Introduction

Into the Cyber Realm

Empirical research on cybersecurity has become highly relevant in this day and age. Although it is useful, we cannot learn enough about cybersecurity simply by reasoning descriptive patterns. Indeed, one of the great things about social sciences is that we can usually make the most out of observations and inferences to problematize and theorize about cybersecurity, for instance, by studying how countries protect and advance their national interest in cyberspace. Current cybersecurity research stems from many disciplines, such as political science, international relations, sociology, criminology, development, international law, psychology, and economics. It deals with various interconnected themes, including the rule of law, the spread of digital technologies, and democratization; most notably, it sheds light on what we can call the governance of cybersecurity. Scholars tend to ask broad questions including: How do states and citizens educate themselves to avoid hackers? How does the United States and China cyber rivalry cascade into the rest of the world? What is the relationship between Internet usage and antigovernment mobilization in developing democracies? Is the Internet increasing crime and terrorism?[1]

Most research acknowledges the fact that the proliferation of information and communication technologies (ICTs) has pushed the boundaries of the use of digital tools for good and bad. Between 2005 and 2018, there were more than 250 state-sponsored cyberattacks. Incidents transpired despite the setup of multilateral frameworks to monitor, deter, and respond to emerging threats in information security sponsored by the African Union, the League of Arab States, Shanghai Cooperation Organization, the Organization of American States, and adopted by intergovernmental entities, including the

Group of 7, the European Union, the North Atlantic Treaty Organization, and the United Nations.

The truth is that there is little common ground on how to enforce the measures required to address cybersecurity. Some Western groups of states tend to consider existing international law sufficient for guiding state behavior in cyberspace. Other industrialized countries, such as China and Russia, would prefer new normative guidance on state use and development of ICTs. International consensus is fragile, and cross-border cooperation does not suffice for real global collaboration.[2]

The outlook seems more gloomy when even global leaders, including UN Secretary-General António Guterres, are pessimistic about reaching a compromise. "When one looks at today's cyberspace, it is clear that we are witnessing, in a more or less disguised way, cyberwars between states. The fact is that we have not yet been able to discuss whether or not the Geneva Conventions apply to cyberwar or whether or not international humanitarian law applies to cyberwar," Guterres argued.[3] Undoubtedly, more intergovernmental, governmental, and nongovernmental discussion on cyberactivities is needed to strengthen international law, national law, and nonbinding cyber norms in different contexts.

In these early days in the history of cybersecurity, scholars have tried to address the implications for stakeholders both in- and outside of academia. Governments are interested in knowing more about how to build expertise to manage their cyber defenses, and civil society is highly responsive to relevant studies promoting open discussion and deliberation online. Private industry, as another major actor, might be the most updated and well-versed source of knowledge regarding cybersecurity issues. Not only do they use research to design and develop the various aspects of ICTs diffused globally, but, more importantly, they also seem to craft the pivotal channels of interactive information in the twenty-first century (i.e., email, blogs, vlogs, wikis, social sites, microblogs, etc.).

Public and private security logics meet at the melting point between government and corporate concerns toward cybersecurity. The health of ICTs and networks is many times dependent on the logic of markets, on profitability, and at the hands of the best buyer in today's competitive trade and commercial environment.[4] Does this mean public authorities have less to say in the governance of cybersecurity? Then why is cybersecurity a national security issue, as many in government have painted it?

As of the writing of this book, a different branch of research has consolidated in the subfield of cyberpsychology. This particular approach

is understood as the "processes underlying and influencing the thinking, interpretation, and behavior" associated with human online interconnectivity.[5] What such a level of study has come to validate is that social, economic, and political forms of action using ICTs and Internet-based technologies ultimately shape new forms of socialization in at least three iterative ways: among citizens, between citizens and authorities, and among two or more nation-states. Mostly, empirical research has addressed these three aspects. Public opinion scholars have studied the application of technical developments and citizenship mobilization, including the equal opportunities presented by satellite communications, smartphones, cable television, and the Internet. Sociological and developmental studies have pointed out the potential use of e-governance and e-democracy toward community building and government information policy. Political scientists and international relations students have explored questions surrounding the idea of cyber conflict breaking out among rival states and issues of global norms among those believed to be allies. Criminologists have emphasized the role of cyberspace in fostering crime, deviance, and other forms of bending the law.

Much of the scholarship produced by international relations scholars and political scientists has involved the underlying meaning of cyberspace and why it raises security concerns. This consequently raises cybersecurity as a state-centered issue. In this literature, cyberspace is defined by Brandon Valeriano and Ryan Maness as the "networked system of microprocessors, mainframes, and basic computers that interact in digital space." More relevantly, they argue that "what happens on the physical layer of cyberspace is where we engage political questions."[6]

Political issues revolving around citizenship, society, and global norms in cyberspace have flourished from a vast array of standpoints, often too many to enumerate. What concerns this book the most is the extent to which practitioners and scholars have underscored the links between digital technologies, cybersecurity, and the military:

> Derived from a realist theory of world politics in which states compete with each other for survival and relative advantage, the principal cybersecurity threats are conceived as those affecting sovereign states, such as damage to critical infrastructure within their territorial jurisdictions. This approach delegates responsibility for the security of cyberspace to military, intelligence, and law enforcement agencies, which together constitute the state's

> national security apparatus. These agencies tend to operate with limited public accountability, oversight, and transparency.[7]
>
> Cyberspace provides even more opportunities or disruptive technological transformation that could provide a decisive advantage, on the one hand, but might also rick uncontrolled escalation on the other.[8]

ICTs are said to have integrated almost fully into how modern states manage their military affairs:

> Unlike the infantry or artillery revolution, the information revolution didn't just create information warriors, it informationized all conventional warriors. These are infantry soldiers, munitions experts, forward air controllers, pilots, and war-fighting staffs that are dependent on digital technologies and information to conduct conventional operations. They are the front-line combatants, armed with M-16s, radios, and combat iPads. It is virtually impossible to separate modern warfare from digital capabilities.[9]
>
> We might have decided to view cybersecurity as a purely civilian issue and conceptualized both current and future cyber "attacks" as criminal matters. But as with humanitarian assistance, rule of law programs, strategic communication, and so much else, the military has jumped in to fill the vacuum created by squabbling and under-resourced civilian agencies.[10]

The military itself recognizes that the continued advancement in technology has changed the conduct of warfare:

> Today's commanders must drive integration of lethal and non-lethal effects across Land, Air, Sea, Space, and Cyberspace to create unity of action while maintaining our competitive military advantage on the battlefield. Our failure to operationalize and normalize the cyberspace domain effectively cedes it to our adversaries, gives them a competitive edge, and ultimately, creates an increased attack vector against our objectives.[11]

States around the world have emphasized the need to invest in the development of cyber military capabilities, and examples of armed forces

adopting new doctrines for such principles are becoming the norm. Experience from battlegrounds in land, sea, and air serve as useful roadmaps for future cyber military operations. However, to some observers, "Tactical terms used in continental warfare such as vital ground and in-contact are not consistent with an environment where bits and bytes are proxies for warriors."[12] For some scholars, the hype behind cyberwarfare is overblown:

> [I]t is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage. That is improbable to change in the years ahead.[13]

> Even if cyberspace exists primarily for war, it does not follow that war would itself become the primary means by which cyberspace would be governed. Unlike land, air, and sea, cyberspace is a sociotechnical institution rather than a natural, physical domain.[14]

There is a dividing line among perspectives:

> The cyber hype perspective would suggest that we are seeing a revolution in military affairs with the advent of new military technologies. The moderate view is guided by careful consideration of what the real dangers are, as well as the costs of the overreaction.[15]

Cybersecurity expertise has grown exponentially. The literature increases so rapidly that the knowledge we think we possess on governance, legislation, and state interactions becomes obsolete very quickly. "Cyber expertise research is like astronomy: what we perceive is actually a snapshot of the past," argued Robert Thompson of the Army Cyber Institute at the U.S. Military Academy.[16] More than ever, studying the cyber domain thus demands innovative claims, rethinking previous theoretical paradigms, marrying sometimes distanced research methodologies, and, more notably, bringing forward new case studies in a nuanced and empirically grounded way that can defy the test of time.

Take the following example. Hacker attacks are deemed the "new normal" in geopolitics, reaching both state and subnational levels.[17] On August 22, 2019, the *New York Times* ran a story about municipalities across the United States held hostage by ransomware attacks. More than

forty local authorities had been victims of unknown hackers that infiltrated their systems and encrypted their data.[18] In ransomware attacks, systems are locked and later unlocked after the victims pay a sum of money, usually in cryptocurrency, to the captors. Victims will say that paying the ransom is cheaper than rebuilding the systems all over again. In cases like this, higher-up authorities are called. Intelligence agencies, the armed forces, police, and public prosecutors will in theory align their resources to try and identify the source of the hacking. Aiding citizens and victims of these types of attacks demands sophisticated countermeasures from trained and well-resourced national agencies. Incidents targeting a municipal library can quickly escalate to threaten other services such as water, power, hospitals, communications, intellectual designs, military secrets, and, what is much feared, the denial of service or destruction of critical national infrastructure. Concurrently, the U.S. justice system has overseen the prosecutions of hacking groups led by nationals from Iran and China for infiltrating domestic computer networks, including those of critical institutions such as the Pentagon.

Researchers in both developed and emerging countries use small-N case-selection or large-N contexts (i.e., systematic surveys) to highlight the way states deal with cyberincidents. Research, either qualitative or quantitative in style, derives inferences that go beyond the particular observations collected.[19] Put simply, cybersecurity scholars observe incidents and states' responses that help us learn about governing the cyber realm. In a large-N pooled time-series analysis, for example, scholars found that in 170 countries surveyed between 1996 and 2010, higher Internet penetration usually came with reports of more stable governance, regardless of regime type.[20] From this type of research, we usually learn about transparency, accountability, and good governance themes, although less about policy action. In contrast, from the small-N example taken from ransomware incidents in municipalities, we learn that some authorities prefer to pay the ransom and that only a few communities in the United States have cybersecurity protocols to counter incidents such as these.

If we were to collect facts systematically, let's say across a vast number of federal states, we might arrive at the conclusion that local authorities are usually cash strapped in their attempts to access appropriate cybersecurity for their systems. We might then infer that, beyond the observations collected, this phenomenon might be common in other countries, as similarly ill-resourced municipalities abound in countries affected by austerity measures. If we had the data to infer that based on a sample from developing

countries, cities are poorer than those in the United States, we might assume that if hackers were to target them, they would be eventually less prepared to avoid such an infiltration in their systems—although maybe, as less able to pay ransom, less appealing to greedy hackers! Nevertheless, the future of cybersecurity in not-so-rich countries is difficult to forecast. Much of cybersecurity's nature is said to depend heavily upon the (good and bad) users themselves.[21]

Cybersecurity Governance

Academic studies surrounding cybersecurity governance have burgeoned in the advanced democracies, notably in English-speaking countries. Little research originates in or uses case studies from developing societies where cybersecurity "uncertainty" seems more significant. This book acknowledges how unclear cybersecurity governance can be and seeks to untangle a few pertaining complexities.

The main concern of the book is the fact that states struggle when dealing with perceived threats that are too difficult to measure and scenarios too complicated to assess.[22] Cyberthreats easily exploit uncertainty. We are more likely to overstate or misjudge the actual danger posed by the threats if we understudy them.

One way to deal scientifically with uncertainty and complexity is to search for generalizations and make inferences. Across the book, I look for such interpretations in the developing world, and explore cybersecurity governance beyond what we know from the advanced democracies (i.e., United States, United Kingdom, European Union, and Australia, among others) and other industrialized states (China and Russia).

Martin Libicki has defined cybersecurity as the "efforts to prevent systems from being compromised."[23] I take this approach a step farther, and define cybersecurity governance as the actions and policies adopted by civilians, the military, industry, and the private sector to safeguard digital space. However, the focus of this book is directed on the military.

The book deals with three much-hyped and highly debated concepts: cyber, security, and governance.[24] I intend to theorize over practical efforts (*governance*) to solving complex problems (*cyber*) that affect the state (*security*). From this standpoint, I shall approach the policy perspective that shapes cyberspace security as a national security issue. While some scholars question the value of "national securitizing" cyberspace—because

it militarizes civilian problems, subjects freedom to vaguely defined controls, and incentivizes rivalry among states—I take into consideration the established trend that many countries have already adopted. A glance at the UN Institute for Disarmament Research (UNIDIR) cyber policy portal confirms that rich and emerging states have constructed, or are in the process of building, vastly prepared cyber military commands and that legislation has been adopted that allows these groups to plan and act against threats concerning cyberspace. Both the Pentagon and NATO have declared cyber a "domain," just like the sea, air, land, and space.

This book is not a justification for national security doctrines. On the contrary, it aims to create awareness of the issues presented when militarizing cyberspace by acknowledging that this has become a standard feature among some nation-states. As others have argued, the "militaries must be very careful about what missions they accept in cyberspace and must circumscribe their forays into cyberspace lest they are overwhelmed by the sheer scope of the domain."[25] My point is that by focusing on actual governing practice across levels, space, and jurisdictions, we are more likely to grasp the cyber, security, and governance arenas without losing touch with reality.

While this book is mainly diagnostic in identifying trends and problems, its contribution is to challenge prescriptive assumptions regarding cybersecurity governance happening in and beyond the industrialized North. I argue that sample bias and the overemphasis by international relations scholars on a few selected cases often distort the analysis and understanding of the broader dynamics of cyber, governance, and security as both separate and combined concepts.

Regarding case studies, it is not my intention to cry wolf and ask social science researchers to select diverse case studies from beyond the rich countries. Methodologies such as most similar cases, most different cases, or single case-study analysis are frequently used to explore new trends in world politics, and most of the time, they are correctly executed. However, by incorporating a sample with understudied diverse case studies—Gerring defines these as "a set of cases that encompasses a range of high and low values on relevant dimensions"[26]—we can account for a full array of variations on the selected variables of interest. That is, if we study cases that rank high and low in different cybersecurity governance dimensions and the role of the military in them, better and stronger representativeness can be claimed.

Entering the cybersecurity realm of research requires, thus, describing and explaining differences. Whether we study many phenomena (i.e., cyberwar, cybercrime, cyberterrorism, cyber espionage, etc.), or just one, describing and explaining demand recollection of many observable implications that make sense of our theories.[27] More specific contributions to the scholarly literature on cybersecurity increase our ability to engage in scientific explanation. Much of the cybersecurity background literature in this book reflects on the fields of political science, international affairs, and criminology but also on other equally relevant subjects (i.e., computer science or cyberpsychology). In sum, to make an interdisciplinary contribution to the study of cybersecurity, I argue that important topics, as observed in advanced democracies, might garner equal explanatory success in developing countries.

The Argument

The book has three main pillars of research: (1) to assess the cybersecurity scenario in developed countries and illustrate current events in the developing Western Hemisphere; (2) to explore the governance of cybersecurity in comparison to other perceived threats to national security in the region; and (3) to illustrate the militarization of cybersecurity policy.

In the first pillar, I consider that states in the Western Hemisphere find themselves in a scenario where global norms call for cybersecurity capacity building. In Latin America, the risk of interstate conflict among countries has diminished, and nations put their limited financial resources into addressing nontraditional and human security threats, including cybersecurity, that call for adequate military resources. The ongoing cybersecurity developments have pushed states to rethink their traditional warfare roles and the equipment their armed forces use against the threats posed by state and nonstate actors such as drug cartels, paramilitaries, organized crime groups, gangs, hackers, and terrorists.

Countries can opt to develop the means of achieving cybersecurity by considering the changing character of war and extreme criminal violence, yet political and economic limitations influence how nations recapitalize their military budgets. Leaders respond differently in a complex and uncertain world. Some craft strategies across a range of contingencies, others adopt a more focused approach. I argue that in times of rapid technological change,

some states might move quickly to utilize resources and skills. In contrast, others stall and postpone any investment in new security contingencies.[28]

My primary goal is to deal with a real-world problem of great social significance: cybersecurity governance as characterized in the industrialized countries and the spillover effect it exerts on developing nations. The focus of the book is on the developing countries, specifically in Latin America. Theoretically, I engage with the prior literature on cybersecurity governance, international relations, comparative politics, and criminology. I have chosen theories from these subfields to illustrate that they might be wrong in their explanation of how developing states craft cybersecurity governance and the role of the military in administering it. I am adamant about the need to engage with the United States' cyber history to tell the case of Latin America. It is not enough to focus just on the history of cybersecurity in Latin America without analyzing events transpiring in North America. Focusing on the history of cyberspace militarization in the most technologically advanced nation in the world opens a door to discussing worldwide events and their cascading effect across the hemisphere. Many in Latin America and elsewhere might not be familiar with such a history, and that is why I write this book.

The book presents in-depth country-by-country research while constantly referring to the industrialized countries' cyber history to contextualize global outcomes. A set of empirical events explained in the book led me to generate observable implications from the theory. In particular, I focus on what I call the first wave of cybersecurity governance in Latin America, which began in the late 2000s. I take Brazil's 2008 National Defense Strategy, which named cybersecurity as one of the critical strategic domains for national security and which consequently launched a full-scale effort to institutionalize a policy designed to unite different sectors and multiple stakeholders across the public and private governance ecosystem controlling national security, defense, and information security.[29]

Brazil's strategy came at the time of the first systematic uses of cyberattacks against one state by another (accompanying a military campaign), when Russia targeted Georgia and, later, Ukraine with cyberattacks and propaganda campaigns during the short wars of 2008 and 2009, respectively. Moscow's raids, together with the Chinese People's Liberation Army's (PLA) and Beijing's "cyber-militia's" conspicuous cyberattacks, led observers to argue that cyberspace had finally turned into a medium for conflict and strategic warfare. Earlier, in 2007, Estonia was the target of a significant cyber hit that originated from inside Russia, which, to some observers, marked a

tipping point comparable to what the Hiroshima and Nagasaki bombings did for the nuclear age.[30] Marina Kaljurand, the Estonian ambassador to Moscow during the crippling 2007 cyberattacks against her country, described retrospectively the daunting effects of the assault:

> Those were the first explicitly political cyberattacks against an independent, sovereign state in history. If put into today's context, the attacks were not very sophisticated—even primitive. But back then, they were very disturbing. By that time, Estonia already had widely established Internet and e-services, and an e-lifestyle; when those services were interrupted—mainly in the banking sector—it was highly disruptive. As to the effects of the attacks? They did not kill anybody, they were not destructive. They were highly disruptive to our lives though.[31]

By the early 2000s, cybersecurity was a matter of policy discourse based on little or no tangible evidence (i.e., the United States launched its first cyber executive review in the *National Strategy to Secure Cyberspace* in 2003). Less than a decade later, more severe political actions unfolded (i.e., NATO placing and resourcing its cyber center command in Estonia soon after the Russian attacks), and policy researchers called for more attention to "cyber defense capabilities" and "cyber deterrence doctrines." Both concepts quickly gained traction among those studying and leading the armed forces' operational realities.[32] "Computer security" no longer sufficed to characterize the cyber domain. Modern "cybersecurity," understood in this context, came to integrate aspects of computer security plus an array of national security elements, henceforth operationalizing the term at the highest levels of policy and politics.[33]

In July 2010, it was publicly disclosed that the Stuxnet computer virus, the product of a joint cyberweapons operation started in 2005 by the U.S. Defense Department and Israel, had infiltrated Iran's nuclear facility Natanz, destroying uranium enriching centrifuges. Today, this kind of malware keeps being disseminated in more sophisticated versions, thus calling for more cybersecurity measures.

Cyberweapons are the multifold tools and technologies used to disrupt or destroy computer network operations.[34] Cyberweapons can also be, as Thomas Rid and Peter McBurney put it, the "computer code that is used, or design to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems and living beings."[35] The

worm Regin, for example, a so-called "cousin" of Stuxnet, according to the private firms that have tracked it, is a powerful spyware created by some government that has targeted public and private organizations in developing countries.[36]

Another example came after the 2016 United States presidential election, won by the Republican candidate Donald Trump, which became known as the most politically significant use of digital technology to that time. No critical infrastructure was brought down; instead hundreds of thousands of low-tech fake accounts, stories, tweets, and other social media platforms were used to influence the political discourse and the election outcome. The national security and intelligence bodies of the United States stepped in and uncovered plausible evidence that Russia was behind the attack. In a "textbook information-warfare operation," Moscow was able to hack the Democratic National Committee, publicizing e-mails from Hillary Clinton's top aides.[37]

Low-level but intense attacks continue to flood the Internet. In June 2019, officials from the White House announced that Donald Trump had ordered cyber retaliation attacks on Iranian military computers as a direct response to Teheran shooting down a U.S. surveillance drone. In August, cybersecurity company Anomali uncovered suspected North Korean hackers as responsible for a phishing campaign that targeted foreign ministries and multiple research centers in the United States and Europe. Hackers mimicked the French Ministry for Europe and Foreign Affairs, tricking users into entering their credentials onto the malicious website, so they could later use the information to spy on the affected inboxes. That same week, Twitter and Facebook announced measures to delete state-led disinformation campaigns disseminated by a spammy network of approximately two hundred thousand accounts originating from mainland China, which they accused of "deliberately and specifically attempting to sow political discord in Hong Kong."[38]

Cyberincidents have led us to rethink what we know about computer network attacks, their scale, and whether they are used in combination with conventional armed conflict scenarios, launched on their own, or used in conjunction with a type of armed conflict that does not qualify as an act of war.[39] More relevantly, it leads us to think about the role of the military in such scenarios.

Table I.1 shows the Global Peace Index (GPI) results for a subsample of Latin American countries. The GPI reviews the state of peace in the world, ranking countries according to three thematic categories: ongoing

Table I.1. Scores of selected countries in security ratings and GDP

Global Peace Index, 2019 Rank	Country	Score	Rank in 2016	Intentional homicides, 2016 (per 100,00 people)	GDP, 2018 (per capita, in US$)
27	Chile	1.635	27	3	15,923
75	Argentina	1.989	67	6	11,652
116	Brazil	2.176	105	30	8,920
140	Mexico	2.600	140	19	9,698
143	Colombia	2.661	147	56	6,651
144	Venezuela	2.671	143	26	16,054*

Note: Venezuela's GDP value is from 2014. An estimate from the IMF puts the 2018 value in US$ 3,373.

Source: Institute of Economics & Peace (2019), IMF (2019), and World Bank (2019).

domestic and international conflict, social safety and security, and militarization. A score closer to 1 estimates higher levels of peace. We see that only Chile ranks in the top thirty most peaceful countries globally. Argentina and Brazil have levels of peace in the middle of the index (where most countries are clustered). Meanwhile, Mexico, Colombia, and Venezuela scored at the bottom of the table.

Indexes such as the GPI frequently show proof of Latin American states entering the perils of the digital age while dragging many other security issues, most notably rising levels of violent crime, along with them. The region remains the world's highest in homicide rates (especially in Central American and the Caribbean), high incarceration rates, and organized crime, all of which is highly detrimental to state and human development.[40] The main question here is whether cyber insecurity is different from these other threats to peace. For some observers, threatening activities in cyberspace also go against human development as they "undermine people's trust in ICTs as well as their wellbeing in cyberspace."[41]

Mapping states' efforts to deal with both international security and domestic violence include cybersecurity capacity building. As they have with terrorism, transnational crime, and human trafficking, among other issues, states have implemented several initiatives to improve drafting strategies, processes, guidance, and laws that typically strengthen the creation of dedicated agencies and response teams. For these purposes, they rely heavily

on international cooperation. One or more countries can make themselves more cybersecure, promoting safer Internet governance between them.[42] When ICTs establish more secure networks, more people can engage in more activities in cyberspace (from electronic commerce to e-government services). The Organization of Americas States (OAS), for example, supports cyber-related capacity building programs for its members via training, crisis management, and exchange of best practices through its Inter-American Committee against Terrorism (CICTE) and Cyber Security Program.[43]

Another way to escape single-handling cybersecurity is through intergovernmental alliances. Most notably, the United States has been keen on facilitating bilateral cooperation on security, including cyber capacity building. Realist scholars argue that the United States has been successful in the role of central authority when it comes to international security in the Western Hemisphere, moderating the chances of interstate conflict, and shaping regional dynamics in response to perceived threats to peace.[44] It is understood that part and parcel of the great powers is to deter conflict and maintain peace by knowing which regional states are likely to initiate conflict, and why, so that they can anticipate and intervene with deterrence mechanisms. Of course, more theoretical development is needed from competing views, as conflict can happen despite deterrence efforts by a regional powerhouse.

By deterrence is understood as, "the means of dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit."[45] The goal of deterrence is to create disincentives and discourage the onset of hostile actions. In cyberspace, a deterrence stance warns other states against any seriously hostile act.[46] For this purpose, states dedicate resources not only to defensive but also toward building retaliatory offensive systems. Cyber deterrence mechanisms need not act solely in the cyber domain. Deterrence and retaliation to a cyberattack can derive from a broad range of tools (trade policy, foreign policy, military responses) and sectors (land, air, sea, space).[47]

A few questions then arise. First, can the United States deter traditional conflict in the so-called hot spots in Latin America for much longer? Second, and more relevant, can the United States deter cyber crisis escalation between regional states? How does Latin America fit in the so-called cyber problem[48] in U.S.-China relations, and what are the most critical military problems? What guides the United States in the Western Hemisphere in light of the dangerous tit-for-tat in cyberspace with Moscow and Beijing

that could bring them into conflict? On the other hand, will the global economic revolution trump cyber rivalries in the long run?

These questions are the crux of this book. I ask them mostly because, beyond any other country's efforts, the U.S. military and civilian experts at the Pentagon have put long-term resources into organizing the state around cyber affairs. Ronald Deibert at the University of Toronto put it this way:

> The recognition that cyberspace is a warfighting domain led to the creation of the US Cyber Command, which centralizes command of cyberspace operations across the US military. That the world's largest military defines cyberspace as a domain within which to project power and to fight and win wars, inevitably has system-wide repercussions, both materially and ideationally. In basic terms, the reorganization of the US military prompts changes among allied armed forces who need to be synched up operationally to cooperate.[49]

It is reasonable to expect that U.S.-made cyber knowledge is traveling abroad through military-to-military diplomacy. Despite the perceived declining U.S. multilateralism on the global stage and little actionable policy toward Latin America in recent years, Washington has not rescinded its commitments regarding enforcing treaties and supporting allies when it comes to security affairs. This strategic demand is what the U.S. government has called building partner capacity, or as former Secretary of Defense Robert Gates put it, "helping other countries defend themselves, or, if necessary, fight alongside the U.S. forces by providing them with equipment, training, or other forms of security assistance."[50] Building the military and security forces of allied countries has been in Washington's repertoire of actions since the Cold War.[51]

However, and considering costly and controversial examples beyond Latin America, including Western Europe, Greece, Philippines, South Korea, and more recently in Afghanistan, Pakistan, Yemen, and Iraq, the United States has receded and picked battles more carefully. "Helping other countries better provide for their security will be a key and enduring test of U.S. global leadership and a critical part of protecting U.S. security, as well," explained Gates.

In the Western Hemisphere, security cooperation has occurred most notably through civil and military bureaucrats pushing policy through

the channels of the Pentagon, State Department, and the U.S. Southern Command stationed in Florida. As an example, I recall that the U.S.-Chile Executive Cyber Consultation mechanism focused on bilateral cooperation, collaboration, and the protection of critical infrastructure, incident response, data security, information, and communication technology procurement, and military and law enforcement cooperation. The consultation mechanism is attended by senior-level officials from the United States, including representatives from the Department of State, the National Security Council, the Department of Homeland Security, the Department of Justice, the Department of Defense, the Department of the Treasury, and the Department of Commerce. The Chilean delegation is led by a senior official from the Ministry of Defense. It includes representatives from the General Secretariat of the Presidency, Ministry of Foreign Affairs, the Public Prosecutor's Office, the National Intelligence Agency, and the Ministry of Interior.[52] A similar mechanism was established in 2017 between the United States and Argentina, another of Washington's cyber allies in South America.

This multitude of state and nonstate bodies engaged around the cybersecurity issue leads me to discuss matters of governance. I do this in consideration of my second pillar. I argue that cybersecurity governance has come to push forward the growing agenda of human security that has captivated policy- and decision makers in the post–Cold War theatre, where traditional conflict has become a lesser priority. This way, the governance for cybersecurity has been set up among a web of decision makers, as conventional and new state resources are used toward countering risks both to the population and to the state. Scholars Lennon Chang and Peter Grabosky theorized on these matters, writing that "the governance of cyberspace is no less a pluralistic endeavor than is the governance of the physical territory," where democratic institutions overlap "to help secure cyberspace."[53]

New governance interpretations have come to challenge the folk versions of politics and policy. Centralized bureaucracies do not rule the policy arena any longer. The expansion of public policy matters to include new actors has led people to believe there is a failure of bureaucracies to solve complex social problems. State actors now try to involve new stakeholders for more extensive and widespread action. These aspects of governance are, by far, well identified, and a large body of literature has discussed their relevance. The governmental "do-it-alone" mode of thinking has given scholars the space to propose new networked, interactive, multilevel, and collaborative forms of governance.[54]

In Brazil, for example, after the 2008 National Defense Strategy was published, the government set up interactive policy communities to review the risks to their critical infrastructure, involving the state-owned Petrobras, and the ministries of defense, external affairs, health, science, and technology, plus other institutions, such as the central bank and the federal government's IT and information and security departments. Consultations on best practices, official guidelines, and monitoring standards revealed evidence of a wide range of vulnerabilities, cybersecurity holes, and network exposure that needed patching. Brazil's growing network of stakeholders now also includes public utilities, private companies, and telecom providers, all collaborating to improve regulation and expand cybersecurity measures on interconnected computer systems.[55]

I also review how countries in Latin America followed Brazil's cybersecurity endeavor by mimicking much of these in the name of national security. I treat the term *national security* in the book as a military matter. Still, I also include other issues, such as economic, climate, energy, and cyber affairs that mandate defense and foreign affairs actions from the government.[56] Brazil's Cyber Defense Command (CDCiber, its acronym in Portuguese), a unit within army, acts as the country's national center and cybersecurity-responsible agency. It is responsible for planning, coordinating, directing, integrating, and supervising cyber operations in the defense area. The CDCiber coordinates with two other agencies, the department of information and communications security, and the federal police's unit for combating cybercrime (URCC). Although the critical position rests with the head of CDCiber, which leads me to my third and final takeaway.

For the militarization of cybersecurity research pillar, I focus on the mushrooming of security networks to argue that what should hold our attention the most insistently is the gradually increasing presence of the armed forces, as steering nodes have started to take over. For example, Brazil's 2013 Defense White Paper identifies cybersecurity as a "fundamental strategic sector for national defense." It goes on to say that "efforts in the cyber sector aim to ensure confidentiality, availability, integrity, and authenticity of data circulating in Brazil's networks, which are processed and saved." It also elevates the CDCiber mandate to match "those of other existing government organizations, including through protection against cyber-attacks." It gives the Navy a role in developing technologies necessary "in particular in the area of cyber warfare," and among its priority projects it includes "the acquisition of the supporting infrastructure, and acquisition

of cyber defense hardware and software solutions (to be implemented in 2010–2023)."[57] Brazil's 2008 defense strategy has a similar rationale, as it identifies the cyber issue "as one of the three fundamental sectors for national defense of strategic importance"; it grants the Navy autonomy "in cyber technologies that guide submarines and their weapons systems, and enable them to work in network with other naval, land and air forces," while it also seeks to enhance "cyber capabilities through the development of cyber training in industrial and military fields."[58] In the United States, the Cyber Command and the National Security Agency (NSA) are under the authority of the same military officer in charge of priming both cyber defense and offense capacity. In Latin America, the same principle reigns: the military is preparing for digital operations for information and control.

Overmilitarization of cyberspace is risky. Express cyber norms of engagement at the international level are unclear despite the initial effort marked by the publication of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. As stated by legal scholar William Banks, the *Tallinn Manual* provided "much-needed confidence for states that international law applies in the cyber domain and supplied a framework for applying to cyberspace widely understood norms from kinetic conflict." However, it is considered that the manual "is not a treatise on international cyber law, nor does it establish new international law or represent the views of any states on their cyber operations. There could be no such treatise at this time because of insufficient state practice, a paucity of official state legal views, and a lack of consensus on norms."[59]

In sum, military and civilian actors enter the global cyber theatre under quite generic, still blurry, and mostly unsettled legal circumstances. In post-transitional democracies, the military's interventionist role in politics has not strengthened democratic stability.[60] Marrying the digital space to highly politicized armed forces is at least troubling.

Plan of the Book

The book presents another eight chapters. Chapter 1 builds my theoretical foundation. It introduces the debate on the case studies and the themes of cybersecurity governance to lay the ground for the networked governance approach to studying state policy and decision making. Chapter 2 reviews the digital pax Latin Americana, a term used to describe the state of peace in the Americas; this is the chapter wherein cyberthreats are pinned to

transnational nonstate parties acting outside international law. I then move on to provide some examples of the risks and opportunities for the Americas' states when they join up cybersecurity governance with the strategic agendas of defense and national security, in other words, the plausible militarization of cybersecurity. I conclude by arguing that in this new scenario of global insecurity, states are at a sensitive stage. As other scholars have highlighted, it is *how* and *when* nations decide to join the cyber era that will mark any nation's potential to use the cyber resource as an advantage.[61] I theorize on the idea that due to the militarization of cybersecurity, the next steps in the digital realm for emerging democracies will be to define their mid- to long-term strategic security dynamics, whether against threats originated in the advanced democracies, from other developing countries that pose today as traditional rivals, or from nonstate organizations with sufficiently developed cyber technologies to constitute serious risks to them.[62]

Chapter 3 debates the changing aspects of military missions and the security and defense industry in the Western Hemisphere. It discusses the political economy of arms industrialization and different policy choices adopted to develop the sector (export liberalization, protectionism, and wealth creation). It argues that cybersecurity governance has as prerequisites both goals and means that involve technologies to manage capacity and capabilities. Chapter 4 analyzes the underlying changing character of war and the strategic threats perceived in the region (interstate conflict, transnational crime, terrorism, paramilitaries and insurgencies, social and ethnic tensions, natural disasters and climate change, and cybersecurity), and how these relate to current military-industrial and economic progress. I use six comparative case studies to review my arguments: Argentina, Brazil, Chile, Colombia, Mexico, and Venezuela.

Chapter 5 surveys the U.S. and Chinese approaches in the remaking of international order and how it has carved new political and security scenarios in Latin America. The issues of cybersecurity lie at the heart of the chapter's discussion. Still, more, and broader, perspectives on commerce, international security, and military diplomacy are brought into question to provide a full picture. By the end of the chapter, I return to the cases of Mexico and Brazil to draw examples of these countries' Internet usage and belief in either the Chinese or American model of development.

Chapter 6 explores in more detail the prospects for U.S.-Latin American cyber partnerships. It argues that U.S.-led cybersecurity efforts in the region come at a moment of the overall revamping of the military's role and mission, which has brought forward, among other issues, the creation

of cybersecurity forces and cyber commands. I review three positive cases where cyber partnerships have happened (Argentina, Brazil, Chile) and three negative cases (Colombia, Mexico, and Venezuela). Chapter 7 explains different dimensions for cybersecurity maturity currently measured by OAS, which provide a review of the "first wave" of cybersecurity measures adopted by Latin American and Caribbean countries.

In writing this book, I collected empirical data from academic literature, official memos and white papers, legislation, surveys, databases, and various other public sources to build robust evidence for my primary research queries. This plan includes the use of qualitative and quantitative sources of information. For the latter, I assume no prior knowledge of mathematics or statistics. I have tried to keep the train of ideas flowing despite the usual repetition of some statistical concepts. Some of the quantitative exercises in the book are supplemented in the appendix, which includes further methodological explanations and statistical estimations.

Integrating quantitative methods to the study of cybersecurity is helpful in at least three meaningful ways. It provides a fundamental approach to understanding the large quantity of the literature being published. Second, it gives the reader a better understanding of research practices in the social sciences. Third, it relates to the current use of big data analytics using statistical methods becoming more relevant today. The idea, nonetheless, is to have first a solid grasp of the theory and then to use it intelligently to guide some exercises of hypothesis testing. The main concern here is the "relationship between theory and empirical work, not the relative merits of quantitative or qualitative approaches."[63]

In the concluding chapter, I discuss relevant results that offer a new interpretation of the theory and practice of cybersecurity governance. The arguments and conclusions will challenge scholars and policymakers to understand cybersecurity's new international and national perspectives as well as the recent policy efforts made by individual countries.

Implications for Policy

Political and economic risks during the Cold War were identified in part by the superpower rivalry between the United States and the Soviet Union. Twenty-first-century political risk is no longer split into blocs but instead crowded with uncertainty rising from state and nonstate actors across the globe.[64] Responses to cybersecurity interweave with international politics