Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: www.tandfonline.com/journals/rcyb20

Cybersecurity and cyber defence in the emerging democracies

Carlos Solar

To cite this article: Carlos Solar (2020) Cybersecurity and cyber defence in the emerging democracies, Journal of Cyber Policy, 5:3, 392-412, DOI: 10.1080/23738871.2020.1820546

To link to this article: https://doi.org/10.1080/23738871.2020.1820546

JOURNAL OF CYBER POLICY
2020, VOL. 5, NO. 3, 392–412
https://doi.org/10.1080/23738871.2020.1820546

Routledge
Taylor & Francis Group

Cybersecurity and cyber defence in the emerging democracies

Carlos Solar

Department of Sociology, University of Essex, Colchester, UK

ABSTRACT

How do we interpret current cybersecurity and cyber defence affairs beyond what we know from the advanced democracies and industrialised states? This article argues that in the emerging democracies, the military is on its way to being the dominant force controlling cyber centres or commands emulating those already established in the global North. There are three main takeaways from such developments when using the case study of the western hemisphere. First, states in the region have decided to manage their cyber affairs through inter-governmental and military-to-military diplomacy with more powerful states, such as the United States. Second, governments are eager to set up interactive policy communities at the national level to review cyber risks together with those in the defence sector. Third, militarising cyberspace in fragile political and policy settings can become somewhat risky for democratic governing. Ultimately, marrying the protection of the digital space to highly politicised armed forces might turn into a challenge when trying to set up a secure and egalitarian internet.

ARTICLE HISTORY
Received 15 January 2020
Revised 27 May 2020
Accepted 11 August 2020

KEYWORDS
Defence; military; cyber command; governance; United States; Latin America

The bulk of research on cybersecurity offers valid inferences by observing how countries protect and advance their national interests. Scholars pose broad generalisations, such as how states and citizens educate themselves to avoid hacks, while also accounting for more specific puzzles, such as why nations give a substantive amount of power to the military in the affairs of cybersecurity (Zittrain 2017). Based on its own merits, the field of cyber defence seems by now an essential object for academic and policy study, more so when global leaders, such as the UN Secretary-General António Guterres, are pessimistic about the prospects of cyber affairs. 'When one looks at today's cyberspace, it is clear that we are witnessing, in a more or less disguised way, cyberwars between states,' Guterres noted recently (UNSG 2018). In this vein, what has captured scholars' attention, and consequently divided perspectives, is the link between digital technologies, defence and the military. Some perspectives take a realist approach that delegates responsibility for cyberspace to the military and the security apparatus. This interpretation assumes that cyber threats affect sovereign states and their critical assets across territorial jurisdictions. The problem is that the armed forces,

CONTACT Carlos Solar carlos.solar@essex.ac.uk

intelligence and law enforcement agencies tend to operate under 'limited public accountability, oversight, and transparency' (Deibert 2018a, 411). To some observers, cyber affairs have integrated almost fully into how modern states manage their military affairs since it has become almost impossible to draw a line between modern warfare and digital capabilities. 'Unlike the infantry or artillery revolution, the information revolution did not just create information warriors; it informationized all conventional warriors', argues Schneider (2019, 843). Among the military themselves, they recognise that the continued advancement of technology has changed the conduct of warfare, while also 'maintaining military advantange in the cyber battefield' (Votel, Julazadeh, and Lin 2018, 19). To others, the hype over cyber defence and warfare is overblown. To them, it is highly unlikely that cyber war will occur. Instead, cyberattacks are 'merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage' (Rid 2012, 6).

There is a dividing line between perspectives. On the one hand, the excitement behind the present and future of cyber speaks to a 'revolution in military affairs with the advent of new military technologies.' On the other hand, the so-called moderate perspective 'is guided by careful consideration of what the real dangers are, as well as the costs of the overreaction' (see Valeriano and Maness 2015, 1). Expertise in both camps has grown exponentially. Scholarly articles have grasped this academic work and shed light on the interrelated topics, including nuclear weapons, artificial intelligence and grand strategy (Choucri and Goldsmith 2012; Lin 2019; Nye 2013; and Van Puyvelde and Brantly 2019). Jonathan Zittrain (2017, 301) highlighted the militarisation of cyberspace, calling out the dangers of states using their hard power against one another through actions over the internet and the overall 'characterization of the digital environment as a martial "cyber" domain.'

From this mass of knowledge, little research uses case studies from the emerging democracies where cybersecurity and cyber defence 'uncertainty' seems greater. Emerging states struggle when dealing with perceived conventional and non-conventional military threats that are too difficult to measure and scenarios that are too complicated to assess. Cyber threats can easily exploit uncertainty, and states are more likely to overstate or misjudge the actual danger posed if we understudy them (see Walt 2019). One way of dealing scientifically with uncertainty and complexity is to search for generalisations from which to make inferences.

In this article, I seek to explore cybersecurity and cyber defence interpretations beyond what we know from the advanced democracies and industrialised states, making a case for a sample of emerging democracies. The regional focus is on the developing countries, more specifically in Latin America. Theoretically, I enter a dialogue with the prior literature on cybersecurity governance, international relations and comparative politics. I chose theories from these subfields as they could be wrong in explaining how the emerging states craft cybersecurity governance and the role of the military in the dynamics of democratisation and institutional configurations. I present three main theoretical takeaways when using the case study of Latin America. First, emerging democracies in the region have decided to manage their cyber affairs through inter-governmental and military-to-military diplomacy with more powerful states, most notably the United States. Second, governments are eager to set-up interactive policy communities to review cyber risks with those in the defence sector. Third, militarising cyberspace in fragile political and policy settings can become somewhat risky for democratic governing owing to the highly politicised armed forces.

The study of cybersecurity is especially relevant in the understudied emerging nations that embraced democracy in the late twentieth century. Dealing with cyberspace has, nonetheless, seemingly 'confused' democratic societies in both the advanced and emerging nations who assign different values and preferences to a radically transformed and cybered world (Demchak 2020, 38). The way we govern cybersecurity sheds light on both democracy's main potential weak and strong governing points, including its governing institutions, economic infrastructure, and social and national security (see Rid and Buchanan 2018). I argue that emerging democracies are put to the test by many standards, including the overall expectation that they will deliver their promises for civil liberties, participation rights, and overall, inclusive and transparent governing.

Martin Libicki (2012, 129) at the RAND Corporation defined cybersecurity as the 'efforts to prevent systems from being compromised.' I take this straightforward baseline approach and define cybersecurity governance as the actions and policies adopted by civilians, the military, industry and the private sector to safeguard the digital space. In the emerging nations, however, the focus should partly lie in the military for a pivotal reason. A glance at the country profiles of Argentina, Brazil, Indonesia, Philippines, Mexico or South Korea in the UN Institute for Disarmament Research (UNIDIR) cyber policy portal confirms that emerging democracies have built or are in the process of building dedicated military agencies, such as cyber commands, and that legislation allows these to plan and take action against threats concerning cyberspace.[1]

Focusing on such developments is not a justification of national security doctrines (highly popular in the global South during the Cold War). On the contrary, it creates awareness of the issues presented when militarising cyberspace by acknowledging that this has become a standard feature among the advanced democracies. The cyber as a 'domain,' just like sea, air, land and space, has encouraged nations to put powerful civil–military agencies to lead cybersecurity governance – namely, Cyber Command in the United States, the National Cybersecurity Centre in Great Britain, Signals Directorate in Australia, the Federal Office for Information Security in Germany, the Cyberspace Administration of China and the Security Council of Russia. In the United States, Cyber Command and the National Security Agency (NSA) are under the authority of the same military officer in charge of priming cyber defence and offence capacity. The point to make here is that in the global South, we find the same backing principle: the armed forces are preparing for digital operations for information and control. As others have foreseen, 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' (Crowther 2017, 63).

To respond to the question 'how do cybersecurity and cyber defence affairs go beyond what we know from the advanced democracies?' the article first presents the context of the western hemisphere. Second, I introduce the complex dynamics occurring in the ongoing United States-Latin America cyber collaborations. Third, I present political and economic arguments questioning the new cybergovernance era. This section focuses on key underlying themes including empirical perceptions of cyber threats and risks and the construction of defence and national cybersecurity agendas, and finally, it lays out what I term the digital pax Latin Americana. Fourth, I shed light on over-militarisation and what implications for policy and governance can be identified as the most crucial. The fifth section presents my concluding arguments.

Case study: cyber defence in the western hemisphere

Latin American states are encountering the perils of the digital age while carrying the weight of many other security issues, most notably, rising levels of violent crime. The region continues to have the world's highest homicide rates (most notably in Central American and the Caribbean) and high incarceration rates. Meanwhile, organised crime is highly detrimental to the everyday life of the state and to human development. Is cyber insecurity any different to these other threats to peace? To some observers, threatening activities online also go against human development as they 'undermine people's trust in ICTs as well as their wellbeing in cyberspace' (Boulanin 2015, 397). While the chances of interstate conflict among countries has diminished, and nations put their limited financial resources into addressing non-traditional and human security threats, including cybersecurity, these tend to call for adequate military resources.

I avoid drawing a grandiose conclusion suggesting that Latin American cybersecurity governance is evenly laid out in the region. Instead, I show that, as tends to happen across all regions in the world, certain commonalities (and differences) are shared within a subgroup of countries regarding how cyber politics and security policymaking have unfolded. I draw examples mostly from those countries in the Americas that are not yet advanced industrialised democracies like Canada and the United States. However, their strategic conditions, above other developing states, have allowed them to improve their technological and security priorities in a regional system less dominated by the United States' hegemony. These states include Brazil, Mexico, Colombia, Argentina, Chile and Venezuela.[2] These have set up domestic policy communities, meaning they have pulled together the multiple bodies that deal on a daily basis with cybersecurity. I present the idea that the first wave of cyber defence governance in Latin America began in the late 2000s with Brazil's 2008 National Defence Strategy as a stepping stone. The strategy cited cybersecurity as one of the critical strategic domains for national security, consequently launching a full-scale effort to institutionalise policy, uniting different sectors and multi-stakeholders across the public and private governance ecosystem on national security, defence and information security (Hurel and Lobato 2018).

Brazil's strategy came at a time when the first use of cyber weapons (from one state to another accompanying a military campaign) became more visible. In 2007, Estonia was the target of a significant cyber hit coming from inside Russia, which to some observers marked a tipping point as significant as the Hiroshima and Nagasaki bombings were for the nuclear age (Kello 2017). Russia then hit Georgia and later Ukraine with cyberattacks and propaganda campaigns during the short wars of 2008 and 2009 respectively. In addition to the conspicuous attacks of China's 'cyber-militias,' observers argued that cyberspace had finally turned into a medium for conflict and strategic warfare. Policy researchers began calling for more attention to 'cyberdefence capabilities' and 'cyber deterrence doctrines' (Libicki 2009). 'Computer security' did no longer suffice to understand the cyber domain. Instead, 'cybersecurity' came to integrate aspects of computer security plus an array of national security elements, henceforth operationalising the term at the highest level of policy and politics.[3]

A second country, Colombia, began its path to stronger cybersecurity in 2009 as recognised by Law 1273 criminalising behaviour connected with cyber offences and information and data protection (i.e. computer and related theft, data interception, violation

of personal data, unauthorised assets transfer, website impersonation, computer damage and unlawful obstruction of a computer system). Colombia's national government set up a partnership with the Organization of American States (OAS), which resulted in the executive requesting the Ministry of Defence to lead the way in implementing cybersecurity policies. By the early 2010s, the military and the defence community were to establish anti-cybercrime and cyberattack policies based on two core ideas. First, that cyber affairs were a matter of national security, and second, that the defence network was the most capable of coordinating the cybersecurity and cyber defence national agenda (National Council on Economic and Social Policy 2011).

United States-Latin America collaborations

My first task is to explore intergovernmental and military-to-military diplomacy around the cyber affair. I argue that the United States has been keen on facilitating bilateral cooperation on security, including nowadays cyber capacity-building. Theoretically, realist scholars argue that Washington has been victorious in playing 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 (Copeland 2012). It is understood that part and parcel of being a great power is the job of deterring conflict and maintaining order by knowing which regional states are likely to initiate battle, and why, so they can anticipate and intervene with deterrence mechanisms.

By deterrence is understood 'the means of dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit' (Nye 2016, 44). For this purpose, states dedicate resources to cyber defence in building retaliatory offensive systems. However, cyberdeterrence mechanisms need not act solely in the cyber domain. The deterrence of and retaliation to cyberattacks can come from a broad range of tools (trade policy, foreign policy, military responses) and sectors (land, air, sea, space) (Nye 2016, 46). In this sense, a handful of questions arise. Can the United States deter traditional conflict in the so-called 'hot spots' in Latin America for much longer? Can the United States deter cyber crisis escalation between regional states? How does Latin America fit in the so-called 'cyber problem'[3] in US-Sino relations, and what are the most critical military problems arising from it? On the other hand, will the new interdependence driven by technology and the global economic revolution trump cyber rivalries in the long run?

The US military and the civilian experts in the Pentagon have put mounting effort into organising state-resources around the affairs of cyber (Deibert 2018b). It is reasonable to expect that such US-made cyber knowledge is travelling abroad through military-to-military diplomacy. Despite the perceived declining US multilateralism on the global stage and little actionable policy toward Latin America in recent years, Washington has not rescinded enforcing treaties and supporting allies when it comes to security affairs. This strategic demand is what the US government has called building partner capacity or as former Secretary of Defense Robert Gates (2010, 2) 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.'

Security cooperation has occurred most notably through bureaucrats pushing policy through the Pentagon, the State Department and the US Southern Command stationed in Florida. As an example, I recall the US-Chile Executive Cyber Consultation mechanism focused on bilateral cooperation, collaboration, 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 US side 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 Defence. 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 (US Department of State 2018). A similar mechanism was established in 2017 between the United States and Argentina, another of Washington's cyber allies in the hemisphere.

This multitude of state and non-state bodies engaged in cybersecurity governance leads me to introduce my second takeaway: governments are keen to create interactive policy communities to guide the way forward for cybersecurity and cyber defence governance.

A new cybergovernance era?

New governance interpretations have come to challenge the folk versions of politics and policy. Some believe that centralised bureaucracies do not rule the policy arena any longer. The expansion of public policy matters to include new actors has led people to think that bureaucracies have failed to solve complex social problems. State actors now try to involve new stakeholders for more extensive and widespread action. These aspects of governance are well-identified, and a large body of literature has discussed their relevance. The government 'do-it-alone' type of thinking has given space for scholars to propose new networked, interactive, multi-level and collaborative forms of governance (Ansell and Torfing 2016).

In Brazil, for example, after the 2008 National Defence Strategy was published, the government set up interactive policy communities to review risk on their critical infrastructure, involving the state-owned Petrobras and the ministries of defence, 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 have revealed evidence of a wide range of vulnerabilities and cybersecurity holes and network exposure that need patching. Brazil's growing network of stakeholders now also includes public utilities, private companies and telecom providers collaborating to improve regulation and expand cybersecurity measures on interconnected computer systems (Muggah and Thompson 2018). Countries in the emerging Americas followed Brazil's cybersecurity endeavour, emulating its cyber defence practices in the name of national security.

Scholars treat the term national security as a military matter. Still, it also encompasses other issues such as economic, climate, energy and cyber affairs that mandate defence and foreign affairs actions from government (Reveron, Gvosdev, and Cloud 2018).

Brazil's Cyber Defence Command (CDCiber, to give its acronym in Portuguese), for example, acts as the country's national centre and agency responsible for cybersecurity. Among its duties, it is responsible for planning, coordinating, directing, integrating and supervising cyber operations in the defence area. The CDCiber coordinates with two other responsible agencies, the department of information and communications security, and the federal police's unit for combating cybercrime.

Brazil's 2013 Defence White Paper eventually identified cybersecurity as a 'fundamental strategic sector for national defence.' 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 secured.' It also elevated the CDCiber's status to match 'those of other existing government organisations, including through protection against cyber-attacks.' Finally, it gave 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 defence hardware and software solutions.'[4]

Threats and risks

Recent events concerning critical information cyber theft highlight data security as a significant concern for advanced democracies and a growing worry for less developed countries. There has been an upward trend in large-scale cyber incidents across the region. In 2013, the costs of cybercrime in Latin America and the Caribbean were roughly US$113,000 million, 'enough to buy an iPad for the population of Mexico, Colombia, Chile and Peru' (Symantec 2014). By 2015, private cybersecurity firms had estimated nearly 400 million attempted attacks using malware. Brazil accounted for 27.6 million attacks and ranked 18th on a global scale. Other countries were equally vulnerable, including Mexico (15.9 million incidents), Colombia (5.1 million), Peru (4.3 million), Venezuela (2 million) and Chile (1.6 million) (BBC 2015). A careless attitude from users and the growing use of mobile technologies has increased the opportunities for cybercriminals, who find little deterrence given the lax enforcement of the states' rule of law (Symantec 2014). Bolder hacks have affected corporations, commerce, businesses and government infrastructure alike, according to the Kaspersky Lab, an anti-virus and security software firm that produces yearly reports on cybersecurity. Data on cybersecurity is hard to project, as there are too many interests at stake, including those of strategic national security. For example, despite its global influence, Kaspersky Lab, a Moscow-based firm, has recently fallen out of favour in some of Washington's political circles. This is due to security concerns in light of the firm having contracts with major government agencies, both in the United States and in the Americas; these contracts seem inappropriate now that Washington-Moscow cyberbullying is at a peak (Shaheen 2017).

In Mexico, the number of technology-based incidents affecting the banking sector and including identity theft and fraud have increased by a third since 2011, with its top three commercial banks' clients reporting almost a million complaints in 2017s first quarter (Rodríguez 2017). In Colombia, the authorities have detected massive malware infections in public services computers sending out fictitious communications from bogus police, criminal justice and other governmental platforms used by millions of users every day (El Tiempo 2017).

The Americas community, through the steering of Ameripol and OAS, has set up reactive policing strategies to combat the most severe and advanced cybercriminal organisations. As Contreras and Barrett (2020), two cybersecurity policy specialists working at OAS, recently put it, the organisation has helped to establish Computer Security Incident Response Teams (CSIRTs) across the region. It has also supported the implementation of national cybersecurity strategies in Colombia, Panama, Trinidad and Tobago, Jamaica, Paraguay, Chile, Costa Rica, Mexico, Guatemala, Dominican Republic and Brazil between 2011 and 2018. The authors argue, nevertheless, that structural and policy efforts have not been in tune with dedicated resources to establish dedicated career professionals, nor with the improvement of legislative frameworks to update security standards.

It is also believed that stronger multilateral cooperation and further prosecution are still pending, especially in terms of crimes that affect national security (Mattern 2014). For example, in 2012, a collective of authorities from Argentina, Chile, Colombia and Spain arrested 25 suspects, allegedly linked to the hacking group 'Anonymous' believed to have launched a series of coordinated cyberattacks against the Colombian Ministry of Defence and some presidential websites as well as Chile's Endesa electricity company (Interpol 2012). The critical industrial sector seems particularly vulnerable in this region. Only Brazil, Colombia, Chile, Mexico, Panama and Peru have implemented ICT infrastructure cybersecurity measures (as mentioned earlier, only at basic standards), leaving the rest of the subcontinent facing severe exposure. In 2015, over half of the continent's governments reported that their budgets for cyber securing their critical infrastructure had not risen in the last year (OAS 2015). The region as a whole does not invest more than US$10 million annually in cybersecurity for its industrial sector, compared to the advanced countries, such as France, where the budget for this has reached up to US$8,000 million (Notimex 2017). In light of its low-level security measures, Mexico was the fifth most disturbed country globally following the ransomware WannaCry attack on Windows-operated IT networks in over 150 nations (Latin American Post 2017).

In part because the technology used behind massive cyberattacks such as in the WannaCry incident once belonged to a governmental cyber espionage programme (stolen and later leaked by hackers), no nation can rule out the suspicion that other more advanced states are still developing cyber strategies with equal or even more damaging abilities to coerce them (see Valeriano, Jensen, and Maness 2018). Take the following example. In 2013, Brazil and Mexico complained to the US Department of State after former contractor Edward Snowden leaked data from the NSA revealing that presidents Dilma Rousseff and Enrique Peña-Nieto had their emails and phones intercepted, the latter even before assuming office (Ohlheiser 2013). In this affair, the United States only seems to amass more indiscriminate surveillance power in the western hemisphere. The Donald Trump administration recently elevated US Cyber Command, formerly a division of the NSA, to the status of a military authority. According to one observer, 'the idea is to turn the internet from a worldwide web of information into a global battlefield for war' (Bamford 2016). For the emerging democracies, this poses at least two strategic challenges.

First, potentially rival states can buy such technologies from the major powers, arguing for the protection of their still vulnerable digital resources. Second, non-state actors roaming globally can quickly get hold of these technologies, as has already been

evidenced, posing as an equally sinister force capable of significant hits to less-prepared nations. Consider the following example. Before the hacking and leaking of the Democratic Party emails during the 2016 election, which the US intelligence community pinned on hackers linked to the Russian intelligence agencies (Shane 2017), Latin America had experienced its dose of indirect voting cyber interference. Andrés Sepúlveda, a Colombian serving ten years in prison for hacking his country's 2014 election, told Bloomberg reporters that he had rigged elections in favour of right- and left-wing candidates in Nicaragua, Panama, Honduras, El Salvador, Colombia, Mexico, Costa Rica, Guatemala and Venezuela. Sepúlveda charged up to US$20,000 a month for using Russian software technologies to create 'a full range of digital interception, attack, decryption and defence' strategies, including the use of fake Twitter and Facebook accounts to influence public opinion and alienate voters (Robertson, Riley, and Willis 2016).

Defence and national security affairs

Recent hacking incidents have exposed what organisations worldwide are capable of doing with such cutting-edge cyber programmes, bringing forward the idea that for the emerging democracies, despite growing global governance on cyber affairs, what prevails is the cyber protection of their strategic priorities. This point has been discussed elsewhere by some scholars to support the thought that most cyber matters – involving both state and non-state actors – rest within the realms of defence and national security (see a debate in Rovner and Moore 2017; Matania, Yoffe, and Goldstein 2017). Two recent examples can illuminate this point. During a visit from the Chinese president, Xi Jinping, to the United States in 2013, Barack Obama claimed in a speech that state-funded cyber espionage and a nuclear-armed North Korea were the two most relevant issues dividing both countries (Lee 2013). Obama made it clear to his counterpart that cyber espionage was now as dangerous and real as Pyongyang having a weapon that could destroy millions of lives in a matter of minutes. In Europe, Denmark, for instance, claimed that Russian cybercrime groups (linked to Moscow's security services) hacked their defence system repeatedly in 2015 and 2016. The move prompted Copenhagen to increase its spending on cybersecurity on top of already significant military efforts in response to Russia's missile deployment in the Baltic (Reuters 2017). For the emerging democracies, the feeling that the cyber factor is a top priority for national security is also becoming deeply rooted.

Cyber confrontation also occurs as state defence communities try to deter organisations from acting outside international law. In 2013, for example, a group of hackers based in Peru, calling itself LulzSecPeru, targeted the email servers of Chile's Air Force (Fach), accessing information on the acquisition of missiles, radar systems and aircraft. These included communications held by the Fach with the French companies Astrium and the Etienne Lacroix Group, the North American firms Cirrus Aircraft, Kaman and General Dynamics, and the Israeli manufacturer, Rafael Advanced Defense System Ltd (Gurney 2014). LulzSecPeru argued that the hit was revenge over a 2009 incident in which Chilean hackers struck a Peruvian government website posting a painting from the War of the Pacific fought between both countries between 1879 and 1883, a war chapter that has driven trilateral enmities ever since. In Brazil, hacktivists exposed personal details of more than 50,000 Rio de Janeiro military police during the middle of a

wave of social protests over police distrust, corruption and authoritarian violence (Wells 2013). Most recently, the website of the Argentinean Army was hacked with an alleged threat from the Islamic State. Although the Triple Frontier area between Argentina, Paraguay and Brazil is recognised as an organised crime haven with possible links to foreign terrorist organisations, the authorities provided no record of members of the Islamic State roaming the country (Infobae 2017). In Colombia, on the other hand, it is said that due to the country's six-decade-long fight against the Revolutionary Armed Forces of Colombia (FARC), the military and the police have acted in coordinating security and defence issues, setting a precedent for other networked governance approaches. This is reflected in its 2011 cybersecurity policy, which brought government institutions and the private sector together to coordinate the protection of critical infrastructures in the country (OAS 2015).

Finally, we can turn to the recent episode when governments in Panama and Mexico allegedly used the military spy-hacking software Pegasus to spy on human rights defenders, journalists, political rivals and anti-corruption activists. The scandal meant Panama's former president, Ricardo Martinelli, currently residing in Miami, was subject to legal charges (Weaver 2017). Although the Israeli NSO Group claimed that it had sold Pegasus for the sole purpose of fighting terrorists, drug cartels and criminal groups (Univision 2017), the blurred line of what constitutes national security in the Americas, now including cybersecurity, is still tainted by never-ending authoritarian abuse.

When it comes to discussing human rights and cyberspace, preliminary studies have shown the correlative relationship between 'the increasing development of capabilities by states and their subsequent use for political and human rights oppression' (Brantly 2014, 142). Civil society lawyers have pointed out that in Latin America, surveillance and social control technologies reinforce structural inequality. Cybered technologies and flawed legal systems with too many grey areas have allowed 'techno solutions' many times at the expense of those being scrutinised, monitored, controlled and discriminated against, argued Venturini (2019). Most recently, over 100 civil society organisations from around the world, including in the western hemisphere, accused various governments and companies of using invasive surveillance techniques to fight the crisis caused by the coronavirus pandemic. In Brazil, for instance, civil society argued against the regional authorities' use of geolocation data to enforce the quarantine. In the past, the authorities in Rio de Janeiro have deployed facial recognition for carnival security, and a large police and military cyber operation took place during the 2016 Summer Olympics. At this point, vulnerable or exposed groups in society are at 'exceptional risk' of being threatened by their governments, and most drastically, those defending citizens' privacy and human rights (Rid and Buchanan 2018, 9).

Digital pax Latin Americana: a double-edged sword

Nowadays, a safe internet is crucial if the emerging democracies want to build robust institutions and tackle other desperate developmental issues (Clemente 2011). In Chile, for example, one of the countries with a higher internet penetration in the region, the government launched its first national cybersecurity strategy with technical support from the OAS Cyber Security Programme of the Inter-American Committee against Terrorism (CICTE) (Ministry of Interior and Public Security 2017). Chile's policy understands

cybersecurity as a 'cross-cutting and multi-factorial concept.' It underscores the creation of a networked policy community to strengthen its information infrastructure and better respond to cyberattacks, setting up policy objectives to be accomplished by 2022. Chile is set to create its first CSIRT, with a specific area dedicated to defence and military affairs. This will cover security risks and threats, including internal leakages, the destruction of critical information infrastructures, espionage and surveillance carried by other state actors, and cybercrime.

Economic growth, as the multilateral organisations are trying to tell governments, should be pursued in a regulated and protected cyber environment. However, incentives for cybersecurity regulation are truncated if countries do not agree on regional practices, especially if they link cybersecurity to public bodies (such as the military) whose job is to suspect and plan for the worst security contingencies. From that aspect, what I call the digital pax Latin Americana is a double-edged sword in the following sense: it enhances network governance collaboration for a peaceful cyber environment, but also adds another layer of military and defence planning where states put their national security at the centre.

Take two examples that illuminate the double-edged sword metaphor with the arguments presented so far. First, the regional bodies have not only permitted the militarisation of cyberspace but have prompted other states to pursue this path as the prime countermeasure. Research shows an increase in military computer network operations units from 2000 to 2017 among a sample of ninety-five countries listed as victims of cyberattacks globally by the Council on Foreign Relations (Craig 2018). Argentina, Colombia, Chile, Mexico and Venezuela have emulated Brazil's Cyber Defence Command and given the armed forces a set of roles and a mission in the protection of cyberspace (see Table 1). In this vein, Argentina is currently working with the US Department of State on a joint partnership on the cyber triad: security, defence and crime. A bilateral working group, set up in early 2017, aims to strengthen Argentina's CSIRT, foster networks of public/private cooperation, and enhance collaboration between both countries' military cyber experts (US Department of State 2017).

Table 2 shows the levels of policy and strategy development in both national cybersecurity and cyber defence across the region as reported by the Inter-American Development Bank and OAS in 2016 (see IDB and OAS 2016). Brazil scored higher in the level of maturity of its cyber defence strategy, reaching the level of 'established.' Since the rest of the countries scored in the 'formative' stage (except Venezuela), to continue improving national cyber defence strategies they need to step up their game by complying with international law and being consistent with national and international rules of engagement in cyberspace.

In Colombia, for example, cyber capacity-building in the defence sector happens at three levels: through the Colombian Ministry of National Defence and its cyber emergency response team; the Police Cyber Centre (CCP), in charge of the operational response to cybercrime; and the Joint Cyber Command (CCOC, formed by army, navy and air force cyberunits), preventing and countering cyber threats or attacks on national assets and interests (see UNIDIR 2020). The Colombian War College (ESDEGUE, to give its Spanish acronym) teaches a master's programme in which students take classes on 'Cyberattack Simulation against Critical Infrastructure for Decision-Making' to learn about decision-making during a 'cyber crisis' (Ortega 2017). The government included

Table 1. Summary of cybersecurity and cyber defence development in selected countries.

	Argentina	Brazil	Chile	Colombia	Mexico	Venezuela
Policy and strategy	National Cybersecurity Strategy Defence White Paper	Information and Communications Security and Cyber Strategy Defence White Paper National Defence Strategy	National Cybersecurity Policy Defence White Paper Digital Agenda 2020	National Digital Security Policy Policy Guidelines on Cybersecurity and Cyber Defence	National Cybersecurity Strategy National Digital Strategy	National Plan for Cybersecurity and Cyber Defence
Dedicated agency within the armed forces	General Directorate of Cyber Defence	Cyber Defence Command	Joint Cyber Defence Command	Joint Cyber Command	Cybersecurity Unit	Joint Cyber Defence Directorate
Summary of roles	*Responsibilities include the planning, formulation, direction, supervision and evaluation of cyber defence policies for the jurisdiction of the Ministry of Defence; it provides control over the Cyber Defence Joint Command of the Armed Forces.*	*Responsible for planning, coordinating, directing, integrating and supervising cyber operations in the defence area.*	*Responsible for planning and executing joint military operations in cyber defence.*	*Strengthening the technical and operational capabilities of the country to enable it to confront computer threats and cyberattacks through the implementation of protection measures, as well as the introduction of cyber defence protocols.* *Protect critical infrastructure, reducing computer risks to the country's strategic information.*	*Plan, conduct and execute information security activities, cybersecurity and cyber defence.* *Help in the national effort to maintain the integrity and stability of the Mexican state.*	*Plan, protect, neutralise, coordinate and conduct operations for cyber defence to ensure integrity in the information systems networks and the Strategic Operational Command's telecommunications, as well as respond to possible cyberattacks, threats and aggression that could affect the critical infrastructure, weapons systems and the security of the armed forces and other agencies of strategic national interest, ensuring the use of cyberspace and safeguarding it against the enemy.*
Source:	https://cyberpolicyportal.org/en/	https://cyberpolicyportal.org/en/	https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf	https://cyberpolicyportal.org/en/	https://www.estadomayor.mx/76656	https://ceofanb.mil.ve/direcciones/direccion-conjunta-de-ciberdefensa

Table 2. Policy and strategy levels of maturity in cybersecurity and cyber defence in selected countries.

	Cybersecurity	Cyber defence
Argentina	Formative	Formative
Brazil	Formative	Established
Chile	Formative	Formative
Colombia	Established	Formative
Mexico	Formative	Formative
Venezuela	Start-up	Start-up

Note: The Inter-American Development Bank and OAS cybersecurity report ranked policy and strategy maturity on a five-fold category, from low to high: 'start-up,' 'formative,' 'established,' 'strategic' and 'dynamic'.
Source: Inter-American Development Bank and Organization of American States (2016).

the issue of cybersecurity and cyber defence in its 2010–2014 National Development Plan 'Prosperity for All,' as part of the *Plan Vive Digital* (see National Council on Economic and Social Policy 2011). Today, the 2016 National Digital Security Policy and the 2011 Policy Guidelines on Cybersecurity and Cyberdefence serve as a roadmap for 'stakeholders to manage digital security risk in their activities' and to 'implement appropriate mechanisms to prevent, provide assistance, control, and offer recommendations on cyber incidents and/or emergencies for protecting critical infrastructure,' respectively (UNIDIR 2020).

Cybersecurity in Venezuela is under the authority of the Joint Cyberdefence Directorate (Dirección Conjunta de Ciberdefensa, in Spanish) at the Strategic Command Operations (Comando Estratégico Operacional, CEO, in Spanish), part of the Ministry of Defence and responsible for guiding the operations of the armed forces. The directorate is in charge of planning, coordinating and executing cyber operations affecting critical national infrastructure, the weapons systems and the telecommunications networks of the armed forces. Its role is to 'ensure the use of cyberspace denying it from the enemy' (Gobierno Bolivariano de Venezuela 2019). Regarding the development of cybersecurity capabilities for the armed forces, Venezuela recently acknowledged Russia's support in sending military experts to train the local ranks. According to a US government official, a Russian military contingent arrived in Venezuela in late March 2019, believed to be made up of special forces including cybersecurity personnel (Spetalnick 2019). Although most Latin American countries have links to foreign nations for military peer-to-peer-knowledge exchange, Venezuela's close relationship with Russia and China is viewed with particular suspicion.

In the past, global norms for international security issues have permeated the region successfully. Let us consider what happened in the early 2000s when countries in the hemisphere adopted financial intelligence units (FIU) to counter money-laundering practices supported by professional bodies such as the Financial Action Task Force (FATF), backed up by the United States and the European Union (Solar 2018). The challenge by then was to counter the finances behind global terrorism. Today, in a similar manner, cyber incidents require a set of knowledge-based capacities, use computerised intelligence, exist at a distance, and are holistic to governance networks for national security, that is, between public and private spheres. Steering and assessing a rapidly changing economic and social environment required governments to adopt policies that were both local and global.

As a second example, internet governance is currently undergoing consultations to advance a freer internet through the meaningful participation of stakeholders and

accountability mechanisms (Fraundorfer 2017). Although Brazil is the flagbearer in such an effort, its militarised approach to cybersecurity puts in doubt whether internet regulation (known for little respecting nation-states' boundaries) can bloom in the hands of such a traditionally state-centred actor without diminishing human rights and the work of democracy activists.

Placing the security and privacy of the web 2.0 in the hands of the military is at least worrying, considering the current state of insecurity and underdevelopment in Latin America, despite not having any active interstate war or any major civil conflicts such as those currently being fought in the Middle East, North Africa and South Asia. Violence in Brazil, Mexico, El Salvador, Honduras, Jamaica, St Kitts and Venezuela, plus a rising trend in the numbers of the disappeared, speak of states unable to provide the rule of law (Muggah, Carvalho and Aguirre 2018). Higher levels of suspicion and inter-agency rivalry have limited the networked effort for crime, justice and other security policies. Moreover, the intelligence agencies in Latin America have, for years, been used to spy on both political rivals and allies for the incumbent government. Policing bodies in the region also suffer from high levels of compartmentalisation in light of federal politics (i.e. Brazil, Mexico and Argentina), on top of a tremendous problem with corrupt practices and political patronage (Solar 2015).

Over-militarisation and implications for policy

My third and final takeaway is a conceptual one, based on the empirical observations presented above. Recently, Dunn Cavelty and Wenger (2020, 8) argued that cyber *security politics*, or the security political aspects of the issue, is different from cyber security *politics*, understood as the politics engaging with questions of cybersecurity more broadly. I posit more emphasis on the second dimension and argue that the over-militarisation of cyberspace is risky for democratic governing in fragile political and policy settings. Express cyber norms of engagement at the international level are unclear despite the initial effort marked by the publication of the *Tallinn Manual*. However, and as stated by legal scholars, the manual 'is not a treatise on international cyber law' (Banks 2017, 1494). Military and civilian actors in the emerging democracies then enter the global cyber theatre under quite generic, still blurry, and mostly unsettled legal circumstances. In post-transitional democracies, the interventionist role of the military in politics has not strengthened democratic stability. Marrying the digital space to highly politicised armed forces is thus troubling when trying to set up a secure and egalitarian internet.

For example, political and economic risks in the western hemisphere during the Cold War were identified by the superpower rivalry between the United States and the Soviet Union, which helped to distinguish allies from adversaries. Twenty-first century political risk is no longer split into blocs. Uncertainty rises from state and non-state actors across the globe, as Rice and Zegart (2018) point out. Responses to cybersecurity interweave changing international politics and dynamic global economic issues. Governing cybersecurity is thus an interactive exercise. It demands political, economic and social systems to come together and produce dyadic relations between national and supranational actors. Studying governance, as a means of collaboration in goal-directed networks, sheds light on the internal mechanics that allow organisations to function together. This approach raises new questions. Is cybersecurity governance a typical case of goal-directed

collaboration? How are actors interconnected? How do they communicate, share responsibility and make decisions?

A closer look into the global South's reality would allow us to know how cybersecurity agencies within regions arrange collaborative agendas, how important decisions are taken, and how power and legitimate authority interact. However, one can always doubt such an argument and ask: does the matter of cybersecurity encourage or hinder collaboration, decision-making and the lawful use of authority? Complex policy issues, even in liberal and participatory forms of democracy, pose serious questions about governance and more so in the emerging democracies where institutions are relatively fragile and have a recent past of authoritarian practices and military dictatorships.

Addressing matters of global governance, practitioners, experts and policymakers have held consultations since 2019 around the UN Open-Ended Working Group (OEWG) and the Group of Governmental Experts on Developments in the Field of Information and Telecommunications (GGE), chaired by Brazil's ambassador Guilherme de Aguiar Patriota.[5] The GGE consults with several organisations, including OAS, on responsible state behaviour in cyberspace. In 2015, it published a report recommending that states 'cooperate to prevent harmful ICT practices,' and in doing so, states 'should guarantee full respect for human rights, including privacy and freedom of expression' (UNGA 2015, 2).

Nevertheless, in the name of national security, many governing processes remain secret and under little or no external accountability beyond a close group of state agencies. In light of cyber defence now taking over cybersecurity issues, other stakeholders might become unwilling to participate if not treated equally. In this sense, overly militarising cyberspace can lure expertise away from civilians. Vertical government structures might lead to fragmentation of policy communities in smaller sub-networks, most notably, between those that prosecute cybercrime, those in charge of cyber defence, and those dealing with cyber espionage. Prosecutors, armed forces and spies are each one of a kind. As it plays out, in the emerging democracies, these institutions have a long way to go until they achieve acceptable democratic governance standards.

Conclusion

Most recent interpretations of cybersecurity argue that while in the last decades the issue was reserved for experts, nowadays, the norms and governance of the internet are a widening endeavour with many political and military ramifications. As Tikk and Kertutunen (2020, 4) argued, 'the discourse [on international cybersecurity] can be read about as (a) the sum of all global cybersecurity fears, (b) as a combination of national cybersecurity concerns, or (c) strictly a matter of peace or war.' In a similar way, and to bridge the north–south gap in cybersecurity studies, in this article I asked, 'how do we interpret current cybersecurity and cyber defence affairs beyond what we know from the advanced democracies and industrialised states?' I systematically presented three main arguments. First, the far superior cyber capacities resting in the hands of the United States have a profound impact on shaping new alliances with different actors in the emerging democracies. I argued that Washington has found willing partners to cooperate and promote dual-use information and telecommunications technologies across Latin America. 'We are connected, not only in the

traditional domains that we think about when we talk about military operations – those domains being land, sea, air, space, and cyber. But we're connected, importantly, by values and democracy,' said Navy Admiral Craig S. Faller, chief of the US Southern Command (US Department of Defense 2019). Today, Washington's allies and other like-minded states face two options: to cyber partner or not. The decision requires strategic decision-making intertwining the economic, military and diplomatic levels. Latin American countries, on the one hand, are welcoming Chinese ICTs with open arms. Since the election of Jair Bolsonaro, Brazil has engaged in serious talks with the Chinese company Huawei to launch its 5G mobile infrastructure. The same has happened in Chile under right-wing Sebastián Piñera, and in Colombia with President Iván Duque. The outcomes are still unclear as these countries have a long record of US diplomatic and military-to-military relations which will not be washed away so easily.

Second, I examined how governments set up interactive cyber policy communities including participants from the defence sector. I brought many examples to the fore but can conclude with a highly illustrative one. In 2016, the Colombian government announced, as part of the National Digital Security Policy, the future creation of its Cybersecurity and Cyberdefense Directorate (Dirección de Ciberseguridad y Ciberdefensa, in Spanish) responsible mainly for reporting cyberattacks and guaranteeing the participation of stakeholders across the executive under the authority of the Deputy Minister of Defence for Policy and International Affairs (Viceministerio de Defensa para las Políticas y Asuntos Internacionales). The end goal, as the policy notes, is to strengthen domestic capacities to allow 'cyber autonomy for the Colombian state' (see CONPES 2016, 59–60). Based on my review of policies and governmental action toward cybersecurity, the evidence collected informs us of a declaratory policy toward building national capacity to articulate cybersecurity, most notably through militarised cyber commands. The proliferation of capabilities for protecting cyberspace seems the norm across emerging democracies in Latin America. However, the upside of the booming 'techlash' is unequally distributed, considering the vast differences in capital intensity, R&D and industrial development across the region (see Muggah 2020).

Finally, I explored how militarising cyberspace in fragile political and policy settings can become somewhat risky for democratic governing. Security, privacy, surveillance and even metadata are usually treated as separate and different from democratic governance, when they are meant to be intrinsically intertwined (Bernal 2016). While the militarisation of cyberspace seems to respond to the collective need for the sovereign security of states, the impact on a broad spectrum of individual and collective rights are at stake. Cybersecurity scholars have put much effort into overlapping explanations on confidence-building, diplomacy and international law. Yet much remains to be explored in order to solve fundamental issues on cybersecurity that do not need to be sequestered by military perspectives. In the article I have identified existing and emerging cyber threats triggered by the expansion of ICTs around the emerging democracies. The UN acknowledges that we live in a world where states develop ICT capabilities for military purposes and their use in future conflicts 'is becoming more likely' (UNGA 2015, 6–7). We should take one step back and ask what we know about the new digital technologies (what they are and what they can do), and who develops and has the power to use them (Dunn Cavelty and Wenger 2020). These questions seem more relevant due to the unique path some emerging democracies are taking towards greater cyber connectivity.

Notes

1. See https://cyberpolicyportal.org/en/.
2. These six countries are part of a larger research project I am currently on cybersecurity governance, states and cyberspace in Latin America. For comparative purposes, I depict them as emerging democracies, although these regimes vastly show different political transitions and transformations if measured by the usual central liberal tenets of democracy. For example, the *Varieties of Democracy* report put Chile in the top 20 and Venezuela in the bottom 10 per cent of its liberal democracy index (see Lührmann et al. 2020).
3. See Harold, Libicki, and Stuth Cevallos (2016).
4. See http://www.defesa.gov.br/arquivos/estado_e_defesa/livro_branco/lbdn_2013_ing_net.pdf.
5. The GGE offers a limited number of memberships per region. Besides Brazil, representatives from Latin America and the Caribbean include only Mexico and Uruguay.

Acknowledgements

I would like to thank the organisers and participants at various venues where preliminary versions of this article were presented including the Latin American Centre in the University of Oxford, the International Studies Association annual convention in San Francisco, the joint workshop organised by the LSE Latin America and Caribbean Centre (LACC), the Department of International Relations at the Pontifícia Universidade Católica de São Paulo (PUC-SP) and the Department of Political Science at UNICAMP, and the British Network on Latin American Politics meeting held at the Institute of the Americas, University College London. I am also extremely thankful to Emily Taylor, Nilza Amaral and Fleur Kinson at the *Journal of Cyber Policy* and the two anonymous peer reviewers for their useful comments and valuable suggestions that helped improving the article. All errors remain solely my responsibility.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributor

Carlos Solar is Lecturer in the Department of Sociology and a member of the Centre for Criminology at the University of Essex. He is the author of *Government and Governance of Security: The Politics of Organised Crime in Chile* (New York: Routledge, 2018). His most recent research appears in *Policy Studies, British Politics, Politics & Policy,* and forthcoming in *Current Sociology*. This article draws from Carlos' next book on cybersecurity governance in the Western Hemisphere. He can be contacted through his website: www.carlossolar.com.

ORCID

Carlos Solar http://orcid.org/0000-0003-4230-3395

References

Ansell, C., and J. Torfing. 2016. *Handbook on Theories of Governance*. Cheltenham: Edward Elgar.

Bamford, J. 2016. "Commentary: The World's Best Cyber Army Doesn't Belong to Russia." http://www.reuters.com/article/us-election-intelligence-commentary/commentary-the-worlds-best-cyber-army-doesnt-belong-to-russia-idUSKCN10F1H5.

Banks, W. 2017. "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0." *Texas Law Review* 95: 1488–1513.
BBC. 2015. "Ciberdelito Aumentó en América Latina." http://www.bbc.com/mundo/noticias/2015/11/151118_tecnologia_cibercrimen_ciberdelito_aumento_america_latina_lb.
Bernal, P. 2016. "Data Gathering, Surveillance and Human Rights: Recasting the Debate." *Journal of Cyber Policy* 1 (2): 243–264. doi:10.1080/23738871.2016.1228990.
Boulanin, V. 2015. "Cybersecurity: A Precondition to Sustainable Information and Communication Technology-Enabled Human Development." https://www.sipri.org/yearbook/2015.
Brantly, A. F. 2014. "The Cyber Losers." *Democracy and Security* 10 (2): 132–155. doi:10.1080/17419166.2014.890520.
Choucri, N., and D. Goldsmith. 2012. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security." *Bulletin of the Atomic Scientists* 68 (2): 70–77. doi:10.1177/0096340212438696.
Clemente, D. 2011. "International Security: Cyber Security as a Wicked Problem." *The World Today* 67 (10): 15–17. https://www.jstor.org/stable/i40091720.
CONPES (Consejo Nacional de Política Económica y Social). 2016. Política Nacional de Seguridad Digital. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.
Contreras, B., and K.-A. Barrett. 2020. "Challenges in Building Regional Capacities in Cybersecurity: A Regional Organizational Reflection." In *Routledge Handbook of International Cybersecurity*, edited by E. Tikk, and M. Kerttunen, 214–217. New York: Routledge. doi:10.4324/9781351038904-5.
Copeland, D. C. 2012. "Realism and Neorealism in the Study of Regional Conflict." In *International Relations Theory and Regional Transformation*, edited by T. V. Paul, 49–72. Cambridge: Cambridge University Press.
Craig, A. 2018. "Understanding the Proliferation of Cyber Capabilities." https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities.
Crowther, G. A. 2017. "The Cyber Domain." *Cyber Defense Review* 2 (3): 63–78.
Deibert, R. 2018a. "Toward a Human-Centric Approach to Cybersecurity." *Ethics and International Affairs* 32 (4): 411–424. doi:10.1017/S0892679418000618.
Deibert, R. 2018b. "Trajectories for Future Cybersecurity Research." In *Oxford Handbook of International Security*, edited by A. Gheciu, and W. C. Wholforth, 532–546. New York: Oxford University Press.
Demchak, C. 2020. "Cybered Conflict, Hybrid War, and Informatization Wars." In *Routledge Handbook of International Cybersecurity*, edited by E. Tikk, and M. Kerttunen, 36–51. New York: Routledge. doi:10.4324/9781351038904-5.
Dunn Cavelty, M., and A. Wenger. 2020. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41 (1): 5–32. doi:10.1080/13523260.2019.1678855.
El Tiempo. 2017. "Colombia También es Víctima del Ataque Global Informático." http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataque-cibernetico-afecta-redes-de-74-paises-87390.
Fraundorfer, M. 2017. "Brazil's Organization of the NETmundial Meeting: Moving Forward in Global Internet Governance." *Global Governance: A Review of Multilateralism and International Organizations* 23 (3): 503–521. doi:10.5555/1075-2846.23.3.503.
Gates, R. M. 2010. "Helping Others Defend Themselves." *Foreign Affairs* 89 (3): 2–6.
Gobierno Bolivariano de Venezuela. 2019. Ciberdefensa: Comando Operacional Estrategico. https://ceofanb.mil.ve/direcciones/direccion-conjunta-de-ciberdefensa/.
Gurney, K. 2014. "Infiltration of Chile Air Force Emails Highlights LatAm Cyber Threats." http://www.insightcrime.org/news-briefs/chile-air-force-peru-hackers-cyber-threat.
Harold, S. W., M. C. Libicki, and A. Stuth Cevallos. 2016. *Getting to Yes with China in Cyberspace*. Santa Monica: RAND Corporation.
Hurel, L. M., and L. Cruz Lobato. 2018. A Strategy for Cybersecurity Governance in Brazil. https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf.
Infobae. 2017. "Hackearon la Página del Ejército Argentino con Supuestas Amenazas de ISIS." http://www.infobae.com/politica/2017/06/19/hackearon-la-pagina-del-ejercito-argentino-con-supuestas-amenazas-de-isis/.

Inter-American Development Bank and Organization of American States. 2016. *2016 Cybersecurity Report Data Set*. Washington, DC: Inter-American Development Bank. https://mydata.iadb.org/dataset/d/cd6z-sjjc/about/.

Interpol. 2012. "Hackers Reportedly Linked to 'Anonymous' Group Targeted in Global Operation Supported." https://www.interpol.int/News-and-media/News/2012/PR014.

Kello, L. 2017. "Cyber Security." In *Beyond Gridlock*, edited by T. Hale, and D. Held, 206–228. Cambridge: Polity.

Latin American Post. 2017. "Wannacry Cyberattack Numbers in Latin America." http://latinamericanpost.com/index.php/living-people/living-future/15225-wannacry-cyberattack-numbers-in-latin-america.

Lee, J. 2013. "Cyber Kleptomaniacs: Why China Steals Our Secrets." *World Affairs* 176 (3): 73–79. doi:12.

Libicki, M. C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Libicki, M. C. 2012. *Crisis and Escalation in Cyberspace*. Santa Monica: RAND Corporation.

Lin, H. 2019. "The Existential Threat From Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 75 (4): 187–196. doi:10.1080/00963402.2019.1629574.

Lührmann, A., S. F. Maerz, S. Grahn, N. Alizada, L. Gastaldi, S. Hellmeier, G. Hindle, and S. I. Lindberg. 2020. *Autocratization Surges: Resistance Grows*. Democracy Report 2020. Varieties of Democracy Institute (V-Dem). https://www.v-dem.net/media/filer_public/f0/5d/f05d46d8-626f-4b20-8e4e-53d4b134bfcb/democracy_report_2020_low.pdf.

Matania, E., L. Yoffe, and T. Goldstein. 2017. "Structuring the National Cyber Defence: in Evolution Towards a Central Cyber Authority." *Journal of Cyber Policy* 2 (1): 16–25. doi:10.1080/23738871.2017.1299193.

Mattern, B. 2014. "Cyber Security and Hacktivism in Latin America: Past and Future." http://www.coha.org/cyber-security-and-hacktivism-in-latin-america-past-and-future/.

Ministry of Interior and Public Security, Chile. 2017. National Cyber Security Policy. http://ciberseguridad.interior.gob.cl/media/2017/04/NCSP-ENG.pdf.

Muggah, R., I. Szabó de Carvalho, and K. Aguirre 2018. "Latin America is the World's most Dangerous Region: But There are Signs it is Turning a Corner." https://www.weforum.org/agenda/2018/03/latin-america-is-the-worlds-most-dangerous-region-but-there-are-signs-its-turning-a-corner/.

Muggah, R. 2020. Latin America's Coming Techlash." https://www.project-syndicate.org/onpoint/latin-america-techlash-by-robert-muggah-2020-04.

Muggah, R., and N. B. Thompson. 2018. "Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks." https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks.

National Council on Economic and Social Policy. 2011. Policy Guidelines on Cybersecurity and Cyberdefense. https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf.

Notimex. 2017. "Latinoamérica Está Expuesta a Ataques Cibernéticos." http://www.excelsior.com.mx/hacker/2017/06/03/1167503.

Nye Jr, J. S. 2013. "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists* 69 (5): 8–14. doi:10.1177/0096340213501338.

Nye Jr, J. S. 2016. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71. doi:10.1162/ISEC_a_00266.

OAS (Organization of American States). 2015. *Report on Cybersecurity and Critical Infrastructure in the Americas*. https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf.

Ohlheiser, A. 2013. "Brazil and Mexico Ask the U.S. to Explain Reports of NSA Spying on Their Leaders." *The Atlantic*. https://www.theatlantic.com/international/archive/2013/09/brazil-and-mexico-want-us-explain-reports-nsa-spying-their-presidents/311546.

Ortega, M. 2017. "Colombian Armed Forces Counter Cybercrime." *Dialogo*. https://dialogo-americas.com/en/articles/colombian-armed-forces-counter-cybercrime.

Reuters. 2017. "Russia Hacked Danish Defense for Two Years, Minister Tells Newspaper." http://www.reuters.com/article/us-denmark-security-russia/russia-hacked-danish-defense-for-two-years-minister-tells-newspaper-idUSKBN17P0NR.
Reveron, D. S., N. K. Gvosdev, and J. A. Cloud. 2018. "Introduction: Shape and Scope of U.S. National Security." In *Oxford Handbook of U.S. National Security*, edited by D. S. Reveron, N. K. Gvosdev, and J. A. Cloud, 2–12. Oxford: Oxford University Press.
Rice, C., and A. Zegart. 2018. "Managing 21st-Century Political Risk." https://hbr.org/2018/05/managing-21st-century-political-risk.
Rid, T. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32. doi:10.1080/01402390.2011.608939.
Rid, T., and B. Buchanan. 2018. "Hacking Democracy." *SAIS Review of International Affairs* 38 (1): 3–16. doi:10.1353/sais.2018.0001.
Robertson, J., M. Riley, and A. Willis. 2016. "How to Hack an Election." *Bloomberg*. https://www.bloomberg.com/features/2016-how-to-hack-an-election/.
Rodríguez, I. 2017. "Reporta Condusef Récord de Presuntos Fraudes." *Jornada*. http://www.jornada.com.mx/ultimas/2017/07/18/reporta-condusef-record-de-presuntos-fraudes.
Rovner, J., and T. Moore. 2017. "Does the Internet Need a Hegemon." *Journal of Global Security Analysis* 2 (3): 184–203. doi:10.1093/jogss/ogx008.
Schneider, J. 2019. "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War." *Journal of Strategic Studies* 42 (6): 841–863. doi:10.1080/01402390.2019.1627209.
Shaheen, J. 2017. "The Russian Company That Is a Danger to Our Security." *New York Times*. https://www.nytimes.com/2017/09/04/opinion/kapersky-russia-cybersecurity.html?_r=0.
Shane, S. 2017. "To Sway Vote, Russia Used Army of Fake Americans." *New York Times*. 7 September. A1.
Solar, C. 2015. "Police Bribery: Is Corruption Fostering Dissatisfaction with the Political System?" *Democracy and Security* 11 (4): 373–394. doi:10.1080/17419166.2015.1098540.
Solar, C. 2018. *Government and Governance of Security: The Politics of Organized Crime in Chile*. New York: Routledge. doi:10.4324/9781315160153.
Spetalnick, M. 2019. "Russian Deployment in Venezuela includes 'Cybersecurity Personnel': U.S. Official." *Reuters*. https://www.reuters.com/article/us-venezuela-politics-russians/russian-deployment-in-venezuela-includes-cybersecurity-personnel-u-s-official-idUSKCN1R72FX?feedType=RSS&feedName=worldNews.
Symantec. 2014. Cyber Security Trends Report. https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf.
Tikk, E., and M. Kertutunen. 2020. "Introduction." In *Routledge Handbook of International Cybersecurity*, edited by E. Tikk, and M. Kerttunen, 1–8. New York: Routledge. doi:10.4324/9781351038904.
UNGA (United Nations General Assembly). 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." https://undocs.org/A/70/174.
UNIDIR (United Nations Institute for Disarmament Research). 2020. Cyberpolicy Portal–Colombia. https://cyberpolicyportal.org/en/states/colombia.
Univision. 2017. "Growing Scandal in Latin America over 'Pegasus' Spy-hacking Program." http://www.univision.com/univision-news/latin-america/growing-scandal-in-latin-america-over-pegasus-spy-hacking-program.
UNSG (United Nations Secretary-General). 2018. "Address at the Opening Ceremony of the Munich Security Conference." https://www.un.org/sg/en/content/sg/speeches/2018-02-16/address-opening-ceremony-munich-security-conference.
US Department of Defense. 2019. "Southcom Chief Outlines Keys for Success in South America." https://www.defense.gov/explore/story/Article/1857725/southcom-chief-outlines-keys-for-success-in-south-america/.
US Department of State. 2017. "Joint Statement on U.S.-Argentina Partnership on Cyber Policy." https://www.state.gov/r/pa/prs/ps/2017/04/270496.htm.

US Department of State. 2018. "U.S.-Chile Executive Cyber Consultation." https://www.state.gov/u-s-chile-executive-cyber-consultation/.
Valeriano, B., B. Jensen, and R. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.
Valeriano, B., and R. Maness. 2015. *Cyber War Versus Cyber Realities*. Oxford: Oxford University Press.
Van Puyvelde, D., and A. F. Brantly. 2019. *Cybersecurity: Politics, Governance and Conflict*. Cambridge, UK: Polity.
Venturini, J. 2019. "Surveillance and Social Control: How Technology Reinforces Structural Inequality in Latin America." https://privacyinternational.org/news-analysis/3263/surveillance-and-social-control-how-technology-reinforces-structural-inequality.
Votel, J. L., D. J. Julazadeh, and W. Lin. 2018. "Operationalizing the Information Environment: Lessons Learned From Cyber Integration in the USCENTCOM AOR." *The Cyber Defense Review* 3 (3): 15–20.
Walt, S. 2019. *The Hell of Good Intentions: America's Foreign Policy Elite and the Decline of U.S. Primacy*. New York: Farrar, Straus, and Giroux.
Weaver, J. 2017. "Will Ex-President Be Sent Home to Panama to Face Charges? His Fate up to Miami Judge." *Miami Herald*. http://www.miamiherald.com/news/nation-world/article165290732.html.
Wells, M. 2013. "Brazil Investigating Hack of Military Police Data." *InsightCrime*. http://www.insightcrime.org/news-briefs/hackers-publish-personal-details-of-50000-rio-police.
Zittrain, J. 2017. "'Netwar': The Unwelcome Militarization of the Internet has Arrived." *Bulletin of the Atomic Scientists* 73 (5): 300–304. doi:10.1080/00963402.2017.1362907.