Small, Smart, Powerful?
Small States and the Competition for Cybertech Superiority in the Digital Age

Madeleine Myatt

"Size matters in international relations," claim Steinsson and Thorhallsson (2017: 1). But does it still matter in the digital age, and on the new terrain of cyberspace? Scholars have long believed that larger states are better equipped for state competition due the size of their populations, economies militaries. This basic assumption needs to be reviewed in light of new theories concerning the competitive advantage conferred by the adoption of digital and emerging technologies. The growing interconnectedness of world society through the internet and other information and communication technologies (ICTs) has created new realities for national and international politics. The digital transformation of public services (e.g. e-Government, e-Voting, e-public-procurement), critical infrastructures (e.g. IT/telecommunication, energy, water, health, public transport), the increasing digitalization of the business world, new forms of digital communication and the strategic value of huge amounts of data and its processing on a daily basis have a transformative impact on national and global affairs (see also Kļaviņš in this volume). They have also created new opportunities for small states to attempt to shape the emergent field of cybertechnology and cyber-power.[1]

To be sure, cyber power is not primarily a field of small powers. Persistent notions of an US/China "Digital or Tech Cold War" (Segal 2020), the emphasis on the use and misuse of digital tech supremacy, and the maintenance of traditional adversary concepts in the cyber domain, keep the spirit of 'great power' competition alive. Larger states are able to shape regulations,

1 I would like to thank the editors for their comments and input throughout the writing process.

norms and processes of technical standardization in ways that reinforce their competitive advantage. At the same time, however, hacking attacks, cyber espionage, disinformation campaigns, electoral interference, surveillance, and different forms of cyber intelligence operations are carried out by big and small states alongside non-state actors (including through the use of proxies). Indeed, small states like Israel, Singapore and Estonia are considered—although for different reasons—as "leading nations" in cyber security and digitalization.

The traditional correlation of size with power is therefore newly contested in the digital age. The following contribution explores how small states influence cyber security politics on the world political stage from a strategic point of view, aiming to describe the strategies Nordic countries, in particular Finland and Estonia, have adopted over the past years in cyber security politics. It further selectively addresses the translation of their strategic approach to digitalization and cybersecurity and highlights the relation of size and power in cyber affairs. The question of how far "cyber power" transcends traditional ways of understanding power is also addressed, and related to the old IR discussion on the relation of size and power (cf. e.g., Alesina/Spolaore 2003, Katzenstein 2015 [1985], 2003). The idea of cyber power rests—in distinction to a more traditional view of power—on an asymmetric notion of efficiency related to the increasing role of decentralized data and information flows, technological supply and services (Areng 2014: 1, Nye 2010). Understanding cyber-power requires a perspective which emphasizes the role of technological innovation and linked strategies of nation branding, specialization and norm shaping. Since cyber is an inherently public-private system, it also requires us to recognize the importance of effective modes of organizing relations between states and the (often transnational) private sector actors who own and operate critical technologies.

The two small states examined here, Estonia and Finland, provide interesting insights into how 'small states' make use of their digital transformation and the linked cybersecurity discourse to strive for a 'leading nation' status. 'Leading' refers to their strategic and quick digital technology adoption; their building of expertise in digital and cyber affairs based on an increasing investment in cybersecurity capacity building to develop best-practice blueprints; their strong regional cooperation, with its associated benefits for knowledge and technology transfer; and their visible striving for core hosting positions in the form of hubs of digital/cyber expertise and/or administrative coordination units within International Organisations (IOs). These expertise hubs which

not only organize cooperation but also serve as discourse arenas which (re-) produce cybersecurity politics. What is more, Estonia and Finland are particularly engaged in cybersecurity regulation, cyber norms, standard setting, the use of emerging technologies as tools and as topics in international affairs, and the fostering of digitalization more generally (domestically, regionally and internationally). Norm-entrepreneurship, a well-known strategy of the Nordic countries, involves promoting interests and shaping, shifting and setting agendas to foster the development and implementation of new norms (cf. Finnemore/Sikkink 1998; Ingebritsen 2002). This strategy and tool to exert influence on decision-making processes has been extensively addressed by scholarship on the EU (Björkdahl 2008, Ingbritsen 2002, Kronsell 2002). Theoretical scholarship on norm diffusion focuses predominantly on the role of normative non-state actors and IOs as platforms. Here, by contrast, light is shed on norm entrepreneurship as a foreign policy tool (Davies/True 2017:1-2; for Norm-Entrepreneurship in Scandinavia States, Ingebritsen 2002).

The contribution at hand analyzes if and how digital technological innovation and the strategic orientation towards cyber security help small states like Finland and Estonia to gain influence and recognition as 'authorities' in global cyber politics. The chapter begins by providing a brief overview of the different attempts to conceptualize small states in the discipline of International Relations. It then offers an equally short discussion on the advantages and disadvantages of being 'small', in order to conceptualize and evaluate the role and choices of small states in influencing world politics in general and pursuing their goals in cyber (security) politics. The chapter then turns to the conceptualization of cyber-power, and in particular the question of how some states come to be recognized as 'authorities' in cyber (security politics). Using Ole J. Sending's adapted field-theoretical lens (2017), it will be shown how states become 'authorities' in cyber-security through an ongoing competition over expertise and technological leadership between different actors. Finally, the strategies of Estonia and Finland, will be discussed in greater detail, including their translation into concrete practices.

Mapping Power, Smallness & Competition in IR: Concepts, Perceptions and Shifts

It is a common view that small states lack significant influence in great power competition (Long 2017a: 186). In a (neo-)realist lens the concept of a 'small

states' is closely linked to power, which is defined as a state's ability to influence outcomes (Browning 2006: 671). From this point of view, power manifests itself in a materially measurable form: population (sometimes understood as 'human capital'), GDP, arsenals of weapons, and armed forces personnel. These indicators are collected, compared, interrelated, and interpreted. In a processed form they are used to define 'smallness' as a relatively small amount of power. 'Smallness' becomes synonymous with 'weakness' in common narratives and political rhetoric.

In recent years, researchers have presented alternative, multifaceted analytical frameworks which compare 'size' from a more complex perspective. The six-size framework of Baldur Thorhallsson (2006) differentiates between a fixed size (population and territory), sovereignty size (e.g. degree of control over territory and borders), political size (military and administrative capabilities, domestic cohesion, foreign policy consensus), economic size (GDP, market size, and development), perceptual size (internal and external recognition), and preference size (the ideas, ambitions, and priorities of domestic elites regarding their role in the international system).

In spite of this additional complexity, however, neo-realist analysis of small states retains a focus on raw military strength and its distribution in what is taken to be an anarchic world political system. This assumption has implications for the interrelations between 'large' and 'small powers'. The freedom and scope of action of small states is considered to be dependent on larger powers in form of their goodwill, strategic interests and the hierarchical network of relations between small states and larger powers. They are classified as a category of states according to the interests (and identities) attributed to them in relation to a theoretical understanding of the logic of anarchy and the balance of power. In that respect, smallness is considered to entail a certain degree of vulnerability and a strategic security problem (Vital 1971: 8–9; Keohane 1969: 299; Knudsen 1996: 3-20; Knudsen 2002: 184, Archer et. al. 2014; cf. Thorhallsson 2018).

Liberal IR theory challenges this neorealist view of small states by focusing on the role and value of institutions and interdependence. Although scholars following this tradition often tend to stick to the established dichotomous lens of a simultaneity of small/weak and large/powerful as a descriptive category, an alternative view of power has been introduced, stressing that it "cannot be considered a homogenous, highly interchangeable commodity." (Keohane/Nye 1973: 160). A driving force for this development was the acknowledgement of an increasing interdependence on the international stage. This

also changed perceptions of the strategic and practical options remain for smaller states with limited capacities under these circumstances. Emphasizing interdependence and the emerging complexity of world politics, Keohane and Nye argue that the context in which power is exercised must be taken into account. They point to the different dynamics and logics of issue areas and the specific forms power can take in each of these (Keohane/Nye 1977: 91–98).

This perspective is reflected in studies of small states to a great extent. For instance, empirical research on the strategic behavioral characteristics of small states has highlighted, alongside their tendency to build alliances (including by 'free-riding' on larger powers [Moghaddam 2017: 310-312]), that small states also seek to foster cooperation through a strong commitment to multilateralism and an international rule-based system, and a certain degree of specialization and concentration of specific issue areas which allow particular small states to occupy a particular niches in world politics (Tarp/Bach Hansen 2013).

The neoliberal argument rests on the assumption that small states rely on and benefit from multilateral organizations more than larger ones (Neumann/Gstöhl 2006: 3-36). It also relies on the assumption that we have witnessed a 'multilateralization' of international politics over time, with an impact on actor constellations striving for multilateral cooperation (see also: Tarp/ Bach Hansen 2013: 6-7). This view of the evolution of the international political architecture has been challenged recently with the rise of populist nationalism around the globe. But it is associated not just with the popular legitimacy of international institutions. The shift in world politics towards multipolarity and 'fragmented authority' goes along with an increasing awareness for the global nature of issues like climate change, sustainability and development, terrorism, cybersecurity, pandemics, digitalization and state building process in post-conflict areas (ibid: 7). These new issue areas have created windows of opportunity for non-state actors, and also for small states to influence global politics through international organizations and institutions.

Multilateral institutions serve as vehicles to influence policies. They provide 'horizontal' discourse arenas with a participatory framework which includes codes of conduct, dispute settlement mechanisms and voting rules. Within these arenas, small states benefit from the access to information and expertise exchange (research bodies), best practice learning, and opportunities to shape the definition, implementation and monitoring of norms, rules, and codes in various issue areas (cf. Karns/Mingst 2004, Steinsson/Thorhallsson 2017: 13-14). Small states can also gain influence by occupying core insti-

tutional positions in the administrative system of international organizations (on this sort of 'network power', see Boyashov in this volume).

Research has shown that small states pursue a variety of strategies in international organizations: direct and indirect forms of lobbying (incl. influencing on the national level (cf. Keohane 1971, Mearsheimer/Walt 2009); the use of 'normative appeals' underlining the legitimacy of/ drawing on international institutions (Steinsson/Thorhallsson 2017: 9); and influencing institutional structures and policy processes, through high-level policy processes and decision making through strategic alliances as well as institutional priorities, and operational practices in international institutions (Tarp/Bach Hansen 2013). In sum, the use of this so-called soft-power toolkit plays a significant role alongside strategic and rational behavior.

A 'good reputation' and the internal and external recognition of the former is an essential element of Nye's concept of "soft power", coined in the late 1980s (cf. Nye 1990, 1999, 2002, 2004, 2006). Contrasting 'soft' with 'hard power', Nye emphasized states' ability to shape the long-term attitudes and preferences of other actors, in particular through civil society such as companies, universities, churches and charitable foundations (Nye 2004). The small states' forms of power have in common that they are not 'tested' on the battleground but depend on symbolic recognition. Liina Areng observes that small states compete over resources, markets, and attention, as well. "In this battle," she concludes, "a small state's success depends on its self-perceptions and the ability to portrait itself to others" (2014: 4). In other words, in order to influence policies and exert power in a certain field, small states have to compete for recognition as both effective and trustworthy actors in international organizations, and effective "experts" in relative policy fields. It is their success in these respects that have allowed small states such as Finland and Estonia to become recognized authorities in the field of cyber-security.

Understanding the ways in which small states have gained positions of recognized authority in a highly technical field such as cyber-security requires us to go beyond both neo-realist understandings of small states in opposition to 'great powers', and neoliberal understandings of small states as effective utilizers of 'soft power' and international organizations. It requires, instead, a more sustained look at the "politics of expertise" (Sending 2017) that structure the competition for authority in global policy fields. Sending's work employs a Bourdieuean field-theoretical lens to observe the competitive dynamics and logics for authority in the realm of global politics (for a more general view on Bourdieu in IR, cf. Adler-Nissen 2012). It offers a fruitful route to capturing

the role of expertise for small states in order to be recognized as authorities in world politics (Sending 2017: 11; cf. Müller/Freistein this volume).

Sending's work emphasizes the competition of actors for authority within policy fields. Authoritative actors decide 'what is to be governed, how and why' (ibid.). They define and determine the 'rules of the game'. This field-theoretical understanding of authority brings in a more comprehensive analytical view on the power of small and big states. It does so by pointing out that the construction and evolution of authority is fundamentally shaped by its relational dimension in the form of recognition and misrecognition (Sending 2017:12-13). For Sending, the emergence of authority on the world political stage rests on an ongoing competition for recognition in more or less distinctive issue areas of world politics (Sending 2017: 13f.) Therefore, it is important to analyze the interplay between the definition process of issues, performed governance practices, the social organization of issue areas and authority claims. For the given context and the focus on cyber and digital affairs, this also means taking a closer look at the role of knowledge and knowledge production in the Bourdieusian tradition (Bourdieu 1971, 1991, 2000). In this sense, 'knowledge' contains more than what we today would subsume under expertise. It also entails a social dimension closely linked to the Bourdieusian concept of *habitus*. It involves knowledge about how to do things, how to act and how to engage in the social sphere.

Scholars have long emphasized the role of expertise as a fundamental source of authority for various actors (e.g. the idea of epistemic communities: Adler/Haas 1992, Cross 2013, Haas 1992, or more generally: Antoniades 2003, Hall/Biersteker 2002, Price 2003). However, the development of a recognized expertise on specific issues has rarely been studied as a source of authority (see also Sending 2017: 15-18). Expertise, and the recognition as a 'leading nation' in the digital age, play a key role in small states' efforts to shape the emergent policy field of cyberspace. There are several examples of states subsumed under the 'small' label which can be discussed as being 'smart' due to their relative success in creating a brand and a recognizable blue-print for a digital or information society, in occupying specific issue areas, and in expanding their influence through the cultivation of expertise. Alongside Estonia and Finland, we might also mention Denmark, Israel and Singapore. Before considering specific cases of small states gaining authority in the field of cybersecurity policy, however, it is necessary to describe the contours of this emergent policy field in more detail.

The Coming of the Digital Age and the Cyber Domain—a New Window of Opportunity

The digital age brings several new opportunities for small states to increase their international standing. The emergence and distribution of ICTs has led to the evolution of a domain of global cyber politics, focused on topics such as internet governance, cybersecurity and cyber norms. This new field entails the development of new issue areas, which accelerate the need for international collaboration and force existing institutions to adapt. As well as being a new issue area within world politics, moreover, ICTs are transforming the ways in which world politics functions, reducing the relevance of geographical distance, and offering new means of communication, participation and observation (see Kļaviņš in this volume).

The emergence of cyber politics as both a major field *within* world politics and a transformational agent *for* world politics has significant implications. First, the cyber space is a challenge to the sovereignty of states. It is a highly integrated feature of everyday life, omnipresent in the social, political and economic sphere. Yet it is also based on the global and decentered interconnectivity, enabling a free and quick flow of data and information across national borders and jurisdictions. The everyday lives of citizens of all states are thereby implicated in transnational networks of communication that are far harder to monitor or control than older telegraph, telephone or postal infrastructures. Against this background, the relevance of borders in relation to cyberspace and cybersecurity issues needs to be addressed (Hare 2018: 1-2). In 2016, NATO and others recognized 'cyber' as an operational domain (NATO 2016). As Forrest Hare (2018: 14-15) highlights 'merely mediums in which we interact, do not have borders' but that does not mean that they do not play a role because borders 'define boundaries of sovereignty.' Second, cyberspace changes the relation between public and private actors. The sheer fact that most of the internet and ICT-infrastructure is privately owned, and that enabling technologies and emerging technological solutions are offered and distributed by private and often globally acting tech companies, requires states to acknowledge these companies as significant political interlocutors. This has boosted the evolution of new forms of 'tech diplomacy' and public/private relations. The former is best illustrated by Denmark's appointment of the first tech ambassador, approaching Silicon Valley and other tech hubs around the globe directly (Danish Ministry of Foreign Affairs 2017). This Danish foreign policy flagship aims to open up a direct diplomatic post to represent Danish

interests before companies like the 'Big Five' tech giants and to promote its tech agenda (incl. norms and values) internationally. The latter manifests itself the huge number of different forms of public/private collaboration to tackle cybersecurity issues. One recent example, the launched collaboration between the UK Government's National Cyber Security Centre (NCSC) and Microsoft for its 2021 Cyber Accelerator programme, aiming to encourage start-ups to support UK cybersecurity efforts (Yates-Roberts 2020). The contractual public private partnership (cPPP) on threat intelligence between the U.S. Department of Homeland Security, the Infrastructure Security Agency (CISA) and U.S company FireEye is another example.

Third, cyber space constitutes a new security challenge. Digitalization and emerging technologies are subject to a high pace of technical innovation and progress. The latter creates new issue areas such as certification, standardization and the need for norms and regulation. Policy action, however, mostly lags behind technological progress. Further, the vulnerabilities, and potential misuse, of the cyber domain create the need for new security and defense frameworks, or at least the modernization of existing ones (see Miadzvetskaya in this volume). Size, in its conventional sense, plays a minor role in the weaponization of digital technologies. Cyber operations such as cyber espionage, hacking attacks, system infiltration and manipulation have been carried out by small and large states alike, including Iran, North Korea, Israel, the US, the UK, China and Russia (incl. state-sponsored activities by using proxies). It seems that there really is a new way to become powerful.

Following Nye's concept of hard and soft power (1990), recent scholarship has focused on power in the digital age. Christopher Walker's essay "The Authoritarian Threat: The Hijacking of 'Soft Power'" (2016) discusses the visibility of a global trend which refers to the use of cutting-edge information technology by authoritarian regimes in order to penetrate, control and influence democracies. This is a recent and urgent matter of concern for western democracies and their institutions, as they face the challenge of being increasingly confronted with authoritarian influence from within (ibid.). Walker argues that this trend is supported and accelerated by the pervasion of digital technology, the evolution of the internet as the backbone structure of the digital age, and the transformation of the media landscape. The projection of authoritarian influence involves efforts in the form of censorship as well as the manipulation of data and content, often in the scope of disinformation campaigns to fuel friction and distrust in democratic institutions (ibid.). The International Forum for Democracy Studies published a report on these phe-

nomena and coined a term for states pursuing this strategy—"sharp power." (NED 2017) The report examines Chinese and Russian influence in four young democracies in Latin America and Central Europe. According to the report, "sharp powers" pursue the strategy to "pierce, penetrate, or perforate" the political and information environments of targeted countries (ibid.:10).

Power in world politics is both a capacity to act and a goal of action which cannot be simply reduced to the use of force. Power in cyberspace means the ability both to produce (in-)security *in* cyberspace and (in)security *through* cyberspace. Cybersecurity appears as a complex and dynamic configuration of state and non-state actors, institutions and clashing jurisdictions (Choucri et.al. 2012: 16; Choucri/Clark 2018). As Lior Tabanski (2016: 54) highlights:

> "Cyber power is not limited to information, but cuts across the other facets, elements and instruments of power, often referred to as Diplomatic, Informational, Military, and Economic (DIME). Cyber connects these elements in new ways to produce preferred outcomes within and outside cyberspace."

Nye points out that "the barriers to entry in the cyber domain are so low that non-state actors and small states can play significant roles at low levels of cost," which will lead to more competition and contestation (Nye 2010: 4). Most importantly, power can shift even to non-traditional actors, who have developed important cyberspace capabilities over time. Nye calls this transition of power from state to non-state actors "power diffusion" (ibid.: 1-2). The cybersecurity technology toolkit offers new and, generally speaking, affordable instruments to pursue political interests' via ICTs and IT-based applications (incl. open-source technologies).

Nye's conceptualization of cyber power and his insight that there are now "different actors sharing the stage" urges political scientists to broaden their perspective (ibid.: 3). Namely, they should focus on the disruptions caused by the ongoing competition for power, authority and ownership in cybersecurity. Relations in cybersecurity transcend distinctions of the public and private, the global and local. They can be observed as a dynamic web which is competitive, conflictual as well as cooperative and sometimes highly coordinated.

Capturing and visualizing "cyber power" by drawing on easily quantifiable technology projections, such as networking and system architecture, cryptography, malware or military commands is not sufficient. Conceptualizing cyber power and translating such a concept into practice requires a more comprehensive view and an understanding of the underlying variables, fundamental for the employment of practices, tools and technologies for wielding power

in cyberspace (cf. Klimburg 2011, Rowland et. al. 2014, Inkster 2017, Bebber 2017). To speak of cyber power in relation to geopolitical competition is to mainly focus on the role of states and their ability to "coordinate and employ" respective tools and practices "on the political, strategic, operational, and tactical levels" (Bebber 2017: 426). That does not mean that non-state actors cannot be powerful in cyberspace; something that is often underlined by the use of proxies in state-sponsored hostile cyber activities (on hacking, see Nissenbaum 2004).

Moreover, impactful cyber-attacks are not just reducible to a respective code. Strategic orchestration, planning, preparation and intelligence gathering play a key role. To attack an adversary at the right time and the right place requires a profound contextual knowledge, encompassing user patterns and internal workflows, system vulnerabilities, and even cultural inducing factors. One prime example of this is the 2016 Bangladesh Bank cyber heist, in which alleged state-sponsored hackers used the Swift messaging system to capture $81 million by exploiting security loopholes and drawing on deep insights in relevant context factors. The SolarWinds supply chain attack, disclosed in December 2020, is another good example of a timely, orchestrated attack. Conceptualizing cyber power more comprehensively also means focusing on the role of designing an effective relationship between ends, ways and means in potentially competitive or adversarial dynamic relations (Tabanski 2016: 54).

Identifying strategic ends is important before focusing on the means and ways used in relation to cyber and the digital realm. Because of the extensive penetration of the cyber realm into all aspects of modern life, it also means uncovering the vision and overarching idea of a given national society in relation to cyberspace.

Table 1: The different Levels of Strategy

Level	Geographic Scale	Temporal Scope	Type of Ends	Type of Power (Means)
Grand Strategy	Global	Long-term (decades)	Highest political ends	All
Strategy	All theatres of War and Conflict	Mid-term (years)	Overall military victory	Military, informational, economic
Operations	One particular theatre of war	Short term (weeks to month)	Campaign Victory	Military, Informational
Tactics	Battlefield	Very short term (minutes to days	Achievement of tactical objectives	Military
Technology	Home front, academia, industry	Variable time horizon	Competitive advantage over enemies	Technical Expertise

Source: Based on William C. Martel (2015: 30), see also: Tabansky 2016: 55.

As technological change is rapid in cyberspace, cyber power also depends on the stability and strength of internal affairs in order to be successful in external affairs. The status of the digital or information society of a country plays a significant role the recognition of that country as an authority in cyberspace. The manner in which a country deals with the digital transformation is also measured by its contacts with its citizens: both through the conduct of elections and other forms of democratic participation, and the management and security of the data generated by citizens' interactions with welfare or identity services. In this sense, digitalization impacts the way people of a society experience and practice citizenship today (e.g. Allen/Light 2015, on youth engagement: Bennett 2008). The increasing diffusion of ICTs in public management and the distribution of public goods is beneficial for small states because it reduces costs and offers the potential to increase efficiency (Areng 2014: 2-3, Kattel et. al. 2011: 61-81).

The Nordic countries are well known for developing concepts and strategies by investing in tech-diplomacy relations with major tech actors to ensure knowledge and technology transfer as well as reinforcing digital approaches to citizenship. As an educational approach 'Digital Citizenship' normally focuses on developing a high level of knowledge and skills to effectively use

digital technologies for communication, social and political participation, including the creation, distribution, and consumption of digital content. It can also extend to introducing emerging technologies like Artificial Intelligence (AI). This approach further includes the distribution of a fundamental understanding of concepts like cybersecurity, privacy, copyright and creative credit regulation, digital footprints, digital and information literacy, netiquette, and codes of conduct.

In order to benefit from and create an image as a blue-print digital society, the innovation system of a country serves further as an important cornerstone. Hence, it is important to take education, science and research into account. Core indicators for the latter are R&D spending (Anderson/Hearn 1996), education, cyber security industry relations and structures, technology export rates as well as transnational network building with view to research collaboration and tech diplomacy (cf. also: Tabansky 2016: 56-59). Even a short analytical view on the figures of R&D spending show that many small states focus on the development of their innovation system (OECD 2020). Furthermore, in order to weigh the power potential of states in the domain, it is also important to engage with principle of internal strength and stability from an institutional point of view, namely, the structure and level of cooperation of ministries in cyber politics (whole-of-government approach and/ or whole-of-society approach).

The relevance of creating a brand of a 'digital and innovative' self- and external perception in order to be recognized through the lens of expertise and a cyber power image, points further to another element of a comprehensive cyber power conceptualization: norm-entrepreneurship. As previously outlined, studies on small states underline the relevance of trying to influence institutional structures and policy processes, high-level policy processes and decision making, institutional priorities and operational practices in international institutions. Hence, being powerful in the cyber domain is also linked to the ability to shape and influence the cyber norm discourse, including technological certification and standardization. This is a strategy which especially small states are well-known for, at least in terms of stimulating and fostering attempts at regulation and standardization. In order to add empirical insights from the reality of small states in the field of global cyber politics, concrete examples, practices and strategies in relation to the cyber domain will be discussed in the following section.

The Evolution of Small State Authority in Global Cyber Politics

Small states are sometimes seen as particularly vulnerable to the perils of the digital age. One line of argumentation in the policy discourse on cyber power argues that small states are more likely to be exposed to cyber-attacks because of their relatively small size of their population, their human resource capacity, limited domestic IT capability, and the resources available for funding cyber security. This argumentation clearly follows in (neo-)realist footsteps.

As I have shown above, however, other scholars highlight the structural advantages of small countries, their efficiency and the adaptability of their domestic specialization. Scholarship on small states emphasizes their governance and bureaucracy structures, which are seen as better organized, with shorter communication channels within and between public agencies and less political distance between local and national governments (cf. Areng 2014:3-4; Kattel et. al. 2011). Moreover, the digital infrastructure and the state of a digital society plays a key role. Namely, internet and ICT-access, deployment of wireless technology and networks (incl. investment in 5G), the application and technical state of digital solutions on the governmental level as well as public management, norms and regulations, fostering digital competences among the population. This points, last but not least, to the important role of cyber capacity building measurements.

In this view, it is not the size of a population, its density or distribution that counts most. Instead, the innovation potential, the coherence of cybersecurity strategies and practices, the effectiveness of public-private relations, norm entrepreneurship and multilateral engagement, and the digital resilience of society—based on a high degree of digital and cybersecurity capacities and capabilities—appear to be relevant sources of power in cyberspace.

The following section discusses the cyber power strategies of small states in greater detail, examining the interaction between domestic strategies for maximizing cyber preparedness and innovation potential, and the pursuit of external influence through international organizations, nation branding, and regional cooperation.

Creating a Nation Brand, Finding Niches and Influencing Institutional Priorities

The Nordic countries are seen as a prime example—both as a region and as individual countries—for being 'smart, small and powerful' in cyberspace. They regularly achieve high positions in rankings on digital and cyber matters. When it comes to the use of ICT or e-governance, they are considerably above the EU average (EUROSTAT 2021). Indicators like the World Economic Forum's Network Readiness Index have listed Sweden, Denmark and Finland in the top 10 for the past several years.

Table 2: Network Readiness Index, Top 10 2019

Rank	Country/Economy	Score (Total)	Technology	People	Governance	Impact
1	Sweden	82,65	82,28	78,17	87,43	82,73
2	Singapore	82,13	78,45	73,55	88,19	88,33
3	Netherlands	81,78	84,34	74,40	88,01	80,37
4	Norway	81,30	77,69	76,00	90,30	81,20
5	Switzerland	81,08	83,47	79,54	87,28	80,27
6	Denmark	81,08	77,22	79,54	87,28	80,27
7	Finland	80,34	78,66	75,28	88,15	79,27
8	The United States	80,32	87,32	73,59	88,74	71,65
9	Germany	78,23	77,51	72,6	83,94	78,87
10	United Kingdom	77,73	78,16	69,81	88,32	74,62

Source: World Economic Forum, Network Readiness Index 2019 (WEF 2019)

Estonia has been one of the first countries to prioritize the development of a comprehensive digital and ICT strategy. This strategy has been consequently followed and implemented by adapting its institutional structure accordingly and investing in the development of cyber capacities and capabilities. The slogan "We have built a digital society and we can show you how", carried on Estonia's "E-Estonia" website, expresses Estonia's nation brand as a role model for the construction of an "efficient, secure, and transparent" digital "ecosystem"—an e-state (E-Estonia 2020). The small country with a population of 1.3 million has the highest level of e-governmental structures with 99% of state

services online and 99% of the population in possession of an electronic ID. Estonia possesses an e-resident system and has established an e-voting system. Image branding constantly underlines how well Estonia has done in international rankings (#2 Internet Freedom Index, #1 entrepreneurial activity (World Economic Forum), #1 digital health index (Bertelsmann Foundation). In sum, Estonia remains an interesting and relevant case to study, as it stands like no other for coping with its comparable small size by increasing its "functional size" through emphasizing "the transformative power of ICTs and innovation" (Areng 2014: 7-8).

Estonia's ambitious e-resident project (which started in 2014) is particularly relevant in this context. This project aims not only to provide e-services to Estonian residents, but to foster investment and get hold of global expertise. Instead of tapping only the IT expertise of Estonia's native population, the e-residency gathers a "borderless digital society" of "global citizens" (E-Estonia 2020). Estonia's image campaign puts forward the idea of a digital fraternity of allied states. With a rising significance of data, which is detached from a nation's territory, data flows become more and more constitutive for a country. The "Data-Embassy" project predominantly stands for this idea in form of exploring options to duplicate vital national databases in highly secure servers abroad, provided through transnational public/private partnerships. The project intends to ensure the digital survival of the state, even if it loses sovereignty over its territory. "Estonia is on its way to becoming a 'country without borders'" (OECD 2018: 5), writes the OECD, and highlights that "the data embassy is one of several Estonian programs that blurs the lines of national borders and sovereign identity in a digital world" (OECD 2018).

Despite and because of Estonia's efforts and achievements in digitalization, it has become a target of cyber-attacks and has experienced a glimpse of what cyberwar can look like. In 2007, Estonia's critical services and digital infrastructure were subjected to severe cyberattacks. It is today believed that they have originated in Russia and were meant as coercive punishment for Estonia's decision to relocate a Soviet military monument. This experience had a fundamental impact on the state's domestic, regional, and international political agenda in terms of prioritizing cybersecurity and fostering security collaboration in the cyber domain. The chain of incidents created furthermore a new awareness on the world political stage, namely the acknowledgement that cyber operations have become an indispensable element of modern, hybrid conflicts. In this sense, cyber means can enhance traditional means or can be a "stand-alone capability that can give substantial asymmetric advantage

to states that are considered weaker in terms of traditional combat power" (Areng 2014:6).

Estonia has accordingly taken on the role of a constant and active player in creating awareness for cyber related issues, especially by pushing cybersecurity and the establishment of cyber norms. The country is hence a prime example for showing off the "ability of militarily aligned small states to function as norm entrepreneurs to increase their own state interests" in the cyber realm (cf. Crandall/Allan 2015: 346). The country plays a leading role in shaping and accelerating the cyber policy discourse, particularly in the NATO and the EU. Estonia's leading role in the development of NATO's first cyber defense policy in 2008, and its numerous contributions of fostering EU initiatives in ICT security, are just a few examples of this. Against this background, it is not surprising that Estonia introduced its 2017 presidency of the Council of the EU under the label of the "digital presidency" (Patriocolo 2017). Many of the themes pushed and implemented during the presidency aimed at digitalization: progression on the taxation of the digital economy and the free movement of data, approval of an ecommerce VAT package, and an agreement on further steps to develop 5G networks across Europe.

Beside Estonia, Finland is usually named as a digital forerunner in Europe. The two countries have a close cross-border relationship especially in digital affairs based on their rather early jump on the digital bandwagon. With respective roots in the late 1990s, Finland and Estonia evaluated their cross-border relationship in advance of Estonia's EU accession in 2004. The final report "Finland and Estonia in the EU" highlighted cross-border cooperation, information society and energy cooperation as common priorities with respective synergy effects ever since (Sirviö 2019).

In many respects, Finland is the stereotype of a small state in the neorealist understanding. It has a rather small population of just above 5.5 million, limited military capabilities, and natural resources. Its territory of 338,455 km² is small from a global, but large from a European perspective. Finland's geopolitical position next to Russia and the former Soviet Union shaped its external and self-perception and has an ongoing impact on its politics. Against the background of having a relatively long border with Russia as well as the previous experience of the rise, expansion and fall of the former Soviet Union, the country preserved a threat narrative which is still powerful. Hence, it is not surprising that besides fostering the digital transformation of the Finnish society and a brand as an innovative tech-nation (e.g the AI governmental

project and the AI online citizen education program 'Elements of AI'[2]), Finland occupied the issue of hybrid warfare in the digital age. As well as making hybrid threats and hybrid warfare a central national political issue, the country took advantage of the contemporary discourse on disinformation, fake news, manipulation and electoral interference through digital means by state and non-state adversaries including cyber espionage and cyber-attacks, to address the role of security relevant grey-zone practices on the world political stage by framing and distributing a concept of 'hybrid warfare' and fostering institutionalization in the respective policy field. Finland's EU Council Presidency, running under the program slogan "Sustainable Europe—Sustainable Future" highlights that in a complex and unpredictable world, innovation is needed, but EU common norms and values are increasingly challenged, online and offline. The digital age and interconnectivity through the cyber domain create a paradox, namely, more connectivity goes along with more vulnerabilities which can be exploited by adversaries. Hence, strengthening the capacities and capabilities to prevent and respond to hybrid threats, including fostering closer NATO/EU relations, was one of the main priorities during Finland's presidency.

Hosting the Hybrid Centre of Excellence for Countering Hybrid Threats (Hybrid CoE9), is not only relevant in order to emphasize the respective genesis of the issue at hand and its interrelation with the evolution of future technologies. The organizational structure of Hybrid CoE is interesting as well in order to capture the relational dimensions of recognition. Hybrid CoE, established in April 2017 based on a collaboration of originally nine participating states (Finland, Sweden, the United Kingdom, Latvia, Lithuania, Poland, France, Germany and the United States), joined by Estonia, Norway and Spain in July 2017, the Netherlands, Italy, Denmark, Czech Republic, Austria, Canada, Romania, and Cyprus during 2018 and Greece, Hungary, Luxembourg, Montenegro, Portugal, Slovenia, and Turkey in 2019, takes on the space of organized transnational political forum.

Finland, which holds the secretariat that manages the center's administration, general functions, and external relations, including the organization of cooperation and liaison with participating states, the EU and the NATO, therefore plays a key role in shaping the center and its transnational discourse arena of practitioners and academic experts. The secretariat moreover coordinates all the relevant activities of the three communities of interest (COI):

2 See for more information https://www.elementsofai.com/ (last access: 02/09/2020).

(1) hybrid influencing, (2) strategy and defense, and (3) vulnerabilities and resilience and the work of linked expert pools, consisting of academics and practitioners of participating member states and IOs. A lot of the organizational and social practices in use clearly reflect and the gatekeeper and management role of Finland, incorporate the dynamics of recognition and misrecognition as a central constitutional element of constructing authority.

Regional Cooperation, Using Institutional Institutions as Platforms and Influencing Institutional Structures

Regional collaboration forms between Baltic and Nordic states in different policy areas has a long tradition, resting on strong political and cultural ties, and is recently omnipresent in the policy fields of digitalization and cybersecurity. This long tradition is especially embodied through the 'Nordic cooperation' which establishes constant collaboration forms between Denmark, Finland, Iceland, Norway, and Sweden as well as the Faroe Islands, Greenland and the Åland Islands. Institutionalized through the Nordic Council of Ministers (inter-governmental format) and the Nordic Council (inter-parliamentary format), it claims to be "one of the most extensive forms of regional co-operation anywhere in the world", seeking to raise "a strong Nordic voice in the world and an in European and international forums. The values shared by the Nordic countries help make the region one of the most innovative and competitive in the world." (NORDEN 2020)

Nordic cooperation can be seen as an attempt to build a regional brand, resting on the attribute ensemble of green, sustainable, innovative, smart and technologically advanced. This set of attributions is moreover used for individual nation branding attempts. Noticeable in this context, it seems that the Nordic countries follow a niche strategy which enables to create country specific external visibility in a specific digital tech niche in line with the engagement in IOs (e.g. Finland: Hybrid Warfare & AI applications, Estonia: Cybersecurity, Denmark: Introducing new ways of Tech.-Diplomacy & Big Data).

This strategy is extended through the Nordic states' visible striving for occupying hosting and gatekeeper positions in the shape of central positions in the bureaucracy networks or in form of hubs of digital/cyber expertise (centers of excellence) within IOs or in strong relation to multiple IOs. States like Estonia (NATO Cooperative Cyber Defense Centre of Excellence (CCD COE), Finland (Hybrid Centre of Excellence (Hybrid CoE)) or Denmark make use of the asymmetric toolbox of 'cyber power' to gain leverage in the interna-

tional security realm, especially by obtaining those strategic positions in addition their national and joint regional attempt to create digital and cyber resilient societies. These expertise hubs which not only organize cooperation and knowledge production, but also serve as discourse arenas which (re-)produce security politics, the involved imaginaries of (cyber) security and insecurity and their visualization.

Furthermore, small states are often very keen to place their nationals in high-ranking positions in IOs (Nordic countries in the UN system, see: Thorhallsson 2012). This pattern is also observable in the context of global cyber as well as digital politics. One example is the Estonian/Brussels revolving door effect with view on staff and personal is remarkable, as former Estonian government and ministry officials increasingly take over key position in the context of the EU Digital Single Market. Similar attempts to establish respective modes of organization, aiming to support the development of sustainable and common ICT-security and regional competitive advantages, are already discussed on a higher political level.

Norm entrepreneurship: being small, smart, and powerful through shaping and influencing cyber norm building

Another important element of cyber power is the ability to influence and shape norms and regulation in relation to cyberspace and cyber security in particular. This involves the enhancement of international normative power by taking on an active role in the adaptation and development of new norms of state behavior for cyberspace. Shaping technical certification and standardization can similarly be perceived as an example of exercising smart power in the cyberage. Therefore, it is no surprise that some small states are explicitly engaged in the global cyber norm forums like the United Nations Group of Governmental Experts (UN GGE) and the UN-mandated Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), in launching and playing a key role in initiatives like the 'Freedom Online Coalition' (e.g. Finland & UKs collaboration on dis-& misinformation) or participating in multi-stakeholder formats like Global Commission on the Stability of Cyberspace (GCSC).

The NATO Cooperative Cyber Defense Centre of Excellence (CCD COE) in Tallinn, and the engagement of Estonia but also other small member states in its activities, is another example. The CCD COE serves a key driver for technical capability and epistemic authority on cyber related issues (Hansen/Nis-

senbaum 2009). The latter entails e.g., the ongoing legal analysis of the applicability of international law to cyber conflict, which led to the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare.

The pursuit of norm entrepreneurship in cyberspace is not restricted to the Nordic states. One of the small states which not only regionally, but also on the global level, advanced recently as a cyber norm entrepreneur with a respective standing is Singapore. Singapore has sought to foster cybersecurity collaboration under the ASEAN umbrella, and collaborated recently with the UN in order to develop a checklist for cyber security norm implementation for countries. The cybersecurity norm implementation checklist continues efforts to encourage the adoption of the eleven voluntary, non-binding norms for responsible behavior in cyberspace which have been proposed by the UN GGE in 2015 (UN GGE 2015).

Conclusion

There is little doubt about the fact that the digital age brings several new opportunities for small states to gain competitive advantages in the light of power politics on the world political stage. The internet and ICTs make it possible for small states to be highly connected by providing new channels of communication and information exchange, creating new opportunities to develop and shape their own ideas of a digital society, especially if their authority and expertise are recognized by others. Moreover, one could argue that the size and density of their digital footprints, which heavily rely on intangible goods, is disproportionately large. Even those voices who are in favor of emphasizing military power must admit that dependencies on digital infrastructure creates new issues, routines and vulnerabilities which cannot be addressed with conventional military means. The digitization of defense technology and increasing pervasion of open-source "dual-use" items increase the complexity of world affairs. Hence, a sheer focus on resource-based and compulsory power appears to be insufficient to assess the power of small states in the digital age. In this sense, the latter may specialize in less conventional ways and means, drawing on institutional, structural, and productive facets of power or non-traditional forms of compulsory power (Long 2017a: 200-201).

Cyber power or "the ability of states to project power in and through cyberspace" (Bebber 2017: 426) is more than a quantifiable technological toolkit and resources. It rests on a set of structural and domestic variables and re-

sources like the innovation system and technology industry, human capital, strategic culture and thinking, the adaption and diffusion of ICTs on the social, political and economic level, the structure of political institutions (incl. inter-agency cooperation), public/private relations, the ability to integrate cyber capabilities and capacities (vertically & horizontally), the digital infrastructure (virtual and physical, e.g., fibre, cable, wireless, social networks), but also the ability to shift and shape global cyber norms and technical standards ore being integrated in international cooperative networks (ibid.: 427-429, for global cyber norms cf. Finnemore/Hollis 2016).

Furthermore, it is important to recognize that the possession of cyber power capabilities and capacities is just one aspect. Translating them into practice and orchestrating these efforts strategically is also fundamental. The comparison of cases of small but powerful states in cyberspace show that countries like Finland, Estonia, Israel or Singapore deploy and manifest their cyber power quite differently. Israel's cyber start-up nation is well-known and recognized on the world political stage for its innovative cyber tech industry, strategic behavior and offensive cyber security and defense capabilities, showed off regularly in—from time to time —controversial cyber operations (cf. Tabansky/Ben Israel 2015). Singapore in contrast is also recognized as an advanced cyber tech nation but recently occupied a strong visibility as normative force based on the recognition that cyber norm and standard-setting are power tools.

Both of these additional examples lead us further to the third important implication. Cyber powers have to be recognized as such, which brings us back to Ole J. Sending's instructive approach. This usefully highlights that authority is not given, nor inscribed into a specific set of actors, but rather induced by the ongoing competition for recognition as an 'authority' capable of determining what is to be governed, by whom and for what purpose (Sending 2017: 3-11). This also points to the relational dimension of power based on processes of recognition and misrecognition. This relational dimension, although not observed through a field-theoretical lens, has also been picked up by scholars of "small states studies". Tom Long (2017b: 163-165) for instance, defines power as an asymmetrical relationship to capture the agency of states.

Countries like Estonia and Finland represent prime examples of a coping strategy with its comparable small size label by increasing its "functional size" through emphasizing "the transformative power of ICT and innovation" (Areng 2014: 7-8) into a competitive advantage in the continuous competition for recognition as an authoritative actor. In this sense, the initial question, if

the triad of being "small", "smart" and "powerful" is a suitable way to address the relative role of size in contemporary world politics, can be answered in the affirmative. But it is not without limitations. One example is the so-called digital divide and the ability to invest, adapt, foster and secure ICTs and an evolving digital infrastructure. Size is not irrelevant in world and global cyber politics. This is *inter alia* visible in the US/China global tech power competition. But in the cyber age, we should nonetheless consider a reformulation of a famous IR remark (Wendt 1992; 2013): "size and power are what states make out of them".

References

Adler-Nissen, Rebecca (2012): "Why International Relations Theory Needs Bourdieu", E-International Relations, October 23 (https://www.e-ir.info/2012/10/23/why-international-relations-theory-needs-bourdieu/).

Adler, Emanuel/Haas, Peter M. (1992): "Conclusion. Epistemic Communities, World Order, and the Creation of a Reflective Research Program." In: International Organization 46/1, pp. 367-390.

Alesina, Alberto/Spolaore, Enrico (2003): The Size of Nations, Cambridge, MA: The MIT Press.

Allen, Danielle/Light, Jennifer S. (2015): From Voice to Influence: Understanding Citizenship in a Digital Age, Chicago: University of Chicago Press.

Anderson, Robert H./Hearn, Anthony C. (1996): An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: 'The Day After…in Cyberspace II', Santa Monica: RAND Corporation.

Andreas Antoniades (2003): "Epistemic Communities, Epistemes and the Construction of (World) Politics." In: Global Society 17/1, pp. 21-38.

Archer, C./Bailes, A.J.K./Wivel, A. (2014): Small States and International Security. Europe and Beyond, Milton Park: Taylor & Francis.

Areng, Liina (2014): "Lilliputian States in Digital Affairs and Cyber Security", The NATO Cooperative Cyber Defense Centre of Excellence Archive, Tallinn Paper Series 4, (https://ccdcoe.org/uploads/2018/10/TP_04.pdf).

Bebber, Robert (2017): "Cyber Power and Cyber Effectiveness: An Analytic Framework." In: Comparative Strategy 36/5, pp. 426-436.

Bennett, W. L. (2008): "Changing Citizenship in the Digital Age." In: W. L. Bennett (ed.), Civic life online: Learning how digital media can engage youth, Cambridge, MA: MIT Press, pp. 1-24.

Bourdieu, Pierre (1971): "Systems of Education and Systems of Thought." In: M. F. D. Young (ed.), Knowledge and Control, New Directions in the Sociology of Education, London: Macmillan.

Bourdieu, Pierre (2000): Pascalian Mediations, Cambridge: Polity.

Bourdieu, Pierre/Thompson, John B. (1991): Language and Symbolic Power, Cambridge: Polity.

Browning, Christopher S. (2006): "Small, Smart and Salient? Rethinking Identity in the Small States Literature." In: Cambridge Review of International Affairs 19/4, pp. 669-684.

Choucri, Nazli/Clark, David (2018): International Relations in the Cyber Age. The Co-Evolution Dilemma, Cambridge, MA: The MIT Press.

Choucri, Nazli/Elbait, Gihan Daw/Madnick, Stuart (2012): "What is Cybersecurity? Explorations in Automated Knowledge Generation." In: MIT Political Science Working Paper 2012/30, pp. 1-27.

Claudia Patricolo (2017): "Estonia: Europe's Little Technological Giant", Emerging Europe, December 14 (https://emerging-europe.com/intelligence/estonia-europes-little-technological-giant/).

Crandall, Matthew/Allan, Collin (2015): "Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms." In: Contemporary Security Policy 36/2, pp. 346-368.

Cross, Maia (2013): "Rethinking Epistemic Communities Twenty Years Later." In: Review of International Studies 39/1, pp. 137-160.

Danish Ministry of Foreign Affairs (2017): "Denmark names first ever tech ambassador", Ministry of Foreign Affairs of Denmark (https://um.dk/en/news/newsdisplaypage/?newsid=60eaf005-9f87-46f8-922a-1cf20c5b527a).

Davies, Sara/True, Jacqui (2017): "Norm Entrepreneurship in Foreign Policy: William Hague and the Prevention of Sexual Violence in Conflict." In: Foreign Policy Analysis 13/3, pp. 701-721.

E-Estonia (2020): "E-Identity", E-Estonia Website (https://e-estonia.com/solutions/e-identity/e-residency/).

Eurostat (2021): "Individuals using the internet for interacting with public authorities", Eurostat, January 26 (http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ei&lang=en).

Finnemore, Martha/Sikkink, Kathryn (1998): "International Norm Dynamics and Political Change." In: International Organization 52/4, pp. 887-917.

Haas, Peter M. (1992): "Introduction. Epistemic Communities and International Policy Coordination." In: International Organization 46/1, pp. 1-35.

Hall, Rodney Bruce/Biersteker, Thomas J. (eds.) (2002): The Emergence of Private Authority in Global Governance, Cambridge: Cambridge University Press.

Hansen, Lene/Nissenbaum, Helen (2009): "Digital Disaster, Cyber Security and the Copenhagen School." In: International Studies Quarterly 53/4, pp. 1155-1175.

Hare, Forrest (2018): "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?", The NATO Cooperative Cyber Defense Centre of Excellence Archive, October 6 (https://ccdcoe.org/uploads/2018/10/06_HARE_Borders-in-Cyberspace.pdf).

Ingebritsen, Christine (2002): "Norm Entrepreneurs: Scandinavia's Role World Politics." In: Cooperation and Conflict 37/1, pp. 11-23.

Ingebritsen, Christine/Neumann, Iver B./Gstöhl, Siegline (2012): Small States in International Relations, Seattle: University of Washington Press.

Inkster, Nigel (2017): "Measuring Military Cyber Power." In: Survival 59/4, pp. 27-34.

Karns, Margaret P./Mingst, Karen A. (2004): International Organizations: The Politics and Processes of Global Governance, Boulder: Lynne Rienner Publishers Inc.

Kattel R./Randma-Liiv, T./Kalvet, T. (2011): "Small States, Innovation and Administrative Capacity." In: V. Bekkers/J. Edelenbos/B. Steijn (eds.), Innovation in the Public Sector, IIAS Series: Governance and Public Management, London: Palgrave Macmillan, pp.61-81.

Katzenstein, Peter J. (1985): Small States in World Markets: Industrial Policy in Europe; Ithaca: Cornell University Press.

Katzenstein, Peter J. (2003). "Small States and Small States Revisited." In: New Political Economy, 8/1, pp.9- 30.

Katzenstein, Peter J. (2015): Small States in World Markets. Industrial Policy in Europe, Ithaca: Cornell University Press.

Keohane, Robert O. (1969): "Lilliputians' Dilemmas. Small States in International Politics." In: International Organization 23/2, pp. 291-310.

Keohane, Robert O. (1971): "The Big Influence of Small Allies." In: Foreign Policy 2, pp. 161-182.

Keohane, Robert O./Nye, Joseph S. (1973): "Power and Interdependence." In: Survival 15/4, pp. 158-165.

Keohane, Robert O./Nye, Joseph S. (1977): Power and Interdependence: World Politics in Transition, London: Little.

Klimburg, Alexander (2011): "Mobilizing Cyber Power." In: Survival 53/1, pp. 43-60.

Knudsen, Olav (2002): "Small States, Latent and Extant: Towards a General Perspective." In: Journal of International Relations and Development 5/2, pp. 182-198.

Knudsen, Olav F. (1996): "Analysing Small State Security: The Role of External Factors." In: Werner Bauwens/Armand Cleese/Olav F. Knudsen (eds.): Small States and the Security Challenge in the New Europe, London and Washington: Brassey's.

Kronsell, Annica (2002): "Can Small States Influence EU Norms? Insights from Sweden's Participation in the Field of Environmental Politics." In: Scandinavian Studies 74/3, pp. 287-304.

Long, Tom (2017a): "Small States, Great Power? Gaining Influence Through Intrinsic, Derivative, and Collective Power." In: International Studies Review 19, pp. 185-205.

Long, Tom (2017b): "It's not Size that Matters, it's the Relationship: from 'Small States' to Asymmetry." In: International Politics 54/2, pp. 144-160.

Martel, William C. (2015): Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy, Cambridge: Cambridge University Press.

Mearsheimer, John J./Walt, Stephen M. (2009): "Is It Love or The Lobby? Explaining America's Special Relationship with Israel." In: Security Studies 18/1, pp. 58-78.

Moghaddam, Fathali M. (2017): The SAGE Encyclopedia of Political Behavior, Thousand Oaks: SAGE.

NATO (2016): "Fact Sheet on Cyber Defense", North Atlantic Treaty Association (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defense-eng.pdf).

NED (2017): "Sharp Power: Rising Authoritarian Influence", National Endowment for Democracy, December 5 (https://www.ned.org/sharp-power-rising-authoritarian-influence-forum-report/).

Neumann, Iver. B./Gstöhl, Sieglinde (2006): "Introduction: Lilliputians in Gulliver's world?" In: Christine Ingebritsen /Iver B. Neumann/Siegline Gstöhl/Jessica Beyer (eds.), Small States in International Relations, Seattle: University of Washington Press, pp. 3-36.

Nissenbaum, Helen (2004): "Hackers and the Contested Ontology of Cyberspace." In: New Media & Society 6/2, pp. 195-217.

NORDEN (2020): "Official Nordic Co-Operation", Nordic Co-Operation Website (https://www.norden.org/en/information/official-nordic-co-operation).

Nye, Joseph S. (1990): "Soft Power." In: Foreign Policy 80, pp. 153-171.

Nye, Joseph S. (1999): "Redefining the National Interest." In: Foreign Affairs 78/4, pp. 22-35.

Nye, Joseph S. (2002): The Paradox of American Power: Why the World's only Superpower can't go it Alone, Oxford: Oxford University Press.

Nye, Joseph S. (2004): Soft Power. The Means to Success in World Politics, New York: Public Affairs.

Nye, Joseph S. (2010): "Cyber Power", Harvard Kennedy School, Belfer Center for Science and International Affairs (https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf).

OECD (2018): "Case Study: The first Data Embassy." In: Embracing Innovation in Government: Global Trends 2018, p. 42-44 (https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf).

OECD (2020): "Gross domestic spending on R&D (indicator)", OECDilibary (https://www.oecd-ilibrary.org/industry-and-services/gross-domestic-spending-on-r-d/indicator/english_d8b068b4-en).

Price, Richard M. (2003): "Transnational Civil Society and Advocacy in World Politics." In: World Politics 55, pp. 579-606.

Rowland, Jill/Rice, Mason/Shenoi, Sujeet (2014): "The Anatomy of a Cyber Power." In: International Journal of Critical Infrastructure Protection 7/1, pp. 3-11.

Segal, Adam (2020): "The Coming Tech Cold War with China: Beijing is Already Countering Washington's Policy", Foreign Affairs, September 9 (https://www.foreignaffairs.com/articles/north-amrica/2020-09-09/coming-tech-cold-war-china).

Sending, Ole Jacob (2017): The Politics of Expertise. Competing for Authority in Global Governance, Michigan: University of Michigan Press.

Sirviö, Ville (2019): "Estonia and Finland—Digital forerunners in cross-border cooperation", The University of Turku, the Pan-European Institute, October 30 (https://sites.utu.fi/bre/estonia-and-finland-digital-forerunners-in-cross-border-cooperation/).

Steinsson, Sverrir /Baldur Thorhallsson (2017): "Small State Foreign Policy." In: Oxford Research Encyclopedia of Politics, Oxford: Oxford University Press.

Tabansky, Lior (2016): "Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy." In: Proceedings of the 8th International Conference on Cyber Conflict, NATO Cooperative Cyber Defense Centre of Excellence, 51-63.

Tabansky, Lior/Ben-Israel, Isaac (2015): Cybersecurity in Israel, New York: Springer.

Tarp, Maria Nilaus/Bach Hansen, Jens Ole (2013): "Size and Influence. How Small States Influence Policy-Making in Multilateral Arenas." In: DIIS Working Paper 2013/II, unpaginated.

Thorhallsson, Baldur (2012): "Small States in the UN Security Council: Means of Influence?" In: The Hague Journal of Diplomacy 7/2, pp. 135-160.

Thorhallsson, Baldur (2018): Small States and Shelter Theory: Iceland's External Affairs, Milton: Routledge.

UN GGE (2015): Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Group of Governmental Experts, Report A/70/174 (https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174).

Vital, David (1971): The Survival of Small States: Studies in Small Power/Great Power Conflict, Oxford: Oxford University Press.

Walker, Christopher (2016): "The Authoritarian Threat: The Hijacking of 'Soft Power'." In: Journal of Democracy 27/1, pp. 49-63.

Wendt, Alexander (1992): "Anarchy is What States Make of it: The Social Construction of Power Politics." In: International Organization 46/2, pp. 391-425.

Wendt, Alexander (2013): "Anarchy is What States Make of it." In: Richard K. Betts (ed.): Conflict after the Cold War: Arguments on Causes of War and Peace, Boston: Pearson.

World Economic Forum (2019) Network Readiness Index 2019 (https://networkreadinessindex.org/2019/).

Yates-Roberts, Elly (2020): "NCSC and Microsoft partner for UK cybersecurity accelerator", TechRecord, November 5 (https://www.technologyrecord.com/Article/ncsc-and-microsoft-partner-for-uk-cybersecurity-accelerator-116960).