global implications.

The definition of cybersecurity is contested and in flux. Cybersecurity is best understood as the set of protocols, technologies, and practices designed to protect against threats mediated by digital technology. The question of *who* or *what* is protected is often at the heart of definitional controversies. Early understandings of ‘information security’ (which is often used interchangeably with cybersecurity), such as the classic ‘CIA model,’ focused on the confidentiality, integrity and availability of information.² Similarly, Kello’s *The Virtual Weapon and International Order* – an influential book on cybersecurity and IR – defines cybersecurity as “measures to protect cyberspace from hostile action,” where “cyberspace” is defined as “all computer systems and networks in existence.”³ However, as von Solms and van Kiekerk point out, cybersecurity goes beyond information security, as the term encompasses not just the protection of information, machines, or networks, but also of the humans that use them. A feminist approach to cybersecurity must be grounded by a focus on harms to humans.

Security analysis papers – in which new technologies are assessed in light of how their security architectures might be compromised by an adversary – are a common cybersecurity practice.⁴ Security analyses commonly begin by ‘threat modelling’: a systematic analysis of the probable attacker’s profile, the most likely attack vectors, and the assets most desired by an attacker.⁵ Threat modelling therefore reflects assumptions about the causes of insecurity among technology users.

Feminist IR theorists have challenged binaries of internal/external and personal/political violence in conventional security studies, arguing these ignore or diminish the threat of gender-based violence and threats to women’s security. Unfortunately, the emerging field of cybersecurity has not incorporated these insights and therefore risks omitting many forms of technological abuse. In this paper, I present a review of smart home security analysis to show how cybersecurity research fails to account for domestic and intimate partner violence (IPV) in its threat models. This is deeply concerning because technology is an increasingly common medium for abuse; if researchers ignore the domestic threat model, it is unlikely designers and practitioners will account for how information architectures can both facilitate and constrain abuse.

The paper proceeds as follows: first, I briefly outline feminist approaches to IR and security studies and argue that the emerging field of cybersecurity risks repeating patterns of gendered omission common in these fields. Second, I present existing research on technologically-mediated abuse in situations of domestic and intimate partner abuse.⁶ Using the case study of the August Smart Lock, I show how security architectures can be bypassed and subverted by abusers. Then, I present the results of a comprehensive overview of existing smart home security analyses, which demonstrates that the threat of domestic violence is almost entirely ignored in the smart home security analysis literature. Furthermore, a closer examination of the only paper which explicitly addresses this threat model shows it is dismissive and displaces the responsibility of protection onto potential targets of abuse. Last, I discuss the dangers inherent in the widespread assumption that the 'owner' of digital devices does not pose a threat, and how cybersecurity practices could improve by incorporating approaches developed in feminist theory.

The Private is Political: Feminist Responses to Security Studies

Feminist IR emerged in the late 1980s among a variety of scholars who sought to incorporate gender concerns into the study of international politics. Notably, Cynthia Enloe's *Bananas, Beaches and Bases* charted the many forgotten roles women play in international politics as plantation sector workers, diplomatic wives, and sex workers on military bases.⁷ Enloe challenged her readers to reconsider what international politics was 'all about', asking them to keep a sharp eye on the ways policies made at the most intimate level to the most distant affect women and men, usually in different ways.

Arenas for state and military decision-making are largely populated by men, and the same is often true of the academic study of IR, particularly security studies.⁸ Feminist IR theorists connect this lack of diversity to over-narrow definitions of 'security' which exclude supposedly 'private,' 'domestic,' or 'individual' security issues such as gender-based violence (including problems like IPV and honour killings).⁹ Tickner notes that while conventional security studies have generally looked at conflict from a top-down or structural perspective, feminists have generally taken a bottom-up approach analysing the impact of war at the micro level.¹⁰ Similarly, the analytical approach of 'feminist geopolitics' challenges the division between 'high politics' and 'private life' by tracing similarities in forms of power, oppression, and resistance

at and between multiple scales (for example the body, home, and nation-state).¹¹

Feminist theorists traditionally argue that the liberal notion of the home as a private place protected from state power and intervention often shields abuse ranging from casual misogyny through to extreme violence.¹² Before the protests of first-wave feminist movements in the 19th century, most legal systems did not prohibit domestic violence, implicitly accepting wife-beating as a valid exercise of a husband's authority over his wife.¹³ Notions of privacy can reinforce the subsidiary status granted to women's (in)security, so that gendered security threats are 'individualised' and taken out of the public and political domain.¹⁴ This observation has led to a long-standing debate on the home among feminist theorists: as Sokoloff and Dupont (2005) know, this critique of privacy comes from a position of privilege, as the situation is more complicated for women who are minoritised or have low socio-economic status, as they are already disproportionately targeted by state intervention. Therefore, calls for the inclusion of these threats within cybersecurity frameworks should be careful of providing justification for unwelcome intrusions into the lives of vulnerable populations.¹⁵

As Tickner notes, the response from the wider IR community to feminist critics has often been 'awkward silence.'¹⁶ However, in the following decades, feminist approaches have become more integrated into the mainstream of the discipline, if only in comments recognizing the discipline's lack of diversity. For example, Buzan and Hansen's intellectual history of security studies notes the "Anglo-centric (and militaristic and patriarchal) bias" of international security studies as a "blind spot," and seeks to remedy this by "[granting] critical approaches more space than they have had quantitatively."¹⁷ Arguably, characterising such omissions as a blind spot diminishes their importance; Bilgin argues the Western-centrism of the discipline should be understood as a constitutive practice rather than a 'blind spot.'¹⁸ The same is likely also true of gendered practice of diminishing or excluding women's insecurities from the discipline of security studies.

Although there is still plenty of omission and awkward silence, IR and security studies increasingly acknowledged feminist approaches and incorporated them alongside other theoretical approaches in both IR introductory texts and teaching syllabi.¹⁹ Unfortunately, the emerging field of cybersecurity seems likely to repeat the same dynamics of exclusion. Consider the example of 'revenge porn' (i.e., non-consensual pornography), a technologically-mediated form of abuse which is highly gendered. Revenge porn is rarely considered a 'cybersecurity issue' among cyberse-

curity experts and practitioners.²⁰ Informally, practitioners in the field have told me this is because it is really a ‘privacy issue.’

Yet when an employee in a company shares confidential information with an unauthorised third party, this is clearly identified as a cybersecurity issue. A subfield of cybersecurity has been developed to protect companies from ‘insider threat,’ (i.e., malicious employees who might leak company data for revenge or profit). To combat insider threat, cybersecurity experts develop social and technical ‘access controls’ which strictly outline who can access information, at what time, and for how long. Cybersecurity teams closely monitor data flows, flagging when employees download large amounts of data at odd hours. When an employee leaves a company, they often immediately lose access to sensitive files, and extensive legal punishments kick in if they somehow manage to share them anyway.²¹ Why do such access controls not exist for relationships? Instead of developing programmes which revoke access to intimate data when a relationship ends and making such programmes accessible to the wider public, online safety advocates often publish guides aimed at teenagers, advising them not to share intimate photos in the first place.²²

Who codes matters: there are serious ramifications when only a narrow section of society builds widely-used technologies. For example, Noble shows that Google search algorithms become racist and sexist precisely because they reflect the biases and values of the people who create them.²³ Critical theorists of technology argue that in restricting participation in technology development, we risk hardcoding prejudice and discrimination into the development of everyday technologies.²⁴ Similarly, Perez documents how countless objects—from smartphones and seatbelts to heart failure tests—are designed around biased data which excludes women, resulting in negative impacts on their health and well-being.²⁵ Cybersecurity is a nascent field which draws on methods and approaches developed in computer science, cryptography, economics, criminology, forensics, international politics, and security studies. However, critiques which incorporate gendered power relations have rarely been applied to cybersecurity. In fact, a Google search for ‘feminist cybersecurity’ yields only a guide developed to help protect feminists from online harassment.²⁶ Although feminists undoubtedly need cybersecurity, cybersecurity needs feminism too.

Technological Abuse in IPV

Domestic violence and IPV is a frequent cause of death worldwide. A 2018 UN report found that women are more likely

to be killed at home than in any other location.²⁷ Of global female homicide victims in 2017, about 34 percent were murdered by an intimate partner and 24 percent by a relative. Although domestic violence can occur between any individuals, women are considerably more likely to be victims, and men are more likely to be perpetrators.²⁸ IPV is still highly prevalent in the UK: domestic abuse-related crimes recorded by the police accounted for 32 percent of violent crimes in the year ending March 2017.²⁹ These dynamics play out differently across different cultures, and intertwine with other forms of social stratification, such as class, race, and sexuality.

As digital technologies increasingly mediate personal relations, they also become wielded in ways that perpetuate existing patterns of control.³⁰ Existing research on technologically-mediated abuse, or ‘tech abuse,’ has examined abusers’ attack strategies,³¹ survivors’ experiences and security practices,³² and how emerging technologies, such as smart home devices, could be used to perpetuate abuse.³³ These studies outline a distinctive and uniquely challenging threat model. The threat actor – an abusive parent or current or former partner – is usually highly motivated, although not necessarily very technically skilled.³⁴ Abusers are often obsessive and devious in finding ways to intimidate and coerce their victims; digital tools of abuse can range from the technologically simple (such as social media stalking) to the highly sophisticated (mobile spyware or ‘spouseware’, which makes exploits developed in government espionage accessible to consumers without advanced skills).³⁵

People targeted by abuse find it extremely challenging to leave abusive relationships, due to threats and intimidation, as well as social and economic dependence on their abuser.³⁶ Targets are at the highest risk of violence and death when they try to leave their abuser; however, tech abuse often escalates in the ‘living apart’ phase, when the abuser no longer has physical access to the target. At this stage, the disclosure of location-based information can result in physical injury and death to the target; this makes the use of social media and smartphones a security problem for domestic violence charities.³⁷

Abusers are also aided by their close relationship with the victim; the abuser and target may still be co-habiting, and abusers are often shared or sole owners of accounts and devices. Intimate photos can be posted online—sometimes alongside details like name or address in a practice called ‘doxxing’—to humiliate former partners.³⁸ Previously obtained access to victims’ accounts leaves them vulnerable to identity theft, blackmail, sabotaged job applications, or even false advertisements claiming the victim is a

prostitute with the victim's new address and phone number. GPS enabled apps like 'Find My Friends' are used to monitor location.³⁹ Smart home appliances like sound systems or remotely-controlled thermometers are used for monitoring targets as well as gaslighting (i.e., making a target doubt their own sanity) by changing music or temperature in the victim's home.⁴⁰

Smart Home Security Analysis

The research outlined in the previous section builds a comprehensive threat model of tech abuse in the context of IPV. However, the wider genre of security analysis – which may be ultimately be more likely to influence the design of security architectures – often fails to consider this threat model. To illustrate this problem, I will start with the case study of the August Smart Lock (one of the early leaders in the smart home market) which introduces the reader to an example of systems security architecture. I then review two papers which assess this security architecture and show that their threat modelling does not sufficiently account for IPV. Last, to demonstrate that this is not an isolated oversight, I present the results from a comprehensive review of smart home security analysis papers.

August Smart Lock System

The August Smart Lock is a Bluetooth-enabled device that attaches to the inside of a standard deadbolt and allows a user to lock and unlock the door with their smartphone. The device also records which users lock or unlock the door.⁴¹ Users of the August Smart Lock are either 'Owners' or 'Guests.' The Owner—effectively the administrator of the system—has many more privileges than the Guest: for example, they can view the lock's activity log, invite new users to be Owners or Guests, and configure when and for how long Guest users can unlock the door (see Figure 1). As Fuller et al point out, an Owner-level access "implies a very high degree of trust, and would typically be granted only to, for example, a spouse or a co-owner of the property."⁴²

TABLE IV
AUGUST SMART LOCK OPERATIONS FOR DIFFERENT USER LEVELS

	Owner	Guest
Lock/Unlock Door	✓	✓
Lock Activity	✓	
Guest List	✓	
User Invitation	✓	
User Level Control	✓	
User Permission Control	✓	

Figure 1. User permissions for August Smart Lock [from Ye et al. 2017, p. 501]

The August Smart Lock system consists of the smart lock itself, a smartphone app, and the August web servers (see Figure 2). Owners and Guests identify themselves by logging into the smartphone app with their phone number or email address and a password they chose. The smart lock communicates with the phone app via Bluetooth, allowing users to lock and unlock the door. The smartphone app, in turn, communicates with the August web servers via Wi-Fi to grant access to other users or change settings. Owners can unlock the door via Bluetooth without Wi-Fi, but guests must communicate with the August web servers via Wi-Fi to unlock the door.

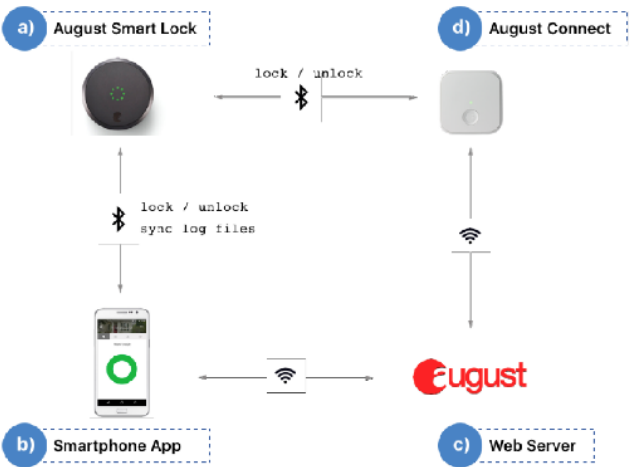


Figure 2: Overview of the August Smart Lock system [from Fuller et al. 2017, p.4]43

Fuller et al and Ye et al both conducted a security analysis of the August Smart Lock. Both papers prioritise a model in which a thief attempts to gain illicit access to the house as well as a scenario in which an adversary with temporary guest-level access (such as an ‘Airbnb tenant or a household worker’) changes their settings to gain access at a different time. In these cases, the Owner is automatically assumed to be the defender, rather than a potential threat.

Fuller et al does consider the following scenario:

1. Alice gives Bob Owner-level access.
2. Alice gets out of Bluetooth range of the lock.
3. Bob maliciously puts his phone in airplane mode, preventing it from communicating with the August servers, but leaving Bluetooth enabled.
4. Alice revokes Bob's access.

In this case, because Alice cannot communicate with the lock (as she is out of Bluetooth range) or Bob’s phone (as he has disabled Internet connectivity), the lock cannot receive the message that Bob no longer has access. This means Bob, who is no longer a legitimate user of the lock, can enter the home at will until Alice is within Bluetooth range. Fuller et al point out that there also appears to be a bug in the lock’s logging code, so that the log files will not report Bob’s access during this period.

However, Fuller et al are surprisingly dismissive of this security vulnerability, saying it is alarming in theory, but unlikely to be a problem in practice, given that:

Owners, by definition, can revoke each other's access. In fact, if Bob were truly malicious, he could have revoked Alice's access after he was granted OWNER status. For this reason, the original owner should not give OWNER status to anyone she does not trust immensely.

Both prongs of this argument are highly suspect. The fact that a malicious Owner can immediately and effortlessly revoke a legitimate Owner’s access to the house should be considered a potential threat. Similarly, in the context of a relationship ending, it is unfortunately the case that immensely trusted parties can suddenly become adversaries with the intention to cause harm. Saying that Alice should not give Owner status to someone she does not trust also places responsibility on her (rather than the manufacturer) to prevent her own abuse.

Of course, in any scenario in which cohabitants lose trust in

each other, the question of which inhabitant is a legitimate owner is much more morally and legally fraught than in the examples of a thief or an errant Airbnb guest. However, security system policies cannot simply ignore these issues, given the serious harm that can result from domestic abuse and stalking.

Review of smart home security analysis

The following section presents the results of a review of the wider smart home security analysis academic literature. To gather a comprehensive data set, I conducted a search in the SCOPUS academic database and collected 40 smart home security analysis papers.⁴⁴ I coded each paper according to what artefact it analysed and which threat models it considered (see Appendix I). The papers varied in specificity, with some analysing a specific product (like the Samsung SmartThings platform) while others considered ‘Internet of Things’ (IoT) or ‘smart home’ devices more broadly (see Table 1).

Artefact	Count
Home	8
Grid/meter	7
IoT	6
Platform	5
Medical	5
Card	3
Lock	2
Vehicle parking/charging	2
Server	1
Television	1
Total	40

Table 1: Artefacts Analysed in Sample Papers

Attacker-centric threat modelling begins by elaborating ‘threat actors’ (i.e., potential adversaries which target the system) before elaborating ‘threats’ (i.e., attacks which might be conducted by threat actors to compromise vulnerabilities in the system).⁴⁵ However, many of these security analyses did not clearly identify threat actors or distinguish between threat actors and threats. 16 papers explicitly mentioned potential threat actors (either in the introduction or as a formal part of the threat model), resulting in 29 threat actors identified in the sample (see Table 2).

Threat actor	Count
Remote network-based attacker	7
External adversary	6
Internal adversary	5
Burglar/thief	2
Privileged insider	2
Arsonist	1
Bad manufacturer	1
Home intruder	1
Malicious user	1
Physically-present attacker	1
Revoked attacker	1
Suppliers and drivers	1
Total	29

Table 2: Threat Actors Considered in Sample Papers

The representations of threat actors in Table 2 and threats in Table 3 below do not seek to categorise threat models, but rather to show how they were represented in the sample papers. For example, the most common threat actor, (i.e., a remote network-based attacker), could be grouped with the similar ‘External adversary’. These papers often used ‘External adversary’ to distinguish from an ‘Internal adversary’ (internal to an organisation); external adversaries could be thieves who are not necessarily remote- and network-based. Likewise, some of the more specific threat actors mentioned, such as ‘Arsonist’ or ‘Home intruder’ could be grouped as external adversaries; however, I have included them to retain the level of specificity in the papers. Table 3 outlines all threats listed in these papers’ threat models.

Threat	Count
Eavesdropping	14
Replay	10
Denial of service	9
Impersonation	8
Man-in-the-Middle	5
Offline password guessing	5
Identity breach	4
Insider attack	3
Tampering	3
Fraud	2
Privacy breaches	2
Privileged insider	2
Smart card security breach	2
Blackhole attack	1
Cache modification	1

Damage to property	1
Denning-Sacco attack	1
Disabled vacation mode of the home	1
Fake fire alarm	1
Firmware manipulation	1
Forgery	1
Handshake key leakage attack	1
Home intruder	1
Integrated attack vector and feature distributed malware	1
Internal adversary	1
Local area attack	1
Network based remote attack	1
Network Interface Card (NIC) firmware	1
Nonlinear modification	1
Node capture and physical damages	1
Node controlling or destroying	1
Offline guessing attack	1
Printer	1
Relay	1
Remote access because of stolen or lost smart card	1
Remote control	1
Revoked access attack	1
Router modification	1
Secretly planted door lock codes	1
Specific firmware attacks using USB	1
Stole existing door lock codes	1
Theft and counterfeiting of fingerprint	1
User info change and disclosure attack	1
Virus attack	1
Total	100

Table 3: Threats Considered in Sample Papers

Domestic violence or an abusive partner or family member was not mentioned explicitly in any of these papers. Arguably, some of the listed threat actors—such as ‘Internal adversary,’ ‘Privileged insider,’ or ‘Malicious user’—could include the domestic violence threat model. But closer inspection shows this is not the case, as all seven papers which consider ‘Internal adversaries’ or ‘Privileged insiders’ discuss ‘insiders’ as employees of the organisation which sells or operates the device. Furthermore, the paper which discusses the ‘malicious user’ threat actor conceives the user as a threat to the manufacturer (rather than other members of the household) as the user might “learn the secrets of the manufacturer, ... sell secrets to third parties, or even attack similar systems.”⁴⁶

The threats considered also reinforce the assumption of a remote, network-based attacker or an external threat such as a

thief. The most common attack—eavesdropping—was described as remote attack (rather than eavesdropping resulting from physical tampering) in all but one paper. Replay, DoS, and Man-in-the-Middle attacks also refer to network-based subversion of security infrastructure. While a domestic abuser could of course theoretically launch any of these attacks, existing research shows that such abusers often use attacks which require only basic computing skills and are unlikely to rely on sophisticated methods.⁴⁷ In contrast, the threats associated with the domestic violence threat model – such as privacy breaches or illicit attempts to enter the home – appear very rarely in the literature. Fuller et al’s security analysis of the August Smart Lock, despite its somewhat dismissive treatment of this threat model, is therefore actually the only paper in this sample which considers a home intrusion by a revoked owner of the device.

Limitations

The academic security analysis literature is not the only source of information on the design of security architectures; in fact, other sources of knowledge like blog posts, news articles, and presentations at security conferences like Black Hat and Def Con may be more influential for cybersecurity practitioners. Therefore, future research should examine which threat models are considered in these venues. Furthermore, the search terms—‘smart home’ and ‘security analysis’—did not capture some relevant work, such as Ur et al’s useful analysis of access controls in commercial smart devices.⁴⁸ Including search terms like ‘audit’ and ‘security policy’ would allow future literature reviews to be more comprehensive.

Lessons for cybersecurity research and technology design

Despite its enduring prevalence in society, domestic abuse is almost entirely ignored in security analysis research on smart home devices. Instead, the threats that most analysts imagine to endanger the home are remote network-based attackers, thieves, domestic workers, and even company employees. The design of the devices described in these papers mostly assume that the ‘Owner’ of the device does not pose a threat to other users of the device. This omission reflects what feminist theorists have long criticised, namely the internal/external binary in which the home is imagined to be a place of safety under threat from external adversaries. Unfortunately, this assumption is far removed from reality. A recent wave of interest in the home among critical and feminist theorists has reaffirmed the home as an ‘intensely political’ site.⁴⁹ As

a result of differences in age, gender, and personality, homes contain hierarchies of power. Just as states or companies have powerful leaders, homes often have ‘hegemons’ with dominant influence or authority over others.⁵⁰ Of course, this authority is constantly negotiated, and most often tempered by familial love, devotion, and affection. But when such bonds break down into abuse and violence, the members of the household with less power suffer disproportionately. The home’s ostensible position as a place of safety and privacy can obscure cases in which domestic relations break down into abuse. My review of smart home security analysis suggests that cybersecurity research risks repeating these dynamics, as targets of IPV are not considered in the design process. The micro-politics of the home need to be incorporated both into technology design and cybersecurity research to challenge this issue. Empirical research has repeatedly confirmed that women report lower computer ‘self-efficacy’—(i.e., confidence about succeeding at a specific task), which influences a person’s use of cognitive strategies, persistence, and strategies for coping with obstacles.⁵¹ Recent news reports have suggested that connected home devices are often installed by men; the partner who considers themselves ‘less technical’ may not know the passwords and functions of various devices.⁵² Future research on the security of smart home devices should empirically answer questions such as: Who installs the smart lock in the household? Who gets Owner status? How is this shaped by gender and other power dynamics in the household? How easy is it for a user to navigate a company website to report that they have been locked out of their home? How do technology providers settle disputes between cohabitants who rely on their designs?

Inequalities in technical ability may exacerbate inequalities in capacity to access shelter or retain a house. For instance, in the example of the Bluetooth-connected smart lock, a legitimate home inhabitant may not know they only have Guest status on the lock (if they have permanent access) and in fact may not know that Owner/Guest statuses exist. This fact will make it extremely difficult to revoke permission or ensure access to the house in the event of a break-up. The rise of ‘smart assistants’ like Amazon’s Alexa and Google Home pose similar problems, as targets of abuse may not be aware that their questions are recorded and can be accessed by the owner of the account.⁵³

To secure the home for all its inhabitants—even those who do buy the devices or think of themselves as ‘tech savvy’—cybersecurity must account for threat models where the nominal owner of a device poses a threat to other users. Researchers at the IPV Tech Research Team have suggested that designers should consid-

er how to develop user interfaces (UIs) that hamper usability for potential abusers, for example by avoiding default location sharing among users.⁵⁴

Feminist principles of consent and autonomy could help guide such design. For instance, in the example of the Bluetooth smart lock, an app which better accounted for consent, and honoured the agency and safety of all its users, would clearly inform users if they are Guests or Owners, and what that status means. It might also allow users the option to not share data about their movements with the company or the 'Owner' of the device. Unfortunately, this is not true in many existing smart home designs. Feminist studies of human-computer interaction have highlighted ways in which norms around issues of accessibility and inclusivity can inform design; however, further research is needed to elaborate how these principles can lead to better cybersecurity design.⁵⁵

Lastly, cybersecurity education should not focus solely on potential targets of digital attacks, as this makes them responsible for preventing their abuse. Education should also be targeted at abusers and sellers of abuse tools, who bear the primary responsibility for the harm the tools cause. While most purveyors and clients of abuse tools may be beyond persuasion, some may not realise their actions are unethical due to a social environment which is friendly to surveillance practices. Feminist principles of consent and respect for individual autonomy could be incorporated into digital ethics and taught from an early age.

Conclusion

The prevalence of technologically-mediated abuse makes it critical that designers incorporate this threat model into the cybersecurity design of their devices. However, despite an increasing body of evidence on gendered tech abuse by ground-breaking researchers, like the IPV Tech Research team at Cornell Tech and the Gender and IoT project at UCL, security analyses of new devices often fail to account for the IPV threat model outlined in this paper. This reaffirms the relevance of the critiques developed in feminist IR, which point out the subordinate status granted to women's (in)securities, and how this status is reinforced by public/private binaries in security research.

Just as feminist theorists critiqued the public/private binary that shielded violence in the home from outside scrutiny, we now need a feminist critique of cybersecurity. Feminist cybersecurity will ask necessary questions: For whom are these technologies made? Where could interventions take place? What trade-offs are made in technology companies when concerns do arise? Whose se-

curity is cybersecurity? Existing cybersecurity practices, technologies, and concepts need to be examined and critiqued. However, as technological innovation continues, such critiques must also provide positive principles—such as consent and egalitarianism—for the design of secure technology.

Lastly, this article reaffirms the importance of the critical study of information architectures and cybersecurity design to the modern study of IR. As the architectures discussed in this paper will be shared by populations across the world, the principles and assumption which underlie their design have direct implications for global security.

Notes

1 IDC, “Worldwide Quarterly Smart Home Device Tracker,” 2018, https://www.idc.com/tracker/showproductinfo.jsp?prod_id=1781.

2 Rossouw Von Solms and Johan Van Niekerk, “From Information Security to Cyber Security,” *Computers and Security*, 2013, <https://doi.org/10.1016/j.cose.2013.04.004>.

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

4 Ahmad W. Atamli and Andrew Martin, “Threat-Based Security Analysis for the Internet of Things,” in *Proceedings - 2014 International Workshop on Secure Internet of Things, SIoT 2014*, 2014, <https://doi.org/10.1109/SIoT.2014.10>.

5 Adam Shostack, *Threat Modeling: Designing for Security* (Indianapolis: Wiley, 2014).

6 Research has increasingly used the phrases ‘intimate partner violence’ and ‘intimate partner abuse’ rather than ‘domestic violence’ to reflect that fact that not all relationships include co-habituating partners and abuse can take forms such as coercive control which are not overtly violent. However, as this paper focuses on smart home technology – which likely affects co-habitants – I will use these phrases interchangeably.

7 Cynthia Enloe, “Gender Makes the World Go Round” in *Bananas, Beaches & Bases. Making Feminist Sense of International Politics*, ed. Cynthia Enloe (Berkeley and Los Angeles: University of California Press, 1989).

8 J. Ann Tickner, “Feminist Responses to International Security Studies,” *Peace Review* 16, no. 1, 2004, <https://doi.org/10.1080/1040265042000210148>.

9 Lene Hansen, “The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School,” *Millennium* 29 no. 2, 2000, <https://doi.org/10.1177/03058298000290020501>.

10 Tickner, “Feminist Responses to International Security Studies.”

11 Vanessa A. Massaro and Jill Williams, “Feminist Geopolitics,” *Geography Compass* 18, no. 4, 2013, <https://doi.org/10.1111/gec3.12054>.

12 Jeannie Suk, *At Home in the Law: How the Domestic Violence Revolution Is Transforming Privacy*, (New Haven: Yale University Press, 2011).

13 Anna Clark, “Domestic Violence, Past and Present,” *Journal of Women’s History*, 23, no. 3 2011, <https://doi.org/10.1353/jowh.2011.0032>.

14 Hansen, “The Little Mermaid’s Silent Security Dilemma and the Absence of Gender in the Copenhagen School.”

15 Natalie J. Sokoloff and Ida Dupont, “Domestic Violence at the Intersections of Race, Class, and Gender: Challenges and Contributions to Understanding Violence against Marginalized Women in Diverse Communities,” *Violence Against Women* 11, no. 1, 2005, <https://doi.org/10.1177/1077801204271476>.

- 16 J. Ann Tickner, "You Just Don't Understand: Troubled Engagements between Feminists and IR Theorists," *International Studies Quarterly* 41, no. 4, 1997, <https://doi.org/10.1111/1468-2478.00060>.
- 17 Barry Buzan and Lene Hansen, *The Evolution of International Security Studies*, (Cambridge: Cambridge University Press, 2009), <https://doi.org/10.1017/CBO9780511817762>.
- 18 Pinar Bilgin, "The 'Western-Centrism' of Security Studies: 'Blind Spot' or Constitutive Practice?," *Security Dialogue* 41, no. 6, 2010, <https://doi.org/10.1177/09670106103882>.
- 19 J. Ann Tickner, "Still Engaging from the Margins?," in *Handbook on Gender in World Politics*, ed. Jill Steans and Daniela Tepe, (Cheltenham: Edward Elgar Publishing, 2016), 5–12.
- 20 Laurence Bradford, "Cybersecurity Needs Women: Here's Why," *Forbes*, 18 October 2018, <https://www.forbes.com/sites/laurencebradford/2018/10/18/cybersecurity-needs-women-heres-why/#7bb1ad5f47e8>.
- 21 Matt Bishop and Carrie Gates, "Defining the Insider Threat," in *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead - CSIIRW '08*, 2008, <https://doi.org/10.1145/1413140.1413158>.
- 22 See for example: "Revenge Porn: What Parents and Teens Need to Know," *Learn Safe*, <https://learnsafe.com/revenge-porn-what-parents-and-teens-need-to-know/>.
- 23 Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, (New York: New York University Press, 2018), <https://doi.org/10.15713/ins.mmj.3>.
- 24 Claude Draude, Goda Klumbyte, and Pat Treusch, "Re-Considering Bias: What Could Bringing Gender Studies and Computing Together Teach Us about Bias in Information Systems?," in *CEUR Workshop Proceedings*, 2018.
- 25 Caroline Criado Perez, *Invisible Women* (London: Penguin Books, 2019).
- 26 "A DIY Guide to Feminist Cybersecurity," *Hackblossom*, <https://hackblossom.org/cybersecurity/>.
- 27 United Nations Office on Drugs and Crime, "Global Study on Homicide: Gender-Related Killing of Women and Girls." 2018, https://www.unodc.org/documents/data-and-analysis/GSH2018/GSH18_Gender-related_killing_of_women_and_girls.pdf [pdf]
- 28 Women are around twice as likely to have experienced domestic abuse as men (7.9 percent of adults aged 16 to 59 years compared with 4.2 percent). Women's Aid, "Domestic Abuse Is a Gendered Crime." <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/domestic-abuse-is-a-gendered-crime/>
- 29 ONS, "Domestic Abuse in England and Wales: Year Ending March 2017," Office for National Statistics, 2017, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2017>.
- 30 In a survey of IPV survivors conducted by Women's Aid (a domestic violence charity), 85 percent of respondents reported online abuse by their partner or ex-partner. "Online and Digital Abuse," Women's Aid, 2018, <https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/online-safety/>.
- 31 Diana Freed et al., "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 2018, <https://doi.org/10.1145/3173574.3174241>; Rahul Chatterjee et al., "The Spyware Used in Intimate Partner Violence," in *Proceedings - IEEE Symposium on Security and Privacy*, 2018, <https://doi.org/10.1109/SP.2018.00061>.
- 32 Jill P. Dimond, Casey Fiesler, and Amy S. Bruckman, "Domestic Violence and Information Communication Technologies," *Interacting with Computers*, 23, no.5, 2011, <https://doi.org/10.1016/j.intcom.2011.04.006>; Tara Matthews et al., "Stories from Survivors: Privacy & Security Practices When Coping with Intimate Partner Abuse," in *Proceedings of the 2017 CHI Conference on Human Factors in*

- Computing Systems - CHI '17, 2017, <https://doi.org/10.1145/3025453.3025875>; Diana Freed et al., "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," *Proc. ACM Hum.-Comput. Interact.*, 2017, <https://doi.org/10.1145/3134681>.
- 33 Leonie Tanczer et al., "Gender and IoT Research Report Technology-Facilitated Abuse," London, November (2018).
- 34 Freed et al., "A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology."
- 35 Thomas Brewster, "Meet The 'Cowboys Of Creepware' -- Selling Government-Grade Surveillance To Spy On Your Spouse," *Forbes*, 16 February 2017, <https://www.forbes.com/sites/thomasbrewster/2017/02/16/government-iphone-android-spyware-is-the-same-as-seedy-spouseware/#fec3d2455cf7>.
- 36 Catherine Kaukinen, "It Could Happen to Anyone: Why Battered Women Stay," *Violence and Victims*, 2005, <https://doi.org/10.1891/vivi.2005.20.2.261>.
- 37 Dimond, Fiesler, and Bruckman, "Domestic Violence and Information Communication Technologies."
- 38 Danah Boyd, "Truth, Lies, and 'Doxxing': The Real Moral of the Gawker/Reddit Story," *WIRED*, 29 October 2012, <https://www.wired.com/2012/10/truth-lies-doxxing-internet-vigilanteism/>.
- 39 Chatterjee et al., "The Spyware Used in Intimate Partner Violence."
- 40 Nellie Bowles, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *The New York Times*, 23 June 2018. <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>
- 41 August, "August Smart Lock," *August.com*, 2017, <https://doi.org/10.1016/j.echo.2016.11.003>.
- 42 Megan Fuller, Madeline Jenkins, and Katrine Tjølsten, "Security Analysis of the August Smart Lock," *Massachusetts Institute of Technology*, 2017, 2.
- 43 Figure 2 also includes the August Connect, an optional accessory device which allows remote control of the lock and will not be discussed in this essay.
- 44 A search for ('security analysis' AND smart AND home) yielded 82 documents. To focus on influential papers, I removed all documents which had no citations, leaving 49 documents. A further nine documents were removed because they did not relate to smart home technology (seven) or because they did not conduct a security analysis (two).
- 45 Shostack, *Threat Modeling: Designing for Security*.
- 46 Atamli and Martin, "Threat-Based Security Analysis for the Internet of Things."
- 47 Freed et al., "A Stalker's Paradise: How Intimate Partner Abusers Exploit Technology."
- 48 Blase Ur, Jaeyeon Jung, and Stuart Schechter, "The Current State of Access Control for Smart Devices in Homes," *Workshop on Home Usable Privacy and Security (HUPS)*, 2013.
- 49 Shelley Mallett, "Understanding Home: A Critical Review of the Literature," *The Sociological Review* 51, no. 1, 2004, <https://doi.org/10.1111/j.1467-954X.2004.00442.x>.
- 50 Jeff Hearn, "A Multi-Faceted Power Analysis of Men's Violence to Known Women: From Hegemonic Masculinity to the Hegemony of Men," *Sociological Review* 60, no. 4, 2012, <https://doi.org/10.1111/j.1467-954X.2012.02125.x>.
- 51 Margaret Burnett et al., "Finding Gender-Inclusiveness Software Issues with GenderMag," *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, 2016), <https://doi.org/10.1145/2858036.2858274>.
- 52 Bowles, "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse."
- 53 Dave Lee, "Amazon Alexa Heard and Sent Private Chat," *BBC News*, 2018.

INTERNET, SOCIAL MEDIA AND CONFLICT STUDIES: CAN GREATER INTERDISCIPLINARITY SOLVE THE ANALYTICAL DEADLOCKS IN CYBERSECURITY RESEARCH?

H. Akin Ünver, Kadir Has University

Abstract

In recent years, computational research methods, digital trace data, and online human interactions have contributed to the emergence of new technology-oriented sub-fields within International Relations (IR). Although cybersecurity scholarship had an initial promise to be the primus inter pares among these emerging fields, the main thrust of this new methodological innovation came through the 'digital conflict studies' sub-field. By integrating Internet and social media research tools and questions into its core topics of sub-national violence, terrorism, and radical mobilisation, digital conflict studies has recently succeeded in addressing some of the data validity and methodology problems faced by cybersecurity scholarship. This article begins by briefly reviewing some of the persistent data and method-oriented hurdles faced by cybersecurity scholarship. Then, it moves on to a more detailed account of how digital conflict studies have been addressing some of these deadlocks by focusing individually on the literature on onset, mobilisation, targeting, intensity/duration, and termination phases of conflicts. Ultimately, the article concludes with the suggestion that cybersecurity scholarship can move past its own deadlocks by building more granular and dedicated research datasets, and also by establishing mechanisms to share event data with the scientific community.

The long-touted theoretical slumber of International Relations (IR) as a discipline¹ was markedly disturbed by the advent of cybersecurity scholarship. Described by many scholars as the 'real fourth domain,' even surpassing the importance of space, digitisation of human power relations, and their competition across an entirely new ground, cyber opened up the way for the 'revival' of IR.² Pre-cyber IR was deadlocked for two main reasons. First, in the aftermath of the Cold War the field had lost its connection to the very origins of its existence—likelihood of large-scale globalised war. With no pressing global threat to study and theorise, the field was split across deconstructivist and post-positivist sub-strands that ran into their own set of limitations.³ Second, the post-9/11 turn in IR had lowered the analytical lens of the bulk of the discipline into terrorism and sub-national violence, making IR more of a surrogate mother of a comparative civil war or rebel dynamics offspring. The field of conflict studies has exploded so much in the last decade that it has ended up almost swallowing up

H. , Akin Ünver "Internet, Social Media and Conflict Studies: Can Greater Interdisciplinarity Solve the Analytical Deadlocks in Cybersecurity Research?," *St Antony's International Review* 15. no. 1 (2019): 101-124.

IR. Yet, it focused more on insurgency and the micro-dynamics of violence, as well as on dyadic socio-political interactions between state and non-state actors, none of which are the central thrust of IR as a discipline.

Cybersecurity promised salvation to IR from being sucked up into the vortex of conflict and terrorism research. It offered scholars a truly global network of state and non-state interactions (both benign and malicious), made some of the more classical concepts of the field (such as bandwagoning, hedging, deterrence, retaliation) relevant again, and offered a new research agenda that went beyond conflict and violence. Attribution problems necessitated a more international and cooperative approach to cybersecurity and brought a new cyber-institutionalist tradition.⁴ 'Attacker's advantage' in cybersecurity re-introduced the question of alliances, balancing, and confidence-building measures.⁵ The fluid and largely uncharted nature of cyberspace reminded scholars of the importance of the anarchy and hegemony debate, as well as the centrality of the rules and norms literature in IR. While cyber hasn't yet influenced the field as much as either conventional or nuclear weapons did back in the Cold War, it has undoubtedly introduced a new wave of issue-broadening nudges, briefly widening the discipline's obsession with sub-national violence.

However, cyber research also ended up in a cul-de-sac of sorts. Due to the sheer magnitude of 'events' in cyber research, it raised a range of conceptual and measurement problems. These problems have led to some unforthcoming answers to essential questions about how to study the field: What constitutes a cyber 'attack'?⁶ How do we disentangle offensive and defensive capabilities in cyber?⁷ How do we acquire and catalogue event data, given the sheer magnitude and near-impossibility of reliably measuring cyber competition? How do we verify the accuracy of attribution? Given attribution problems, how do we reliably establish norms and minimise commitment problems in compliance? Who are we establishing norms for, and who are we rallying against? On the other end of the debate is the 'megafauna' argument that criticised the field's over-emphasis on a small number of politically critical cyber events (usually with physical implications), overlooking the importance of the large volume of 'smaller events' that don't have a measurable or visible impact on infrastructure or systems.⁸ Both ends of the debate present us with a different hurdle facing cyber research: do we have too much, or too little measurable data to work with? All of these data availability and quality issues of cyber haven't prevented theorising about it in IR, but made empirical tests of those claims highly difficult.

Ultimately, IR's cybersecurity scholarship ran into two difficulties: first, an inability to grow beyond the confines of traditional IR and second, dangerously treading on 'purely theoretical' territory. Even when thinking solely in terms of the disruptive effects of cyber, the nuclear analogy ran into a number of problems. After all, nuclear weapons had a binary nature—they are either detonated or not detonated. Their deterrent nature came from the possibility of detonation. Cybersecurity, on the other hand, is any-

thing but binary. DDoS, MitM, spear phishing, SQL injection, and XSS are different attack types that serve a different purpose. Often, the target learns about the fact that it was attacked weeks after the actual incident. More sophisticated forms of cyberattacks are also hard to notice, measure, and turn into event data, and are even harder to attribute to an actor. Its twists and turns, intensity, and type all require a much more nuanced understanding of the engineering aspects of the field compared to nuclear weapons. It also rendered a truly multi-method approach, through combining the forces of computer engineers, data scientists, and IR specialists, but this kind of sustained interdisciplinarity is still rare in the scholarship. Furthermore, persistent problems in generating a statistically meaningful, let alone representative, dataset make cybersecurity theories difficult to test empirically.

As cybersecurity scholarship dealt with these structural problems, Internet and social media studies began solving some of those persistent problems in harvesting trace data to help build new theories on technology and IR. The power of social media, both as a form of real-time communication and also as a networking hub, has been demonstrated most visibly during the Arab Spring demonstrations in the MENA region and in the Occupy movements across Europe and North America, as well.⁹ Then with the onset and intensification of the Syrian, Iraqi, and Ukrainian civil wars, the power of digital interconnectedness as an enabler of mobilisation, resource generation, propaganda, and issue framing has been further bolstered.¹⁰ The highly interactive and public nature of social media platforms not only increased the speed of communication between actors, but also rendered this communication visible to the broader social media community all around the world. Social media has become a new marketplace of ideas, equally disliked and needed, by politicians, diplomats, international institutions, civil society groups, and violent groups alike.

Compared to cybersecurity, where data is both uncontrollably large, elusive, and fast, Internet research has rendered the study of human interactions in digital space more manageable. Although data size and speed can still be an issue, social media data is less elusive compared to cybersecurity data, and depending on the platform and topic, scraping entire sets of public data can be far easier compared to cataloguing cyber event data. The secrecy and covertness of cybersecurity research can be a deterrent factor for social scientists, which might explain why more of them are switching to the open source nature of social media research. Furthermore, although cyber research is significantly important for IR theory, it lies distant to the wider empirical debates on sample size, representativeness, measurement, causal effects, and behavioural variances.¹¹ Ultimately, until cybersecurity researchers solve the riddles of data extraction, dataset sharing, and measurement, cybersecurity research risks the danger of remaining an elite-focused, small-N field, compared to the large-scale 'social' scope of social media research. This has led to a rapidly developing field of computational social science: the use of coding and programming tools to study social dynamics, behaviour, and choice.¹² Despite enriching other sub-fields in IR, however, Internet and so-

cial media studies have primarily benefited the conflict and political violence discipline. To that end, when exploring how Internet Communication Tools (ICTs) affect IR, the bulk of the scholarship again comes from the conflict studies camp.

The remainder of this paper will discuss how the 'digital conflict studies' field has incorporated the 'technological turn' in IR into its main theoretical thrust, by building upon and expanding the framework used by Lars-Erik Cederman and Manuel Vogt¹³ on the main phases of conflicts: onset/initiation, resource mobilisation, target prioritisation, duration/intensity, and conflict termination, peacebuilding, and re-integration. Although a similar phasing or periodisation is hard to model exactly on cybersecurity scholarship, this review aims to provide a more structured framework for the empirical study of cybersecurity. Furthermore, this periodisation may help future cybersecurity scholars to structure their data observation, extraction, and sharing mechanisms to test existing IR-related cybersecurity theories and build new ones.

Internet, Social Media, and Conflict: Primary Analytical Foci

As outlined in the critical review articles by Anita Gohdes¹⁴ and Thomas Zeitzoff,¹⁵ there is quite a rapid development of robust, empirically sophisticated studies on how digital interconnectivity impacts contentious politics and human conflict. The earlier studies inspired by the Arab Spring and the Occupy movement focused on the effect of digital media on protests, focusing mainly on onset and state responses against digital mobilisation.¹⁶ As protests evolved into deadlier conflicts, the field has also evolved into explaining how ICTs affected violence in civil wars like in Syria, Iraq, and Ukraine.¹⁷ Important studies, some of which will be explored in this paper, have primarily focused on conflict initiation, recruitment, propaganda, terrorist attacks, narrative-building, branding/marketing of armed groups, and state responses.

However, there are several fundamental conflict dynamics that are still understudied, such as conflict duration, bargaining/negotiation and conflict termination, group disbanding, and political transition of violent conflicts. Furthermore, although there are ample studies on how social media radicalises individuals,¹⁸ there is an insufficient body of empirical investigation on how digital interconnectedness de-radicalises or moderates users. This section is divided into five sub-sections that deal with some of the main works in their respective sub-fields, and the current analytical limitations of those respective sub-fields. These are namely: conflict onset; resource mobilisation; target selection; intensity/duration; and conflict termination, peacebuilding, and reintegration.

Onset: Grievance/Greed Framing

Social media has expedited the dissemination of frames related to sustained political grievances and opportunities.¹⁹ Its scope

and speed led to the emergence of non-geographical communities of grievance, all receiving information about repression, disenfranchisement, and oppression respective to their areas of concern.²⁰ Similarly—this strategy best employed by ISIS—opportunity structures in conflict, such as wealth, prestige, and social acceptance are now transmitted across the world, leading to the mobilisation at an unprecedented level of diversity in recruits.²¹ Much of the digital recruitment tactics popularized by ISIS were later used en masse across the world, including Western far-right groups. Of course, social media is not the only medium through which such frames have been disseminated in the past. Newspapers, novels, and motion pictures have all helped communicate grievances and greed narratives in the past. What makes social media novel, however, is its speed and size. Compared to older forms of media (perhaps, with the slight exception of live broadcasting technologies), social media and the Internet offer real-time dissemination of narratives to a far larger audience. Some of the time-lag and media access (urban/rural, rich/poor) constraints that were the hallmarks of older examples of grievance/greed narratives' diffusion are less relevant in the case of social media. Owing to the lowered barriers of entry, digital communication thus increases the speed and size of both the responses to framing stimuli and also the materialisation of counter-narratives.

In addition to speed and scale, ICTs also offer a permanent, non-physical, and omni-accessible archival function for users.²² This is especially valid for grievance diffusion,²³ which is a crucial driver of early mobilisation. By both spreading and permanently recording events and narratives in digital space, users bestow an archival power to digital media. This, in turn, allows grievances to be not only communicated more quickly, but also consumed in a sustained and at-will manner. In addition to enabling masses to mobilise quickly, this sustained grievance effect of ICTs also intensifies existing social, ethnic, and religious tensions, through daily access and consumption of grievance-related content.²⁴ This does not only impact the likelihood and frequency of conflicts but also determines the size and social support for these conflicts. In a way, the real-time archival utility of social media both drives violence onset likelihood, as well as how intense these acts of violence become. This is true both for the digital content disseminated by a single source to multiple individual users (propaganda and information cascades), and also content sought and acquired by the users themselves (information-seeking).

ICTs and conflict onset are relatively well-studied as a dyad. Currently, some of the frontiers in this sub-field are the use of fake news, trolls, and bots—deliberate information manipulators—and identifying how they impact greed/grievance dynamics differently than the flow of accurate information.²⁵ Does disinformation, for example, enable the spread of emotional and mobilising content better than deliberate and accurate information?²⁶ Do non-state actors use disinformation as part of their extensive strategic logic, or do they find disinformation as a potentially trust-mitigating factor?

Much of these research questions were tested overwhelmingly with ISIS, rendering the group as a litmus test of some of the most prominent political communication theories in digital space.²⁷ Yet, the scholarship that lies at the intersection of political communication and computer science fields does try to address a broader range of cases beyond ISIS. Purohit (et al.)²⁸ and Karuna (et al.)²⁹ use text-mining tools to look at how digital frames on gender-based violence are disseminated online, using a corpus-based latent Dirichlet analysis (LDA). Both studies find a greater collaboration between grievance campaigns in geographically distant communities and discover a significant degree of 'digital cross-pollination' between physically disconnected online campaigns. De Choudhury (et al.)³⁰ on the other hand, explore how images and videos on social media contribute to the intensification or de-sensitisation of emotions in Mexico, related to cartel-based violence. They focus on sub-district level digital content across two years and find that both the state and cartels strategically deploy images to deter and assert psychological dominance against each other, as well as the local populace, in a methodical way. Similarly, Monroy-Hernandez (et al.)³¹ dissect to what extent 'civic bloggers' (locals who document cartel violence on weblogs and social media) have any effect on conflict awareness and mobilisation. They discover that districts that contain more public media bloggers, and are thus exposed to greater volumes and frequency of conflict reporting, have a greater tendency to be desensitised and are less likely to participate in violence.

Wang (et al.)³² on the other hand, explore the digital impact of the Sandy Hook shooting on users' sentiments on gun control, discovering that anti-violence (pro-gun control) sentiments linger on much longer compared to anti-gun control content in the aftermath of the shooting. They also demonstrate that these pro-gun control sentiments linger on longer in Connecticut (the incident state), compared to other states in the United States, invalidating the main premise of the 'terror management theory.' In the same vein, Ayers (et al.)³³ conduct large-scale scraping of websites, forums, social media sites, and online advertisements in the US, revealing that online awareness-building campaigns and tailored ads on digital platforms could measurably mitigate gun-related deaths. While most of the 'images and frames' literature rely on text-based methods, Won (et al.)³⁴ focused on images shared on social media websites to draw a causal link between emotions that those images trigger and the actual intensity of the relevant protest event. Drawing on more than 40,000 geotagged protest images, the researchers find that greater protest duration and intensity are correlated with the emotional triggering capacity of the images shared from the protest area. Finally, Muller and Schwartz demonstrate a causal relationship between anti-refugee sentiment in German-speaking Facebook and physical anti-refugee violence in Germany at the municipality level,³⁵ while Patton (et al.)³⁶ draw direct links between 'Internet bragging' and the tendency to exhibit gang violence-related behaviour in Chicago. Building a predictive model, Patton (et. al.) demonstrate a high level of reliability in

enabling social workers to recognise gang violence-related themes and engage in better targeted preventive action.

These studies push the field strongly into the domain of automated-recognition and prediction foci. Most of these studies are also heavily concentrated on the US or the UK, requiring a significant broadening of the cases beyond the Global North. Some of the untapped research questions include how regional inequality, linguistic or ethnic fractionalisation, and regime type influence the ICT-onset literature.

Resource Mobilisation

Not all successful cases of greed/grievance communication lead to violence. Without pre-existing social forces and trust relations, purely digital networks have a low level of success of mobilising or remaining mobilised for an extended period.³⁷ One of the main drivers of the staying power of movements is how well they mobilise resources.³⁸ This mobilisation is not just limited to manpower or financial resources, but also includes sustenance of frames, attention, alliances, commitment, and organisational cohesion. To that end, the advent of Internet and social media are primarily thought as positive drivers of resource mobilisation. After all, this was one of the main reasons why the early works on the Arab Spring and the Occupy movement were quick to call them ‘social media revolutions.’³⁹ When dissidents discovered their latent power through digital interconnectivity, they were able to come together and challenge hegemony, or so the logic went. However, later studies have proved that this was not always the case.⁴⁰ Social media was a significant development but was also exaggerated in its effect on social movements. ICTs did drive attention and awareness, but these two variables had a mixed effect on actual mobilisation, commitment, and staying power. Rather, ICTs’ effects relied on pre-existing traditional networks and trust relations.

This necessitates a greater empirical focus on the analytical sweet spot that delves into how traditional social networks use and deploy ICTs to generate sustained framing and identity-building resources. Mostly, studies omit this context and try to draw a straightforward causal link between how much movements use social media and how well they mobilise as a result. Furthermore, past the onset and mobilisation mark, few studies explore how movements sustain both ideological and material resources, especially when the rival actor is also a non-state actor.⁴¹ To that end, most scholarship focuses on how protestors, rioters, militias, and terrorist groups utilise ICTs against state actors, but not as much on how this interaction materialises between and within non-state actors themselves. Some of the most novel ways of studying mobilisation dynamics can be seen in Gahot (et al.)⁴² where the authors use epidemiological modelling to visualise the diffusion and sustaining of the 2005 French riots. This is one of the better experiments in bringing greater interdisciplinarity into social research, as the authors pay specific attention to social dynamics (neighbourhood relations, district social networks, and protestor

community proximity) in their contagion model. In a similar vein, Davies (et al.)⁴³ explore how the 2011 London riots have been mobilised against police crackdown, using digital communication tools to build a contagion dataset of both onset and sustained resource-generation dynamics. Ultimately, the authors discover that there is a Pareto-optimal level of police presence per each riot district that deters rioter resource mobilisation; any less or more police deployment causes greater protest mobilisation and resources deployed in the riot.

The ICT-religion nexus is a potentially helpful disciplinary link to conflict studies, especially in terms of exploring how loose belief networks retain membership, income, and resource-generation practices in digital space. Heidi Campbell demonstrates how Christian congregations that are geographically distant can retain 'online congregations' through live-feed sermons and chat groups.⁴⁴ These online congregations not only build awareness and disseminate frames, but also play a significant role in the material domain, in terms of fundraising and mustering numbers for protests and social responsibility projects.⁴⁵ In the same vein, Ellison and Boyd illustrate how this 'online congregation' dynamic can be observed in Islam and Judaism as well, as individuals discover and often at times identify with their digital congregations more than their physical ones.⁴⁶ Mellor and Rinnawi focus specifically on the Islamic use of ICTs and exemplify how digital congregations are more important drivers of resource mobilisation in diaspora Islamic communities in Europe and the United States, whereas in predominantly Muslim countries too, the effect of social media leads to the emergence of diverging loyalties.⁴⁷ Such diverging loyalties create an '*à la carte* Islam' where the pious can choose from different sermons and *fatwas* issued by the online or offline imams, demonstrating hybrid loyalties based on which congregation or imam supplies the version of theological interpretation they require. In the case of Judaism, Nathan Abrams demonstrates how social media leads to 'post-denominational Judaism,' where identity construction and mobilisation dynamics display the similar congregational hybridity that we see in Islam.⁴⁸

Target Prioritisation

Once movements attain critical mass and are directed in unison towards a common goal, the next step becomes target selection. In the case of non-violent movements, this target becomes a key building, central square, or a historic site to occupy or conduct a sit-in at, whereas in violent movements these range from military installations/checkpoints, critical infrastructure, or (with terrorist groups) civilian areas. What is the role of social media on how groups pick their targets and guide their followers to that target? Some of the earlier works on this question had a slight reporting bias around areas of high Internet connectivity,⁴⁹ although newer forms of scholarship have begun developing unique ways to disentangle violence occurrence from violence reporting.⁵⁰ Some of the most prominent studies on violence targeting empha-

size four trends: strategic area/zone focus, critical infrastructure focus, political focus, and intimidation focus. There is currently no major work on how ICTs affect any particular focus. Rather, most target-related studies explore how social media sustains and intensifies ongoing conflict dynamics, evidenced best in Thomas Zeitzoff's work on the 2012 Gaza Conflict.⁵¹ Also, Jibon Naher and Matiur Rahman Minar look at how social media posts drive chat groups or page followers to particular types of violence, including the target(s) of such acts in Bangladesh.⁵² They demonstrate how ICTs not only impact the speed and size of violent mobilisation, but also drive users towards key ethnic or religious targets.

Targeting presents a very specific causal problem in the ICT-conflict nexus. The majority of existing studies can explain how ICT use can guide mobilisation, intensity, polarisation, and radicalisation, but there is not much robust evidence on whether the popularity of particular target types on ICTs really affect targeting behaviour on the ground. This is a challenging puzzle to solve, because it is hard to disaggregate targeting choice as a result of its social media popularity, from its choice as the order of a commanding superior.⁵³ Further problems arise in determining whether ICTs influence commanders or troops on the ground in hand picking a particular set of targets. Especially with regard to communal violence, the role of ICTs in instigating certain ethnic or religious groups using targeted messaging and imagery is under-explored. Similar to military targeting, there is much to be done on exploring whether the decision to attack a particular target or community follows a strict hierarchy (i.e., communal elders or propagandists) or to generate a mob mentality (autonomous crowd behaviour). Some tangential journalism work on this is done through WhatsApp-related gang violence in India.⁵⁴ Some of the most relevant findings on this line of inquiry are that digital targeting practices through text or images contribute substantially to the unearthing of dormant social tensions, leading to attacks on women specifically. This gender dimension in violent group targeting prioritisation is an important avenue for further research and connects somewhat to another strand of literature on digital shaming and harassment.⁵⁵ Furthermore, due to the real-time effects of ICTs, the time gap between designating a target in digital space and the actual mobilisation of the masses around the designated target is much less.

My co-author and I have discovered this targeting effect of ICTs when exploring the mobilisation dynamics during the failed coup in Turkey in July 2016.⁵⁶ Sharing videos, images, and text in large numbers, anti-coup protestors were extremely quick in mobilising and overwhelming checkpoints, military installations, and other hotspots of conflict. In most cases, it is possible to draw direct linkages between the emergence of a particular hotspot or target on social media, and the masses of crowds gathered around it within an hour or less. We also, however, warn against the existing social network dimension of these targeting preferences. It is not only ICTs that guided people to specific locations—rather it is the dissemination of these targets by family members, friends, or re-

ligious congregation channels (all trusted pre-existing networks) through ICTs that created the trust network required to march towards designated spots. Future ICT-targeting studies have to take this digital-physical interaction into account.

Intensity and Duration

Scholarly research on conflict intensity and duration has grown increasingly popular in the last decade, owing to new datasets and measurement types that allow greater analytical focus. The primary thrust of the conflict intensity/duration literature has been to inform policy on the ways of shortening conflicts.⁵⁷ By reducing conflict duration, as the conflict literature asserts, conflict intensity would also be reduced.⁵⁸ However, premature freezing of conflicts due to external pressure(s) also frequently leads to a re-escalation of those conflicts once international attention wanes.⁵⁹ Therefore, the causal relationship between duration and intensity is still being negotiated in the literature, as this link works differently in various political contexts. Although conflict intensity (measured as casualties) and duration (measured as months) have been explained most popularly through combatant motivation, financing, public commitment, capacity, and external support,⁶⁰ the role of ICTs has been a relatively nascent inquiry. The common consensus in the conflict literature is that ICTs make conflicts more intense.⁶¹ This finding is being increasingly challenged by a new scholarship that focuses on the availability bias and measurement level problems of these findings. Nils Weidmann, for example, asserts convincingly that access to ICTs creates a reporting bias.⁶² This reporting bias is related both to the communication of violent cases that would remain uncommunicated without ICTs, and to the oversharing of violent events over non-violent events that occurs among those with access to ICTs in conflict zones. This highlights the need for interdisciplinarity to solve some of the availability bias and data-gathering problems related to proximity to ICT infrastructure.

Guo (et al.),⁶³ for example, demonstrate how betweenness centrality can offer a better explanation on why certain geographies become more conflict-prone than others. They emphasise cities as hubs of communication, and thus bestow greater importance on the cities for their narrative and frame-dissemination capacity that in turn influence conflict intensity and duration patterns. In their view, conflict intensity and duration are both proportional to their distance to major cities, and also the betweenness centrality measure of major cities themselves. Walther (et al.),⁶⁴ on the other hand, focus on the Sahel-Sahara to aggregate digital and pre-digital communication and archival data, generating a militant attack database. Using this database, they are able to infer which national communication and counter-insurgency policies worked better in terms of mitigating the intensity and duration of Al-Qaeda in Mali (AQIM)'s violence in the Sahel region. However, with the exception of these few examples, the ICT-duration or intensity literature is still very young. A potential analyti-

cal field to approach the intensity/duration problem would be to engage more with the digital political communication literature.

Echo chambers and polarisation are proper proxy measures to solve this deadlock. Barberá (et. al.)⁶⁵ demonstrate how political preferences are disseminated across accounts that are similar in political ideology, but that such similarity disappears in non-political issues. This could be an inspirational point of departure for conflict studies as the dissemination of conflict-related information along ideological or identity lines would potentially have a significant influence on conflict intensity. Del Vicario (et al.),⁶⁶ on the other hand, demonstrate how the dissemination patterns of disinformation is especially contingent upon network ideology. Focusing on how conspiracy theories flow on Facebook, the authors demonstrate that polarisation becomes more observable in the dissemination of false narratives rather than accurate information. Bastos (et al.)⁶⁷ test the same hypothesis in the Brexit campaign and discover that both accurate and inaccurate types of content were shared across a more dense and central network in the Leave camp, and followed a looser and less dense network in the Remain camp. This finding is important as it hints at the role of political ideology in the dissemination of accurate and false-type conflict-related content. In a more recent study, Cota (et al.)⁶⁸ looked at a large dataset of Twitter messages from Brazil related to the impeachment of President Dilma Rousseff and discovered that more extreme content was disseminated across a broader audience, compared to less extreme and more moderate content that had a lower level of spread. This study sheds some light on potential conflict communications literature on the degree to which extreme versus moderate content becomes popular during emergencies, escalations, and critical political moments.

Termination, Peacebuilding, Re-integration

How do ICTs impact the decision to end a conflict? The literature is skewed so much on the initiative and sustaining dynamics of ICTs on conflict that the analytical 'wave' hasn't yet reached the final stages of the violence cycle. This is due partly to the fact that recent years have witnessed much more conflict initiation and escalation compared to conflict termination.⁶⁹ Most conflict termination scholarship focuses on tangible factors, such as the decline of manpower, funds, or other resources to explain de-escalation and termination dynamics.⁷⁰ Other studies explain how external interventions, infighting, leadership change, and social shifts might lead to similar outcomes.⁷¹ However, there have been no empirical studies yet on how ICTs impact the de-escalation and termination aspects of conflicts.

Earlier hypotheses on how ICTs might influence conflict offered promising notes. Most of them thought greater interconnectedness and on-hand information availability have a normalising effect on violent interactions. Importing from more traditional theories on media and conflict, the early ICT literature suggested that warring factions or mobilised masses could be 'convinced' to

stand down and attain greater mutual understanding with rival groups (or governments) by digital messaging (i.e., ICTs), resulting in conflict termination.⁷² Most of the peacebuilding initiatives in the 1990s thus emphasised 'greater communication' and frequent socialisation between the opposing sides, and by the 2000s most of these initiatives welcomed the idea of digital communication as a peace enabler.⁷³ However, the evidence yielded a more complex and nuanced picture. One main misjudgement about the ICT-peace link was the fact that ICTs grew into multi-directional media systems, as opposed to the uni-directional nature of television, motion pictures, or the radio. This meant that 'feeding content' to warring factions, in the same manner that propaganda dissemination worked in the past, was impossible.⁷⁴ Content consumers are now also content producers and curators, causing far too many narratives to spread online for any single actor to dominate the mainstream media.⁷⁵ The prevalence of multiple and competing narratives, along with the ever-present shadow of disinformation, also have the potential to intensify existing divisions, rather than heal them.⁷⁶ To counter these effects, along with attempts to skew these discussions by combing out 'unwanted content,' governments have also become increasingly reliant on censorship, Internet restrictions, and the strategic deployment of bots and trolls to further contaminate the information ecosystem.⁷⁷ However, these tools are still not in dominant use in most conflict-prone countries as instability prevents the establishment of functioning Internet infrastructure. This severs the link between ICTs and affected communities in rural areas or poor urban districts, rendering any uni-directional move towards mediation inefficient.

From existing empirical evidence, it is hard to hypothesise whether ICTs will have any standalone effect on conflict termination and peacebuilding, without interacting with material factors on the ground. Some of these material factors are already well-covered by the non-ICT conflict termination literature: external intervention, combatant resolve, leadership change, resource depletion, social change, and so on. ICTs may indeed bolster peacekeeping efforts, provided that the material resources of peacekeeping are sufficiently in place.

The final link in the conflict chain is attaining sustained non-violence and community-building in the affected territories. Currently, there is no significant work in the field of how ICTs impact peacekeeping and community-building, leaving a sizeable analytical gap in the literature. This originates from the overwhelming focus on the earlier onset/mobilisation aspects of violence, leaving a plethora of untapped topics on the later phases of violence. Yet, the literature will inevitably gravitate towards the more positive and constructive aspects of ICTs on conflict. Community-building and re-integration phases of the conflict cycle have a higher likelihood of being impacted by purely ICT-led efforts. When willingness to fight is diminished and the societal-political consensus is in place, then ICT tools can work through a multitude of ways to help bolster peace agreements and their enforcement. The most direct and visible use of ICTs in this phase has been the monitor-

ing of ceasefires and other commitment violations, enabling all parties to keep an eye on the other in a more direct way.⁷⁸ When the speed and scale advantages of ICTs are deployed after peace is attained, then these assets can significantly bolster confidence-building measures and render community-building and re-integration efforts more robust. In other words, ICTs will work when there are 'physical' attempts towards reconciliation, and will remain ineffective without any social consensus or driver towards mediation.

Conclusion

This article has sought to trace some of the current analytical fronts of digital conflict studies to offer a framework for IR's cybersecurity scholarship on how it can escape some of the short-term methodological and conceptual deadlocks. Specifically, the cybersecurity field suffers from an absence of granular and representative (or even indicative) data generation, and a sharing mechanism for the purposes of the scholarly community. This prevents an empirical testing of the majority of the claims made in cybersecurity theory, as well as impairs how much we can import from the oft-mentioned 'nuclear analogy' in IR for the purposes of cybersecurity scholarship. One of the main reasons why the digital conflict studies discipline could surmount most of the hurdles posed by the emerging technologies is that the field has been building granular and representative event datasets since the 1960s. From the founding blocks of the Correlates of War Project in the 1960s, UCDP/PRIO and START-UMD datasets emerged, leading the way for the emergence of many other dataset projects, including the ICEWS, ACLED, ViEWS, and GDELT projects. Multiple long-term open source scientific research datasets have helped to advantage the conflict literature as it adapts to the requirements of the technological turn in IR. The absence of a long-term scientific event dataset has steered cybersecurity researchers of IR to work with an ambiguous sample of cybersecurity events that will remain structurally insufficient for robust theory-building and theory-testing.

A second major difference is that digital conflict studies has developed far more interdisciplinary and collaborative ties than cybersecurity scholarship has. By focusing on human trace data to infer human conflict dynamics, digital conflict literature has largely retained the social and human prerogatives of the field. In contrast, cybersecurity scholarship is still largely distant to the core questions of political and social fundamentals of digitalised human interactions, so far refraining from directly dealing with the role of psychological, sociological, and ethnographic aspects of cybersecurity. One recent exception is Nadiya Kostyuk and Yuri Zhukov's exploration of how cyber-attacks influenced conflict dynamics on the front lines in Ukraine.⁷⁹ This article provides one of many potential trajectories for cybersecurity scholarship in addressing the data availability and validity issues.

ICTs bring a set of welcome challenges and opportunities for conflict research. However, the most immediate task for IR in general is to escape yet another conflict studies entrapment when

successfully adapting to the question of how emerging technologies impact world events. ICTs bring a wide array of analytical opportunities to test IR's existing mainstream theories, as well as develop new ones, as digital communication enables the harvesting of both more abundant and more granular data types. These data types will not only improve our understanding of how states interact with their societies and other states in the digital domain, but will also lead the way to the formulation of more advanced types of international institutions and cooperation architectures. Regardless, conflict studies will likely continue to spearhead IR's broader disciplinary focus on the ICTs.

While there is quite an abundance of attention on the earlier phases of social movements and violent events, there is currently a gap in the more advanced phases of such phenomena. The field is still burgeoning in explaining how ICT use affects target selection, intensity/duration, and peacebuilding efforts, but holds a relatively more robust set of findings on the onset and mobilisation phases. To remedy this gap, digital political communication literature seems to be the most apparent linkage for the conflict studies community. Some of the most prominent works in PolCom already have theoretical answers to how violence affects attention, emotion, and mediation in critical political events and debates.

Yet, the bulk of that literature focuses on American or European contexts, where both Internet penetration and social media use are significant enough to yield robust results.⁸⁰ The challenge of the conflict studies literature is two-pronged: first, tackle data availability and parity issues in comparative works on countries with uneven access to ICTs, and second, disentangle conflict reporting frequency from conflict occurrence frequency. Both problems may eventually solve themselves as global interconnectivity widens and ICT data becomes more representative and comparable. However, studies can still benefit significantly from exploring how yearly, generational, or geographical changes in ICT use impact all five phases of conflicts discussed above. Rather than waiting for ICT data to become eventually representative, scholars may find a plethora of topics to dig into across cases in areas with different levels of digital access. Greater interdisciplinarity across the fields of computer science, physics, biology, and complexity fields will enable conflict researchers to generate more sophisticated models and more robust findings on this emerging frontier.

Another largely untapped topic is the role of technology companies in driving/mitigating conflict. Platform architecture, as well as the increased relevance of big tech companies during crises and emergencies, render them *de facto* actors in all conflicts.⁸¹ Direct effects of platform influence on conflicts, such as the decision to censor and emphasise certain types of content, or decisions to partner with governments or certain civil society actors will have an increasing influence on all phases of conflicts. However, indirect effects, such as algorithmic bias,⁸² attention economy,⁸³ and rent-generation structures of social networks⁸⁴ will also impact conflicts and conflict actors significantly. Given the fact that platforms run on advertisement revenue and those advertisements

target engagement metrics, it will be inevitable for platforms to push more extreme content that elicits an emotional response, thus generating more revenue.

The success of the emerging field of digital conflict studies can offer three main lessons for the developing cybersecurity field. First, 'cyber IR' has to prioritise building event datasets that strike a balance between data size and quality. Given the fact that conflict studies has several important datasets and data processing projects unique to the field (UCDP/PRIO,⁸⁵ ICEWS,⁸⁶ ACLED,⁸⁷ UMD-START,⁸⁸ or ViEWS⁸⁹), the field is better-suited to incorporate digital media and communication-related data types. Although the Center for Strategic and International Studies⁹⁰ and the Council on Foreign Relations⁹¹ have their IR-specific 'major events' data, the cases are a very unhelpfully small fraction of cybersecurity events that happen on a daily basis. Furthermore, both datasets bring in the question of 'major event according to whom?', given the heavy bias in favour of attacks against American infrastructure. Even data from Norse Corporation, FireEye, Kaspersky, Fortinet, or similar cybersecurity companies, are by no means representative or transparent in terms of the methodology behind data generation. Furthermore, their full datasets aren't available for public use, which brings its own set of replication problems. Second, cyber IR scholarship has to reach beyond the confines of traditional IR theories and begin engaging more with the techno-sociology and techno-politics literature. How do states and societies perceive and prioritise the dangers of threats originating from the cybersecurity/defence domain? What is the impact of organisational, political, and social differences between and within countries in politicising and securitising cyber threats? How do we incorporate disinformation, information overload, and digital distraction into IR's threat spectrum? How do the 'modes of production' of digital hardware, software, and data impact balance of power between countries and alter state-society relations on a global scale? Should the field deal primarily with the threats faced by states (infrastructure damage, national secrecy, and confidential data hacking), or society (surveillance, data capitalism, private data protection)? Finally, cybersecurity scholarship will have to broaden its focus of interest beyond what the major powers are doing and study the impact of major power rivalry on the rest of the world, with specific emphasis on inter-state and sub-state inequalities. Given the fact that access to advanced cybersecurity technology is a distinct privilege of only the wealthiest of nations, it is expected to create another form of hegemonic balancing and counter-balancing behaviour. How do we study regional and systemic inequalities in access to cybersecurity hardware and software infrastructure and how do these inequalities shape state behaviour and state-society relationships across different regimes and security cultures?

Ultimately, ICTs will occupy a more important place in the media-conflict nexus compared to the historical effects of the telegram, radio, television, or motion picture. This is because access to ICTs are more intimate (i.e., through smartphones that are always nearby), real-time, multi-directional, and at-will compared to all

previous forms of mass communication. This will also render ICTs a key analytical topic in all aspects of human relations, including conflict. More focus on the communicative aspects of mobilisation, movements, and violence will ultimately unlock new ideas and theories of human behaviour. To do this, however, this article argues in favour of the analytical value of greater interdisciplinarity and more risk-taking across fields.

Notes

- 1 David A. Lake, "Theory Is Dead, Long Live Theory: The End of the Great Debates and the Rise of Eclecticism in International Relations," *European Journal of International Relations* 19, no. 3 (2013): 567–87, <https://doi.org/10.1177/1354066113494330>; Rosa Vasilaki, "Provincialising IR? Deadlocks and Prospects in Post-Western IR Theory," *Millennium: Journal of International Studies* 41, no. 1 (2012): 3–22, <https://doi.org/10.1177/0305829812451720>; Stefano Guzzini, "The Ends of International Relations Theory: Stages of Reflexivity and Modes of Theorizing," *European Journal of International Relations* 19, no. 3 (2013): 521–41, <https://doi.org/10.1177/1354066113494327>; Barry Buzan and Richard Little, "Why International Relations Has Failed as an Intellectual Project and What to Do About It," *Millennium: Journal of International Relations* 30, no. 1 (2001): 19–39, <https://doi.org/10.1177/03058298010300010401>.
- 2 Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2012), <https://papers.ssrn.com/abstract=2178586>; Chintan Vaishnav, Nazli Choucri, and David Clark, "Cyber International Relations as an Integrated System," *Environment Systems and Decisions* 33, no. 4 (2013): 561–76, <https://doi.org/10.1007/s10669-013-9480-3>; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 7–40, https://doi.org/10.1162/ISEC_a_00138.
- 3 Jonathan Havercroft and Raymond Duvall, "Challenges of an Agonistic Constructivism for International Relations," *Polity* 49, no. 1 (2016): 156–64, <https://doi.org/10.1086/689978>; Jarrod Hayes, "Reclaiming Constructivism: Identity and the Practice of the Study of International Relations," *PS: Political Science & Politics* 50, no. 1 (2017): 89–92, <https://doi.org/10.1017/S1049096516002213>; David M. McCourt, "Practice Theory and Relationalism as the New Constructivism," *International Studies Quarterly* 60, no. 3 (2016): 475–85, <https://doi.org/10.1093/isq/sqw036>; Thomas J. Biersteker, "Critical Reflections on Post-Positivism in International Relations," *International Studies Quarterly* 33, no. 3 (1989): 263–67, <https://doi.org/10.2307/2600459>; Thomas Diez and Jill Steans, "A Useful Dialogue? Habermas and International Relations," *Review of International Studies* 31, no. 1 (2005): 127–40, <https://doi.org/10.1017/S0260210505006339>.
- 4 Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012): 229–44, <https://doi.org/10.1093/jcsl/krs019>; Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, no. 1–2 (2015): 4–37, <https://doi.org/10.1080/01402390.2014.977382>.
- 5 Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38.
- 6 Scott W. Beidleman, "Defining and Deterring Cyber War," *Defence Technical Information Center* (Carlisle, PA: US Army War College), January 6, 2009, <https://>

apps.dtic.mil/docs/citations/ADA500795.

7 Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72–109, https://doi.org/10.1162/ISEC_a_00267.

8 Alexander D. Kent, "Cyber Security Data Sources for Dynamic Network Research," *Security Science and Technology* 1 (May 2016): 37–65; Radu F. Babiceanu and Remzi Seker, "Big Data and Virtualization for Manufacturing Cyber-physical Systems: A Survey of the Current Status and Future Outlook," *Computers in Industry* 81 (2016), 128–137.

9 Nahed Eltantawy and Julie B. Wiest, "The Arab Spring: Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory," *International Journal of Communication* 5 (2011): 18; Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad, "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?" SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2011) <https://ssrn.com/abstract=2595096>; Gadi Wolfsfeld, Elad Segev, and Tamir Sheaffer, "Social Media and the Arab Spring: Politics Comes First," *The International Journal of Press/Politics* 18, no. 2 (2013), 115–137.

10 Philip N. Howard and Muzammil M. Hussain, "The Role of Digital Media," *Journal of Democracy* 22, no. 3 (2011): 35–48; Daniel Byman and Jennifer Williams, "Jihadism's Global Civil War," *The National Interest* 136 (2015), 10–18; for a broader range of cases, see Joshua Tucker, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation, 2018.

11 Jean Camp, Lorrie Cranor, Nick Feamster, Joan Feigenbaum, Stephanie Forrest, Dave Kotz, Wenke Lee, Patrick Lincoln, Vern Paxson, Mike Reiter, Ron Rivest, William Sanders, Stefan Savage, Sean Smith, Eugene Spafford, and Sal Stolfo, "Data for Cybersecurity Research: Process and 'Wish List,'" *National Science Foundation Workshop on Cyber Security Data for Experimentation*, 2010.

12 David Lazer et al., "Life in the Network: The Coming Age of Computational Social Science," *Science* 323, no. 5915 (2009): 721–23, <https://doi.org/10.1126/science.1167742>; R. Conte et al., "Manifesto of Computational Social Science," *The European Physical Journal Special Topics* 214, no. 1 (2012): 325–46, <https://doi.org/10.1140/epjst/e2012-01697-8>.

13 Lars-Erik Cederman and Manuel Vogt, "Dynamics and Logics of Civil War," *Journal of Conflict Resolution* 61, no. 9 (2017): 1992–2016.

14 Anita R. Gohdes, "Studying the Internet and Violent Conflict," *Conflict Management and Peace Science*, October 25, 2017, <https://doi.org/10.1177/0738894217733878>.

15 Thomas Zeitzoff, "How Social Media Is Changing Conflict," *Journal of Conflict Resolution* 61, no. 9 (2017): 1970–91, <https://doi.org/10.1177/0022002717721392>.

16 Mohammad-Munir Adi, *The Usage of Social Media in the Arab Spring* (LIT Verlag Münster, 2014); Maximilian Hänska Ahy, "Networked Communication and the Arab Spring: Linking Broadcast and Social Media," *New Media & Society* 18, no. 1 (January 1, 2016): 99–116, <https://doi.org/10.1177/1461444814538634>; Nahed Eltantawy and Julie B. Wiest, "The Arab Spring | Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory," *International Journal of Communication* 5 (2011): 18; Philip N. Howard et al., "Opening Closed Regimes;" Habibul Haque Khondker, "Role of the New Media in the Arab Spring," *Globalizations* 8, no. 5 (2011): 675–79, <https://doi.org/10.1080/14747731.2011.621287>; Axel Bruns, Tim Highfield, and Jean Burgess, "The Arab Spring and Social Media Audiences: English and Arabic Twitter Users and Their

Networks," *American Behavioral Scientist* 57, no. 7 (2013): 871–98, <https://doi.org/10.1177/0002764213479374>.

17 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," *Studies in Conflict & Terrorism* 38, no. 1 (2015): 1–22; Thomas Elkjer Nissen, "Terror.com: IS's social media warfare in Syria and Iraq," *Contemporary Conflicts* 2, no. 2 (2014): 2–8; Farwell, "The Media Strategy of ISIS;" Jad Melki and May Jabado, "Mediated Public Diplomacy of the Islamic State in Iraq and Syria: The Synergistic Use of Terrorism, Social Media and Branding," *Media and Communication* 4, no. 2 (2016): 92–103; Olga Onuch, "EuroMaidan Protests in Ukraine: Social Media Versus Social Networks," *Problems of Post-Communism* 62, no. 4 (2015), 217–235; Jacob N. Shapiro and Nils B. Weidmann, "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq," *International Organization* 69, no. 2 (2015): 247–274.

18 Robin L. Thompson, "Radicalization and the Use of Social Media," *Journal of Strategic Security* 4, no. 4 (Winter 2011): 167–90; Scott Gates and Sukanya Podder, "Social Media, Recruitment, Allegiance and the Islamic State," *Perspectives on Terrorism* 9, no. 4 (2015): 107–16; Lieven Pauwels and Nele Schils, "Differential Online Exposure to Extremist Content and Political Violence: Testing the Relative Strength of Social Learning and Competing Perspectives," *Terrorism and Political Violence* 28, no. 1 (2016): 1–29, <https://doi.org/10.1080/09546553.2013.876414>; Matthew Costello et al., "Who Views Online Extremism? Individual Attributes Leading to Exposure," *Computers in Human Behavior* 63 (2016): 311–20, <https://doi.org/10.1016/j.chb.2016.05.033>.

19 Paul Collier and Anke Hoeffler, "Greed and Grievance in Civil War," Policy Research Working Paper (Washington DC: The World Bank, May 2006); Paul Collier, Anke Hoeffler, and Dominic Rohner, "Beyond Greed and Grievance: Feasibility and Civil War," *Oxford Economic Papers* 61, no. 1 (2009): 1–27, <https://doi.org/10.1093/oep/gpn029>; Marc L. Hutchison, Salvatore Schiano, and Jenifer Whitten-Woodring, "When the Fourth Estate Becomes a Fifth Column: The Effect of Media Freedom and Social Intolerance on Civil Conflict," *The International Journal of Press/Politics* 21, no. 2 (2016): 165–87, <https://doi.org/10.1177/1940161216632362>.

20 Sebastián Valenzuela, Arturo Arriagada, and Andrés Scherman, "The Social Media Basis of Youth Protest Behavior: The Case of Chile," *Journal of Communication* 62, no. 2 (2012): 299–314, <https://doi.org/10.1111/j.1460-2466.2012.01635.x>; Sarah Anne Rennick, "Personal Grievance Sharing, Frame Alignment, and Hybrid Organisational Structures: The Role of Social Media in North Africa's 2011 Uprisings," *Journal of Contemporary African Studies* 31, no. 2 (2013): 156–74, <https://doi.org/10.1080/02589001.2013.781322>; Sebastián Valenzuela, "Unpacking the Use of Social Media for Protest Behavior: The Roles of Information, Opinion Expression, and Activism," *American Behavioral Scientist* 57, no. 7 (2013): 920–42, <https://doi.org/10.1177/0002764213479375>.

21 Farwell, "The Media Strategy of ISIS;" J.M. Berger, "The Metronome of Apocalyptic Time: Social Media as Carrier Wave for Millenarian Contagion," *Perspectives on Terrorism* 9, no. 4 (2015): 61–71; Anita Peresin and Alberto Cervone, "The Western Muhajirat of ISIS," *Studies in Conflict & Terrorism* 38, no. 7 (2015): 495–509, <https://doi.org/10.1080/1057610X.2015.1025611>.

22 Andrew T. Little, "Communication Technology and Protest," *The Journal of Politics* 78, no. 1 (2015): 152–66, <https://doi.org/10.1086/683187>; Zeynep Tufekci and Christopher Wilson, "Social Media and the Decision to Participate in Political Protest: Observations From Tahrir Square," *Journal of Communication* 62, no. 2 (2012), 363–79, <https://doi.org/10.1111/j.1460-2466.2012.01629.x>.

23 Qiongyou Pu and Stephen J. Scanlan, "Communicating Injustice?" *Information, Communication & Society* 15, no. 4 (May 1, 2012): 572–90, <https://doi.org/10.1080/10590414.2012.683187>.

- org/10.1080/1369118X.2012.665937; Rebecca Kay LeFebvre and Crystal Armstrong, "Grievance-Based Social Movement Mobilization in the #Ferguson Twitter Storm," *New Media & Society* 20, no. 1 (January 1, 2018): 8–28, <https://doi.org/10.1177/1461444816644697>.
- 24 Anita Breuer, Todd Landman, and Dorothea Farquhar, "Social Media and Protest Mobilization: Evidence from the Tunisian Revolution," *Democratization* 22, no. 4 (June 7, 2015): 764–92, <https://doi.org/10.1080/13510347.2014.885505> ; Gary Tang, "Mobilization by Images: TV Screen and Mediated Instant Grievances in the Umbrella Movement," *Chinese Journal of Communication* 8, no. 4 (October 2, 2015): 338–55, <https://doi.org/10.1080/17544750.2015.1086398>.
- 25 Meital Balmas, "When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism," *Communication Research* 41, no. 3 (2014): 430–54, <https://doi.org/10.1177/0093650212453600>; Samuel C. Woolley and Philip N. Howard, "Automation, Algorithms, and Politics | Political Communication, Computational Propaganda, and Autonomous Agents — Introduction," *International Journal of Communication* 10 (2016).
- 26 For a good overview of the emerging literature on US disinformation, see: Brendan Nyhan, "How Misinformation and Polarization Affect American Democracy," in Tucker et al., *Social Media, Political Polarization, and Political Disinformation*.
- 27 Farwell, "The Media Strategy of ISIS"; Elizabeth Pearson, "Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media," *Studies in Conflict & Terrorism* 41, no. 11 (2018): 850–74, <https://doi.org/10.1080/1057610X.2017.1352280>; Yair Galily et al., "The Boston Game and the ISIS Match: Terrorism, Media, and Sport," *American Behavioral Scientist* 60, no. 9 (2016): 1057–67, <https://doi.org/10.1177/0002764216632844>.
- 28 Hemant Purohit et al., "Gender-Based Violence in 140 Characters or Fewer: A #BigData Case Study of Twitter," *ArXiv:1503.02086 [Cs]*, March 6, 2015, <http://arxiv.org/abs/1503.02086>.
- 29 Prakruthi Karuna et al., "On the Dynamics of Local to Global Campaigns for Curbing Gender-Based Violence," *ArXiv:1608.01648 [Cs]*, August 4, 2016, <http://arxiv.org/abs/1608.01648>.
- 30 Munmun De Choudhury, Andrés Monroy-Hernández, and Gloria Mark, "‘Narco’ Emotions: Affect and Desensitization in Social Media during the Mexican Drug War," *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14*, 2014, 3563–72, <https://doi.org/10.1145/2556288.2557197>.
- 31 Andrés Monroy-Hernández et al., "The New War Correspondents: The Rise of Civic Media Curation in Urban Warfare," *ArXiv:1507.01291 [Cs]* July 5, 2015, <https://doi.org/10.1145/2441776.2441938>.
- 32 Nan Wang, Blesson Varghese, and Peter D. Donnelly, "A Machine Learning Analysis of Twitter Sentiment to the Sandy Hook Shootings," *ArXiv:1609.00536 [Cs]*, September 2, 2016, <http://arxiv.org/abs/1609.00536>.
- 33 John W. Ayers et al., "Can Big Media Data Revolutionize Gun Violence Prevention?" *ArXiv:1611.01148 [Cs]*, November 3, 2016, <http://arxiv.org/abs/1611.01148>.
- 34 Donghyeon Won, Zachary C. Steinert-Threlkeld, and Jungseock Joo, "Protest Activity Detection and Perceived Violence Estimation from Social Media Images," *ArXiv:1709.06204 [Cs]*, September 18, 2017, <http://arxiv.org/abs/1709.06204>.
- 35 Karsten Müller and Carlo Schwarz. "Fanning the flames of hate: Social media and hate crime," *SSRN Scholarly Paper* (Rochester, NY: Social Science Research Network, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082972.

- 36 Desmond U. Patton, Jeffrey Lane, Patrick Leonard, Jamie Macbeth, and Jocelyn R. Smith Lee, "Gang Violence on the Digital Street: Case Study of a South Side Chicago Gang Member's Twitter Communication," *New Media & Society* 19, no. 7 (2017): 1000-1018.
- 37 Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven: Yale University Press, 2017); José Van Dijck, Thomas Poell, and Martijn De Waal, *The Platform Society: Public Values in a Connective World* (New York: Oxford University Press, 2018); Bernard Enjolras, Kari Steen-Johnsen, and Dag Wollebæk, "Social Media and Mobilization to Offline Demonstrations: Transcending Participatory Divides?," *New Media & Society* 15, no. 6 (2013): 890-908; Anita Breuer, Todd Landman, and Dorothea Farquhar, "Social Media and Protest Mobilization: Evidence from the Tunisian Revolution," *Democratization* 22, no. 4 (2015): 764-792.
- 38 Kristen Lovejoy and Gregory D. Saxton, "Information, Community, and Action: How Nonprofit Organizations Use Social Media," *Journal of Computer-Mediated Communication* 17, no. 3 (2012): 337-53, <https://doi.org/10.1111/j.1083-6101.2012.01576.x>; Breuer, Landman, and Farquhar, "Social Media and Protest Mobilization"; Enjolras, Steen-Johnsen, and Wollebæk, "Social Media and Mobilization to Offline Demonstrations."
- 39 Khondker, "Role of the New Media in the Arab Spring," Bruns, Highfield, and Burgess, "The Arab Spring and Social Media Audiences," Christopher Wilson and Alexandra Dunn, "The Arab Spring: Digital Media in the Egyptian Revolution: Descriptive Analysis from the Tahrir Data Set," *International Journal of Communication* 5 (2011): 1248-1272.
- 40 Eltantawy and Wiest, "The Arab Spring: Social Media in the Egyptian Revolution," Michael Hoffman and Amaney Jamal, "Religion in the Arab Spring: Between Two Competing Narratives," *The Journal of Politics* 76, no. 3 (2014): 593-606, <https://doi.org/10.1017/S0022381614000152>.
- 41 Gohdes, "Studying the Internet and Violent Conflict."
- 42 Laurent Bonnasse-Gahot et al., "Epidemiological Modelling of the 2005 French Riots: A Spreading Wave and the Role of Contagion," *Scientific Reports* 8, no. 1 (2018): 107, <https://doi.org/10.1038/s41598-017-18093-4>.
- 43 Toby P. Davies et al., "A Mathematical Model of the London Riots and Their Policing," *Scientific Reports* 3 (2013): 1303, <https://doi.org/10.1038/srep01303>.
- 44 Heidi A. Campbell, *Digital Religion: Understanding Religious Practice in New Media Worlds* (New York: Routledge, 2012), 58; Heidi A. Campbell, "Understanding the Relationship Between Religion Online and Offline in a Networked Society," *Journal of the American Academy of Religion* 80, no. 1 (2012): 64-93, <https://doi.org/10.1093/jaarel/lfr074>.
- 45 Heidi A. Campbell, *When Religion Meets New Media* (Routledge, 2010), 126, <https://doi.org/10.4324/9780203695371>.
- 46 Nicole B. Ellison and Danah M. Boyd, "Sociality Through Social Network Sites," in *The Oxford Handbook of Internet Studies*, ed. William H. Dutton, Oxford Handbooks (Oxford, UK: Oxford University Press, 2013).
- 47 Noha Mellor and Khalil Rinnawi, *Political Islam and Global Media: The Boundaries of Religious Identity* (New York, NY: Routledge, 2016), 126, 135.
- 48 Nathan Abrams, "Appropriation and Innovation: Facebook, Grassroots Jews and Offline Post-Denominational Judaism," in *Digital Judaism: Jewish Negotiations with Digital Media and Culture*, ed. Heidi A. Campbell (New York, NY: Routledge, 2015).
- 49 Jan H. Pierskalla and Florian M. Hollenbach, "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa," *American Political Science Review* 107, no. 2 (2013): 207-24, <https://doi.org/10.1017/S0003055413000075>; Allan Dafoe and Jason Lyall, "From Cell

- Phones to Conflict? Reflections on the Emerging ICT–Political Conflict Research Agenda,” *Journal of Peace Research* 52, no. 3 (2015): 401–13, <https://doi.org/10.1177/0022343314563653>.
- 50 Nils B. Weidmann, “A Closer Look at Reporting Bias in Conflict Event Data,” *American Journal of Political Science* 60, no. 1 (2016): 206–18, <https://doi.org/10.1111/ajps.12196>; Mihai Croicu and Joakim Kreutz, “Communication Technology and Reports on Political Violence: Cross-National Evidence Using African Events Data,” *Political Research Quarterly* 70, no. 1 (2017): 19–31, <https://doi.org/10.1177/1065912916670272>.
- 51 Thomas Zeitzoff, “Does Social Media Influence Conflict? Evidence from the 2012 Gaza Conflict,” *Journal of Conflict Resolution* 62, no. 1 (2018): 29–63, <https://doi.org/10.1177/0022002716650925>.
- 52 Jibon Naher and Matiur Rahman Minar, “Impact of Social Media Posts in Real Life Violence: A Case Study in Bangladesh,” *ArXiv:1812.08660 [Cs]*, December 19, 2018, <http://arxiv.org/abs/1812.08660>.
- 53 Lisa Hultman, Jacob Kathman, and Megan Shannon, “United Nations Peacekeeping and Civilian Protection in Civil War,” *American Journal of Political Science* 57, no. 4 (2013): 875–91, <https://doi.org/10.1111/ajps.12036>; Jessica A. Stanton, “Regulating Militias: Governments, Militias, and Civilian Targeting in Civil War,” *Journal of Conflict Resolution* 59, no. 5 (August 1, 2015): 899–923, <https://doi.org/10.1177/0022002715576751>.
- 54 Vindu Goel, Suhasini Raj, and Priyadarshini Ravichandran, “How WhatsApp Leads Mobs to Murder in India,” *The New York Times*, July 18, 2018, <https://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-india-killings.html>; Marcos Martinez, “Burned to Death Because of a Rumour on WhatsApp,” *BBC News*, November 12, 2018, <https://www.bbc.com/news/world-latin-america-46145986>.
- 55 Jessica Megarry, “Online Incivility or Sexual Harassment? Conceptualising Women’s Experiences in the Digital Age,” *Women’s Studies International Forum* 47 (2014): 46–55, <https://doi.org/10.1016/j.wsif.2014.07.012>; Jesse Fox and Wai Yen Tang, “Women’s Experiences with General and Sexual Harassment in Online Video Games: Rumination, Organizational Responsiveness, Withdrawal, and Coping Strategies,” *New Media & Society* 19, no. 8 (2017): 1290–1307, <https://doi.org/10.1177/1461444816635778>.
- 56 H. Akin Unver and Hassan Alassaad, “How Turks Mobilized Against the Coup,” *Foreign Affairs*, September 14, 2016, <https://www.foreignaffairs.com/articles/2016-09-14/how-turks-mobilized-against-coup>.
- 57 E. Elbadawi and N. Sambanis, “Why Are There so Many Civil Wars in Africa? Understanding and Preventing Violent Conflict,” *Journal of African Economies* 9, no. 3 (2000): 244–69, <https://doi.org/10.1093/jae/9.3.244>; Ibahim Elbadawi and Nicholas Sambanis, “How Much War Will We See?: Explaining the Prevalence of Civil War,” *Journal of Conflict Resolution* 46, no. 3 (2002): 307–34, <https://doi.org/10.1177/0022002702046003001>.
- 58 Megan Shannon, Daniel Morey, and Frederick J. Boehmke, “The Influence of International Organizations on Militarized Dispute Initiation and Duration,” *International Studies Quarterly* 54, no. 4 (December 1, 2010): 1123–41, <https://doi.org/10.1111/j.1468-2478.2010.00629.x>.
- 59 Elena Pokalova, “Conflict Resolution in Frozen Conflicts: Timing in Nagorno-Karabakh,” *Journal of Balkan and Near Eastern Studies* 17, no. 1 (2015): 68–85, <https://doi.org/10.1080/19448953.2014.986378>; Stephen Blank, “Russia and the Black Sea’s Frozen Conflicts in Strategic Perspective,” *Mediterranean Quarterly* 19, no. 3 (2008): 23–54.
- 60 Håvard Hegre, “The Duration and Termination of Civil War,” *Journal of Peace Research* 41, no. 3 (2004): 243–52, <https://doi.org/10.1177/0022343304043768>;

- Karl R. de Rouen and David Sobek, "The Dynamics of Civil War Duration and Outcome," *Journal of Peace Research* 41, no. 3 (2004): 303–20, <https://doi.org/10.1177/0022343304043771>; James D. Fearon, "Why Do Some Civil Wars Last So Much Longer than Others?" *Journal of Peace Research* 41, no. 3 (2004): 275–301, <https://doi.org/10.1177/0022343304043770>.
- 61 T. Camber Warren, "Explosive Connections? Mass Media, Social Media, and the Geography of Collective Violence in African States," *Journal of Peace Research* 52, no. 3 (2015): 297–311, <https://doi.org/10.1177/0022343314558102>; Dinissa Duvanova et al., "Violent Conflict and Online Segregation: An Analysis of Social Network Communication across Ukraine's Regions," *Journal of Comparative Economics* 44, no. 1 (2016): 163–81, <https://doi.org/10.1016/j.jce.2015.10.003>.
- 62 Weidmann, "A Closer Look at Reporting Bias in Conflict Event Data."
- 63 Weisi Guo et al., "The Spatial Ecology of War and Peace," *ArXiv:1604.01693 [Physics]*, April 6, 2016, <http://arxiv.org/abs/1604.01693>.
- 64 Olivier Walther, Christian Leuprecht, and David Skillicorn, "Wars Without Beginning or End: Violent Political Organizations and Irregular Warfare in the Sahel-Sahara," *ArXiv:1606.02705 [Physics]*, June 8, 2016, <http://arxiv.org/abs/1606.02705>.
- 65 Pablo Barberá et al., "Tweetering From Left to Right: Is Online Political Communication More Than an Echo Chamber?" *Psychological Science* 26, no. 10 (2015): 1531–42, <https://doi.org/10.1177/0956797615594620>.
- 66 Michela Del Vicario et al., "Public Discourse and News Consumption on Online Social Media: A Quantitative, Cross-Platform Analysis of the Italian Referendum," *ArXiv:1702.06016 [Physics]*, February 20, 2017, <http://arxiv.org/abs/1702.06016>; Michela Del Vicario et al., "Polarization and Fake News: Early Warning of Potential Misinformation Targets," *ArXiv:1802.01400 [Cs]*, February 5, 2018, <http://arxiv.org/abs/1802.01400>.
- 67 Marco T. Bastos, Dan Mercea, and Andrea Baronchelli, "The Spatial Dimension of Online Echo Chambers," *ArXiv:1709.05233 [Physics]*, September 15, 2017, <http://arxiv.org/abs/1709.05233>.
- 68 Wesley Cota et al., "Quantifying Echo Chamber Effects in Information Spreading over Political Communication Networks," *ArXiv:1901.03688 [Physics]*, January 11, 2019, <http://arxiv.org/abs/1901.03688>.
- 69 Nils-Christian Bormann, Lars-Erik Cederman, and Manuel Vogt, "Language, Religion, and Ethnic Civil War," *Journal of Conflict Resolution* 61, no. 4 (April 1, 2017): 744–71, <https://doi.org/10.1177/0022002715600755>.
- 70 Joakim Kreutz, "How and When Armed Conflicts End: Introducing the UCDP Conflict Termination Dataset," *Journal of Peace Research* 47, no. 2 (2010): 243–50, <https://doi.org/10.1177/0022343309353108>; J. Michael Quinn, T. David Mason, and Mehmet Gurses, "Sustaining the Peace: Determinants of Civil War Recurrence," *International Interactions* 33, no. 2 (2007): 167–93, <https://doi.org/10.1080/03050620701277673>; David E. Cunningham, Kristian Skrede Gleditsch, and Idean Salehyan, "It Takes Two: A Dyadic Analysis of Civil War Duration and Outcome," *Journal of Conflict Resolution* 53, no. 4 (2009): 570–97, <https://doi.org/10.1177/0022002709336458>.
- 71 Monica Duffy Toft, "Ending Civil Wars: A Case for Rebel Victory?" *International Security* 34, no. 4 (2010): 7–36, <https://doi.org/10.1162/isec.2010.34.4.7>; Barbara F. Walter, "Does Conflict Beget Conflict? Explaining Recurring Civil War," *Journal of Peace Research* 41, no. 3 (2004): 371–88, <https://doi.org/10.1177/0022343304043775>; Michael Tiernay, "Killing Kony: Leadership Change and Civil War Termination," *Journal of Conflict Resolution* 59, no. 2 (2015): 175–206, <https://doi.org/10.1177/0022002713499720>.
- 72 Devon E. A. Curtis, "Broadcasting Peace: An Analysis of Local Media Post-Conflict Peacebuilding Projects in Rwanda and Bosnia," *Canadian Journal of Develop-*

- ment Studies / Revue Canadienne d'études Du Développement 21, no. 1 (2000): 141–66, <https://doi.org/10.1080/02255189.2000.9669886>; Wilhelm Kempf, "Media Contribution to Peace Building in War Torn Societies," Working Paper, Diskussionsbeiträge Der Projektgruppe Friedensforschung (Konstanz: University of Konstanz, 1998), <https://kops.uni-konstanz.de/handle/123456789/10701>.
- 73 Monroe E. Price and Mark Thompson, "Intervention, Media and Human Rights," *Survival* 45, no. 1 (2003): 183–202, <https://doi.org/10.1093/survival/45.1.183>; Gadi Wolfsfeld, Eitan Y. Alimi, and Wasfi Kailani, "News Media and Peace Building in Asymmetrical Conflicts: The Flow of News between Jordan and Israel," *Political Studies* 56, no. 2 (2008): 374–98, <https://doi.org/10.1111/j.1467-9248.2007.00683.x>.
- 74 Clay Shirky, "The Political Power of Social Media: Technology, the Public Sphere, and Political Change," *Foreign Affairs* 90, no. 1 (2011): 28–41.
- 75 Oliver Boyd-Barrett, "Ukraine, Mainstream Media and Conflict Propaganda," *Journalism Studies* 18, no. 8 (2017): 1016–34, <https://doi.org/10.1080/1461670X.2015.1099461>.
- 76 Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* 63, no. 2 (2019): 317–47, <https://doi.org/10.1177/0022002717737138>; Theodore P. Gerber and Jane Zavisca, "Does Russian Propaganda Work?" *The Washington Quarterly* 39, no. 2 (2016): 79–98, <https://doi.org/10.1080/0163660X.2016.1204398>; Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the Media: The Case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017): 1027–42, <https://doi.org/10.1177/0163443716686672>.
- 77 Gary King, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, no. 2 (2013): 326–43, <https://doi.org/10.1017/S0003055413000014>; Yi Mou, Kevin Wu, and David Atkin, "Understanding the Use of Circumvention Tools to Bypass Online Censorship," *New Media & Society* 18, no. 5 (2016): 837–56, <https://doi.org/10.1177/1461444814548994>; Anita R. Gohdes, "Pulling the Plug: Network Disruptions and Violence in Civil Conflict," *Journal of Peace Research* 52, no. 3 (2015): 352–67, <https://doi.org/10.1177/0022343314551398>; Howard et al., "Opening Closed Regimes."
- 78 David Patrikarakos, *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century* (New York, NY: Basic Books, 2017); Christian Christensen, "Twitter Revolutions? Addressing Social Media and Dissent," *The Communication Review* 14, no. 3 (2011): 155–57, <https://doi.org/10.1080/10714421.2011.597235>; Matthew L. Williams et al., "Policing Cyber-Neighbourhoods: Tension Monitoring and Social Media Networks," *Policing and Society* 23, no. 4 (2013): 461–81, <https://doi.org/10.1080/10439463.2013.780225>; Gohdes, "Studying the Internet and Violent Conflict."
- 79 Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution*. 63, no. 2 (2019): 317–347.
- 80 A further line of inquiry would be whether heavy scholarly and policy attention on disinformation in Western liberal democracies render disinformation and organised distraction easier and more likely in countries outside NATO and/or are not liberal democracies. For a range of time-frequency analyses on countries beyond mainstream scholarly focus, see: Rolf Fredheim-led 'Robotrolling' reports, available at: <https://www.stratcomcoe.org/robotrolling-20171>.
- 81 Anne Helmond, "The Platformization of the Web: Making Web Data Platform Ready," *Social Media + Society* 1, no. 2 (2015): 1–11, <https://doi.org/10.1177/2056305115603080>; Jean-Christophe Plantin et al., "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook," *New Media &*

- Society 20, no. 1 (2018): 293–310, <https://doi.org/10.1177/1461444816661553>.
- 82 Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, 1st ed. (New York, NY: New York University Press, 2018).
- 83 Zeynep Tufekci, “‘Not This One’: Social Movements, the Attention Economy, and Microcelebrity Networked Activism,” *American Behavioral Scientist* 57, no. 7 (2013): 848–70, <https://doi.org/10.1177/0002764213479369>; Zeynep Tufekci, “Engineering the Public: Big Data, Surveillance and Computational Politics,” *First Monday* 19, no. 7 (2014), <https://doi.org/10.5210/fm.v19i7.4901>; Bernard J. Jansen et al., “Twitter Power: Tweets as Electronic Word of Mouth,” *Journal of the American Society for Information Science and Technology* 60, no. 11 (2009): 2169–88, <https://doi.org/10.1002/asi.21149>.
- 84 David Lazer, “The Rise of the Social Algorithm,” *Science* 348, no. 6239 (2015): 1090–91, <https://doi.org/10.1126/science.aab1422>; Gunn Sara Enli and Eli Skogerbo, “Personalized Campaigns in Party-Centred Politics,” *Information, Communication & Society* 16, no. 5 (2013): 757–74, <https://doi.org/10.1080/1369118X.2013.782330>.
- 85 Department of Peace and Conflict Research, Uppsala University and the Centre for the Study of Civil War at the Peace Research Institute Oslo (PRIO). “UCDP/PRIO Armed Conflict Dataset.” Accessed May 16, 2019. <https://www.prio.org/Data/Armed-Conflict/UCDP-PRIO/>.
- 86 Lockheed Martin. “Integrated Crisis Early Warning System (ICEWS).” Accessed May 16, 2019. <https://www.lockheedmartin.com/en-us/capabilities/research-labs/advanced-technology-labs/icews.html>.
- 87 “Armed Conflict Location & Event Data Project (ACLED).” Accessed May 16, 2019. <https://www.acleddata.com/>.
- 88 National Consortium for the Study of Terrorism and Responses to Terrorism – University of Maryland. “START.” Accessed May 16, 2019. <https://www.start.umd.edu/>.
- 89 Department of Peace and Conflict Research – Uppsala University. “Violence Early-Warning System (ViEWS).” Accessed May 16, 2019. <https://www.pcr.uu.se/research/views/>.
- 90 Technology Policy Program – Center for Strategic and International Studies. “Significant Cyber Incidents.” Accessed May 16, 2019. <https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity>.
- 91 Council on Foreign Relations. “Cyber Operations Tracker.” Accessed May 16, 2019. <https://www.cfr.org/interactive/cyber-operation>

FEATURE INTERVIEW: MS STEPHANIE SNYDER

In this feature interview, STAIR speaks with Stephanie Snyder, Senior Vice-President and Commercial Strategy Leader for Cyber Solutions at Aon, to gauge some of the top concerns facing private sector actors in cyberspace. Aon is a professional services firm that provides risk and insurance consulting services to companies around the globe. Ms Snyder works with businesses to adapt to a new digital economy and manage cyber risk. She talks with STAIR about innovative ways that her clients are building cybersecurity risk management strategies to face an ever-changing landscape of threat.

STAIR: Thanks for speaking with us. Could you just start by just telling us a bit about your role?

Stephanie Snyder: My title is SVP and Commercial Strategy Leader for Cyber Solutions at Aon, a professional services firm, and my role is twofold. I am an insurance broker for cyber insurance for large commercial organisations, which means my expertise, with regards to cyber risk and cybersecurity, really comes from a risk standpoint, because I work with many first-time buyers of cyber insurance. Cyber insurance has been around roughly since the year 2000, and it's been rapidly evolving, [just] as cyber risk has been rapidly evolving. So, we are seeing a ton of interest by organisations in purchasing a stand-alone cyber insurance policy. But even in 2019, only about thirty to forty percent of organisations of all sizes and industries do purchase a stand-alone cyber insurance policy.

Because of that, we are doing a lot of first-time placements, where we sit down with clients and talk to them about their organisations from a cyber risk exposure standpoint, and how we look to insurance to transfer some of that risk off of their balance sheets. So that is my more technical role. I also serve as commercial strategy leader for our cyber solutions team, which not only includes our brokerage services, but also our proactive and reactive cybersecurity solutions, as well as our assessment and quantification tools, relative to cyber risk and cybersecurity.

STAIR: From your perspective, working specifically on cyber insurance, what are the top three challenges that you see today for cybersecurity risk management?

"Ms Stephanie Snyder," *St Antony's International Review* 15 no. 1 (2019): 125-132.

SS: I would have trouble narrowing it to three. I would say first and foremost—you use the term ‘cybersecurity risk management’. There really is no true field of cybersecurity risk management; there are a lot of silos within commercial organisations that are addressing cyber risk in different ways. There’s not one individual that is addressing it across the organisation. We see the IT security professional or the Chief Information Security Officer (CISO), who’s looking after protecting the network, and partnering with various entities industry-wide to try to get threat intelligence. There’s a lot that falls onto a Chief Information Security Officer because he or she is really tasked with looking after cybersecurity for the firm.

Yet, sitting over across the other side of the firm, you have a Chief Financial Officer (CFO) or General Counsel or a Risk Manager who’s tasked with protecting the firm from risk. They may be responsible for the insurance purchase, and cyber insurance may be a part of that portfolio of insurance policies, or it may not be. The risk manager may be trying to use a property insurance to pick up the potential business disruption associated with a breach. Then you look across the firm in another way—what HR is doing in terms of employee on-boarding, in terms of ways employees leave the organisation, so that there’s no [intellectual property] leaving with that employee.

You have the board—trying to make sure that they know enough about cybersecurity to be able to provide oversight and the right budget to the CISO, Risk Manager, and to HR. And then you have different parts of the organisation that may be looking after business continuity and disaster recovery. So, I like the term ‘cybersecurity risk management’. I think one day we will get there. I think in commercial organisations, we’re slowly seeing IT security and risk management coming together. I would say in the financial institutions industry today, [and] at a lot of the large banks, these roles are one and the same. Also, for a lot of large banks, they are probably the most sophisticated, from a cybersecurity standpoint, relative to other industries. We’re seeing a lot of industries at very different levels of sophistication when it comes to addressing cybersecurity risks.

STAIR: One of the most contested aspects in this field is reporting structure. As you have said, in cybersecurity risk management—or the way that we think about IT security—there are so many different pieces. You can look at a different firm that you might be working with, and it is structured in so many different ways where those reporting structures would work differently. Do you think every company needs to do this differently? Do you think Chief

Security Officers need to report directly to the CEO or the board? Or do you think it is industry dependent?

127

SS: I have worked with a lot of different organisations in different industries, and most of them are structured differently. Often-times, we'll see Chief Information Security Officers report to the audit committee, or report to the Chief Information Officer. Certainly, it's important that CISOs have time to be able to educate the board on the risk. Certainly, for publicly traded organisations in the US, the Securities and Exchange Commission (SEC) has become very active around not only ensuring that cybersecurity risk factors are included in public filings, but also, they have begun fining companies relative to breaches. So, the board needs to stay involved.

I think that it depends, frankly, on the size and complexity of the organisation as to what makes sense for a reporting structure. You really see it in a lot of different ways. The most important part is that there's some degree of collaboration across the various stakeholders, in whatever way that that happens.

Sometimes we see a lot of collaboration come out of cybersecurity table-top exercises, where the organisation is pulling various stakeholders across the organisation to test their incident response plan. It's during the course of that table-top exercise that they can identify that 'it doesn't make sense that we're doing it this way, we could do it that way'. Whether that's reporting structure, or whether that's purely how they respond to an incident, that is the one time that we see a lot of those stakeholders come together. But I think collaboration is definitely the key.

STAIR: What were your other two challenges in this field?

SS: Cybersecurity risk is evolving, and many organisations are just trying to play catch up. A real trend that we see for organisations in 2019 is the idea of digital transformation. So many organisations are moving and changing their business models to embrace the digital, and frankly trying to modify what they're able to do, whether that's through using greater amounts of data, through acquisition of smaller technology firms, or through new operations, such as software-as-a-service. We're definitely seeing a shifting dynamic for a lot of organisations as they employ greater uses of technology and try to monetise it. I think that is additionally challenging to be able to address that across the firm from a cybersecurity standpoint. It's really changing the risk profile of the company, at the same time that we're seeing the hackers continuing to update their tactics.

STAIR: Looking at Aon's 2019 Cyber Security Risk Report, one of the risks that you highlight is these governance and responsibility issues. There's a quote about the proliferation of overlapping cyber regulations, and how that's actually creating more cyber risk, not less. How are US companies are navigating this shifting landscape? Just as you said, the US government and other governments are playing catch up in this field too and trying to figure out ways to regulate this space.

SS: The challenge for a lot of organizations—and the details are in that report—is keeping up with these regulations. It's kind of an alphabet soup of regulations. You have the European Union's General Data Protection Regulation (GDPR), the upcoming California Consumer Privacy Act (CCPA) — and then overlay that for US companies, all 50 states have different notification laws in case of a breach, with many states following California in introducing additional privacy regulation. I think that the CCPA is concerning for a lot of US companies, in the way that GDPR may not have been, because some US companies don't have information on European citizens, and therefore were not exposed to the GDPR. And the CCPA is still evolving; it's not going to be set in stone in terms of what that regulation is until we're closer to 2020, and we're seeing movement in that regulation. California has also introduced an Internet of Things (IoT) law which is going to be effective in 2020, which requires that connected devices have 'reasonable cybersecurity'. The big question is, will this need to be solved through litigation, as to what constitutes 'reasonable'?

It's very difficult, and it is only getting more complex, because we don't have a federal law in the US. And then you go outside the United States and various countries have different laws. Certainly, GDPR is the most onerous in terms of the 72-hour reporting and potential fines. It's introducing another layer of compliance into what is already a very difficult challenge that these organisations face, in terms of their own IT security and staying ahead. There's a lot of organisations that we're working with that have introduced bug bounty programs, because they are like, 'Hey, if you can't beat them, join them'. They think, 'let's at least pay people to be white hat hackers who can find these vulnerabilities before the bad hackers do'. A lot of organisations are getting creative in terms of trying to figure out how they can stay ahead.

STAIR: In addition to bug bounty programs, a lot of US companies have established their own threat sharing intelligence platforms, particularly because there's a lot of vulnerability associated with sharing with the government, with the number of hacks and ex-

posure. I'm wondering if you have any thoughts about that. Is it a useful tool or does it just add additional compliance issues?

SS: There are industry ISACs (Information Sharing and Analysis Centres). Almost all of the clients that I deal with are large complex organisations and they participate in an ISAC as a way of gathering threat intelligence and getting information. We see a lot of that; certainly, there are a lot of vendors out there that can be helpful with threat intelligence, but I think that ISACs are particularly helpful.

STAIR: Do you think that there's a chance to build something like that with governments or is that a non-starter?

SS: I don't have much perspective from speaking with various CISOs in terms of how they feel about partnering with public entities. I'm really speaking from my experience, in terms of what information my clients are sharing, and where they look for organisations and knowledge sharing.

I see a good number of CISOs that have previously worked in the federal government, so they have those relationships that don't necessarily go away when they move over to the private sector.

STAIR: Cybersecurity risk management may not be an established field, but there's certainly a lot more need for people to be going into this. What kind of training is useful for going into this space and being able to actually help companies figure out how to do this in a way that's not just playing catch up, but being more proactive?

SS: First of all, there are not enough individuals to fill all the cybersecurity positions. A lot of organisations do rely on third party vendors to help them in terms of being proactive. And that's one of the things that we do within Aon; we have a lot of proactive services in terms of testing, table-tops, and incident response planning. We recognise that you need to be able to address things as proactively as possible. But that's where I think a lot of the third-party vendors are filling in, in helping companies build out their proactive strategy. That being said, many organisations may only have hired a CISO a couple of years ago.

For many organisations, cybersecurity was traditionally under IT. And it's only in recent times that organisations have built out a formal cybersecurity vertical and recognise that they need to be proactive and need a team of individuals to execute. I mean, frankly, for many organisations, IT security is still a capital ex-

pense, not an operating expense. And it changes once a company has a breach. All of a sudden, the CISO gets the budget so that they can go out and do what they always wanted to do from a cybersecurity standpoint. So, while the approach to cybersecurity is changing, it's changing, frankly, a lot more slowly than it should.

The prevalence of ransomware attacks that we're seeing, it's not slowing down. In 2019, if an organisation doesn't have appropriate cybersecurity controls and infrastructure, and they have a ransomware attack, then they're in a situation where they almost have to pay that ransom to be able to secure their network, because they may not have the appropriate backup tools. They may not have the appropriate cybersecurity infrastructure. There's NIST, and there are other cybersecurity frameworks that are out there. But I think that organisations need to focus on building out roles that look at cybersecurity on a holistic basis across the organisation. Because that's how the risk exists in the organisation, yet everybody has their own pockets and silos. So, you're trying to address this unbelievable risk, but the best way you can do it is have one quarterback who can run a team of people to be able to attack it.

A lot of organisations still have this siloed way of thinking in terms of who's doing the blocking, tackling, and so on and so forth. The whole concept of 'Cybersecurity Risk Manager' is someone who works hand-in-hand with all these different stakeholders within the organisation to ensure that everything is addressed as it should be because you have different silos that address things and the concern is that things get missed somewhere. And then, lo and behold, an organisation has a breach, and it's very expensive.

STAIR: A lot of people talk about 'baked-in versus bolted-on' security. If you are a rapidly growing start-up, it wasn't in your interest to be worried that much about security until a few years ago. You were much more worried about getting as many users as possible and launching on as many platforms as possible. Is Aon ever brought in early enough where you can help build a holistic cybersecurity portfolio? Or are you more on the troubleshooting side, where it's a well-established organisation that already has all of these stakeholders and has to do more of a 'bolted-on' approach?

SS: As a professional services organisation, we're really helping organisations to assess or quantify, or proactively or reactively address their cyber risk, through various product solutions that we have. But I think what I hear you talking about is a whole concept of 'security by design' which is interesting. I agree that so many organisations are moving so fast that security is often an after-

thought. Even for organisations that are moving onto the cloud, security can also be an afterthought. And I think that that's changing. Again, is it changing as fast as it could be? No, I think that depending on the organisation, if you have a fifty-year-old organisation, they have legacy systems, and they're trying to build a digital overlay on these legacy systems just to make sure that they're not going to be hacked. So, for younger organisations, absolutely, they should be baking security in as they're growing. Are they moving too fast and not baking in enough security? Probably. But the challenge really is when you have more established organisations and more established technology infrastructure, that are then trying to overlay security at that point. And then you think about organisations that go through mergers and acquisitions over many years, which has the potential to produce a lot of different bolted-on network systems. So, the ideal would be for every organisation to use security by design, certainly when they can, although for many organisations, it's not necessarily possible. But for organisations that are implementing new technologies, or where the Chief Information Security Officer has a seat at the table, that's where we're seeing things start to shift, because their job is to drive security in the workplace.

STAIR: What about hacking back? Many CISOs, especially on the legal side of companies, will say, 'Oh it's really not a good idea; it opens a company, and particularly a U.S. company, to so much liability'. But there's a growing field of public sector active defence or 'hacking back'. Is it a useful trend to think about a public sector role for protecting companies while insulating them from the liabilities of actually being involved in hacking back against the black hat hackers out there? Or is that something that you would just prefer not to touch?

SS: If you look back to Target, Home Depot, Anthem – those breaches were very much done by hackers to make money off of personally identifiable information. Instead, now we're seeing the hackers shift into more ransomware-driven attacks. Again, it's because it's a money-making business. But then you have these significant disruptions such as 2017's WannaCry and NotPetya attacks. These are question marks because we don't necessarily know the full facts of who's behind those attacks. But the amount of destruction and the amount of financial loss that they caused to private sector organisations was significant. This begs the question of what role the government should play when it comes to protecting commercial organisations.

STAIR: Going back to the idea of cybersecurity education—there are just not enough people working in this field. What advice do you have for young professionals who want to enter this space?

SS: There's few people that have been working in cyber insurance for twenty-plus years because it hasn't existed for twenty-plus years. We have trouble trying to find people to fill roles because it is a newer type of insurance. And that it is probably one of the best areas to get into. I would say cybersecurity and/or cyber insurance is such a great area because there's a lot of job security. The fact is there is a lot of change going on in terms of the digital transformation of organisations; the continuing risk that bad actors or even employees cause; the potential for cyber terrorism or warfare and the associated disruption, etc. All of this is early days [and] the challenges are only going to become more complex.

How organisations address these risks is going to be more at the forefront and I believe that there is going to need to be a cybersecurity risk management role. Things are not going to slow down in any way, shape, or form because the risk only continues to be more complex.

STAIR: Is there a background that you wish you saw more of when you're thinking about filling these roles? Obviously, we need more experts in cybersecurity, [but] for new academics who are interested in working in this field, what is really missing?

SS: It's more of the business education that is missing: being able to talk to people and collaborate is huge. A lot of what I do in my role is just sit down with a risk manager, a CFO, and a Chief Information Security Officer, and explain to them why I think they have a significant amount of cybersecurity risk within their organisation and how they can use insurance as a solution. Alternatively, they can use other various proactive cybersecurity solutions, and that really takes not necessarily understanding the hyper technical, but really understanding okay, what are the goals of the CISO, what are the goals of the risk manager or the CFO? Why do we need to bring them together, why do we need them to collaborate? That goes back to the concept of cybersecurity risk management. You need that one person at an organisation who's going to be able to pull people together and get them to talk to each other so that they can say, 'Oh yes, we do need to work together, because together we're going to be able to solve this better than if we just sit in our individual silos'. I think it's a mix between not only having that technical cyber security risk education, but also having business acumen and the ability to communicate and collaborate.

IMPLICATIONS OF MIGRATION FOR THE CONTEMPORARY STATE: PARADOXES OF CONVENTIONAL STATEHOOD IN LIBERAL WORLD ORDER

Hassan Fiaz, SOAS University of London

Abstract

Predominant theories of international relations have conceptualised the state as a self-evidently autonomous legal entity, primary source of world power, and the predominant if not exclusive arbiter of authority over its populace. This specific and somewhat static conception of the state has considerably influenced ways in which contemporary migration has been constructed in literature and referred to in policy circles. Beginning with a literature review of the ways in which more nuanced and complex understandings of the state have evolved beyond this conceptualisation, as well as the significance of these understandings for scholarship on migration politics, this paper contextualises the state-migration paradigm within a wider backdrop of liberal order and globalised economic forces, in order to evaluate the migratory implications for contemporary statehood. This critical juxtaposition will illustrate the relationship between migration and the contemporary state as providing a potent framework for exposing a 'liberal paradox', in which competing global economic and domestic security issues vie for prominence. The functional implications arising from the different ways in which states navigate this paradox will be explored through case studies focussing on sovereignty and national identity, economic development, and subversive transnationalism, in which divergent economic and political considerations have driven state responses to migration.

This paper demonstrates that migration creates complex and interrelated implications for each of the main components of statehood – a territory defined by physical borders, a distinct population subject to its control, and a sovereign capacity to govern its citizens. Challenging the notion that these characteristics represent immovable virtues of the state, this paper will use migration as a framework to explore their malleability, alongside a critical analysis of how these characteristics have influenced the ways in which governments understand and construct migratory implications as problems to be navigated.

Hassan Fiaz, "Implications of Migration for the Contemporary State: Paradoxes of Conventional Statehood in Liberal World Order" *St Antony's International Review* 15. no. 1 (2019): 133-152.

Shifting Conceptualisations of the State and its Role in Global Political Economy

International relations scholarship has continued to make significant strides in positing more nuanced and complex understandings of the ways in which international politics and global events are driven by forces external to state institutions and power. However, predominant applications of international relations theory have tended to assume and interpret the state as the central component in world politics, with the coexistence of sovereign states serving as the foundation of international law and order.¹ Worldviews in which states act as the focal point around which ‘power and authority continues to revolve’ have prevailed since the Peace of Westphalia in 1648, from which the notion of the ‘inviolability of the nation state’ became widespread, concurrent with the global rise of European influence.² This ‘inviolability’ is encapsulated within the essential requirements for a prospective state outlined in the 1933 Montevideo Convention, which codified the declarative theory of statehood. These include “a territory, with a permanent population, subject to the control of a government, and the capacity to conduct international relations (sovereignty).”³

This emphasis on territorial sovereignty and the state’s capacity to wholly and effectively manoeuvre its influence in the world whilst exerting authority over its citizenry has resulted in the state being defined within international relations primarily in terms of its security or military function. The conventional characteristics of the Westphalian state are thus synonymous with the description of a “garrison state”,⁴ correlating with understandings of the state as a masculine construction and a projection of patriarchal society, in which state officials take on the stance of ‘masculine protector’ against external ‘threats’ for the safety of the motherland, as part of what Young describes as an “authoritarian security paradigm.”⁵

However, the singularity of this ‘garrison state’ has been offset to a large extent by what Rosecrance describes as the ‘trading state’, which arises out of economic openness, stimulated by the need to facilitate the securement of material wealth to reinforce economic and political power.⁶ International relations theory has in recent times consequently moved away from the classical realist

tradition, developing a more complex and nuanced understanding of the state which acknowledges that power is manifest to varying extents in ‘hard’, ‘soft’, and ‘smart’ capacities.⁷ At the heart of this diffusion of power are globalised policies of free trade and the increasingly interdependent world created through linkages of trade and finance, which force states to “alter their grand strategies and seek new ways to cooperate.”⁸

Introducing the ‘Liberal Paradox’

Hollifield concludes that as a result of this interplay between security and economic imperatives, “states are trapped in a liberal paradox,” referring to a specific manifestation of some of the “contradictions inherent in liberalism.”⁹ These contradictions relate to opposing forces at play since the end of the Second World War, in which globalisation, the proliferation of neoliberal policies and institutions, and economic forces such as trade and migration have pushed states towards greater openness, whilst powerful domestic political forces empowered via the international state system continue to enforce closure within and between states. This conflict has stimulated a paradigm in which global mobility has increased parallel to the intensified securitisation of borders.¹⁰ It is how states have chosen to navigate this liberal paradox that has largely informed their problem construction of migration and policy narratives.

The State in Migration Politics

Taking into account the above analysis of the changing conception of the state and the juxtaposition between the power of states as sovereign actors and globalised economic drivers, a number of migration theorists have endeavoured to fill scholastic gaps in relation to the role of the state in international migration trends. Weiner makes the case that questions of how “state actions shape population movements” and what “governments do in their domestic policies to adjust to or influence population flows” are issues that have been largely neglected in international relations and international migration discourse.¹¹ Addressing this deficit, Wiener considers state sovereignty as the central consideration in developing theories of international migration, noting dissonance between the perspective that sovereignty is critical to understand-

ing the role of states in relation to migration and the perspective that state sovereignty is an eroding concept.

Understanding the latter position is crucial to comprehending the relationship between international relations and international migration.¹² Wiener concludes from his analysis of entry rules and migration policy that with the exception of a few countries such as the United States, “entry rules are only marginally shaped by economic considerations even for those countries that are relatively open to the flow of trade, capital, and technology,” and that it is “how a people define their national identity and their receptivity to other peoples with different identities” that conditions how governments respond to labour demand changes.¹³

Teitelbaum also notes surprising deficiencies within theories of international migration when assessing the role of states in “initiating, selecting, restraining, and ending international migration movement.”¹⁴ In analysing the dissonance encapsulated by international migration between state autonomy and ‘overwhelming’ economic, social, and political forces which drive international flows of people, Teitelbaum concludes that “in reality, all modern states do intervene—with greater or lesser effectiveness—to influence the size and composition of international movements,” with varying policy trends between types of ‘sending’ and ‘receiving’ states.¹⁵ Whilst acknowledging the power of globalisation trends and international human rights conventions to limit states’ control over transnational population movements (including restrictive measures on migrant populations), Teitelbaum concludes that “claims that increasing potentials for international migration are so powerful that states cannot affect them seem greatly overstated.”¹⁶

Read in conjunction with the work of Weiner, Zolberg provides important perspectives recognising sovereignty as a central theme within international migration theory. Starting with the formation of the modern state as “the political organization of world space into mutually exclusive sovereignties that delineates the specificity of international migration,” Zolberg identifies the distinctive feature of international migration as the “transfer from the jurisdiction of one sovereign to another,” which, particularly if permanent, represents “a deviation from the norm in terms of which the world is politically organized.”¹⁷ Whilst this deviation has overt implications for states which project ethnic or civic nationalism as the basis for boundary-marking and social cohesion,

migration also tests the limits of contemporary liberal democratic states, which are often assumed to foster greater openness and pluralism.¹⁸

Adamson, Triadafilopoulos, and Zolberg provide an interdisciplinary understanding of the ways in which migration stretches the limits of the 'liberal state'. They argue that liberal norms are deployed for exclusionary purposes, in effect simply replacing or supplementing alternative boundary-markers (such as ethnic nationalism) in the construction and implementation of migration and integration policies, as opposed to effectively undermining those boundary markers.¹⁹ Adamson notes migrants are often viewed as a 'fifth-column' with potential dual loyalties, particularly in times of conflict,²⁰ whilst increasingly multicultural populations stimulate migration-based transnational networks that circulate ideas as well as material goods, creating a simultaneity that challenges "notions of the territorial state as a bounded entity with a clearly demarcated territory."²¹ This has the effect of undermining autonomy via the need for a more interdependence-based approach to security.²²

The preceding review of migration literature suggests that, in addition to analysis of the political/ideological construction of states as driving forces in determining responses to international migration, due regard must be given to the significance of the state as a construct and the norms it projects as an autonomous actor. While much of the literature has focussed on how migration trends are influenced by the role of states, this paper will specifically assess the ways in which the *state itself is impacted* by migration, which will provide a valuable scholastic basis to understand how and why states construct migration and respond to it. This review has also enabled the identification of three core notions of statehood that are central to consolidating a review of migratory-state relationships. These are:

- 1) A *physical territory* with definitive demarcated boundaries.
- 2) A *distinct population* subject to state control.
- 3) A *sovereign capacity* to govern citizens and exhibit autonomy in international relations.

This paper will use this triumvirate as a guiding framework, reaching conclusions relevant to each point of reference.

Weaponising Migration: The State, Nationalism, and Conceptualising 'Others' as the Raison D'être of Boundary-Marking

One of the most significant features of migration's relevance to the state is that it appears inherently antithetical to the construction of nationalism and boundary-marking that underpins much of the state-based international system. From the perspective that this represents one of the liberal paradox's most pronounced and divisive manifestations, this section will utilise a range of circumstantially distinct but conceptually linked case studies to contextualise the significance of this dissonance in international migration.

Methodological nationalism is a term used to refer to the assumption within the social sciences that "the nation/state/society is the natural social and political form of the modern world,"²³ an idea which serves to naturalise the global regime of nation-states. This discursive naturalisation both reinforces and is reinforced by the centrality of nationalism to the functioning of global politics: a common identity and notions of 'belonging' serve as an ideological foundation for the state's existence and its role as masculine protector of its own sovereignty and its population's security.²⁴

Although so-called 'multinational states', in which no single ethnic group overwhelmingly dominates, are often contrasted with nation states, this paper posits that nationalism is central to the foundational functioning and legitimacy of all states, regardless of whether they purport to constitute an ethnically homogeneous group. Symbols of national identity—flags, anthems, official languages, national holidays, pledges of allegiance, citizenship requirements, and sporting teams—are all examples of constructions in nation-building which consolidate the state's legitimacy and right to sovereign autonomy.²⁵ Through these symbols, states inherently induce homogeneity, which is essential to the claims of authority, enabling them to control and govern their populations.

One of the key distinguishing features of migration from other forms of transnationalism is its ability to significantly alter the composition of societies, disrupting what Koslowski describes as the "demographic boundary maintenance regime."²⁶ The most significant potential implication of this disruption is that "the citizenry or the demographics may be transformed in such a way as to violate the social contract, undermine the legitimacy of the gov-

ernment, and the sovereignty of the state itself.”²⁷ Indeed, even in the US, a supposedly multinational and ethnically disassociated state, comments attributed to President Trump deriding migration from ‘shithole countries’ brought to the surface existential ideological conflicts over what constitutes American identity, in which the significance of race cannot be ignored.²⁸

This paper will approach migration from a nuanced and critical perspective to demonstrate that it is not the movement of people per se that creates implications for the state in relation to demographics and the liberal paradox, but the concept of peoples considered other to the nationalism upon which state power is based. The degree of otherness largely determines the state’s construction of migration as a problem, and its responses to it.

Regulating the ‘Demographic Boundary Maintenance Regime’ - Migration as a Threat to the Nationalist Foundations of Statehood

One of the most common myths perpetuated in migration discourse is the assumption that the current era represents a distinctive and unprecedented ‘age of migration’, despite the fact that the proportion of migrants in the total world population remains at a similar level to that of a century ago.²⁹ However, what does distinguish the late 20th and 21st centuries is the increased visibility of global migration. This is a consequence of decolonisation, concentrated wealth accumulation, and enhanced perceptions of global inequality within the developing world, all of which have stimulated the “unprecedented settlement of non-Western, culturally and physically distinct, immigrants’ into Western societies.”³⁰ The divergent ways in which states construct this as a problem and the varying policies for regulating the demographic boundary maintenance regime will now be explored through the case studies of Germany and Hungary, both members of the European Union (EU), but with notably distinct perspectives of liberal values which manifest in their divergent approaches to contemporary migration.

Hungary’s response to migration in recent years has represented a significant marker in the country’s progression away from liberalism towards increasingly nationalist populism. This process has been amplified by the recent refugee crisis, in which significant numbers of non-European peoples sought refuge, sta-

bility, and opportunity in the European Union, an institution considered to embody the values of global liberalism.³¹ Anti-migrant rhetoric has long been central to the ruling Fidesz party's ability to garner populist appeal amongst the electorate. This strategy has contributed to the growing success of the party, which recently won a third consecutive term in April 2018 with an overwhelming majority.³² In an explicit confirmation of this anti-migrant stance, following the 2015 attacks against the offices of satirical newspaper *Charlie Hebdo* in Paris, Viktor Orban unequivocally declared: "We will never allow Hungary to become a target country for immigrants. We do not want to see significantly sized minorities with different cultural characteristics and backgrounds among us. We want to keep Hungary as Hungary."³³

It is imperative to note that in conflating the issues of migration and domestic violence, the Hungarian government has effectively militarised the concept of migration, with 'violations' of its borders characterised as attacks on the safety and sovereignty of the state.³⁴ The national conversation around migration has thus intentionally been driven to a fever pitch by the machinations of state power. State institutions and media are used to frame the issue in intentionally war-like terms: migration as 'invasion', border control as 'defence', and the government as 'protectors' of Hungary. This language draws on historical imagery of the Soviet occupation of Hungary to transform the issue of migration into a matter of survival for the Hungarian state itself.³⁵ This narrative has inevitably translated into physical action, with fences, surveillance, and soldiers militarising the border as a buffer against external threats.³⁶

In relation to the liberal paradox, the anti-migrant policies of the Fidesz government must be understood in the wider context of the Hungarian state's general transition away from liberalism towards nationalism and authoritarianism, characterised by a calculated projection of Hungary as a strong and sovereign state. Restrictions on freedom of the press, the closure of educational institutions considered subversive, and constraints on civil liberties have become defining features of the Fidesz government.³⁷ This goes some way to explaining the apparent incongruity between the government's hyperbolic narrative and the actual, immediate implications of migration in Hungary. The vast majority of migrants consider Hungary to be a 'transitory' state in their migratory route, with their ultimate objective onward migration

to the more liberalised, open, and economically stronger states of western Europe, as opposed to settlement within Hungary itself.³⁸ Thus, a wider contextual scrutiny suggests that it is not so much a physical violation of borders that is an issue for the Hungarian state, but a symbolic violation, with the border representing an emblem of the sanctity of the state as a protector and promoter of national integrity.

In sharp contrast to Hungary, Germany's economy has developed to become significantly dependent upon maintaining a growing level of productive labour, which in conjunction with an ageing population and declining native birth rates, has stimulated a liberal and embracing attitude towards migration.³⁹ Faced with notable demographic changes, the progressive movements of the 70s and 80s pursued the 'multikulti' public policy, which played a defining role in how the German state has construed the implications and 'problem' of migration. This approach sees migration as an issue of adaptation, in contrast to one of preservation, as expressed by Hungary. The multikulti approach redefined nationalism to reflect the demographic changes wrought by migration, defining the nation state as belonging to a recognisable population of German people.⁴⁰ The multicultural worldview redefined the foundation for the state's existence, away from ethnic Germanness. Instead, the 'other' was seen as firmly a part of Germany's territorial landscape, nullifying perceptions of threats from the 'other'.

However, the German state's attempts to reconstitute the nationalism underpinning the identity and sovereignty of the state has not passed without resistance. Capitalising on perceptions that migration has eroded the German state's sovereignty and altered its demographics and social fabric to the extent that the German state no longer constitutes a distinctive nation, opposition movements, such as the Alternative for Deutschland (AfD) party, have gained increasing momentum and support amongst the electorate.⁴¹ A divisive slogan posited by the AfD – 'New Germans? We'll make them ourselves' – alongside the party's general emphasis on an ideological 'alternative' to the liberal status quo, serve as valuable reminders that the state operates at multiple levels and amidst a quagmire of forces and considerations.

Internal conflict within the state remains a powerful shaper of policy and ideological direction amidst the influence of external global forces. In Hungary, liberal parties received considerable support in the capital Budapest, where economic considerations

outweighed the nationalist sentiment that had taken root in the country's less urbanised areas.⁴² These two case studies encapsulate what Koopmans and Statham identify as the postnational challenge ("external erosion of sovereignty") and the multicultural challenge ("internal cultural differentiation of liberal nation-states").⁴³ It can thus be deduced that the liberal paradox is an ongoing and ever-evolving dilemma which states navigate depending on a range of interrelated contextual factors.

Regulating the 'Demographic Boundary Maintenance Regime' - Migration as a Consolidation of Nationalism and State Homogeneity

In further developing this premise, it will now be demonstrated that if the migration of peoples perceived as foreign to the sovereign state's nativism challenge its legitimacy, it follows that the migration of people whose identities are harmonious with the nationalism upon which state sovereignty is based can in fact consolidate the state's legitimacy. This critical approach to migration and demographics will be discussed within the context of an unconventional case study: Han migration into China's restive Xinjiang region, historically home to the country's ethnically and linguistically distinct Uyghur Muslim minority.

Although this example of internal migration does not constitute a form of transnationalism within the confines of international law, this case study is particularly interesting given the strong and historical basis for Xinjiang constituting an independent 'East Turkestan' state, meeting each of the statehood criteria outlined in the Montevideo Convention, with the exception of the physical means of acquiring territory away from the Chinese state. China has long viewed the region and its inhabitants with considerable suspicion and unease, leading to an increasingly suppressive cycle of authoritarian measures and subsequent doubling down on dissent, conveniently framed by the Chinese state in the wider context of global jihad and terrorism.⁴⁴ The Uyghurs thus find themselves within the borders of the nation state in the physical sense, but outside its borders in the ideological sense.

The Chinese state has long initiated a series of policies to 'bind Xinjiang' to the rest of the Republic, as part of which internal migration by Han Chinese into Xinjiang has provided considerable momentum in the pursuit of "integrating its peripheries into the

core.”⁴⁵ The Han population is actively encouraged by the state to settle in Xinjiang under the pretext of driving its development, whilst largely undermining engagement of the local population in this development process. The Han population of Xinjiang in 2008 was estimated to be around 40%, compared to just 6.7% in 1949.⁴⁶ This intensive ‘Hanification’ of Xinjiang through the resettlement of China’s dominant ethnic group is serving to significantly diminish the distinctiveness of Xinjiang and its historical roots as a Turkic region, leading to its more effective integration into the Chinese nation-state.

With particular significance for states in the Global South, Zolberg notes how the formation of new states following the dissolution of empire was and is in of itself a ‘refugee-generating’ process. This has continuing implications for states which consider consolidation of the nation-state to be an urgent precondition for affording political strength of leverage to overcome underdevelopment.⁴⁷ Groups on the margins of state-constructed nationhood thus often find themselves on the receiving end of policies which directly or indirectly force their migration. This is of contemporary significance in the postcolonial world given that “some of the world’s regions have not yet finished sorting themselves into independent nation-states.”⁴⁸

The relevance of this critique to the concept of the liberal paradox is the understanding that the extent to which migrants are considered ‘other’ determines how migration is constructed as a specific threat to sovereignty. Indeed, this sentiment recently materialised into policy in Poland, which in spite of its similar ideological stance to that of Hungary, has welcomed significant numbers of predominantly Slavic, Christian refugees from Ukraine fleeing the impact of conflict with Russia.⁴⁹ Ultimately, the state represents an inherently xenophobic construct which sets limits on tolerable levels of homogeneity, meaning that the political element of the liberal paradox relates fundamentally to state nationalism and the process of disassociating the state from otherness.

Monetising Migration: Migrants as Agents of Development

Having assessed the implications of migration for the state as it exists conceptually, this paper will now analyse the relationship between migrants themselves and the state in more tangible terms, first in relation to development. It is necessary to consider

migration in the context of prevailing neoliberal emphasis on the centrality of ‘human capital’—a metaphorical expression of the “commodification of human abilities and an alienating notion of human potential.”⁵⁰ This worldview is an extension of ‘economization’, one of the hallmarks of neoliberalism: the “conversion of non-economic domains, activities and subjects into economic ones—to all spheres of life.”⁵¹ Thus, global migration is constructed by policymakers under the purview of neoliberalism as primarily a function of global economics, in which the educational attainment, prospects, skills, cultural contribution, and family lives of migrants are quantified as economic gains and losses for the sending and receiving states.

The dominance of this neoliberal framing has facilitated short-termism and one-dimensionality within prevailing understandings of migration’s implications for sending and receiving states. Current understandings are predicated on a ‘zero-sum’ view, whereby increased engagement with one country leads to decreased engagement with the other or a side-by-side relationship of coexistence where engagement with one state has no impact on the other.⁵² This has resulted in discursive emphasis being placed on such outcomes as the benefits of cheap labour for receiving states and the costs of brain drain for sending states, neglecting the principle of simultaneity so central to transnationalism.⁵³

Once it is understood that the relationship between sending and receiving states is inextricably linked, a more complex understanding of migratory implications emerges; for example, long-term, significant ‘brain gain’ for sending states, stimulated by the “counterflow of remittances, investments, trade relations, new knowledge, innovations, attitudes and information.”⁵⁴ The most obvious impact of migrants to sending states’ development is financial, with remittances constituting a significant portion of GDP for many major sending states. These remittances are often crucial to the establishment and growth of infrastructural, social, health, and educational institutions, whilst also stimulating the economic activity of individual and communal ‘stay-behinds.’⁵⁵ As such, migrants can very much be understood as active agents of development.

However, migration in and of itself is no panacea for underdevelopment, and the impact of remittances is largely dependent upon the pre-existing development conditions in sending states. De Haas also notes that ‘apocalyptic scenarios of a massive influx

of migrants' are based on the myth that "poverty and misery are the root causes of migration,"⁵⁶ undermining the significance of relative deprivation. Certain levels of socioeconomic development are required to sustain emigration, given the costs, risks, knowledge, and social networks associated with cross-border movement across the international state system.

The significance of this fact is that, although migration and poverty are often discussed in conjunction, the role of migration in relation to development applies primarily to developing states which are not amongst the least developed. Thus, although migration has tangible implications in facilitating development for states which have already attained a certain level of economic parity, the econocentric structuring of migration in the international system of states (with emphasis on the economic value of migrants) arguably entrenches global inequality and absolute poverty in the least developed countries. This exemplifies the complex nature of migratory implications for states, with significant nuances even between states which are often talked of in generalised terms as 'developing countries.'

The lack of acknowledgment of simultaneity, and the centrality of the zero-sum perspective in migration debates, has also impacted how receiving states view migrants as development agents. As a reflection of the predominantly neoliberal framing of global migration, Dutch politicians in 2002 campaigned against the investments of migrants in their countries of origin, perceiving them as a 'disappearance' of income from the Netherlands and a barrier to successful integration.⁵⁷ However, this assumption is based on the myth that financial and social loyalty to sending states must necessarily be in conflict with good citizenship in host states. This idea is debunked when considering the concurrent entrepreneurial, political, and social engagements that migrants exhibit in both sending and receiving states as part of a simultaneously reinforcing transnationalism.⁵⁸

Although such economic simultaneity is often viewed from liberal perspectives as a reinforcing, positive phenomenon, insights have been provided into the coercive significance of 'migration interdependence,' through which a host state can leverage a sending state's economic dependence on migration for its own politically-motivated ends.⁵⁹ This form of interdependence, particularly between liberal and non-liberal states, also challenges the universal applicability of the 'liberal paradox.' Tsourapas recently

makes the case that for many non-liberal sending states in the Global South, migration in fact induces an ‘illiberal paradox,’ with contradictory imperatives arising from political and economic considerations.⁶⁰ In cases where the state does not anticipate economic benefit from transnational mobility, it will be more likely to securitise its emigration policy, and in cases where migration represents a powerful economic force, the state will more likely securitise its diaspora policy.⁶¹ As will be explored in the following section, simultaneous transnationalism is especially significant, as it has significant implications for the state’s role as sovereign authority over the population within its borders.

Subversive Transnationalism: Diasporas and the Shifting Nature of State Boundaries and Authority

Having discussed the implications for states from first a broadly conceptual and then broadly economic standpoint, this paper will now focus upon the implications of the state’s role as sovereign authority over its population. It will be demonstrated that the multi-layered transnationalism of diaspora populations has effectively resulted in a symbolic and conceptual shifting of borders with considerable implications for governmentality.

Foucault’s concept of ‘governmentality’ is generally equated with governments’ work to produce a citizenry whose mentalities and behaviours are in line with its policies.⁶² Relating this back to the constitutive dimensions of statehood, the legitimacy of state governmentality stems from the state’s role as direct sovereign authority over the population within its territory. Diasporas, therefore, have come to represent the paradigmatic ‘other’ of the nation state, simultaneously distinguished as independent actors that actively influence their homeland and also subjects for which states must find new ways to secure coercion.⁶³

Diasporic political activism is generally expressed via the same activities as domestic activism: the production of literature, journalism, NGOs, and engagement with opposition parties and movements.⁶⁴ However, diasporic political engagement creates new and distinct implications for states, given diaspora communities’ unique agency as actors operating both within and outside the confines of the state. Diasporic voices of dissent are also often amplified in liberal states, free from many of the political and physical constraints which stifle opposition movements in their

home states.⁶⁵ This has profound repercussions for non-liberal sending states, who find their conventional expressions of governmentality considerably undermined.

In the 1970s, the Moroccan state initiated a series of policy measures which sought to reinforce 'the boundaries of the national community by insisting upon the economic, political, and cultural 'Moroccanness' of its diaspora.⁶⁶ The move was triggered by domestic political developments in France, labour union activism, and student rebellion, all of which challenged the allegiance of the Moroccan diaspora to the sovereign rule of its monarchy. The Moroccan state's attempts to bureaucratically maintain sovereignty over its citizens were centred around the formation of 'widdadiyat', or friendship societies, whose official purpose was to establish and centralise bodies concerned with the social welfare of Moroccan emigrants and their families, but whose broader objective was to maintain tenable levels of control and authority over its citizens abroad.⁶⁷

In appropriating and centralising the offering of a range of benefits and amenities, such as access to practical information, language classes, and social activities, the Moroccan state extended its influence and authority abroad. Policies of monitoring, infiltration, and intimidation enabled the coercion of its diaspora communities.⁶⁸ Whilst this case represents state policies responding to diasporic activity, nations such as the Philippines have introduced pre-emptive measures to maintain social order by ensuring economic and political fealty to the state from its overseas citizens.⁶⁹ The Philippines has progressively institutionalised the export of large numbers of nursing and domestic workers. The Filipino state, in conjunction with the Catholic Church, works to remind female migrants in particular "of their (financial) responsibilities towards their family members left behind' whilst exhorting them 'to be faithful to their country."⁷⁰

Laffey and Nadarajah further develop the premise of 'shifting borders' by exploring how diasporas' forging of transnational security linkages between sending and receiving states provoke security and governmentality implications for host states and the liberal order itself.⁷¹ In their critical juxtaposition of Tamil diaspora activism with the pursuit of liberal peace in Sri Lanka, they frame the role of the Liberation Tigers of Tamil Eelam (LTTE) in the civil conflict as a driver of ethno-nationalist separatism and thus antithetical to the liberal peace objective of a unified liberal

market democracy. The “discursive separation between the LTTE and ‘the Tamils’ inherent to liberal peace interventions in Sri Lanka” was also applied to diaspora actors, with members of the Tamil diaspora categorised in binary terms as either ‘supporters’ or ‘opponents’ of the LTTE, and thus by default either ‘extremists’ or ‘moderates.’⁷² This construction of the Tamil diaspora thus served to “reproduce the hybridity of liberal peace,”⁷³ whilst encapsulating the border-shifting function of transnational networks.

This synthesis between liberal and non-liberal spaces resulted in the UK determining the limits of the Tamil diaspora’s agency “to a great extent by international relations with *Sri Lanka* – rather than, as might be assumed, the other way round.”⁷⁴ The implications for host state policy were manifest in the UK’s echoing of the Sri Lankan policy narrative in relation to the LTTE. This resulted in such measures as increased surveillance, restrictions on police permissions, arrests, and even covert constraints outside the boundaries of conventional legal frameworks.⁷⁵ Practices of transnational security governance had effectively served to “reproduce diaspora as hybrid subjects.”⁷⁶ again serving to emphasise simultaneous transnationalism as a defining feature of migration, and the reinforcing relationships forged between states involved in the migratory process.

Construction of distinctly transnational populations via the migratory process has effectively transformed the border into what Arnold and Pickles astutely describe as “a complex network of social relations that extend well beyond actual state boundaries and operate at multiple scales.”⁷⁷

Conclusion

This paper has produced a critical overview of the direct links between the political implications of migration and the ‘triumvirate of rights’ afforded to states under international law. Amidst the driving forces of globalism and simultaneous transnationalism, migrants possess the capacity to undermine territorial integrity, subvert the principle of sovereign rule, and bring into question the notion of political independence. However, migration also serves as a poignant reminder that despite the perceived sovereignty and complete autonomy of the state in international relations, nations do not operate in a vacuum. Under the prevailing liberal order guided by globalist ideals, migration is first and fore-

most a consequence of powerful economic forces, reflected in the function of migration to offload surplus populations, maintain a constant supply of labour, and manoeuvring development.

Thus, this interplay between globalisation and the international system of states has resulted in migration encapsulating conflict between powerful economic and political forces with significant and evolving implications for the state while amplifying ideological divisions and exposing paradoxes in the liberal world order. As states choose to navigate these contradictions through increasingly divergent means, it becomes progressively clear that specific types of governmental approaches to migration will always be defined by distinct problem constructions and policy narratives. Ultimately, the perceived centrality of the state's role as sovereign authority over territories and populations has considerably guided how implications of migration are identified and understood. This premise must be effectively critiqued in order to develop more cohesive understandings of state responses to migration.

Notes

- 1 John M. Hobson, *The State and International Relations* (Cambridge: Cambridge University Press, 2000), 15.
- 2 James F. Hollifield, "The Emerging Migration State," *International Migration Review* 38, no. 3 (2006): 885-912, 887.
- 3 Paul R. Williams "What Makes a State? Territory," *Proceedings of the Annual Meeting (American Society of International Law)* 106 (2012): 449-450, 449.
- 4 Hollifield, "The Emerging," 888.
- 5 Iris M. Young, "The Logic of Masculinist Protection: Reflections on the Current Security State," *Women and Citizenship* 29, no.1 (2003): 15-34, 15.
- 6 Richard N. Rosecrance, *The Rise of the Trading State: Commerce and Conquest in the Modern World* (New York: Basic Books, 1986).
- 7 Ernest J. Wilson, "Hard Power, Soft Power, Smart Power," *The Annals of the American Academy of Political and Social Science* 616, no. 1 (2008): 110-124, 110.
- 8 Hollifield, "The Emerging," 888.
- 9 *Ibid.*, 886.
- 10 Jef Huysmans, "The European Union and the Securitization of Migration," *JCMS: Journal of Common Market Studies* 38, no. 5 (2000): 751-777.
- 11 Myron Weiner, "On International Migration and International Relations," *Population and Development Review* 11, no. 3 (1985): 441-455, 441.
- 12 Weiner, "On International," 442.
- 13 *Ibid.*, 443-444.
- 14 Michael S. Teitelbaum, "The Role of the State in International Migration,"

- Brown Journal of World Affairs 8, (2002): 157-167, 157.
- 15 Teitelbaum, "The Role," 158.
- 16 Ibid., 166.
- 17 Aristide R. Zolberg, "Changing Sovereignty Games and International Migration," *Indiana Journal of Global Legal Studies* 2, no. 1 (1994): 153-170, 153-154.
- 18 Fiona B. Adamson, Triadafilos Triadafilopoulos, and Aristide R. Zolberg. "The Limits of the Liberal State: Migration, Identity and Belonging in Europe," *Journal of Ethnic and Migration Studies* 37, no. 6 (2011): 843-59, 843.
- 19 Ibid., 843-59.
- 20 Fiona B. Adamson, "Crossing Borders: International Migration and National Security," *International Security* 31, no. 1 (2006): 165-199, 167.
- 21 Adamson, "Crossing Borders," 175.
- 22 Ibid., 176.
- 23 Andreas Wimmer and Nina Glick Schiller, "Methodological Nationalism and Beyond: Nation-state Building, Migration and the Social Sciences," *Global Networks* 2, no. 4 (2002): 301-334, 302.
- 24 Young, "The Logic of Masculinist Protection," 17.
- 25 Gabriella Elgenius, *Symbols of Nations and Nationalism: Celebrating Nationhood* (Basingstoke: Palgrave Macmillan, 2011).
- 26 Rey Koslowski, *Migrants and Citizens: Demographic Change in the European State System* (Ithaca, NY: Cornell University Press, 2000), 38.
- 27 Hollifield, "The Emerging," 887.
- 28 Marla A. Ramirez, "The Making of Mexican Illegality: Immigration Exclusions Based on Race, Class Status, and Gender," *New Political Science*, 2018, 1-19.
- 29 Hein De Haas, "International Migration, Remittances and Development: Myths and Facts," *Third World Quarterly* 26, no. 8 (2005): 1269-1284, 1270.
- 30 Ibid.
- 31 Cathrine Thorleifsson, "Disposable Strangers: Far-right Securitisation of Forced Migration in Hungary," *Social Anthropology* 25, no. 3 (2017): 318-334, 318.
- 32 Nick Thorpe, "The Man Who Thinks Europe Has Been Invaded," *BBC News*, April 6, 2018.
- 33 Ibid.
- 34 Thorleifsson, "Disposable Strangers," 320.
- 35 Ibid., 328.
- 36 Ibid., 323.
- 37 Attila Agh, "The Decline of Democracy in East-Central Europe. Hungary as the Worst-Case Scenario," *Problems of Post-Communism* 63, no. 5-6 (2016): 277-287.
- 38 Thorleifsson, "Disposable Strangers," 322.
- 39 Peter Stalker, "Migration Trends and Migration Policy in Europe," *International Migration* 40, no. 5 (2002): 151-179.
- 40 Sabine V. Dirke, "Multikulti: The German Debate on Multiculturalism," *German Studies Review* 17, no. 3 (1994): 513-536.
- 41 Rüdiger Schmitt-Beck, "The 'Alternative Für Deutschland in the Electorate': Between Single-Issue and Right-Wing Populist Party," *German Politics* 26, no. 1 (2016): 124-148.
- 42 Thorpe, "The Man."
- 43 Ruud Koopmans and Paul Statham. "Challenging the Liberal Nation-State? Postnationalism, Multiculturalism, and the Collective Claims Making of Mi-

- grants and Ethnic Minorities in Britain and Germany," *American Journal of Sociology* 105, no. 3 (1999): 652-696, 652.
- 44 Sean R. Roberts, "The Biopolitics Of China's "War on Terror" and the Exclusion Of The Uyghurs," *Critical Asian Studies* 50, no. 2 (2018): 232-258.
- 45 Victoria Terhune and Jonathan Matusitz. "The Uighurs Versus the Chinese Government: An Application of Realistic Conflict Theory," *Journal of Applied Security Research* 11, no. 2 (2016): 139-148.
- 46 Anthony Howell and C. Cindy Fan. "Migration and Inequality in Xinjiang: A Survey of Han and Uyghur Migrants in Urumqi," *Eurasian Geography and Economics* 52, no. 1 (2011): 119-139, 119.
- 47 Aristide R. Zolberg, "The Formation of New States as a Refugee-Generating Process," *The Annals of the American Academy of Political and Social Science* 467, no. 1 (1983): 24-38.
- 48 Zolberg, "The Formation," 38. For further critique on the role of migration in state building processes, see also: Audie Klotz, *Migration and National Identity in South Africa, 1860-2010* (New York: Cambridge University Press, 2015).
- 49 Evon Huber, "Poland Weighs Benefits of Surge in Migrants from Ukraine," *Financial Times*, May 28, 2017
- 50 Marnie Holborow, "Neoliberalism, Human Capital and the Skills Agenda in Higher Education—The Irish Case," *Journal for Critical Education Policy Studies* 10, no. 1 (2012): 93-111, 93.
- 51 Wendy Brown, "Sacrificial Citizenship: Neoliberalism, Human Capital, and Austerity Politics," *Constellations* 23, no. 1 (2016): 3-14, 3.
- 52 Takeyuki Tsuda, "Whatever Happened to Simultaneity? Transnational Migration Theory and Dual Engagement in Sending and Receiving Countries," *Journal of Ethnic and Migration Studies* 38, no. 4 (2012): 631-649.
- 53 *Ibid.*, 632-634.
- 54 De Haas, "International Migration," 1272.
- 55 Thomas Faist, "Migrants as Transnational Development Agents: An Inquiry into the Newest Round of the Migration–Development Nexus," *Population, Space and Place* 14, no. 1 (2007): 21-42.
- 56 De Haas, "International Migration," 1271.
- 57 *Ibid.*, 1275.
- 58 Tsuda, "Whatever Happened," 631-649.
- 59 Gerasimos Tsourapas, "Labor Migrants as Political Leverage: Migration Interdependence and Coercion in the Mediterranean," *International Studies Quarterly* 62, no. 2 (2018): 383-395.
- 60 Gerasimos Tsourapas, "The Long Arm of the Arab State," *Ethnic and Racial Studies*, (2019): 1-20.
- 61 Tsourapas, "The Long," 1-20.
- 62 Thomas Lemke, "Foucault, Governmentality, and Critique," *Rethinking Marxism* 14, no. 3 (2002): 49-64.
- 63 Khachig Tölölyan, "The Nation-State and Its Others: In Lieu of a Preface," *Diaspora: A Journal of Transnational Studies* 1, no. 1 (1991): 3-7.
- 64 Laurie A. Brand, *Citizens Abroad: Emigration and the State in the Middle East and North Africa* (Cambridge: Cambridge University Press, 2008), 24-45.
- 65 *Ibid.*
- 66 Brand, *Citizens Abroad*, 46.
- 67 *Ibid.*, 71.
- 68 *Ibid.*, 72.

69 Helma Lutz, "Gender in the Migratory Process," *Journal of Ethnic and Migration Studies* 36, no. 10 (2010): 1647-1663, 1656.

70 Ibid.

71 Mark Laffey and Suthaharan Nadarajah, "The Hybridity of Liberal Peace: States, Diasporas and Insecurity," *Security Dialogue* 43, no. 5 (2012): 403-420

72 Ibid., 414.

73 Ibid., 416.

74 Ibid., 413.

75 Ibid., 414.

76 Ibid., 405.

77 Dennis Arnold and John Pickles, "Global Work, Surplus Labor, and the Precarious Economies of the Border," *Antipode* 43, no. 5 (2011): 1598-1624, 1599.

CHINA, THE BELT AND ROAD INITIATIVE, AND THE HAMBANTOTA PORT PROJECT

Shantanu Roy-Chaudhury, University of Oxford

Abstract

This paper examines the Hambantota Port project in Sri Lanka in the context of China's Belt and Road Initiative (BRI). It discusses the growing geo-economic importance of the Indian Ocean and how China's dependence on energy resources has led to the so-called Malacca Dilemma and forced China to manoeuvre around this constraint. Following a discussion of Sri Lanka's geo-strategic importance, the article considers the country's role in the broader BRI and how major Chinese projects and investments in Sri Lanka have extended Beijing's reach into the Indian Ocean. The article focuses in on China's investments in the Hambantota Port and describes how Sri Lanka's inability to repay its debt led it to lease the port to the Chinese for ninety-nine years. Overall, it argues that China's growing investments will negatively impact Sri Lanka in the long run, having already left the country deeply in debt. Finally, the article reflects on the affair's implications for both Sri Lanka's future as well as that of its neighbour, India, which has found China's growing footprint in Sri Lanka deeply disquieting.

Introduction

China's international economic role and success—increasingly the focal point of world politics—has been most noticeable in the Asia-Pacific region, the global economy's centre of gravity.¹ The Belt and Road Initiative (BRI), which was announced by Chinese President Xi Jinping in 2013, has significantly boosted China's external economic engagements around the world. BRI has been said to entail

a series of overland roads, pipelines, railways,
and other infrastructure through Central Asia,
South Asia, and the Middle East to Europe [and]
a series of ports and maritime trade routes
through the South China Sea and the Indian

Shantanu Roy-Chaudhury, "China, the Belt and Road Initiative, and the Hambantota Port Project," *St Antony's International Review* 15. no. 1 (2019): 153-164.

It took nearly two years for BRI's full scope to come into focus: in 2015, a blueprint was released, and the initiative incorporated into the Chinese government's Thirteenth Five-Year Plan. Slightly more than a year later, Xi declared that fifty-seven countries had become active participants in the initiative, with thirty formally concluding BRI cooperation deals.³

Since then, China has successfully initiated projects in many more countries in Europe, Asia, and Africa; it is now seeking to extend its reach to Latin America. According to the World Bank, BRI aims to strengthen infrastructure, trade, and investment links between China and some sixty-five other countries accounting collectively for more than thirty percent of global GDP, sixty-two percent of the world's population, and seventy-five percent of its known energy reserves. As one analyst writes, "President Xi Jinping has dramatically reshaped China's presence and power on the world stage, touting a 'new model' for developing countries to follow and advocating a 'new type of international relations.'"⁴ According to an American Enterprise Institute study, the total combined value of China's overseas investment and construction is approaching \$1.9 trillion (USD).⁵

China's rise has seen the country aggressively expand its presence in South Asia, where India has viewed China's growing footprint through the lens of southern neighbour Sri Lanka, an important BRI player and the recipient of billions of dollars' worth of investment from China. This article examines China's increasing presence in Sri Lanka with a focus on the Hambantota Port project, China's largest project in Sri Lanka and a major national security concern for India, whose coast is located barely 160 kilometres from Sri Lanka. Unable to repay its massive debt to China, Sri Lanka opted to cede majority control of the port to Beijing, eventually leasing it and 15,000 acres of surrounding land—and with them Mattala Rajapaksa International Airport—for ninety-nine years. I argue that growing Chinese investments will negatively impact Sri Lanka in the long run.

The following paper is divided into four sections. The first two sections will provide background on the following: the growing geoeconomic importance of the Indian Ocean and how China's dependence on energy resources flowing through it has produced the so-called Malacca Dilemma, around which Beijing seeks to manoeuvre; and Sri Lanka's geostrategic importance, its role in the BRI, and major Chinese projects in the island nation. The third section describes Chinese investments in Hambantota Port and

recounts how it came to be leased to the Chinese for ninety-nine years. The final section considers the affair's implications for Sri Lanka's future—and India's.

The Geoeconomic Significance of the Indian Ocean

China's rise during the last decade has drawn the attention of foreign observers to the Indian Ocean, which is extremely important to India and China given its status as the world's third-largest body of water, its connectivity, and the volume of trade and amount of energy resources that pass through it. 9.84 billion tonnes of commercial goods are transported annually by nearly 90,000 vessels, along with forty percent of the world's oil supply and sixty-four percent of its oil trade.⁶ Running through it are critical maritime trade routes that connect the Middle East, Africa, and South Asia to the broader Asian continent to the east and Europe to the west.⁷

China's impressive expansion has led it to India's doorstep. BRI in particular has strengthened China's investments and its ambitions to not only connect global markets but also, and more importantly, ensure the safe passage of energy resources from the Middle East and avoid the Malacca Dilemma, a major concern for the Chinese government. In China's view, "[a]ny disruption to the free flow of energy resources into China could derail the economic growth on which the Chinese government depends to shore-up its legitimacy and pursue its great power ambitions,"⁸ making its heavy use of, and dependence on, the narrow Malacca Strait a serious vulnerability. Beijing has consequently sought out alternatives to the strait, especially amid American scrutiny of its projects and aspirations.

The Role of Sri Lanka

As one such alternative, BRI's Maritime Silk Road (MSR) component entails the construction of "enormous amounts of hard infrastructure such as high-speed railways, highways and truck roads, air and sea ports, utility stations and power grids, oil and natural gas pipelines and telecommunication networks."⁹ Although Sri Lanka is just one of many countries participating in the MSR, its strategic position between the Indian Ocean's east-west shipping routes makes it an essential part of the initiative: millions of dollars' worth of cargo and energy resources pass between Southeast Asia's Strait of Malacca and the Middle East's Hormuz and Bab el-Mandeb straits. The island nation "has the capacity to be a regional industrial hub to tap into the emerging economies in

the region,” regional observers have pointed out.¹⁰

Although the Malacca Dilemma is not the only reason why the Chinese are interested in Sri Lanka, it dovetails with China’s larger objectives and global ambitions. Indeed, Beijing has remained interested in Hambantota despite the negative coverage it has received for the weak performance of its port and the frequency with which the port’s financial viability has been questioned, fueling the impression that Hambantota only serves China’s broader strategic interests of securing crucial trade routes and protecting international supply chains from disruption.¹¹ Since 2005, China has invested in numerous projects in the country and become the leading source of official development assistance to, and foreign direct investment (FDI) in, Sri Lanka: its share of FDI increased from just under one percent (\$16.4 million) in 2005 to thirty-five percent (\$338 million) in 2015.¹² One of the largest of these ventures is the Hambantota Port development project—China has leased the port for ninety-nine years, and the Colombo Port City project.

The port, in particular, has greatly worried India due to the possibility of its use as a naval base by China, which Sri Lanka has long considered an indispensable partner. Well before BRI, Sri Lanka received from China arms and ammunition along with diplomatic cover at the UN Security Council, where Beijing kept human rights abuses in Sri Lanka off the agenda during the country’s bloody civil war from 1983 to 2009.¹³ Bilateral relations and investments have flourished since that time, and major Chinese projects in Sri Lanka other than Hambantota Port and Colombo Port City today include the rehabilitation of roads in the country’s north (\$302 million); the Greater Kurunegala water supply and sewerage project (seventy-nine million dollars); the Norochcholai coal power plant (\$891 million); the Nagananda International Institute for Buddhist Studies in Colombo (one hundred million dollars); the Colombo–Katunayake Expressway (\$104 million); the Broadlands hydropower project (\$69 million); the Colombo Lotus Tower (\$104 million); the Moragahakanda–Kalu Ganga project (\$214 million); Mattala Rajapaksa International Airport in Mattala (\$292 million); the Southern Expressway (\$1.26 billion); and, finally, the extension of the Southern Railway (\$278 million).¹⁴

In July 2018, Sri Lanka received a gift of \$295 million from China, to be utilized for any project; it was spent on the building of a kidney hospital in Polonnaruwa, a characteristically large sum contributed in a characteristically opaque manner.¹⁵ It came amid heavy criticism of a Chinese firm alleged to have financed the 2015 campaign of former President Mahinda Rajapaksa, and can be understood as an attempt by China to cosy up to the administration

of President Maithripala Sirisena, who has been widely viewed as more pro-Indian, pro-Western, and less China-friendly than his predecessor.¹⁶

Chinese Investments in Hambantota

Hambantota is the Hambantota District's main town; the district is located in Sri Lanka's Southern Province. Since the 2004 Indian Ocean tsunami, by which it was severely affected, the district has undergone several development projects. Under Rajapaksa, a native of this region, Sri Lanka's government sought to turn Hambantota into a major hub second only to Colombo, the capital city. The Hambantota Port is one of four ports being developed in Sri Lanka to boost the country's economy and enhance trade. Apart from its proximity to international shipping lanes, the Hambantota Port's construction is intended to reduce traffic at Sri Lanka's main port in Colombo, which handles 6,000 ships annually and does not have sufficient capacity for increased maritime traffic. Moreover, the China Communication Construction Company (CCCC) promised the creation of 83,000 new jobs through this investment,¹⁷ fuelling the Sri Lankan government's hopes that the port would, among other things, reduce poverty in the country's south and in doing so address the regional economic imbalance.

Far from novel, the idea of developing a Hambantota port had been floated for many years yet rejected by successive governments, which questioned its economic viability. As one news report recounted, "It was only when an individual named Ariya Wickramanayake funded his own research into the port's potential, and presented it to Rajapaksa, back then a minister, that the idea took hold."¹⁸ When Rajapaksa came into power in 2005, the project gained momentum. Although India initially offered to collaborate with Sri Lanka, New Delhi's concerns about the project's economic viability won out in the end, and the project was awarded to China in a move that was widely seen as an attempt by Sri Lanka to cement good relations between the two countries, according to a US diplomatic cable released by WikiLeaks.¹⁹

The construction of the Hambantota Port project involves three stages. Construction of the first phase started in 2008 and was completed in November 2010 with an investment of approximately \$361 million and as a joint venture of Sinohydro and the China Harbour Engineering Company (CHEC). Eighty-five percent of funding came from China's Export-Import Bank through a loan at 6.3 percent interest; fifteen percent came from the Sri Lanka Ports Authority. Sinohydro is a Chinese state-owned hydropower

and engineering company that specialises in, among other things, architectural projects and electric power investments. It invests and provides project financing, consultation, and construction services, and has projects around the world, from a power plant in Pakistan to a dam in Honduras. CHEC is an engineering contractor and subsidiary of CCCC, which focuses on infrastructure construction, including marine engineering, dredging, and reclamation. As the world's second-largest dredging company, CHEC is active in Asia, Africa, and Europe.

The Export-Import Bank, for its part, is a state-funded and -owned policy bank dedicated to supporting China's foreign trade, investment, and international economic cooperation. According to its website, "the Bank plays a crucial role in promoting steady economic growth and structural adjustment, supporting foreign trade, and implementing the 'going global' strategy."²⁰ As the *New York Times* reported in 2018, "to obtain the loan [from the Export-Import Bank], Sri Lanka was required to accept Beijing's preferred company, China Harbor, as the port's builder,"²¹ leaving the island nation with little choice in the matter. This first phase also involved the construction of shipbuilding, bunkering, crew-changing, and ship repair facilities. Furthermore, two breakwaters, a 600-metre turning circle, a 600-metre general purpose berth, a 610-metre oil quay, a 105-metre service berth, roads, and associated buildings were constructed, a 210-metre-wide entrance channel dredged, and a seventeen-metre-deep basin area excavated.²²

Construction of the second phase started in 2012, soon after the completion of the first phase. At first it was slightly delayed by a huge rock whose presence at the entrance of the harbour prevented vessels from entering before it was forcibly removed at a cost of forty million dollars. This phase—also financed by the Export-Import Bank—cost \$810 million and was developed by CCCC. CCCC is also a multinational engineering and construction company; it is primarily engaged in the design, construction, and operation of infrastructure assets. According to plans, this phase is subdivided into three additional stages. The first stage involves the construction of a 2,140-metre-long quay wall accommodating four 100,000-tonne and two 10,000-tonne wharf berths; the second stage the development a 50-hectare offshore artificial island with an elevation of eight metres; and the final stage the construction of a 300-metre-long and seventeen-metre-deep oil container terminal, four 100,000 tonnes deadweight (DWT) container berths, one 100,000 DWT oil wharf, and two 30,000 DWT feeder berths. Furthermore, 400,000 square metres of roads, a 490,000-square metre harbour basin, and sixty hectares of yard area with associated yard handling equipment would be developed.²³ This phase is

still in progress.

The project's third phase is expected to be completed by 2023 and will involve the addition of a dockyard. Moreover, an investment of \$550 million will see a tax-free zone established for ship-building, repairing, and warehousing.²⁴ Once completed, the port will occupy 4,000 acres of land and be the largest in South Asia, with the capability to accommodate thirty-three vessels at a time.

China has also invested heavily in Mattala Rajapaksa International Airport, one of two international airports in Sri Lanka. Construction began in 2009, and the airport was opened in 2013. The project, which cost the Sri Lankan government \$209 million, with a \$190 million loan issued by the Export-Import Bank,²⁵ has been dubbed a 'white elephant'²⁶—an investment project with a negative social surplus²⁷—and hailed as the world's emptiest airport²⁸ due to a lack of flights.

Sri Lankan Debt and the Transfer of the Port

What may initially seem like a straightforward development project is, in fact, complicated by the nature of Chinese investments and Rajapaksa's Chinese ties, factors making possible the port's eventual use by the Chinese Navy. The stated rationale for building the port has been questioned from the start. According to the *New York Times*, "officials questioned the wisdom of a second major port, in a country a quarter the size of Britain and with a population of 22 million, when the main port in the capital was thriving and had room to expand." Furthermore, "[f]easibility studies commissioned by the government had starkly concluded that a port at Hambantota was not economically viable."²⁹

Nonetheless, the project was pushed through by Rajapaksa, and Sri Lankan debt to China began to grow in what many consider a prime example of debt diplomacy,³⁰ whereby a creditor country intentionally extends excessive credit to a debtor country with the intention of extracting economic or political concessions from the latter once it becomes unable to honour its debt obligations. Indeed, Beijing's willingness to provide loans near or at market rate, with minimal conditions attached, has made Chinese loans exceedingly attractive in many parts of the world.³¹ By contrast, for decades, Western countries offered developing countries high interest market rate loans, a strategy that misfired when the latter failed to repay the interest acquired. Developing countries have also tended to prefer Chinese bailouts to International Monetary Fund (IMF) ones.³²

When China "revised its loan interest rates from 1–2% floating to 6.3%, it became clear Hambantota was more than just an

investment opportunity for China.”³³ It was also found that during the 2015 elections, “large payments from the Chinese port construction fund flowed directly to campaign aides and activities for Mr. Rajapaksa, who had agreed to Chinese terms at every turn and was seen as an important ally in China’s efforts to tilt influence away from India in South Asia.”³⁴

Sri Lanka is one of many “smaller countries [that] have found themselves owing debts they cannot pay” amid a growing Chinese footprint in the Indian Ocean.³⁵ Facing mounting debt, Sri Lanka formally transferred 80 percent of the port’s ownership to the China Merchant Port Holding Company (CMPHC) in December 2017, leasing it and 15,000 acres of surrounding land for ninety-nine years. Critics of Sri Lanka’s government have charged it with threatening the country’s sovereignty, and say that its dealings with China recall a time when the country was colonised and subjugated by major powers. Indeed, in 2018, the government was set to repay an estimated \$12.68 billion in debt to the likes of China, Japan, the World Bank, and the IMF.³⁶ Sri Lanka also owed more than \$8 billion to various state-controlled Chinese firms; valued at \$1.1 billion, the Hambantota Port deal was necessary to reduce Sri Lanka’s debt burden.

Furthermore, once the debt began to rise, “Sri Lankan officials became desperate to get the debt off their books” and “the Chinese demands centered on handing over equity in the port rather than allowing any easing of terms.”³⁷ Although Rajapaksa was voted out of office in 2015, Sri Lanka’s new government, which had threatened to cancel numerous Chinese projects and reduce the country’s dependence on China if elected, quickly realised that its options were few amid growing debt. Still, it reconsidered some deals and halted the construction of many projects, delaying revenues that could have been generated, and made it even more difficult to service loans.

With the suspension of the Port City project in Colombo costing the CCC \$380,000 per day, demands were made for \$125 million to compensate the delaying of the project for more than a year.³⁸ With the debt piling up and increasing pressures, the Sri Lankan government had no choice but to hand over the Hambantota Port, first doing so during a 2014 visit to Sri Lanka by Xi that saw his Sri Lankan counterpart quietly grant Chinese firms operating rights to four of the seven container berths at Hambantota on a thirty-five-year lease.³⁹ This, after a year in which Hambantota had fewer than a hundred vessels berth and the Sri Lankan government spent thirty million dollars on the interest alone. The entire port along with 15,000 acres of land around it was formally handed over for 99 years due to Sri Lanka’s struggle to pay its

debts to Chinese firms.⁴⁰

Sri Lanka's situation highlights the dire consequences a debt trap can have for a country. Despite having handed over the port to China, Sri Lanka remains mired in massive debt, an extremely precarious position. Should Sri Lanka fail to service Chinese loans, Hambantota may turn out to be just the first of many Chinese takeovers there. To further complicate matters, only select passages from the Hambantota agreement have been disclosed, with the Sri Lankan government reluctant to share the document with Parliament.⁴¹ Already, voices in the country have spoken out against the giving away of Sri Lankan land to China.⁴²

In addition to the economic and political implications of China's growing footprint in the country, Chinese projects in Sri Lanka have also had significant social and environmental repercussions that Sri Lanka's government cannot afford to ignore. Chinese projects have led to encroachment on large swathes of agricultural land in the Hambantota region.⁴³ Meanwhile, stretches of highways have cut through key elephant corridors, and elephant habitats have been affected by the construction of Mattala Rajapaksa International Airport, which saw wildlife officials summoned to chase the animals off the runway.⁴⁴

In a regional context, Chinese control of the Hambantota Port has fuelled national security concerns in India, whose government has been a vocal yet lonely critic of BRI from the start. New Delhi refused to send a representative to the 2017 Belt and Road Forum, disquieted by the fact that the China–Pakistan Economic Corridor (CPEC) runs through the territory in Kashmir disputed over by India and Pakistan. China's growing footprint in Sri Lanka has also led to worries that Beijing's projects may double as military assets: already, in November 2014, Chinese submarines docked at the port of Colombo, something that could easily happen again at Hambantota, which may be a naval facility in the making.

Amid reports that China is contemplating gifting a frigate to the Sri Lankan Navy, "it seems clear that a process for the creation of a Chinese naval outpost in India's near-neighbourhood has just begun. Beijing's move creates the grounds for the insertion of PLAN training and support teams at Sri Lanka's naval command, which is bound to result in the positioning of greater Chinese naval assets at the facility," regional observers have said.⁴⁵ "New Delhi feels that this affects its security concerns and also is a violation of the 1978 accord between Sri Lanka and India that promises that neither country will let its ports be used for activities that would affect the other's 'unity, integrity and security.'"⁴⁶

The present article has shown how BRI has unfolded in the

Sri Lankan port of Hambantota. For China, which has sought to extend its reach and avoid the Malacca Dilemma, Sri Lanka is critical to the success of MSR. Given its proximity to the Indian Ocean's sea lanes, if developed, it could become a major hub like Dubai or Singapore. The port of Hambantota, the centrepiece of China's growing footprint in Sri Lanka, is to be built in three phases and expected to be completed in 2023: phase one has already been completed, and phase two is underway. However, the Sri Lankan government has found itself in a bind thanks to the Chinese government's approach to extending loans to the island nation.

The Sri Lankan government has taken on massive debt, allowing China to use debt diplomacy as a means to turn bad loans into strategic investments and convert economic losses into geopolitical gains. The strategic port of Hambantota, leased to China for ninety-nine years, has become a casualty of this practice. Valued at one billion dollars, the port has reduced Sri Lanka's debt to China yet disquieted the government of India, which must be proactive in strengthening its relations with Sri Lanka and ensuring that Colombo does not come too far under China's influence—for its own good.

Notes

1 Avery Goldstein, "A Rising China's Growing Presence: The Challenges of Global Engagement," in *China's Global Engagement*, ed. Jacques deLisle and Avery Goldstein (Brookings Institution Press, 2017), 1-33.

2 Howard J. Shatz, *U.S. International Economic Strategy in a Turbulent World* (Santa Monica: RAND Corporation, 2016), 85-110.

3 Jeff M. Smith, "China's Belt and Road Initiative: Strategic Implications and International Opposition," Heritage Foundation Backgrounder 3331 (2018), accessed December 15, 2018, https://www.heritage.org/sites/default/files/2018-08/BG3331_2.pdf.

4 Guest Blogger for Joshua Kurlantzick, "China Steps Out: Beijing's Major Power Engagement with the Developing World': A Review," Council on Foreign Relations, April 2, 2018, accessed December 11, 2018, <https://www.cfr.org/blog/china-steps-out-beijings-major-power-engagement-developing-world-review>.

5 Derek Scissors, "China Global Investment Tracker," American Enterprise Institute, January 19, 2019, accessed April 23, 2019, <http://www.aei.org/china-global-investment-tracker/>.

6 Dhruva Jaishankar, "Indian Ocean Region: A Pivot for India's Growth," Brookings Institution, September 12, 2016, accessed December 13, 2018, <https://www.brookings.edu/opinions/indian-ocean-region-a-pivot-for-indias-growth/>.

7 Eleanor Albert, "Competition in the Indian Ocean," Council on Foreign Rela-

tions, May 19, 2016, accessed July 10, 2018, <https://www.cfr.org/background-er/competition-indian-ocean>.

8 Ian Storey, "China's 'Malacca Dilemma,'" Jamestown Foundation China Brief 6, no. 8 (2006), accessed November 27, 2018, <https://jamestown.org/program/chinas-malacca-dilemma/>.

9 Jean-Marc F. Blanchard and Colin Flint, "The Geopolitics of China's Maritime Silk Road Initiative," *Geopolitics* 22, no. 2 (2017): 223–245.

10 M. H. Rajesh, *China in the Indian Ocean: One Ocean, Many Strategies* (New Delhi: Pentagon Press, 2018), 275.

11 Iain Marlow, "China's \$1 Billion White Elephant," *Bloomberg*, April 17, 2018, accessed April 23, 2019, <https://www.bloomberg.com/news/articles/2018-04-17/china-s-1-billion-white-elephant-the-port-ships-don-t-use>.

12 Rajiv Bhatia, Kunal Kulkarni, Lina Lee, Shivani Gayakwad, "Chinese Investments in Sri Lanka," *Gateway House*, December 1, 2016, accessed August 25, 2018, <https://www.gatewayhouse.in/chinese-investments-sri-lanka-2/>.

13 Peter Popham, "How Beijing Won Sri Lanka's Civil War," *Independent*, May 23, 2010, accessed March 26, 2019, <https://www.independent.co.uk/news/world/asia/how-beijing-won-sri-lankas-civil-war-1980492.html>.

14 Rajiv Bhatia, Kunal Kulkarni, Lina Lee, Shivani Gayakwad, "Chinese Investments in Sri Lanka."

15 SAM Staff, "Lankan President welcomes US\$295 million 'gift' from Beijing," *Southasian Monitor*, July 23, 2018, accessed April 23, 2019, <https://southasian-monitor.com/2018/07/23/lankan-president-welcomes-us295-million-gift-from-beijing-despite-controversy/>.

16 Maria Abi-Habib, "How China Got Sri Lanka to Cough Up a Port," *New York Times*, June 25, 2018, accessed April 23, 2019, <https://www.nytimes.com/2018/06/25/world/asia/china-sri-lanka-port.html>.

17 Walter Wuthmann, "Port City to Create 83,000 Jobs for Lankans," *Daily News*, May 11, 2018, accessed April 23, 2019, <http://www.dailynews.lk/2018/05/11/local/150637/port-city-create-83000-jobs-lankans>.

18 Ship Technology, "The Story of Hambantota Port: A Flunking Token of Political Corruption," *Ship Technology*, September 18, 2018, accessed November 29, 2018, <https://www.ship-technology.com/features/hambantota-port-china-sri-lanka/>.

19 US Government, "Sri Lanka: Chinese Influence on the Rise," *WikiLeaks*, July 29, 2009, accessed March 26, 2019, https://wikileaks.org/plusd/cables/09COLOMBO745_a.html.

20 Export-Import Bank of China, "Introduction – The Export-Import Bank of China," accessed March 26, 2019, http://english.eximbank.gov.cn/tm/en-TCN/index_617.html.

21 Abi-Habib, "Cough Up a Port."

22 Ship Technology, "Port of Hambantota," accessed March 29, 2019, <https://www.ship-technology.com/projects/port-of-hambantota/>.

23 Ship Technology, "Port of Hambantota."

24 Ibid.

25 Mandana Ismail Abeywickrema, "Concerns Over Mattala Performance," *Sunday Leader*, May 12, 2013, accessed November 30, 2018, <http://www.thesundayleader.lk/2013/05/12/concerns-over-mattala-performance/>.

26 Wade Shepard, "The Story Behind The World's Emptiest International Airport," *Forbes*, May 28, 2016, accessed April 23, 2019, <https://www.forbes.com/>

- sites/wadeshepard/2016/05/28/the-story-behind-the-worlds-emptiest-international-airport-sri-lankas-mattala-rajapaksa/#69adbf417cea.
- 27 James A. Robinson and Ragnar Torvik, "White Elephants," *Journal of Public Economics* 89 (2005): 197–210.
- 28 Shepard, "World's Emptiest International Airport."
- 29 Abi-Habib, "Cough Up a Port."
- 30 Sam Parker, Gabrielle Chefitz, "Debtbook Diplomacy," Policy Analysis Exercise Harvard Kennedy School, March 2018, accessed April 23, 2019, <https://www.belfercenter.org/sites/default/files/files/publication/Debtbook%20Diplomacy%20PDF.pdf>.
- 31 Celia Hatton, "China's Secret Aid Empire Uncovered," BBC News, October 11, 2017, accessed December 11, 2018, <https://www.bbc.com/news/world-asia-china-41564841>.
- 32 Celia Hatton, "Secret Aid Empire."
- 33 Abhijit Singh, "China's Strategic Ambitions Seen in the Hambantota Port in Sri Lanka," Observer Research Foundation, July 27, 2018, accessed March 26, 2019, <https://www.orfonline.org/research/chinas-strategic-ambitions-seen-in-the-hambantota-port-in-sri-lanka/>.
- 34 Abi-Habib, "Cough Up a Port."
- 35 Ibid.
- 36 Shihar Aneez, "Sri Lankan Economy Remains Vulnerable Due to High Debt – IMF," Reuters, March 9, 2018, accessed March 26, 2019, <https://www.reuters.com/article/imf-sri-lanka/update-1-sri-lankan-economy-remains-vulnerable-due-to-high-debt-imf-idUSL4N1QR4UR>.
- 37 Abi-Habib, "Cough Up a Port."
- 38 GCR Staff, "Chinese firm demands compensation for Colombo Port City suspension," *Global Construction Review*, April 8, 2016, accessed April 23, 2019, <http://www.globalconstructionreview.com/news/chinese-firm-demands-compensation-on-colombo-port-city/>.
- 39 Nitin A. Gokhale, "China, India and the Sri Lanka Elections," *The Diplomat*, January 5, 2015, accessed April 23, 2019, <https://thediplomat.com/2015/01/china-india-and-the-sri-lanka-elections/>.
- 40 Kai Schultz, "Sri Lanka, Struggling With Debt, Hands a Major Port to China," *The New York Times*, December 12, 2019, accessed April 23, 2019, <https://www.nytimes.com/2017/12/12/world/asia/sri-lanka-china-port.html?module=inline>.
- 41 Abhijit Singh, "China's Strategic Ambitions."
- 42 Yogita Limaye, "Sri Lanka: A Country Trapped in Debt," BBC News, May 26, 2017, accessed March 26, 2019, <https://www.bbc.co.uk/news/business-40044113>.
- 43 Amantha Perera, "Local Fears Grow Over Chinese Projects in Sri Lanka," *Eco-Business*, November 30, 2018, accessed March 26, 2019, <https://www.eco-business.com/news/local-fears-grow-over-chinese-projects-in-sri-lanka/>.
- 44 Amantha Perera, "Local Fears Grow."
- 45 Gunjan Singh, "Hambantota Port and Indian Security Concerns," *Asia Times*, July 6, 2018, accessed April 23, 2019, <https://cms.ati.ms/2018/07/hambantota-port-and-indian-security-concerns/>.
- 46 Singh, "Indian Security Concerns."

THE TRIAD TRIALS: CONSEQUENCES OF COOPERATION BE- TWEEN CHINESE ORGANIZED CRIMINAL GROUPS AND POLITICAL SOCIETY

Brody Weinrich, Georgetown University

Abstract

In recent decades, Asia has experienced substantial economic growth amidst fundamental changes caused by globalisation. Organized crime has evolved into an enduring transnational problem, as drug and human trafficking, financial crime, and other illicit activities continue to harm impoverished and marginalized populations. Although organized criminal groups in Asia boast a long history that, in the case of the Chinese triads, dates back to the seventeenth century, the twentieth century saw organized criminal groups become profoundly involved in politics. Criminal groups have cooperated with governments on numerous occasions, providing security in ways the latter cannot and helping politicians achieve otherwise unrealistic goals – often through violence. Organized criminal groups have accumulated political capital and influence over time and used them to seize opportunities to invest in both legitimate and ‘grey’ enterprises as part of a larger restructuring effort aimed at capturing the newly-opened Mainland Chinese market’s massive profits and ensuring their survival in the modern world. These new businesses provide a façade of legitimacy, even as organized criminal groups use their extensive, fluid networks to continue their illegal activities. This paper focuses on the Shanghai Green Gangs and the Hong Kong-based triads in its analysis of how political actors have cooperated with criminal gangs, and argues that the political dimensions of triad activity have played a crucial role in Chinese organized criminal groups’ integration in regional as well as transnational crime, to which they are central today.

Introduction and Context: Modern Asian Transnational Crime

Tour agencies in northern Thailand advertise trips to the infamous Golden Triangle, where Myanmar, Laos, and Thailand converge along the Mekong River. The mountains dotting this border region’s landscape are the epicentre of some of the world’s most sophisticated narcotics networks. Since the opening up of China starting in 1978, the Golden Triangle and southern China have become key centres for the mass production of methamphetamines,

Brody Weinrich, “The Triad Trials: Consequences of Cooperation Between Chinese Organized Criminal Groups and Political Society,” *St Antony’s International Review* 15. no. 1, (2019): 165-182.

fentanyl, and other dangerous substances,¹ which complex criminal networks traffic through China and Hong Kong to distribute around the world, netting massive profits in the process.² Gangs use these same networks for wildlife and human trafficking, illegal e-waste disposal, counterfeit medicine production, and other harmful enterprises.

As China and Southeast Asia continue to grow economically, heavy investment in infrastructure linking countries has supplemented free trade agreements with neighbours to promote cross-border trade traffic.³ China's Belt and Road Initiative has prompted multilateral efforts to build stronger international links in road, rail, and related transport infrastructure. However, limited cooperation in developing an integrated security apparatus has left the region's governments woefully underequipped to meet new transnational security challenges.⁴ Amid the prioritisation of raw economic growth, police forces can do little more than maintain order. Harsh policing responses to drug trafficking have been ineffective, as in Rodrigo Duterte's Philippines, where violent crackdowns have simply consolidated criminal groups and created tragic spillover effects that primarily affect civilians.⁵ Innovations in security cooperation have not accompanied economic and infrastructural integration, leaving the region vulnerable to organized crime.

The modern organized criminal group has unique traits that require governments to fundamentally change the way they approach the issue. Long-established criminal groups have merged with regional networks and become more decentralised, looser, and less visible.⁶ More fluid and less rigidly hierarchical in organization, they receive cover from skyrocketing migration numbers and use modern technologies and advanced logistical and operational methods to do business with larger markets that are further away while evading detection. Yet they have maintained their forceful, functional presence, using violence strategically so as to ensure smooth operations. In many cases, so-called red-black networks connect organized criminal groups with corrupt state elements, especially in Chinese local politics.⁷

If policymakers in Asia intend to address these emerging challenges more accurately, they must carefully investigate how criminal networks have become so entrenched in the region. Chinese organized criminal groups represent key twentieth-century players, particularly in Hong Kong, with its role as the gateway to

Mainland China and as an ideological battleground between the Chinese Communist Party (CCP) and the Guomindang (GMD). Said criminal groups have seized opportunities to not only survive but thrive because of two twentieth-century trends. First, organized crime has exploited engagement with politics. Today's organized gangs have proactively involved themselves with politicians and in the political process, and some governments have even reached out to, and offered to cooperate with, organized criminal groups. These interactions provide gangs with social and economic capital and leave them deeply ingrained in society. Second, using this newfound capital, organized criminal groups have initiated what has been called 'professionalisation',⁸ using ill-gotten economic resources and resorting to illegal methods to establish either legal or 'grey' enterprise forcibly in pursuit of legitimacy and new profit pipelines. The harmful effects of these trends in organized crime – from environmental damages and extortion to human trafficking and armed violence – have been largely borne by the region's poor.⁹ In 2015, farmers and unemployed persons accounted for nearly 80 percent of drug-related arrests in China,¹⁰ and while Southeast and East Asia continue to prosper, their neediest fall further behind.

This paper turns to China and Hong Kong to examine how key organized criminal networks have evolved. China and Hong Kong have long been central to transnational crime in Asia. After the conclusion of the Chinese Civil War in 1949, the ideological struggle between the CCP and GMD persisted in Hong Kong, home to the increasingly powerful triads. This paper examines how Chinese triads and related groups have uniquely interacted with and utilized the political arena to build influence as well as how they have used this capital to legitimize themselves and deeply integrate themselves into society's mainstream. This paper argues that although triads and related groups served important short-term functions for state elements, the former's engagement with political bodies compromised the latter's ability to eradicate these criminal networks and directly enabled gangs to effectively legitimize themselves and frame their operations as integral, functional components of society. This analytical account provides those policymakers hoping to combat the enduring transnational criminal networks we see in the region today with critical context.

With a history that sometimes overlaps with mythology, today's organized criminal groups in China originate from centuries-old secret societies. The Chinese triads were preceded by the seventeenth-century Hung Mun, a secret society of 'blood brothers' with explicit political goals.¹¹ The Hung Mun (unsuccessfully) attempted to overthrow the Qing dynasty and restore China's former Ming rulers. Among the traits the group shared with today's triads were a clear hierarchy, initiation ceremonies, and codes of conduct based on loyalty, righteousness, secrecy, and brotherhood.

Similar self-help groups for marginalized rural workers were formed on Shanghai's outskirts in the 1700s.¹² Elites viewed these loose coalitions as a political threat at various points in the eighteenth and nineteenth centuries. While the Hung Mun gradually fragmented into various secret societies that later became some of today's best-known triads, these Shanghai boatmen's alliances coalesced in the 1870s as the Anqing Daoyou, the legendary Shanghai Green Gangs' direct predecessor. These self-help groups also resolved disputes and provided their members with social support.¹³ Only in response to suppression did these groups enter the illicit economic sectors with which triads are associated today. These new 'dark societies' maintained traditional characteristics yet began to compete for control over illegal activities, especially after European colonial powers established footholds for opium trafficking.

Britain's victory in the First Opium War opened several ports to foreign traders, allowing British merchants to continue importing opium from colonial India into China, with its lucrative market.¹⁴ In addition to the establishment of colonial concessions in Shanghai, Hong Kong Island also came under the control of the British crown, which, by the turn of the century, had long-term leases on both the Kowloon Peninsula and the New Territories.¹⁵ Hong Kong's cession to the British had the most profound impact of any Treaty of Nanking provision. Hong Kong links South and Southeast Asia to China's most populated coastal provinces. While the Chinese government maintained sovereignty and authority over colonial Shanghai, the British gained full possession of Hong Kong.¹⁶ The legal and governmental systems and institutionalized financial networks imported by Britain facilitated opium trafficking,¹⁷ while the colony's transient character as a trading hub meant

that its disproportionately male, temporary residents mixed with displaced individuals from the mainland, creating an environment in which vice could thrive.¹⁸ The secret societies dissolved into smaller triad gangs and related groups, such as the famous Sun Yee On triad, and competed for control of these illicit markets.¹⁹

The most iconic symbol of the triad presence in Hong Kong is the Kowloon Walled City, the only part of Hong Kong that China refused to cede to Britain. Over time, this northeastern Kowloon settlement, which was, at one point, more than four times denser than modern-day Manhattan,²⁰ became isolated from the mainland but remained free from formal British authority. As residents built upward and inward, the city's precarious legal status and hazardous environment discouraged the Hong Kong authorities from consistent or thorough policing.²¹ The resulting power vacuum provided Sun Yee On, 14K, and other gangs with a base of operations. The Walled City became a hotbed for opium dens, brothels, dog meat restaurants, and similar businesses. Outside the Walled City, triads resorted to extortion, money laundering, and fraud to supplement their profits.²² They also corrupted Hong Kong policemen, whose meagre incomes were supplemented by bribes. The British regime ignored or tolerated these entrenched police-triad alliances until the latter half of the twentieth century.²³

The colonial government began reforming the Hong Kong police in the 1970s, but triad groups utilized their massive capital and influence to adapt.²⁴ After the CCP took power in Mainland China in 1949, Hong Kong became the only major point of access to Mainland China's enormous population. Hong Kong's status as the gateway to China propelled its economic growth and bolstered its regional status, which combined with growing concentrations of organized criminal and other unruly groups to form a hotbed for political violence and organized crime. Organized crime and triads became involved in political and ideological power struggles and trafficked humans, drugs, and other counterfeit or prohibited goods between the mainland and Hong Kong.

Twentieth-century Chinese society offers a myriad of examples of how political organizations and organized criminal groups have engaged with one another proactively. It also demonstrates how organized criminal groups have used ill-gotten wealth and resorted to illicit methods to infiltrate the legitimate economy and gain greater mainstream acceptance. To better understand how to combat organized crime today, it is vital to understand how orga-

nized crime has capitalized on opportunities to engage with political actors and how organized criminal groups have evolved to survive in a changing world.

Cooperating with Crime: Twentieth-Century Chinese Political-Criminal Engagement

For several decades in the early 1900s, the Shanghai Green Gangs dominated Shanghai's political life. Shanghai's three jurisdictions – the Chinese-run city, the International Settlement, and the French Concession – competed with one another and remained under-resourced and consequently incapable of handling basic security functions. Green Gang groups that trafficked opium flourished in this environment.²⁵ Because colonial governments could not properly manage Shanghai's complex social relations, they enlisted the Green Gangs to fill the power vacuum and police the concessions.

Organized criminal groups' involvement in policing and security left them with powerful political contacts, from the French Concession authorities to both of that era's major revolutionary parties, the GMD and the CCP. The Green Gangs pragmatically worked with both sides of the revolutionary struggle. The GMD's most influential leader, Chiang Kai-shek, actively built close ties to Du Yuesheng's Green Gang. The CCP, however, acted with caution in the face of that Green Gang's influence among both Shanghai's labourers and its elites. Chiang's GMD allowed Du's opium rackets to operate unimpeded on the condition that Green Gang members acted as paid 'shock troops', violently attacking CCP-affiliated workers' organizations.²⁶

An alliance with Du's Green Gang was a double-edged sword. These organized criminal groups became indispensable arms of government. The GMD incorporated the Green Gangs into their vision for a Chinese state, using them to reconcile the diverse interests of workers, elites, and the state. The French colonial government desperately needed Green Gang members to serve as both police functionaries and intermediaries between the French authorities and Chinese government officials.²⁷ Consequently, the Green Gangs gained *de facto* legitimacy, and for two decades after the 1927 GMD coup, in which he played a key role, Du enjoyed immense political power and wielded leverage allowing him to continue pursuing his own interests. Several mob bosses assumed

formal positions of power in the French Concession's Provincial Concession, and Du was made the chairman of the elite Shanghai Civic Association. This pragmatic alliance with GMD elements proved to be a wise investment, with the French forced to tolerate organized criminal activities as an alternative to chaos and disorder.

When the CCP eventually triumphed over the GMD in 1949, Mao Zedong set about eradicating even those gangs that had assisted the CCP,²⁸ forcing Du and other Green Gang members to leave Mainland China or risk execution. The Taiwanese GMD honoured Green Gang members as heroes for their role in fighting communism. When Du died in 1951, Taiwanese businessmen sent their condolences, and the Taiwanese government erected a statue of him out of gratitude.²⁹

Nevertheless, the ideological struggle between the CCP and the now-exiled GMD shifted to the battleground of Hong Kong. Its heavy triad presence allowed cooperation between organized crime and state elements to continue. Both political parties used local gangs for espionage, incitement and suppression of protests, and other underhanded activities.³⁰ Just like Shanghai's Green Gangs, Hong Kong's triads saw these connections as practically useful, advancing their own interests by leveraging the principle of *guanxi*, a traditional system of reciprocity and mutual trust. A few key incidents highlight how triads and state elements cooperated in the political sphere.

A GMD general founded the 14K triad in 1947 to fight communists in southern China.³¹ It received intelligence support from Taiwan and financial support from GMD businessmen as it set up base in Kowloon Walled City.³² In 1956, on Double Ten Day, the national day of the GMD-run Republic of China, mass protests began after the Hong Kong authorities cracked down on displays of support for Taiwan. 14K and other groups appropriated the movement and incited riots, fanning the flames of anger and directing it against Hong Kong's seemingly pro-Beijing police.³³

Inspired by the Cultural Revolution shortly after it began in Mainland China, activists in Hong Kong took to the streets in 1967. The Cultural Revolution's violence similarly spilled into Hong Kong, and the ensuing Maoist riots saw fifty-one people killed over several months.³⁴ Organized criminal groups incited violence with at least tacit support from Beijing; bombings killed several people, and mainland Chinese militia shot others at the

Sha Tau Kok border. Other triads helped quell the violence, working with the Hong Kong police to restore order, leading to the birth of a more systemic triad–police alliance.³⁵ Powerful elements of Hong Kong society came to view organized criminal business as just another form of business—one that may operate in the dark yet is still profitable. The public viewed triad–police ties as inextricable, a perception that endured even after serious policing reforms undertaken in the 1980s in anticipation of reunification with the mainland.³⁶

The 1980s and 1990s witnessed brazen government–triad cooperation. In 1984, Deng Xiaoping introduced the idea of ‘patriotic triads’, drawing from the United Front strategy that Chinese communists had long employed to co-opt potential rivals.³⁷ Tao Siju, who served as China’s public security minister from 1990 to 1998, echoed these sentiments in 1993, claiming that “as long as these people are patriotic [and] concerned with Hong Kong’s prosperity and stability, we should unite with them.”³⁸ CCP officials leveraged mainland networks to create unprecedented economic opportunities for Hong Kong-based triads in return for their cooperation. For instance, National Committee Vice Chairman Ye Xuanping lent his image—and with it his legitimacy—to a film production centre owned by the Sun Yee On. Beijing paid these groups in social capital for contributing to ‘patriotic’ causes.³⁹ These groups, in turn, seized opportunities to expand amid the opening up of China, making it easier for Beijing to carry on the ideological struggle in Hong Kong, such as by intimidating pro-democracy protesters and activists.

Beijing espoused three major goals.⁴⁰ First, it sought to prevent the emergence of a triad–activist nexus. Following the Tiananmen Square unrest in 1989, Hong Kong triads had helped smuggle leaders of the pro-democracy movement out of China. Second, because many Hong Kong residents distrusted Beijing and because of public questions surrounding the proposed ‘one country, two systems’ model’s structure and effectiveness, the CCP prioritized the maintenance of order and prosperity in Hong Kong during its handover. Third, because of past GMD efforts to establish an ideological base in Hong Kong, Beijing feared that Taiwan would use its United Bamboo triad to gain a physical foothold in the colony or otherwise directly penetrate Hong Kong’s political system.⁴¹

Beijing’s concerns were not unfounded. In addition to em-

bracing gang members as GMD heroes and making them United Bamboo members, Taiwan had developed a unique form of organized criminal activity: *heijin zhengzhi*, or black-gold politics, which saw organized criminal groups and powerful business interests join forces to influence Taiwanese politics. Even today, many Taiwanese chief executives have ties with, or are members of, triad groups, and up to one-third of elected officials in Taiwan are believed to have been gang members at some point.⁴² The GMD also carried out covert operations in the Golden Triangle. Beginning in the 1950s, the GMD convinced rural farmers to expand – or coerced them into expanding – opium and heroin output by up to twenty times, utilizing taxes and profits to finance anti-CCP activities.⁴³ The GMD's extensive legacy of using organized crime for underhanded actions dates back to Chiang and directly led to *heijin zhengzhi*, leaving the Taiwanese state dependent on organized crime for regular political functions and, in the context of its confrontation with the CCP, ideological war.

Deng's pursuit of the United Front strategy coincided with China's economic liberalization and its opening up to the world. As much of China's enormous population rapidly rose out of poverty, organized criminal groups noted the massive potential profit this market promised with a growing appetite for vice and leisure. In preparation for Hong Kong's reunification with the mainland, these groups began competing for mainland Chinese business and territory. Given the structure of China's government, political officials carried profound influence, and so the United Front strategy presented said groups with an ideal means to capitalize on ties with CCP officials to gain social capital and beat the competition.⁴⁴

Triads and other gangs have remained involved in Hong Kong politics on a smaller scale and in less visible ways.⁴⁵ Their social and political capital has allowed them to expand their activities and shift or extend some to Mainland China. Governments have turned to criminal groups when their goals have required that they resort to politically unviable methods or when they have been physically incapable of delivering key social services. In other cases, they have openly co-opted criminal groups as part of ideological or violent struggles. Overall, the Green Gangs and triads have demonstrated how organized criminal groups can, on some occasions, threaten the political establishment, yet on others become vital components of existing social and political structures.⁴⁶

Organized Crime and the Mainstream: From Political Links to Grey Society

The political-criminal nexus that developed on the basis of the symbiotic relationships between political parties and criminal gangs provided criminals with substantial political capital. Triads and related groups not only enjoyed unprecedented access to government officials; they now also had more power over them. These groups utilized their ties to expand into the economy's legitimate sectors, and by combining their political capital and ill-gotten wealth, they diversified their investments and entrenched themselves even more deeply by entering either fully legal or 'grey-area' sectors of the economy. Although these efforts involved various criminal activities, they successfully secured a place for said groups in mainstream commerce, legitimized crime bosses, and cemented the place of said groups as integral components of society. Especially as Mainland China was opened up to the world anew, said groups quickly took advantage of their ties with mainland officials to enter the new markets, surviving – and profiting – as semi-legitimate enterprises.

Large, highly organized criminal groups still have safe havens in the region. Still, the patience of the public as well as the state has tended to run out quickly whenever a given operation or site has become too burdensome or gained too much notoriety. Kowloon's Walled City survived until its 1993 demolition; more recently, the Chungking Mansions in Tsim Sha Tsui, Hong Kong gained a reputation as a refuge for drugs and criminals before being cleaned up by the Hong Kong police.⁴⁷ Gangs wishing to avoid the uncertainty of such an ephemeral existence have looked to society's grey area. Even Mong La – a city along the China–Myanmar border ruled by the warlord Lin Mingxian and de facto independent of Burmese government control – has followed this trend. Once the headquarters of a highly organized drug syndicate,⁴⁸ Lin claims that opium no longer passes through Mong La. The jungle paths once used to traffic drugs into China now accommodate Chinese tourists seeking to circumvent travel restrictions.⁴⁹ While Mong La's autonomy and isolation make it an ideal sanctuary for vice, even Lin has pivoted from drug trafficking to greyer industries such as gambling.

Du used his unrivalled political influence in Shanghai to pursue sustainable economic prosperity. After around 1932, Du limited the use of gangster tactics so as to not appear to threat-

en Shanghai's political and commercial elites.⁵⁰ He leveraged his opium monopoly and political stature to differentiate Green Gang investments across banking, general shipping, and city food supply. Du gained tangible respectability among these segments of Shanghai urban society, enabling him to continue blending organized crime and legitimate business. For instance, Du took control of the Zhonghui Bank and set up his own shipping business to enhance his opium business's independence and diversify his shipping activities. Du's gang became so deeply embedded in the Shanghai economy's legitimate and illegitimate sectors that it took a violent, ideological campaign to remove him.

Late twentieth-century Asia's rapid economic development, along with globalization more broadly, has made these legitimisation strategies not only more necessary, but also more lucrative. In addition to their growing ties to the vast Chinese diaspora, triads derived social capital from their links with CCP officials.⁵¹ For example, Macau retains its status as China's only jurisdiction in which gambling is legal. Hong Kong-based triads control Macau's most active casinos and associated prostitution and drug ventures and prey on corrupt Chinese officials, who have been known to spend more than US \$10 million in state funds on their gambling trips.⁵² These profit opportunities also allow triads to build contacts with CCP officials, ties that, in turn, frequently create investment opportunities in Mainland China. These so-called grey entrepreneurs so thoroughly blurred the lines between organized crime and business that the two become indistinguishable.⁵³ Not only did gambling rackets, laundering, and fraud multiply their profits, they also offered known triad bosses a chance to reinvent themselves.

The outsourcing by businesses and governments of illegal or politically unpopular activities to triad groups enabled the entry of criminal groups into legitimate sectors of the economy. While triad bosses gained political and commercial influence through these reciprocal relationships, their behaviour became socially acceptable, with the violent enforcement of contracts and the use of intimidation and other underhanded tactics – even the intimidation of corporate stakeholders at meetings – no longer disqualifying or delegitimizing for a triad-owned enterprise. Businesses' criminal connections ceased to be controversial.

One Sun Yee On boss, Jimmy Heung, founded major media businesses in Hong Kong, propelling him to popularity as a

producer and director. Heung had taken advantage of the United Front strategy and received immense social capital from Beijing in return,⁵⁴ using it to cooperate with a mainland Chinese corporation and manipulate company stock prices in Hong Kong to launder his money and enrich himself. His brother, Charles, does not deny his family's history, but he claims no involvement in triad activities.⁵⁵ Whether or not he worked with triads, Charles's Sun Yee On connections left him with similarly substantial social capital to use in Mainland China. Shortly after Tao applied the patriotic triads concept to Hong Kong's gangs, Charles and Tao opened a jointly owned nightclub in Beijing.⁵⁶ Heung's triad background provided him with both the financial resources and the political connections required to penetrate Mainland China's markets.

Hong Kong gangs began funding crime and business in Mainland China using connections built thanks to the United Front strategy in response to market liberalisation and in anticipation of reunification with the mainland. Competition for domination of the mainland's illicit markets generated crime waves and violence, especially in areas neighbouring Hong Kong such as Shenzhen.⁵⁷ Law enforcement proved to be ill-trained at best and corrupt at worst, and triads eagerly met a growing demand for violence, both as protectors and as enforcers. Triad gangs also leveraged ties with local and county-level Chinese officials to invest in grey enterprises in Mainland China, welcomed by the Chinese authorities as businesspeople regardless of where they came from, be it the increasingly inhospitable Taiwan or Hong Kong.⁵⁸ The authorities came to function as a *baohusan*, or protective umbrella,⁵⁹ and, in exchange, extracted millions of yuan from said businesses through a combination of bribery and joint ownership.⁶⁰

When the governments of Hong Kong and Taiwan turned away from organized criminal groups and launched forceful anti-triad campaigns, triads migrated to the mainland, drawn to its massive market and profit-minded government officials. Organized criminal gangs have since built vast grey empires in mainland Chinese industries,⁶¹ operating through businesses that exist legally yet engage in racketeering and other illicit activities in secret: consider that many karaoke clubs serve fronts for prostitution rings. The mostly male residents of, and the myriad businessmen who visit, the factory city of Dongguan in Guangdong have fostered a robust sex industry.⁶² Recent estimates suggest that 10 percent of Dongguan's workforce is in the sex trade, and local offi-

cials are believed to hold shares in most of the businesses involved in the sex trade.⁶³ Like any other business, Dongguan's sex industry has standardized recruitment, training practices, and marketing campaigns.⁶⁴

At times, organized criminal groups have used their illegal profits to enter legitimate sectors of the economy. But more often, they have strived to maintain a business-like façade while sticking to underhanded approaches. This strategy ensures their survival as they grow large enough to sway powerful interests and gain in stature in the public's eyes. With rigid, hierarchical structures relegated to the past, modern triads increasingly rely on informal, flexible social connections, both within and between organized criminal groups, to break the law with impunity,⁶⁵ scaling up and down as needed to seize opportunities and avoid detection.⁶⁶ This strategy also ensures that these groups thrive and are able to reap large profit margins in a global market with large-scale business ventures that is more interconnected than ever before. To be sure, Chinese triad groups are not the only organized criminal groups resorting to these tactics. However, Chinese and Hong Kong triads have uniquely capitalised on opportunities to carry out key functions for the region's governments and on this basis gained political influence allowing them to profit handsomely and come to be accepted as integral components of their societies.

Conclusion: Organized Crime's Penetration of Society's Mainstream and Its Consequences

The Hong Kong police strictly regulate 'triad' status, itself a source of social capital that can impede law enforcement if a criminal gang without the proper resources and standing receives it. It is associated with patriotism because organized criminal groups' predecessors, the secret societies, sought to overthrow China's Qing rulers, who were Manchus.⁶⁷ Nor has it been forgotten that the triad-linked brotherhoods began as self-help organizations for marginalized, lower-class groups. All this makes reckless application of the 'triad' label potentially damaging to the fight against organized crime.

The ideological struggle between the GMD and the CCP served as the backdrop for Chinese organized crime's engagement with the governments of Mainland China and Hong Kong. GMD and CCP leaders and colonial authorities readily cooperated with

powerful organized criminal groups to further their political and ideological goals and carry out security functions. At times, political and economic elites hired thugs to do that which they could not do themselves, such as when the GMD hired United Bamboo to assassinate the political dissident Henry Liu.⁶⁸ Incidents continue in Hong Kong, where in 2017 a pro-Beijing group assaulted the young activist Nathan Law; three years earlier, Shui Fong triad-linked motorcyclists attacked the outspoken newspaper editor Kevin Lau with a meat cleaver, an act for which they were paid handsomely.⁶⁹ The authorities and CCP-linked triad bosses have cooperated in dispersing pro-democracy activists, such as during the 2014 Occupy protests.⁷⁰

The engagement of the governments of China and Hong Kong with organized criminal groups combined with the geopolitical importance of Hong Kong and southern China to leave these triad gangs more influential and resilient than ever before. Still, the political-criminal nexus and criminal groups' penetration of legitimate sectors of the economy have been designated as priorities by law enforcement officials in almost every Asian country.⁷¹ Chen Xiaocun, an official in the Criminal Investigation Division of China's Ministry of Public Security, has publicly called these two issues the two largest concerns of his organization.⁷²

The case of Chinese triads demonstrates the dangers of both trends. Organized crime specializes in violence entrepreneurship, and when state elements cooperate with it, they erode the state's legitimacy and authority, which are derived in large part from the state's monopoly on violence. To engage with organized criminal groups is to forfeit that monopoly and subvert state sovereignty in profound ways: states come to depend on crime bosses to carry out state functions, and crime bosses gain real influence in the government.

Both Chiang's cooperation with Du and the CCP's United Front strategy provided organized criminal groups with legitimacy as social organizations and facilitated their expansion and their consolidation of power. Triad gangs launched operations in China; corruption became mundane and extremely difficult to eradicate. Although these gangs helped the authorities accomplish political goals, the trade-off proved to be dangerous, with powerful negative side-effects. Furthermore, as triad bosses spent their social capital and wealth to set up respectable businesses and distance themselves from their illegal activities, they continued to use dis-

persed, fluid networks to pursue illicit enterprises and conceal their criminality.

Their roots in marginalized communities and successful execution of vital social functions have meant that Asian organized criminal groups, from the Japanese yakuza to Chinese dark societies, are widely tolerated by the public. The yakuza have formal addresses and telephone directory entries, while the Shanghai Green Gangs have had their own publications.⁷³ However, as economic development and integration into the world economy reshapes Asia, criminal groups will come under greater public pressure to professionalise and adapt. They have managed to successfully penetrate politics, the economy, and society in the past; whether they are able to do so again in the twenty-first century will determine their survival.

Notes

1 United Nations Office on Drugs and Crime (UNODC), Myanmar Opium Survey (Bangkok: UNODC Regional Office for Southeast Asia and the Pacific, 2017), accessed December 2018, https://www.unodc.org/documents/southeastasiaand-pacific/Publications/2017/Myanmar_Opium_Survey_2017_web.pdf; Julie Makinen, "Drug Seizures Soar in China; Most Suspects Are 'Farmers and Unemployed,'" Los Angeles Times, February 18, 2016, accessed November 2018, <https://www.latimes.com/world/asia/la-fg-drugs-china-meth-ice-20160218-story.html>.

2 Roderic Broadhurst, "Asia Is in the Grip of a Transnational Crime Crisis – but Governments Look Away," The Conversation, December 6, 2016, accessed November 2018, <http://theconversation.com/asia-is-in-the-grip-of-a-transnational-crime-crisis-but-governments-look-away-69780>; Makinen, "Drug Seizures Soar."

3 Jeremy Douglas, "Parts of Asia Are Slipping into the Hands of Organized Crime," CNN, November 14, 2018, accessed November 2018, <https://www.cnn.com/2018/11/14/opinions/asia-organized-crime-intl/index.html>.

4 Douglas, "Parts of Asia."

5 Broadhurst, "Transnational Crime Crisis."

6 Broadhurst and Lee King Wa, "The Transformation of Triad 'Dark Societies' in Hong Kong: The Impact of Law Enforcement, Socio-Economic and Political Change," Security Challenges 5, no. 4 (2009): 1–38.

7 Broadhurst, "Transnational Crime Crisis."

8 The Global Initiative Against Transnational Organized Crime, "SE Asia Piracy: criminal networks, corporate collusion and corruption," The Global Initiative Against Transnational Organized Crime, September 14, 2015, accessed January 2019, <https://globalinitiative.net/se-asia-piracy-criminal-networks-corporate->

- collusion-and-corruption/.
- 9 Broadhurst, "Transnational Crime Crisis."
- 10 Makinen, "Drug Seizures Soar."
- 11 Rachel Blundy, "A Brief History of Hong Kong's Triad Gangs," *South China Morning Post*, February 4, 2017, accessed December 2018, <https://www.scmp.com/news/hong-kong/law-crime/article/2067890/brief-history-hong-kongs-triad-gangs>.
- 12 Brian G. Martin, *The Shanghai Green Gang: Politics and Organized Crime, 1919–1937* (Berkeley: University of California Press, 1996).
- 13 Broadhurst and Wa, "Triad 'Dark Societies.'"
- 14 Steve Tsang, *A Modern History of Hong Kong* (Hong Kong: Hong Kong University Press, 2004).
- 15 Kam C. Wong, *Policing in Hong Kong: History and Reform* (Boca Raton: Taylor & Francis, 2015).
- 16 C. F. Fraser, "The Status of the International Settlement at Shanghai," *Journal of Comparative Legislation and International Law* 21, no. 1 (1939): 45.
- 17 Tsang, *Modern History*.
- 18 Allan Y. Jiao, *The Police in Hong Kong: A Contemporary View* (Lanham: University Press of America, 2007).
- 19 James O. Finckenaue and Ko-lin Chin, *Asian Transnational Organized Crime* (New York: Nova Science Publishers, 2007).
- 20 John Carney, "Kowloon Walled City: Life in the City of Darkness," *South China Morning Post*, March 16, 2013, accessed December 2018, <https://www.scmp.com/news/hong-kong/article/1191748/kowloon-walled-city-life-city-darkness>;
- Wong, *Policing in Hong Kong*.
- 21 Wong, *Policing in Hong Kong*.
- 22 Blundy, "A Brief History."
- 23 Wong, *Policing in Hong Kong*.
- 24 Jiao, "Police in Hong Kong."
- 25 Martin, *Shanghai Green Gang*.
- 26 Ibid.
- 27 Ibid.
- 28 Bertil Lintner, *Blood Brothers: The Criminal Underworld of Asia* (New York: Palgrave Macmillan, 2003).
- 29 Lintner, *Blood Brothers*.
- 30 Jeffrey Ngo, unpublished conversation with author, December 2, 2018.
- 31 Lintner, *Blood Brothers*, 122.
- 32 Blundy, "A Brief History."
- 33 Lintner, *Blood Brothers*.
- 34 Gary Ka-wai Cheung, *Hong Kong's Watershed: The 1967 Riots* (Hong Kong: Hong Kong University Press, 2009).
- 35 Broadhurst and Wa, "Triad 'Dark Societies.'"
- 36 Louisa Lim, "The Thugs of Mainland China," *New Yorker*, October 8, 2014, accessed December 2018, <https://www.newyorker.com/news/news-desk/thugs-mainland-china-hong-kong-protests>.
- 37 T. Wing Lo, "Beyond Social Capital: Triad Organized Crime in Hong Kong and China," *British Journal of Criminology* 50, no. 5 (2010): 851–872.
- 38 Lim, "Thugs of Mainland China."
- 39 Lo, "Beyond Social Capital."
- 40 Ibid.

- 41 Finckenauer and Chin, *Asian Transnational Organized Crime*.
- 42 Ibid.
- 43 Lintner, *Blood Brothers*.
- 44 Lo, "Beyond Social Capital."
- 45 Asia Sentinel, "China Uses Triads against Democracy Movement," October 4, 2014, accessed January 2019, <https://www.asiasentinel.com/politics/china-uses-triads-democracy-movement/>; Lim, "Thugs of Mainland China."
- 46 Lo, "Beyond Social Capital."
- 47 Kylie Knott, "48 Hours in Hong Kong's Chungking Mansions: Life in Another World," *South China Morning Post*, September 8, 2016, accessed December 2018, <https://www.scmp.com/lifestyle/article/2017086/48-hours-hong-kongs-chungking-mansions-life-another-world>; Blundy, "A Brief History."
- 48 Lintner, *Burma in Revolt: Opium and Insurgency Since 1948* (Boulder: Westview Press, 1994), 325.
- 49 Paul Vrieze, "Inside Mong La, the Myanmar Town Where You Can Buy Drugs, Sex, and Endangered Animals," *Vice*, December 14, 2015, accessed November 2018, https://www.vice.com/en_us/article/avyq3g/inside-mong-la-the-myanmar-town-where-you-can-buy-drugs-sex-and-endangered-animals.
- 50 Lintner, *Blood Brothers*.
- 51 Lo, "Beyond Social Capital."
- 52 Evan Osnos, *Age of Ambition: Chasing Fortune, Truth, and Faith in the New China* (New York: Farrar, Straus and Giroux, 2014), 88–92.
- 53 Osnos, *Age of Ambition*, 88–92.
- 54 Lo, "Beyond Social Capital."
- 55 Li Xueying and Pearl Liu, "Hong Kong Triads Hide Behind Veil of Respectability," *Asia One*, March 10, 2014, accessed December 2018, <http://www.asiaone.com/asia/hong-kong-triads-hide-behind-veil-respectability>.
- 56 Lintner, *Blood Brothers*; Lo, "Beyond Social Capital."
- 57 Broadhurst and Wa, "Triad 'Dark Societies.'"
- 58 Federico Varese, *Mafias on the Move: How Organized Crime Conquers New Territories* (Princeton: Princeton University Press, 2011), 151–153.
- 59 Finckenauer and Chin, *Asian Transnational Organized Crime*.
- 60 Broadhurst and Wa, "Triad 'Dark Societies.'"
- 61 Fiona Tam, "Crackdown Fails to Scare Dongguan's Sex-Trade Veterans," *South China Morning Post*, November 26, 2009, accessed December 2018, <https://www.scmp.com/article/699410/crackdown-fails-scare-dongguans-sex-trade-veterans>; Broadhurst and Wa, "Triad 'Dark Societies.'"
- 62 Tom Phillips, "Inside Dongguan, China's Sin City," *Telegraph*, May 1, 2013, accessed December 2018, <https://www.telegraph.co.uk/news/worldnews/asia/china/10030014/Inside-Dongguan-Chinas-Sin-City.html>.
- 63 Phillips, "Inside Dongguan, China's Sin City."
- 64 Tam, "Dongguan's Sex-Trade Veterans."
- 65 Lo, "Beyond Social Capital."
- 66 Douglas, "Parts of Asia."
- 67 Lintner, *Blood Brothers*.
- 68 Ibid.
- 69 Jasmine Siu, "Nathan Law Felt His 'Life Was under Grave Threat' in Hong Kong Airport Attack by Pro-China Mob," *South China Morning Post*, November 1, 2017, accessed December 2018, <https://www.scmp.com/news/hong-kong/law-crime/article/2117960/nathan-law-felt-his-life-was-under-grave-threat>

hong-kong; Lim, "Thugs of Mainland China."

70 Lim, "Thugs of Mainland China"; Asia Sentinel, "China Uses Triads."

71 Finckenaue and Chin, Asian Transnational Organized Crime.

72 Ibid.

73 Economist, "Why the Yakuza Are Not Illegal," September 30, 2015, accessed November 2018, <https://www.economist.com/the-economist-explains/2015/09/29/why-the-yakuza-are-not-illegal>; Lintner, Blood Brothers.

MAKING PEACE, AND PEACE TALKS, LAST: FACTORS BEHIND THE SUCCESSFUL RESOLUTION OF THE SALVADORAN CIVIL WAR

Joshua S. Ebner,
California State Polytechnic University, Pomona

Abstract

Since 1945, civil wars have become the world's dominant form of armed conflict. This paper examines the influence of two variables—the nature of civil war and its respective parties and third-party (and the nature of) intervention—on civil war outcomes. It highlights how internal and external conditions interact in both the negotiation and enforcement of peace agreements, analyzing obstacles—including information failures and credible security guarantees—that prevent parties from initiating and completing the process of negotiation. To demonstrate the impact of the aforementioned variables, this paper evaluates the case of the 1979–1992 Salvadoran Civil War. It does not establish a categorical rule applicable to all civil wars. However, it does attempt to better our understanding of peace talks—a complex process—and their durability.

Introduction

Civil wars have spiked since the end of World War II, heralding a transition from conventional interstate wars: since 1945, there have been four times as many civil wars as there have been interstate wars.¹ Civil wars typically last longer, collectively kill and displace more people, and are more difficult to resolve—in both the short- and the long-term.² Walter maintains that civil wars have a high recidivism rate, with “57 percent of all countries that suffered from civil war” after 1945 “experienc[ing] at least one [related] conflict thereafter.”³

Like interstate wars, civil wars are generally concluded either through a negotiated peace agreement or by military victory.⁴ However, a mere twenty percent of civil wars since 1945 have been resolved through peace agreements; the remaining eighty percent have ended with the “extermination, expulsion, or capitulation of the losing side,”⁵ something that is cause for concern and indicative of the difficulty warring parties have experienced in trying to resolve armed conflicts. Civil wars are distinguished from

Joshua S. Ebner, ““Making Peace and Peace Talks, Last: Factors Behind the Successful Resolution of the Salvadoran Civil War,” *St Antony's International Review* 15. no. 1, (2019): 183-198.

interstate wars by, among other things, the former's tendency to result in "inconclusive and recurring episodes of fighting, stalemate, or exhaustion"⁶— a process known as the conflict trap, whereby countries that experience civil war report higher conflict recurrence rates.⁷

The conflict trap results from the failure of peace negotiations, itself the product of two uncertainties. The first is the struggle of parties to reach a consensus as to what issues will be addressed in the resulting agreement. According to Lounsberg and Pearson, more than seventy-five percent of civil wars are driven by the desire of parties to either control the central government or secede and create a sovereign nation.⁸ Parties involved in these conflicts espouse starkly opposed goals, making the conflicts' non-military and peaceful resolution highly unlikely. As Walter writes, "negotiations fail because civil war opponents are asked to do what they consider unthinkable."⁹ The second uncertainty is the matter of enforcing the terms of the peace agreement through credible security guarantees that neither party will renege on their deliverables. Countries that have recently experienced civil war typically lack a government that is widely let alone universally recognized as legitimate and/or legal institutions with the requisite resources and political willpower that will enforce a peace treaty fairly and effectively. The second uncertainty is a barrier that is often more difficult to overcome.

The issue, then, is not necessarily *the terms* of the agreement. Rather, the issue is enforcing it after its codification and credibly assuring the parties that its terms will be honoured. Accordingly, many peace negotiations involve third-parties whose participation is designed to reduce distrust between parties and ensure that all parties commit to the agreement's implementation.¹⁰ However, third-party involvement in the negotiation and enforcement of a peace agreement does not guarantee its success. Scholars have maintained that there are at least two factors that directly impact the outcome of peace negotiations. The first concerns the nature of the civil war and its parties. Lounsberg and Pearson maintain that the "substance of the conflict; characteristics of the warring side [...] sustainability of the combat; economic and political power-seeking behavior; and agenda of issues" under negotiation must be considered.¹¹ The second concerns the third-party intervention itself: its timing relative to the civil war's duration;¹² the intervening party's alignment with one of the warring parties;¹³ their competence and credibility in issuing security guarantees;¹⁴ and their behaviour more generally.¹⁵

Combined, these factors affect the likelihood that an agreement will be successfully upheld. The Salvadoran Civil War,

and the peace negotiations that ended it, allow us to examine the aforementioned components. This paper seeks to determine the salience of the enumerated factors for securing lasting peace by looking at the Salvadoran Civil War and focusing on its changing nature as well as the role of the international community. This paper argues that conflict resolution is malleable and that its success depends on conditions that can change radically. This paper does not establish a categorical rule applicable to all civil wars. Rather, it examines and analyzes factors of relevance to the Salvadoran Civil War in an attempt to better our understanding of this complex process, assist practitioners in their efforts to resolve armed conflicts, from facilitating peace talks to enforcing the peace agreements they produce, and inspire future research.

The Case of El Salvador

Although the Salvadoran Civil War officially began in 1980, the causal variables that contributed to its outbreak can be traced back decades: mounting frustration resulting from socioeconomic inequality that was exacerbated by modernisation, political and ideological disparities, and government oppression.

For several centuries, El Salvador was a Spanish colony. Madrid's "political, economic, social, and cultural institutions ... imperfectly penetrated" Salvadoran society¹⁶ as Spain's colonial conquest of Latin and Central America (early 16th century – late 19th century) saw its domestic institutions exported to the region; these later served as the basis for the region's contemporary institutions, with institutions of land, labour, and "concentration and authoritarian exercise of political power" in particular exemplifying this lineage.¹⁷ As Spanish military power declined in the early 19th century, Central American countries began to declare independence. El Salvador did so in 1821, and in 1823, the United Provinces of Central America, consisting of the provinces of Costa Rica, Guatemala, Honduras, Nicaragua, and El Salvador, was officially formed.¹⁸

Old conflicts and rivalries between the confederation's members led to years of war, a situation exacerbated by the power vacuum left by colonial Spain's departure. The confederation eventually dissolved in 1838, its former members becoming independent states; El Salvador followed suit in 1840. Its early political and nation-building priorities included commerce, education reform, judicial reform, infrastructure development, international communication, and transportation.¹⁹ However, tensions between former members of the confederation persisted, periodically causing the outbreak of military conflict as well as

foreign interference in domestic affairs.

Despite this instability, El Salvador established itself as a sovereign nation. Its leaders developed and reformed its various institutions enough to distinguish them from their colonial predecessors, though some colonial features remained, from the “concentration of land ownership and income in the hands of a small economic elite”²⁰ to the agrarian elites’ control of the production, processing, and export infrastructure.²¹ Since El Salvador remained a mono-cultural economy (its largest exports were cacao, indigo, and coffee respectively) after independence, it was highly vulnerable to the international market’s boom and bust economic cycles.²² Moreover, political and economic power became concentrated with owners of large estates, creating “a subservient, impoverished, landless rural labor force.”²³ As Paige maintains, the colonial roots of these economic and political structures “both reflected and accentuated the varying political and economic structures inherited from the colonial past.”²⁴

By the late nineteenth century, coffee had replaced indigo as the staple of El Salvador’s economy. This demand created a rippling effect on the country’s domestic affairs, namely, “the acquisition and control over land, organization and rationalization of production, mechanization and finance of processing, and finance and control over exports.”²⁵ Coffee was a lucrative crop for large estates. It gave financial power to the “planter elite,” who used their capital to enhance the efficiency of their estate’s production system and expand land acquisition efforts.²⁶ Consequently, large portions of the rural population experienced high rates of underemployment and unemployment. Coffee is an intensive crop to cultivate and process, which created a high demand for “large pools of cheap labour sourced from the residents of rural communities.”²⁷

This practice led to discontent among rural communities, whose protests led to a “major uprising” between 1872 and 1898.²⁸ Haggarty indicates that the coffee industry was successful in influencing the Salvadoran armed forces to provide security to their estates, institutionalising the subtle suppression of rural dissent.²⁹ The oligarchs’ financial power transcended the political and legal realms, establishing an “invisible government” with connections to the president.³⁰ By the early twentieth century, plantation owners became politically active, with the Melendez and Quinonez families securing electoral victories to form strong political dynasties.

Several iterations of El Salvador’s constitution similarly benefited the elites insofar as they suppressed communal landownership in favour of private landownership, and “enfranchised literate male adults” despite high rates of illiteracy

throughout the country.³¹ Burns argues that their economic and political power was consolidated, allowing coffee planters to control the export and processing industry, manipulate elections, repress the impoverished majority, and neutralise the military.³² During this period, El Salvador's government amounted to an oligarchy controlled by a few wealthy families who "advocated for free enterprise and economic modernization," while simultaneously suppressing the indigenous population who constituted a source of cheap labour.³³

Between 1900 and 1932, economic and political prosperity became increasingly concentrated within the coffee plantation oligarchs. To meet the growing global demand for coffee, the estates continued to expand their production into indigenous lands.³⁴ Meanwhile, large portions of the population experienced "recurrent food shortages" and 'economic desperation,'" which was further exacerbated by a growing population.³⁵ In 1932, the indigenous population and urban working class initiated nonviolent movements to protest unequal economic conditions and government corruption. The government responded with violence, killing over 30,000 people who were known to be (or suspected of being) involved in the protests.³⁶ This government action represented "a warning of the extreme violence that lay beneath the surface of Salvadoran life" and would resurface "in a more complex social and political context in the 1970s."³⁷ Thus, the grievances remained, as did the cycle of corruption, violence, and terror against opposition groups.

During the 1970s, numerous factions of armed resistance groups developed to challenge the Salvadoran government.³⁸ These groups drew membership from union workers, poor farmers, university students, and academics who endeavoured to enable "mass organization to arise outside the traditional party structure."³⁹ These organisations staged protests and strikes, which were frequently met with government-led violence. As social unrest and military violence increased, new tactics to alleviate the tensions were introduced. A military coup led by conservative army officers in 1979 "led to the establishment of a junta with both civilian and military representatives."⁴⁰

Although the coup was initially presented as "an alternative to leftist revolution and to prevent El Salvador from becoming 'another Nicaragua,'" many of the central promises, such as agrarian reform, never materialised.⁴¹ The opposition factions consolidated into the Farabundo Marti National Liberation Front (FMLN) in 1980 to challenge the government.⁴² These organisations "were separated by profound differences" and had deep-seated mistrust of each other.⁴³ Yet, they embraced the Marxist-Leninist banner to

end decades of unrest through agricultural land reform.⁴⁴ FMLN implemented a highly localised political strategy that “aimed at consolidating its support among the population through the provision of education and health services and the establishment of local ‘popular’ governments.”⁴⁵

Violence intensified in the 1980s as both the government and FMLN increased the frequency and scope of their military operations. Licklider contends that the military balance between warring parties is particularly salient insofar as it shapes their “perceptions of the future.”⁴⁶ At this point of the war, the only desirable outcome for either party was complete military victory. The government’s response to FMLN was “indiscriminate violence, mass displacement, and death squads” that targeted rural civilian populations and political opponents.⁴⁷ FMLN adopted the philosophy that “violent change was necessary” to bring about the end of inequality and exclusion.⁴⁸

In 1980, the Revolutionary Democratic Front (FDR) was founded as a political alliance between “almost all of the important leftist and centrist popular organizations and political parties.”⁴⁹ The FMLN and FDR “established a strategic alliance” (herein referenced as FMLN-FDR) that year to provide a political platform for government opposition groups.⁵⁰ Among their ranks were members of the Social Christian Popular Movement, the social-democratic National Revolutionary Movement, the Jesuit Central American University, and the University of El Salvador.⁵¹ The FMLN-FDR alliance developed a political agenda demanding “the dissolution of the army and security forces, agrarian reform, the dissolution of state powers, and the passing of a new constitution.”⁵² Although FMLN-FDR witnessed a notable increase in their ranks, they were still militarily weak in comparison to the Salvadoran government.

On January 10, 1981, FMLN guerrilla forces launched an operation “dubbed, prematurely and inaccurately, the ‘final offensive,’” aiming to “establish operational control over Morazán Department and to declare it a ‘liberated territory.’”⁵³ While the Salvadoran army prevented FMLN from achieving this end, its forces managed to develop military strongholds within organisations like the Chalatenango Department.⁵⁴ FMLN forces retreated to the “rural north and northeast areas of the country, and the conflict turned into a grand-scale civil war.”⁵⁵ President Carter provided the Salvadoran government military and economic resources to prevent a leftist takeover of the government, and to protect human rights as the number and manner of deaths in El Salvador drew international attention.⁵⁶ After the “final offensive,” US aid to El Salvador grew markedly, especially under the Reagan

Administration, with the development of military capacity in the form of new hardware and training,⁵⁷ and democratic characteristics like free elections being heavily promoted.⁵⁸ Between 1980 and 1991, US aid totalled more than three billion US dollars, of which nearly \$1.1 billion funded the Salvadoran military's efforts to war against the FMLN.⁵⁹

US aid was intended to boost the Salvadoran government's resilience against the guerrilla forces. However, it is more likely that it contributed to creating a protracted conflict, wherein both the FMLN forces and Salvadoran government were unable to decisively win the war. FMLN-FDR received foreign aid from the Soviet Union, Cuba, and Nicaragua, though to a significantly smaller degree compared to US assistance to the Salvadoran government.⁶⁰ However, FMLN-FDR began to experience wavering public support as the war progressed, especially when it was found responsible for military actions against civilian targets.⁶¹ Nevertheless, FMLN forces had effectively challenged the Salvadoran government and were positioned to win the civil war in 1983. Four attempts at peace talks between 1984 and 1989 failed as both parties disagreed on several key issues.⁶² FMLN-FDR called for political reforms, balanced economic development, and protection of civil rights. The government demanded a full surrender, while both refusing to accommodate FMLN-FDR's grievances and failing to provide it with security guarantees.

The government's demands could be attributed, at least in part, to its US aid packages, which increased its resilience against the FMLN forces' attempts to overthrow it. Yet, FMLN forces continued to successfully "attack economic infrastructure and military targets," exploiting the government's poor operational planning and strategic gaps in military tactics and its military personnel's lack of experience.⁶³ It is true that US aid contributed to an overall decrease in political violence against civilians and promoted respect for human rights.⁶⁴ Even so, serious violations continued to be committed by both warring parties throughout the duration of the civil war.⁶⁵ The government in particular sanctioned atrocious crimes against Salvadorans, killing nearly 800 people on average each month during the war.⁶⁶

Discussion

It is now timely to apply the two factors that contribute to the outcome of peace negotiations to the case study at hand. The first factor concerns the nature of the civil war and its respective parties, while the second concerns third-party intervention. It is difficult to cleanly bifurcate the two factors, so, the forthcoming

discussion highlights their overlapping interactions. For instance, the sustainability of combat was largely influenced by third-party involvement in the civil war, insofar as the US provided substantial aid to the Salvadoran government. The US pursued this policy decision because it aligned with its global mission to quell communism globally.

According to Regan, the duration of civil wars follows a curvilinear model which “posits that the probability of a conflict ending is a function of both efforts to manage the conflict and the timing of those efforts.”⁶⁷ Similarly, Balch-Lindsay (etal.) indicates that third-party support extended by entities like international organisations and foreign governments to the domestic government in a civil war, enable the latter to subsidise the cost of its activities in the conflict.⁶⁸ US aid thus made it easier for the government to continue its war efforts since it had a comparative advantage over FMLN forces in terms of its disposable resources. Moreover, the government was less dependent on public resources to fund its activities which allowed it to shore up additional political support while reducing the opposition’s ability to gain popular alliance.⁶⁹

Peace negotiations were not practically feasible until 1989. The Soviet Union began to falter during this period, as its legitimacy slowly eroded under intense public scrutiny.⁷⁰ As Soviet leadership focused on addressing its internal instabilities, its involvement in foreign affairs decreased. Its military presence was withdrawn from Czechoslovakia and Hungary while countries like Lithuania, Estonia, and Latvia declared themselves sovereign nations.⁷¹ Military aid to the Salvadoran government and FMLN dissipated respectively, signalling a shift in foreign intervention in El Salvador’s affairs.

Prior to 1989, the US almost categorically focused on supporting the existing government rather than explicitly encouraging conflict resolution.⁷² Widespread war fatigue created strong public support for peace negotiations.⁷³ Meanwhile, FMLN launched its final offensive which routed the Salvadoran military forces. This led to FMLN’s military occupation of portions of San Salvador, and more densely populated cities including Soyapango, Escalon, and San Benito.⁷⁴ These attacks sent the fight to the “backyards of the urban elites” and cast doubt on the government’s ability to defeat FMLN.⁷⁵ Still, FMLN was not in a position to completely overthrow the government, making the civil war’s end an elusive achievement.

These factors converged in a manner which encouraged both parties to adjust their initial approaches and attitudes towards negotiation. FMLN-FDR minimised its communist-

leaning ideology, promoted more democratic tenets, and reduced its militarism in effort to garner more international support.⁷⁶ Concurrently, Alfredo Cristiani's election in 1989 proved favourable in getting the government to seriously consider accommodating some of the FMLN-FDR's demands. Cristiani indicated that he would "conduct direct talks" with FMLN-FDR leaders to end the civil war, signifying an important step towards developing a comprehensive peace accord.⁷⁷ Until this point, the government adamantly refused to consider any of FMLN-FDR's requests, seriously underestimating the latter's military capabilities and discipline. Thus, the government's willingness to communicate and negotiate with FMLN-FDR could be attributed to the change in leadership, overwhelming public support for the peaceful resolution of the war, and significantly reduced international aid that formerly funded the war effort.

The Salvadoran Civil War persisted, in part, because of two strategic dilemmas: information failures and credible commitments. Information failures occur when groups "cannot acquire or share the information necessary to bridge the bargaining gap."⁷⁸ Both parties – hoping to gain an advantage over their adversary – withheld strategic information that, if revealed, would compromise their security. The government exhibited an information failure through its underestimation of FMLN's military capabilities and discipline. This miscalculation exacerbated the government's military weaknesses and strengthened FMLN's strategic advantages, resulting in their successful, though temporary, occupation of the country's capital and three of its most populated cities in 1989. Credible commitments are mutual reassurances that each party involved in a mutually beneficial agreement will uphold their commitment. If parties are not sufficiently certain that an agreement can be made and honoured, they may be inclined to "absorb [the] high costs of war today to avoid being exploited tomorrow."⁷⁹ In this case, peace negotiations repeatedly failed because the government refused to accommodate FMLN-FDR's requests to provide security guarantees during and after negotiations.

Arguably, the greatest challenge to a successful peace treaty concerns credible guarantees that "eliminate the possibility of post-treaty exploitation."⁸⁰ As proven by the Salvadoran Civil War, such an arrangement is difficult to design without third-party security guarantees. For example, Chavez maintains the 1989 peace negotiations in Mexico City failed because the ongoing violence created tense and uncertain relations.⁸¹ When reports surfaced that the Salvadoran military murdered six Jesuit priests, their housekeeper, and the housekeeper's daughter, FMLN-

FDR withdrew from the peace talks in protest. It subsequently called upon the United Nations (UN) to take a more active role in mediating the civil war. Meanwhile, the US's aid reduction heightened the political pressure on the Salvadoran government to accommodate negotiation efforts.

In 1990, the UN answered this call by bringing together representatives from the two parties to initiate negotiations in Geneva.⁸² This first step in the multi-treaty agreement aimed to provide sufficient assurances that both parties would fully participate and fulfil their respective commitments to bring about a peaceful conclusion to the war. Over the next two years, a series of agreements were codified. The first was the San Jose Agreement which promised political reforms to develop El Salvador's capacity to promote and protect human rights, through two main channels. The first concerned criminal justice reforms which would improve the rule of law, establish an independent judicial system, protect legal rights and due process, and end extra-legal procedures such as night arrests, torture, and politically motivated arrests and detention.⁸³ The second concerned the development of the United Nations Observer Mission in El Salvador (ONUSAL), tasked with verifying the compliance of all parties with Salvadoran law and ratified international treaties alike once the cease-fire began.⁸⁴

The second accord was the New York Negotiations, a complex power-sharing agreement whereby the FMLN-FDR agreed to give up "their long-standing demand to merge with or disband the army," in exchange for the development of, and their incorporation into, the newly formed National Civilian Police (PNC).⁸⁵ The PNC's membership would be "20% FMLN, 20% old National Police, and 60% new recruits."⁸⁶ An ad hoc committee chartered by ONUSAL was developed to screen and train new recruits to ensure compliance.

The third accord, the Chapultepec Accords of 1992, officially ended the Salvadoran Civil War. It contained provisions that reformed the judicial and political systems, resolved long-standing land and property issues, and ensured the political participation of the FMLN-FDR in exchange for its demilitarisation and demobilisation.⁸⁷ The provisions of the Chapultepec Accords are monitored by the National Commission for the Consolidation of Peace, whose members included representatives of the FMLN-FDR, the government, and all political parties.⁸⁸ ONUSAL was tasked to oversee the implementation of the Accords and to investigate complaints of noncompliance. Critically, ONUSAL provided security and credibility reassurances to the government and FMLN-FDR. Accordingly, the UN's presence throughout the peace negotiation process and the structure and implementation

of the peace accords played an important role in ending the Salvadoran Civil War. Its involvement specifically addressed the second strategic dilemma, by providing assurances to the FMLN-FDR and the government. These assurances contributed to the parties' commitment to ending the war on agreeable conditions and complying with those terms.

Conclusion

This paper has examined two interwoven factors that contribute to both the duration of civil wars and the likelihood of warring parties to establish a peaceful conclusion to that conflict. As demonstrated in this analysis, these factors are subject to a complex interaction between domestic and international influences, and variables that may either promote or discourage peaceful remedies to a civil war. For instance, the Salvadoran Civil War's duration was largely influenced by the US's support of the Salvadoran government as it provided resources that bolstered its military capabilities and subsidised its cost of participating in the war. As long as the aid continued, the Salvadoran government enjoyed more leverage during the initial attempts at negotiations than FMLN-FDR.

In the meantime, FMLN-FDR's only recourse was to sustain conflict rather than submit to the government's unilateral demands. Reiterating Walter's observation, one of the most salient impediments to successful peace negotiations is "designing credible guarantees on the terms of the agreement."⁸⁹ Reliable and effective national institutions, especially those "in the area of administration of justice and the police," are critical to overcoming impediments insofar as those institutions both enforce the terms of a peace agreement and provide reassurance that the members of the parties are not exploited after the ceasefire.⁹⁰ In the absence of these institutions, peaceful resolution and honest adherence to peace agreements are difficult to guarantee.

Examining the conflict in the context of global politics, it is reasonable to conclude the civil war was prolonged because of third-parties' willingness to intervene. Since the Salvadoran Civil War took place during the height of the Cold War, both the US and the Soviet Union viewed the conflict through their own competitive and ideological lenses. The Salvadoran war, like other conflicts throughout Asia, Africa, and Latin America, were considered necessary components of a broader struggle for ideological influence. The end of the Cold War removed these lenses and thus eliminated the incentive (or ability) for third-parties to continue supporting the war. Similarly, international

attention shifted towards human rights violations which forced both the Salvadoran government and FMLN-FDR to adjust their image and platform to mitigate pressure and gain support.

The shift in domestic factors also played an important role in ending the Salvadoran Civil War. A military stalemate between FMLN forces and the Salvadoran government eliminated both parties' certainty of a decisive military victory. The duration and intensity of the conflict produced strong national support for conflict resolution. Moreover, the lack of credible security guarantees prevented the government and FMLN-FDR from mediating and negotiating peace on their own. Thus, it became advantageous for both parties to seek assistance from the UN. With strong international support to resolve the conflict, the UN played a pivotal role throughout the entirety of the peace negotiation and implementation process, because it ensured an otherwise unobtainable level of stability and security.

In short, both domestic and international factors led to the development of a peace agreement that addressed the underlying concerns that built up to the civil war. Some of those issues were addressed through power-sharing agreements such as the development of PNC and the integration of FMLN-FDR into the electoral process as an official political party. Others were addressed through institutional reforms in the judicial system and law enforcement bodies to recognise and protect human rights. To a lesser extent, socioeconomic disparities were mitigated through land reforms, such as the arms-for-land programme, that reintegrated those most affected by the conflict into society.⁹¹ Although these are imperfect solutions, the agreement has prevented El Salvador from regressing back into a state of civil war. From this perspective, the peace negotiations were successful. Still, the country has "deeply entrenched" economic, security, and legal challenges to overcome.⁹²

*Acknowledgements: I am grateful to Professor Marc Scarcelli for inspiring my interest in this topic and helping develop this paper's arguments and structure. This paper greatly benefitted from Samantha Hunt's insights and comments on previous drafts. A special thank you to my parents and grandparents for their continual support in all my endeavours.

Notes

1 Marc Scarcelli, "Ethnic Conflict," Lecture at Cal Poly Pomona, Pomona, California, United States, March 21, 2017.

2 Paul Collier, V. L. Elliott, Harvard Hegre, Anke Hoeffler, Marta Reynal-Querol, and Nicholas Sambanis, *Breaking the Conflict Trap: Civil War and Development Policy* (Washington, D.C.: World Bank, 2003), 93–118.

- 3 Barbara F. Walter, *Conflict Relapse and the Sustainability of Post-Conflict Peace* (Washington: World Bank, 2010), 1.
- 4 Marie Olson Lounsbury and Frederic Pearson, *Civil Wars: Internal Struggles, Global Consequences* (Toronto, CA: University of Toronto Press, 2009).
- 5 Walter, "The Critical Barrier to Civil War Settlement," *International Organization* 51, no. 3 (1997): 335.
- 6 Lounsbury and Pearson, *Civil Wars*, 155.
- 7 Collier et al., *Conflict Trap*, 103–104.
- 8 Lounsbury and Pearson, *Civil Wars*, 160.
- 9 Walter, "Civil War Settlement," 335.
- 10 Chong Chen, "Negotiated Settlement and the Durability of Peace: Agreement Design, Implementation, and Mediated Civil Wars" (M.S. dissertation, Utah State University, 2015).
- 11 Lounsbury and Pearson, *Civil Wars*.
- 12 Patrick M. Regan, "Third-Party Interventions and the Duration of Intrastate Conflicts," *Journal of Conflict Resolution* 46, no. 1 (2002): 55–73.
- 13 Dylan Balch-Lindsay, Andrew J. Enterline, and Kyle A. Joyce, "Third-Party Intervention and the Civil War Process," *Journal of Peace Research* 45, no. 3 (2008): 345–363.
- 14 Hans J. Giessmann and Oliver Wils, "Seeking Compromise? Mediation Through the Eyes of Conflict Parties," in *Advancing Conflict Transformation*, ed. Beatrix Austin, Martina Fischer, and Giessmann (Opladen and Framington Hills: Barbara Budrich Publishers, 2011), 184–204.
- 15 Regan, "Third-Party Interventions."
- 16 E. Bradford Burns, "The Modernization of Underdevelopment: El Salvador, 1858–1931," *Journal of Developing Areas* 18, no. 3 (1984): 295–297.
- 17 Burns, "Modernization of Underdevelopment," 296.
- 18 BBC News, "El Salvador Profile – Timeline," May 16, 2018, accessed April 10, 2019, www.bbc.com/news/world-latin-america-19402222.
- 19 Burns, "Modernization of Underdevelopment," 300.
- 20 Alberto Martin Alvarez, "From Revolutionary War to Democratic Revolution: The Farabundo Martí National Liberation Front (FMLN) in El Salvador," *Berghof Transitions Series Paper* no. 9 (2010): 8.
- 21 Jeffery M. Paige, *Coffee and Politics in Central America: Revolution and the Rise of Democracy in Central America* (Cambridge: Harvard University Press, 1985), 1–71.
- 22 Richard A. Haggerty, *El Salvador, a Country Study* (Washington: US Library of Congress Federal Research Division, 1990), xix.
- 23 Burns, "Modernization of Underdevelopment," 297.
- 24 Paige, *Coffee and Politics*, 2.
- 25 *Ibid.*, 4.
- 26 *Ibid.*, 31–35.
- 27 *Ibid.*, 7.
- 28 Burns, "Modernization of Underdevelopment," 303.
- 29 Haggerty, *Country Study*, 11.

- 30 Ibid., 13.
- 31 Burns, "Modernization of Underdevelopment," 303.
- 32 Ibid., 305.
- 33 Cara E. McKinney, "Twelve Years a Terror: U.S. Impact in the 12-Year Civil War in El Salvador," *International ResearchScape Journal* 2 (2015): 2.
- 34 Elisabeth Jean Wood, *Insurgent Collective Action and Civil War in El Salvador* (Cambridge, UK: Cambridge University Press, 2003).
- 35 Burns, "Modernization of Underdevelopment," 311.
- 36 T. David Mason, "The Civil War in El Salvador: A Retrospective Analysis," *Latin American Research Review* 34, no. 3 (1999): 179–196.
- 37 Haggerty, *Country Study*, xx.
- 38 McKinney, "Twelve Years a Terror," 3.
- 39 Ibid., 3.
- 40 Raymond Bonner, "The Agony of El Salvador," *New York Times*, February 22, 1981, accessed April 7, 2019, <https://www.nytimes.com/1981/02/22/magazine/the-agony-of-el-salvador.html>.
- 41 Haggerty, *Country Study*, xxi.
- 42 Susan Ram, "El Salvador: Perspectives on a Revolutionary Civil War," *Social Scientist* 11, no. 8 (1983): 3–38.
- 43 Alvarez, "Revolutionary War," 17.
- 44 Michael Wilkerson, "Security and Democracy in El Salvador: An Undeniable Connection," *Stanford Journal of International Relations* 10, no. 1 (2008): 32–41.
- 45 Charles T. Call, "Assessing El Salvador's Transition from Civil War to Peace," in *Ending Civil Wars: The Implementation of Peace Agreements*, ed. Stephen John Stedman, Donald S. Rothchild, and Elizabeth M. Cousens (Boulder: Lynne Rienner, 2002), 546.
- 46 Roy Licklider, ed., *Stopping the Killing: How Civil Wars End* (New York: New York University Press, 1993), 309.
- 47 World Peace Foundation, "Mass Atrocity Endings: El Salvador," August 7, 2015, accessed April 8 2019, <https://sites.tufts.edu/atrocityendings/2015/08/07/el-salvador/>.
- 48 Michael E. Allison, "The Transition from Armed Opposition to Electoral Opposition in Central America," *Latin American Politics and Society* 48, no. 4 (2006): 145.
- 49 Call, "El Salvador's Transition," 546.
- 50 Alvarez, "Revolutionary War," 16.
- 51 Ibid., 16.
- 52 Ibid., 17.
- 53 Haggerty, *Country Study*, 41.
- 54 Ibid., 41.
- 55 Alvarez, "Revolutionary War," 18.
- 56 Haggerty, *Country Study*, 42.
- 57 McKinney, "Twelve Years a Terror," 9.
- 58 Haggerty, *Country Study*, 43.

- 59 Call, "El Salvador's Transition," 383–420.
- 60 US Government, *Communist Interference in El Salvador* (Washington: US Department of State Bureau of Public Affairs, 1981), accessed April 8, 2019, <https://www.cia.gov/library/readingroom/docs/CIA-RDP85M00363R001403210042-9.pdf>.
- 61 US Government, *El Salvador: Guerrilla Capabilities and Prospects Over the Next Two Years* (Washington: US Central Intelligence Agency Directorate of Intelligence, 1984), 11, accessed April 8, 2019, https://www.cia.gov/library/readingroom/docs/DOC_0000808520.pdf.
- 62 US Government, *El Salvador: Military Assistance Has Helped Counter but Not Overcome the Insurgency* (Washington: US General Accounting Office, 1991), 2, accessed April 9, 2019, <https://www.gao.gov/assets/160/150509.pdf>.
- 63 US Government, *Military Assistance*, 3.
- 64 *Ibid.*, 4.
- 65 *Ibid.*, 4.
- 66 Philippe Bourgois, "The Power of Violence in War and Peace: Post-Cold War Lessons from El Salvador," *Ethnography* 2, no. 1 (2001): 5–34.
- 67 Regan, "Third-Party Interventions," 59.
- 68 Balch-Lindsay, Enterline, and Joyce, "Civil War Process," 345–363.
- 69 *Ibid.*, 345–363.
- 70 US Government, *Rising Political Instability under Gorbachev: Understanding the Problem and Prospects for Resolution* (Washington: US Central Intelligence Agency, 1989), accessed April 9, 2019, http://chnm.gmu.edu/1989/archive/files/cia-raising-instability_4b36a35d0d.pdf.
- 71 Benjamin B. Fischer, ed., *At Cold War's End: US Intelligence on the Soviet Union and Eastern Europe, 1989–1991* (Washington: US Central Intelligence Agency, 2000).
- 72 Call, "El Salvador's Transition," 383–420.
- 73 Wilkerson, "Undeniable Connection," 32–41.
- 74 Joaquín M. Chávez, "How Did the Civil War in El Salvador End?" *American Historical Review* 120, no. 5 (2015): 1784–1797.
- 75 Wilkerson, "Undeniable Connection," 36.
- 76 Chávez, "Civil War in El Salvador," 1784–1797.
- 77 *Ibid.*, 1788.
- 78 David A. Lake and Donald Rothchild, "Containing Fear: The Origins and Management of Ethnic Conflict," *International Security* 21, no. 2 (1996): 46.
- 79 Lake and Rothchild, "Containing Fear," 48.
- 80 Walter, "Designing Transitions from Civil War: Demobilization, Democratization, and Commitments to Peace," *International Security* 24, no. 1 (1999): 135.
- 81 Chávez, "Civil War in El Salvador," 1784–1797.
- 82 Wilkerson, "Undeniable Connection," 32–41.
- 83 UN General Assembly and Security Council Resolutions A/44/971 and S/21541 (1990), accessed April 5, 2019, https://peacemaker.un.org/sites/peacemaker.un.org/files/SV_900726_SanJoseAgreement.pdf.

- 84 Margarita S. Studemeister, ed., "El Salvador: Implementation of the Peace Accords," *Peaceworks* no. 38 (2001).
- 85 Vanessa Jaramillo-Cano, "An Examination of the Varying Role of the United Nations in the Civil Wars of Rwanda and El Salvador" (B.A. paper, University of Nevada, Las Vegas, 2012), 99.
- 86 Jaramillo-Cano, "Varying Role," 99.
- 87 UN General Assembly and Security Council Resolutions A/46/864 and S/23501 (1992), accessed April 5, 2019, https://peacemaker.un.org/sites/peacemaker.un.org/files/SV_920116_ChapultepecAgreement.pdf.
- 88 Wilkerson, "Undeniable Connection," 37.
- 89 Walter, "Transitions from Civil War," 129.
- 90 Lounsbery and Pearson, *Civil Wars*, 160.
- 91 Graciana del Castillo, "Post-Conflict Reconstruction and the Challenge to International Organizations: The Case of El Salvador," *World Development* 29, no. 12 (2001): 1975.
- 92 Clare Ribando Seelke, *El Salvador: Background and U.S. Relations* (Washington: US Congressional Research Service, 2017), 12.

LUCAS KELLO, *THE VIRTUAL WEAPON
AND INTERNATIONAL ORDER*. PUBLISHER:
NEW HAVEN, CT: YALE UNIVERSITY
PRESS, 2017.

Samuel Forsythe

Roughly half a century after the emergence of networked computer systems, it has become abundantly clear that, while the technologies of cyberspace afford humans the benefits of globally accessible knowledge and mass communication, they have also made us dependent upon technical configurations that appear to be defined by their systemic insecurity and susceptibility to malicious manipulation. For the field of international affairs and security studies, the degree to which this insecurity entails political risks, or might be instrumentalised for strategic purposes, is an open and ongoing enquiry. It is in the context of these technological, social, and political changes that Lucas Kello's *The Virtual Weapon* tries to make sense of this seemingly new adversarial domain, and to understand how the weaponised capabilities of information technology are transforming the international system.

Over the past few decades, the security studies discourse on cyber issues has seen a somewhat sparse but nonetheless rigorous debate—one in which Kello has been a vocal participant—between those who warn of the catastrophic implications of 'cyber war' and those who are sceptical of such alarms.¹ For Kello, firmly located within the former camp, this question has a clear answer: The strategic implications of cyber weapons—'malicious computer code designed to manipulate the functions of machines or else seize, corrupt, or disclose their sensitive data'—are as transformative for strategic theory and practice as were those of nuclear warfare in the previous century.² Motivated by this sense of urgency, Kello proposes a complete re-engineering of the concepts with which security studies scholars might address the properties, limits, and effects of cyber weapons in the digital environment of international relations.

The book opens by proclaiming the revolutionary effects of cyber weapons. Kello argues that a disturbance of the rational order of international relations is precipitated by new and untested potencies, formidable technical complexity, and the exploitation of uncertainty, unpredictability, and deception. The central contention of *The Virtual Weapon*—and perhaps its most radical claim—is that '[i]nformation is no longer just a source of power; it has become force *itself*'.³ This new modality of conflict, Kello contends, transforms the 'moral order' of international relations: it empowers states with revolutionary or despotic ideologies and enables militant and civilian non-state actors to wield global influence beyond the reach and influence of traditional diplomacy and statecraft. Kello's realist framing foresees chaotic and destabilising interactions between cyber politics and the already anarchic arena of international security unsettling strategic theories of deterrence and proliferation, and undermining the established conditions of peace.

Throughout the book, Kello's aim appears to be threefold: i) to understand how the effects and capabilities of 'virtual weapons' are transforming the global order of international relations; ii) to develop a set of concepts capable of compressing complex technical ideas into manageable tools for formulating policy; and iii), to disparage those scholars whom he deems sceptics and 'Clausewitzians', a rather obtuse term that Kello uses to describe a purported reluctance to see the revolutionary truth of cyberspace and abandon a force-centric, state-centric view of the international system, and as shorthand for staid and blinkered academicians, unable to see beyond their own conceptual limits. While Kello's attention, for the most part, is given to the first two points of enquiry, throughout the book he exerts considerable energy criticising and castigating these ominous and elusive 'Clausewitzians', often without obvious benefit to the argument.

The first part of the book deals primarily with defining terms and developing concepts, exploring the character and limits of strategic cyber studies. This includes an analysis of how cyber weapons affect the strategic balance between defender and attacker, and the need for what Kello calls a 'Congress of Disciplines'. On the first point two points, Kello argues that technical details and conceptual analyses have hampered discussion in the past, limiting discussion to mere 'explanation and description' rather than affording active policy development. In response, Kello largely

sidesteps the discourse of previous scholarship, instead proposing his own vocabulary for defining the field of inquiry. While the purpose of the effort is clear, his notions of ‘cyberweapons’, ‘technological revolution’, and ‘unpeace’ receive neither substantive conceptual treatment, nor an explanation of how they are superior to the concepts they are intended to replace. This brief treatment seems to belie Kello’s call for a ‘congress of disciplines’, Kello’s proposal for a collective effort to attend to common aims within the discourse on cyber issues and security.

Despite this somewhat idiosyncratic approach, Kello’s efforts—and the reader’s—are rewarded by useful definitions of the primary units of analysis and their properties (e.g. actors and capabilities), their effects on existing strategic considerations (balance of attack and defence), and their overall effect on global affairs. Kello organises the effects of cyber weapons into three orders of ‘systemic revolution’ and clarifies which actors are subsequently enabled or constrained. This might serve as a framework for those wishing to determine the thresholds at which cyberattacks are considered to be mere disruptions, or acts with more serious consequences. On this level, one might, however, suggest that Kello is himself not able to escape his own ‘Clausewitzian’ judgments: his analysis often remains focused on the politically instrumental use of force (now translated into ‘harm via information’). Moreover, despite his attention to the empowering of non-state actors, it often limits itself to a discussion of their effects within the ambit of traditional political actors. Nevertheless, Kello’s analysis of the effects of cyber weapons on the strategic issue of deterrence provides an interesting perspective on the ways in which information eludes attempts at classification within traditional strategic frameworks. Furthermore, he does a commendable job of illustrating how both direct and indirect effects must be considered in any solution to the challenges of cyber deterrence and the risks of escalation.

Throughout *The Virtual Weapon*, Kello’s polemic against his ‘Clausewitzian’ adversaries—which largely appears as an uncharitable reduction of a variety of positions—fails to do justice to previous efforts in cyber theory, and often distracts from both the subject matter and his analysis. Kello’s disparagement of the field is a discouraging symptom of what might, at best, be considered his sense of urgency and the seriousness of the subject and, at worst, an equivalent short-sightedness and unwillingness to

engage with ideas other than his own. Considered from a somewhat more convivial position, one wonders whether these other perspectives, concepts and contributions to security studies are in fact what Kello has in mind when he proposes a 'congress of disciplines'. The latter concept refers to an interdisciplinary and collaborative effort to understand, discuss and respond to complex changes.⁴

While Kello's polemic may turn away readers already familiar with the broader field and discourse, his analysis of cyber issues in international relations is sufficiently detailed and provocative to warrant a close reading, even if only to learn whether the forcefulness of his critique can be counter-balanced with an equally strong positive proposal.

Notes

1 See: Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement", *International Security* 39:2, (2014), 181-192.

2 Lucas Kello, *The Virtual Weapon*, 1.

3 *Ibid.*, 5.

4 For further positions, concepts and discussions see: Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge: MIT Press, 2001); Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007); Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008); David J. Betz and Tim Stevens, *Cyberspace and the state - Toward a Strategy for Cyber Power*, (New York, Routledge, 2012); Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013); Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford: Oxford University Press, 2015)

JAMIE BARTLETT, *THE PEOPLE VS
TECH: HOW THE INTERNET IS KILLING
DEMOCRACY (AND HOW WE SAVE IT)*,
PUBLISHER: LONDON: PENGUIN/
RANDOM HOUSE, 2018.

Anisa Kassamali

The People vs Tech: How the Internet Is Killing Democracy (And How We Save It) tackles the fundamental incompatibility between two key features of many societies: technology and democracy. Author Jamie Bartlett argues that the two systems are products of different eras: democracy is best suited to hierarchical nation-states and industrialised economies, not the decentralised and data-driven world of technology companies. In essence, “democracy is analogue rather than digital” and must change if it is to survive in the digital age.¹

Bartlett identifies six key pillars of democracy: active citizens, a shared culture, free elections, shared equality, competitive economy, civic freedom, and trust in authority. The chapters consider how each pillar is threatened by technology. The challenges are both familiar and novel in that existing issues such as unemployment and political apathy have been combined with concerns about the impact of invisible algorithms on traditional power structures. For instance, Bartlett’s opening suggestion is that the collection of our personal data by technology firms might not only lead to more targeted advertising but actually stunt our political maturity. Bartlett argues that a requisite for such maturity is the freedom to develop one’s own views without fear of retribution. However, consistent data collection creates a permanence that actively discourages the expression of potentially controversial opinions. Well-known individuals are routinely cast into the spotlight for past comments made on social media – remarks that they themselves may no longer recall. Self-censorship is subtly encouraged, since the memory of data is longer than that of humans.

Bartlett similarly explores the impact had on democracy when Artificial Intelligence (AI) performs tasks hitherto assigned to human beings. It is a widespread concern that intelligent machines will take jobs away from people, contributing to unemployment. Bartlett takes this further and suggests that AI will better perform routine cognitive jobs generally carried out by the middle-class in democratic societies. The removal of these forms

of employment will lead to a “barbell-shaped economy” in which only high- and low-skilled jobs will be available.² Bartlett argues that such an economy will lead to a shrinking tax base while also producing a society with growing rates of crime, depression, drug abuse, and infant mortality.

The People vs Tech concludes with a projection of what democratic societies will look like if current technological trajectories continue uninterrupted. It offers some recommendations to try and avert this. In essence, Bartlett believes that democratic institutions will have neither the ability nor the resources to govern the nation-state effectively. Growing inequality resulting from the rise of AI will not only aggravate existing social problems, from crime to alcoholism, but also divide society further along social and ethnic lines. The falling tax base will also render the government less capable of dealing with these challenges. This will generate distrust among citizens who, in a cyclical fashion, will further refuse to comply with the government and will withhold resources. Large numbers of people will eventually agree that democracy is no longer workable and instead welcome a “gentle, effective and subtle techno-authoritarianism.”³ This can only be avoided if democracy is able to adapt to the technological world within the next twenty years. Bartlett therefore puts forward a series of recommendations, ranging from the imposition of new laws and regulations to changes in individual behaviour at the citizen’s level.

Bartlett’s individual arguments are mostly compelling and accessible. Bartlett is a senior fellow at Demos, a cross-party think tank that develops evidence-based solutions to issues across a range of social policy areas and where at the time of writing Bartlett led the Centre for the Analysis of Social Media. His centre studies how the rise of the digital world affects politics, policy, and decision-making. Bartlett’s knowledge-base therefore encompasses the somewhat unusual combination of political philosophy, social policy, and technological expertise. He is able to guide the reader from a detailed explanation of technological issues to consideration of more existential questions surrounding the roles of the state and the citizen in a functioning democracy. In doing so, he draws on the established Western canon of political philosophy and on first-hand interviews with individuals working in technology firms in equal measure. The end result is a book that is both well-researched and eloquently argued.

The main shortcoming of *The People vs Tech* is perhaps its breadth. Bartlett tries to cover a large amount of material in a relatively concise volume and does not always sufficiently expand on some of his ideas. Thus, in Chapter 5, Bartlett argues that the nature of digital technologies makes monopolies more likely, as

they often allow businesses to provide a superior service for which consumers are more likely to opt. He is critical of the role of tech companies in this and touches on the broader capitalist structure that enables such behaviour. However, he tries to keep such analysis succinct and in doing so only partially presents his views. Bartlett does refer in passing to a “degree of inequality [that] is inevitable and necessary in a free market economy” and includes a mini-epilogue on the idea of universal basic income.⁴ However, these comments are not integrated into his broader argument on technology companies’ monopolisation of certain services and industries.

Bartlett could also have provided a more thorough explanation of his theoretical foundations. He clearly defines the scope of ‘democracy’ and ‘technology,’ limiting the latter to the “the digital technologies associated with Silicon Valley – social media platforms, big data, mobile technology and artificial intelligence”⁵ and the former to “modern liberal representative democracy.”⁶ However, he provides little explanation for, or background to, the six pillars of democracy around which the book is centred. This would have been useful, given the importance of these features to Bartlett’s subsequent arguments.

The People vs Tech is an accessible and timely read. It posits an ambitious yet significant thesis: democracy is losing in an insidious battle with technology and will need to adapt, if it is to ensure its own survival. Bartlett seeks to explain this through the systematic analysis of each of democracy’s core elements and the erosive effect of the rise of technology. The book could have benefited from greater detail in certain areas but is mostly coherently and eloquently argued.

Notes

1 Jamie Bartlett, *The People vs Tech: How the Internet is Killing Democracy (And How We Save It)* (London: Penguin/Random House, 2018), 9.

2 Ibid., 117.

3 Ibid, 198.

4 Ibid, 121.

5 Ibid, 1.

6 Ibid, 3.

BRUCE SCHNEIER, *CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD*, PUBLISHER: NEW YORK: W.W. NORTON & COMPANY, 2018.

Claudine Tinsman

The internet was never designed with security in mind. Initially, the internet was used mainly to connect computers controlled by a small number of academics and researchers. Now, it connects everyone and everything. In *Click Here to Kill Everybody: Security and Survival in a Hyperconnected World*, Bruce Schneier sets himself a daunting task: explaining to novices, policymakers, and engineers alike why is it urgent to secure the technology that affects our daily lives, what *should* be done, and what *can* be done. At just 250 pages, the book is short and to the point, providing anyone seeking an introduction to cybersecurity with a good starting point.

Part I of *Click Here* begins by taking the reader on a guided tour of the history of the cybersecurity vulnerabilities of what Schneier calls the 'Internet +'. This concept encompasses 'the internet of things' and 'the internet of everything else,' from social networks through to medical devices and critical infrastructure. Rather than approach the insecurity of the 'Internet +' from a technical perspective, Schneier wisely chooses to frame the problem in economic terms: the 'Internet +' is insecure because neither manufacturers nor providers nor governments are incentivised to improve it. Manufacturers of connected devices have no economic incentive to invest in security because it is expensive. For reasons of profit and national security, respectively, service providers and governments are interested in protecting users' data and communications from hackers but not from their own prying eyes.

As long as the status quo is maintained, the 'Internet +' will remain insecure, with potentially disastrous consequences. The more everything is connected to the internet, the more vulnerable it is to attack. A car could be hacked and caused to crash, killing the driver. A power station could be hacked in the dead of winter, cutting off heating and causing thousands of people to freeze. A 'bio-printer' could be remotely reprogrammed to mass-produce a virus that kills thousands. In other words, as the book's title implies, a single click could 'kill everybody.'

Having established that the insecurity of the ‘Internet +’ has the potential to endanger lives, Schneier sets about proposing solutions. At the core of his security recommendations lies the belief that the market should not be left to manage cybersecurity. The responsibility to secure the ‘Internet +’ through functional regulation lies with governments. Schneier points to other cases in which major technological shifts have been accompanied by beneficial regulations. For instance, regulation of airline manufacturing so strongly discourages manufacturers from compromising on security that it is the one aspect of airline travel not subject to competition.¹ As a result of this regulation, air travel went from being one of the most dangerous forms of transport to one of the safest. If manufacturers were forced to adhere to similarly stringent minimum thresholds for cybersecurity, the security of the ‘Internet +’ would improve dramatically.

Although his arguments in favour of regulation and government control are compelling, Schneier acknowledges that what should happen is not what will probably happen. First, both the private sector and government – the US government in particular – benefit from a market model that favours insecurity. Security will have to be prioritised over surveillance before effective regulation can be legislated and implemented. Second, regulation is crafted and passed by legislators who have repeatedly displayed ignorance when it comes to cybersecurity.

As a result, national legislatures are unlikely to lead the regulatory charge worldwide, and it is actors others than national legislatures whose solutions are the most likely to be viable. Schneier points to the EU as the most likely driver of cybersecurity regulation. The EU’s implementation of the far-reaching General Data Protection Regulation (GDPR) has illustrated that regulation in one market can have a global impact. If service providers and manufacturers are forced to adhere to EU security standards on internet-connected goods, they are more likely to sell that iteration of the product worldwide than create different versions of it for different markets.

A possible shortcoming of *Click Here* is that it does not delve into the politics behind turning recommendations into policy. Schneier himself acknowledges that it is a “gaping hole” in the book he lacks the expertise to fill.² To be sure, an exploration of the politics of cybersecurity would certainly have been interesting. Ultimately, however, Schneier’s work is fundamentally an overview of current and future cyber challenges about which everyone should be worried, and it proposes concrete measures to address them, a message from which a detailed discussion on the politics of policymaking could have detracted.

Click Here's author knows that cybersecurity is a problem that affects everyone but is understood by too few. By providing a short and accessible overview of the world's major cybersecurity problems and their origins, it succeeds at narrowing this knowledge gap. As such, it is an excellent introductory text on cybersecurity that is extensively footnoted for those interested in closely examining any of the issues raised by Schneier.

Notes

1 Bruce Schneier, *Click Here to Kill Everybody: Security and Survival in a Hyperconnected World* (New York: W.W. Norton & Company, 2018), 144–145.

2 Schneier, *Click Here*, 11.

BEN BUCHANAN, *THE CYBERSECURITY
DILEMMA: HACKING, TRUST AND FEAR
BETWEEN NATIONS*, PUBLISHER: NEW
YORK, N.Y: OXFORD UNIVERSITY PRESS,
2017.

Rachel Hirshman

In *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Ben Buchanan synthesises international relations scholarship on the traditional security dilemma paradigm with the technical and political realities of nation-state cyber activity. Buchanan's perspective is refreshing and novel. Most scholars have studied international relations in cyberspace either through analogies from previous technological innovations or by intently analysing cyberspace in a vacuum. Very few authors have systematically analysed how prevailing theories in international relations apply, if at all, to the cyber domain. Buchanan's book is perhaps the first comprehensive attempt to bridge this gap.

That being said, *The Cybersecurity Dilemma* is, above all, a political science publication. Despite its dominant political science narrative, however, Buchanan's book is accessible to all readers: technical cybersecurity experts, politicians, and intelligence operatives alike. Furthermore, unlike most political science scholarship on cyber issues, Buchanan does not eschew technical details. He strikes the right balance between complexity and comprehensibility, explaining the necessary technicalities of cyber operations while ensuring his main theoretical argument is easily understood. Emphasising the cyber domain above all, Buchanan charts the reader through a comprehensive, albeit sometimes excessively thorough, account of all elements that lay the groundwork for and exacerbate the cybersecurity dilemma. He does so while leaving little unanswered.

The book is structured around one overarching conclusion: "To assure their own cybersecurity, states will sometimes intrude into the strategically important networks of other states and will threaten—often unintentionally—the security of those other states, risking escalation and undermining stability".¹ Buchanan creatively and thoughtfully adopts the security dilemma, popularised by Robert Jervis in the 1970s, to the cyber realm. The security dilemma explains the phenomenon whereby a state takes actions to increase its own security and power but, in doing so, decreases

the security and power of other states. With an inquisitive mind and attention to detail, Buchanan walks the reader through cyber operations from both the defender's perspective and the offender's perspective in support of his argument. He strays from more conventional scholarship in explaining the fundamentals of cyber operations without conceding to the temptation of leveraging analogies from other military domains.

Notwithstanding the clarity with which Buchanan presents a complex and often misunderstood domain and concept, his argument does however fail to address the nuances of state activity in the cyber domain that have direct relevance to the emergence of the cybersecurity dilemma. In omitting most considerations of the complexities of state responsibility, Buchanan does not jeopardise the salience of his claims. Rather, accounting for a broader categorisation of 'state actor' challenges Buchanan's conclusion of the severity on the cybersecurity dilemma he outlines, not its existence in the first place.

Buchanan acknowledges himself that "[i]n order for the cybersecurity dilemma to be relevant, states have to know whom to fear".² Therefore, in chapter seven, Buchanan carefully assesses the potential counterargument of the difficulty of attribution and its influence on the relevance of the cybersecurity dilemma. However, attribution is only one element of the equation and the only one on which Buchanan focuses. Beyond attribution, there is the additional problem of determination of state responsibility. Jason Healey's article, "The Spectrum of National Responsibility for Cyberattacks" is perhaps the best encapsulation of the levels of potential involvement of a state in a cyberattack. Healey notes, "To make progress, the cyber defense community must accept the idea that national policy makers often need to know the *responsibility* for an attack, not the technical attribution, to drive their decisions and responses. 'Who is to blame?' can be more important than 'who did it?'"³ The question of *who* is responsible is also explored by Herbert Lin in his article "Attribution of Malicious Cyber Incidents: From Soup to Nuts". Lin provides a complementary paradigm of responsibility in explaining three possible and non-mutually exclusive units of responsibility: a machine, a specific human, and a responsible party.⁴

Three of the categories that Healey identifies are state-encouraged, state-ordered, and state-executed. State-encouraged, according to Healey, means that "[t]hird parties control and conduct the attack, but the national government encourages them as a matter of policy".⁵ State-ordered is when "[t]he national government directs third-party proxies to conduct the attack on its behalf."⁶ Finally, state-executed is defined as when "[t]he

national government conducts the attack using cyber forces under their direct control.”⁷ While the mechanism and extent of state involvement varies in all three cases from indirect influence to direct execution, the state bears some level of responsibility for the attack.

Yet, because Buchanan’s model only applies to state actors and the networks and systems critical to the security of those actors, his model seemingly only addresses state-executed cyberattacks. In the spirit of robust political science analysis, Buchanan makes a conscious choice to limit his analysis in this way. However, accounting for the wider spectrum of state responsibility, it becomes clear that the cybersecurity dilemma can be more acute than just in the ways Buchanan presents it. The number of groups and systems that states will intrude upon to ensure their own security increases significantly. Presumably, states would feel a need to penetrate the networks of third parties who have already been identified as acting on behalf of, or with encouragement from, states. However, they would also need to penetrate those groups or organisations that have the potential to be influenced or encouraged by a state actor in the future.

To be clear, this is not an argument for the inclusion of non-state actors into Buchanan’s model. Rather, the point is that ‘state actor’ can mean much more than what Buchanan lays it out to be. If one state actor is concerned about the behaviour of another state and seeks to bolster its own security, it likely must do so at the behest of organisations or institutions directly owned and operated by the perpetrator state. Its actions would also implicate those third parties, or even, as Lin argues, machines acting or likely to be acting within some spectrum of state involvement. The risk of miscalculation or undesired escalation only grows as the number of systems that a state intrudes upon increases, as does the fear of the targeted state. Further research into the potential scope of third parties and systems invoked by acknowledging the spectrum of state responsibility would help to shed more light on how Buchanan’s model fairs when a broader conception of ‘state actor’ is considered.

Overall, Buchanan presents a persuasive argument for the existence of a cybersecurity dilemma which incentivises states to intrude in each other’s networks consistently, motivated by defensive and offensive objectives. Yet a shortcoming of his argument is a seemingly narrow categorisation of ‘state actor’. Extending Buchanan’s argument to account for the variations in responsibility does not disprove the existence of the cybersecurity dilemma; instead, it merely challenges Buchanan’s categorisation of the severity of the dilemma. Considering Buchanan’s objective,

212 he presents a convincing, comprehensive, and novel argument that is likely to maintain its relevance for years to come.

Notes

1 Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (New York, NY: Oxford University Press, 2017): 3.

2 *Ibid.*, 143.

3 Jason Healey, "The Spectrum of National Responsibility for Cyberattacks," *Brown Journal of World Affairs* 18, no.1 (2011): 57.

4 Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts." Hoover Institution Aegis Paper Series on National Security, Technology, and Law (2016): 5.

5 Healey, "The Spectrum of National Responsibility for Cyberattacks," 60.

6 *Ibid.*, 60.

7 *Ibid.*, 61.

SAMUEL C. WOOLEY & PHILIP N.
HOWARD (ED.), *COMPUTATIONAL
PROPAGANDA: POLITICAL PARTIES,
POLITICIANS AND POLITICAL
MANIPULATION ON SOCIAL MEDIA*, NEW
YORK, N.Y: OXFORD UNIVERSITY PRESS,
2018.

James Sullivan

From Martin Luther's use of the printing press to disseminate his famous Theses in 1521,¹ through Riefenstahl's innovative use of the film medium in World War II,² to the modern-day use of bots and 'sock puppets' to mould online agendas and opinions, the ability of those in power, or those striving for it, to leverage any technologies available to them has been a constant throughout time.

Woolley and Howard's edited volume takes a geographic-case-study approach to examine the newest uses of technology in propaganda. Coining the term 'computational propaganda', they refer to the use of algorithms, automation, and human curation to purposefully manage and distribute misleading information over social media networks.³ The volume's case studies span the globe, including Asia (China, Taiwan, Japan), Europe (Germany, Russia, Ukraine, Poland), and the Americas (Canada, United States and Brazil).

The authors address a very straightforward question, namely: which computational propaganda campaigns had a significant impact on attitudes and opinions, and how might they be prevented in the future? The case studies presented, taken in their totality, address this core question as well as a series of themes critical to the overall view.

1) Are inward-focused computational propaganda schemes more acceptable?

The volume analyses the domestic and foreign actors involved in propaganda efforts, as well as the locus of those targeted—domestic or international. China, for example, is presented as an example of primarily domestically focused propaganda.⁴ We note that this view of China as a primarily domestically-focused actor

has been challenged in other research into their internationally focused efforts, including collaboration with foreign universities,⁵ extensive ‘united front’ quasi-government organisations,⁶ and aggressive use of venture-capital funding to gain access to and influence on technological development.⁷

Whereas some may argue that domestically-focused efforts are less of a threat to international relations, linking the China and Russia case studies leads one to the alternative conclusion. Significant domestic tools were developed in Russia to assist with agenda-setting and domestic political support, particularly during Russian President Dmitry Medvedev’s tenure.⁸ However, these tools were swiftly repurposed to support Russia’s international efforts to influence events in Ukraine and Crimea. The Russia case study presented in the volume, as well as the cross-case comparisons made in its concluding chapter,⁹ suggest that Chinese computational propaganda tools could be increasingly aimed outward, should the need arise.

2) Should automation of influence-attempts be the primary concern?

Significant attention has been paid to attempts to automate influence attempts, for instance, via automated bots acting without human intervention. The volume makes a convincing case by deeming automated bots a rather ineffective manipulation tool. The importance of automation and bots is not in direct manipulation of opinion, but in agenda-setting. As McCombs and Shaw state in their 1972 piece on the subject, paraphrasing Berelson: “On any single subject many ‘hear’ but few ‘listen’.”¹⁰ The ability of bots and ‘sock puppets’ to drive overall agenda-setting is covered in detail in the volume,¹¹ estimating that this agenda-setting helped drive US \$5 billion worth of free media coverage towards Donald Trump’s presidential campaign, versus only US \$3 million for Hillary Clinton’s campaign.

The lack of a guaranteed automated impact on public opinion has driven significantly more manual or quasi-manual (‘cyborg’) efforts. It is important to note that the majority of Russian interference during the 2016 US election through the Saint Petersburg-based Internet Research Agency was accomplished through individuals crafting posts, with limited automation involved. In China, a similar phenomenon occurs with a large majority of posts created by government employees supporting certain initiatives.¹² Manipulation of public opinion appears to be better pursued with human rather than bot-led efforts.¹³

The core mission of the volume does not stop at diagnosis, but also requires prescriptions. What can be done to address growing concerns regarding electoral integrity and foreign influence? The volume explores several attempts, including the leveraging of existing legislation in Canada, Brazil, and Germany. It also chronicles significant public education efforts in other countries, such as Taiwan. Taken together, the volume presents a credible array of options for governments and corporations looking to address this issue. It then closes by suggesting, in a constructive fashion, a series of additional areas of potential analysis. These research questions include the impact of automated social media accounts on individual political attitudes, trust in institutions, and overall citizen engagement.¹⁴

Overall, the volume presents a series of valuable case studies, which delve into challenging definitional and analytical issues surrounding the development of computational propaganda. The combination of qualitative and quantitative research pursued in the preparation of these case studies provides a view of both the current—as well as developing—tactics, techniques, and procedures at play in this evolving environment. Perhaps the only critique of the volume rests in the questions hinted at, but not fully voiced or suggested for follow-up research. This is perhaps a limitation of the analytical format chosen, namely geographic case studies. A more fluid analytical structure that allows for cross-industry, rather than solely geographic case studies, might enable these issues to be addressed more fully.

Several case studies begin to discuss potential screening mechanisms that could be leveraged to identify and block automated influence attempts, but the discussion stops there. One cross-industry, rather than cross-geography, case study that could flesh-out this merely alluded to question in greater depth would be a time series case study of the global development of email infrastructure.

Following the commercialisation of email as a communication medium, malicious actors leveraged automated tools to inundate users' inboxes—what we now refer to as 'spam'—estimated to drive anywhere from 53% (statistica.com) to over 85% (CISCO/Talos) of global email traffic – causing annual costs to companies of US \$20-50 billion and generating revenue for spammers of approximately US \$200 million.¹⁵ Developing filters to counter these automated tools is one factor that led to significant consolidation of a handful of global email providers. This same industry consolidation is present in the social media networks targeted by computational

propaganda, implying a useful case study that the geographic focus of the volume disallows. More research into the ability of 'spam-like' screening tools to counter automated bot attempts at agenda-setting would be desirable.

Another large question merely hinted at, but not fully addressed, is the issue of fake accounts leveraged to manipulate opinions. This issue is a constant across most of the case studies presented, but is addressed neither directly in the volume, nor in the suggested incremental research required.

The foundational ideal that the internet was an unregulatable space, combining anonymity with access, was a function of both the state of technology at the time, as well as specific decisions made by early pioneers. As Lessig argues, the structure of the internet has always been a political decision.¹⁶ Initially, these decisions were made in favour of openness and anonymity. Many countries have since made divergent political decisions, namely to require 'passports' in the virtual world. China is perhaps the best example, but only one among a growing number of country-cases. Free flow of goods and people is clearly good for the world. We do not, however, permit passport-free travel through most jurisdictions. While an unpopular idea, we must now consider this dynamic in the virtual world as well, or risk the consequences.

Notes

1 Bagchi, David. "Printing, Propaganda, and Public Opinion." *The Oxford Encyclopedia of Martin Luther*, 2017.

2 Ullrich Volker and Chase S. Jefferson, Hitler. First American ed. (New York: Alfred A. Knopf, 2016), 534.

3 Woolley and Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York, NY: Oxford University Press, 2018), 79.

4 *Ibid.*, 212.

5 Alex Joske. *Picking Flowers, Making Honey*. International Cyber Policy Centre Policy Brief, Australian Strategic Policy Institute, 2008

6 Larry Diamond and Orville Schell. *Chinese Influence & American Interests* (Stanford, CA: Hoover Institution Press, 2018)

7 Michael Brown and Pavneet Singh. *China's Technology Transfer Strategy*. Defense Innovation Unit Experimental, 2018.

8 Woolley and Howard, *Computational Propaganda*, 21-40.

9 *Ibid.*, 245.

10 M. McCombs and D. Shaw. "The Agenda-setting Function of Mass Media." *Public Opinion Quarterly* 36, no. 2 (1972): 176-87.

- 11 Woolley and Howard, *Computational Propaganda*, 190-196.
- 12 *Ibid.*, 216.
- 13 *Ibid.*, 33.
- 14 *Ibid.*, 244.
- 15 Justin M. Rao and David H Reiley. "The Economics of Spam." *Journal of Economic Perspectives* 26, no. 3 (2012): 87-110.
- 16 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York, N.Y.: Basic Books, 1999).