Journal of Political Science and International Relationship (JPSIR)

ISSN: 3065-6125 (ONLINE)

VOLUME 3 ISSUE 1 (2026)

PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

Journal of Political Science and International Relationship (JPSIR)

Volume 3 Issue 1, Year 2026
ISSN: 3065-6125 (Online)
DOI: https://doi.org/10.54536/jpsir.v3i1.6935
https://journals.e-palli.com/home/index.php/jpsir

Small States and Domain-specific Power: Estonia's Cyberdiplomacy and the Scope Conditions of Neorealist Theory

Guilherme Barcha Cardoso Schneider[1*]

Article Information

Received: December 10, 2025

Accepted: February 07, 2026

Published: July 27, 2026

Keywords

Cyber Governance, Cyberdiplomacy, Estonia, Neorealism, Norm Entrepreneurship, Scope Conditions, Small States

ABSTRACT

Neorealist theory posits that power derives from material capabilities and that small states exercise limited agency within great power-dominated hierarchies. Estonia, with 1.3 million citizens and minimal military capacity, has achieved notable influence in shaping international cyber norms. This paper investigates whether Estonian cyberdiplomacy reflects independent agency or a permissive great-power consensus. Through process tracing of Estonia's institutional initiatives (2007-2024), comparative analysis with Latvia and Lithuania, and systematic examination of success and failure cases, this research demonstrates that Estonia exercises meaningful but circumscribed agency through norm entrepreneurship. The findings reveal that power operates differently across issue domains: in technical-legal domains characterized by high complexity, mutual vulnerability, and nascent institutionalization, small states with concentrated expertise can exercise influence through epistemic authority and institutional positioning. Influence remains contingent on alignment with great power interests. When interests diverge, as in the 2017 UN Group of Governmental Experts collapse, Estonian advocacy fails. These findings specify scope conditions under which neorealist predictions about small state powerlessness do not apply, demonstrating that domain-specific analysis supplements rather than replaces structural theory in technical-legal domains.

INTRODUCTION

In July 2017, the Fifth United Nations Group of Governmental Experts (GGE) failed to reach consensus after two years of deliberations. Russia, China, and Cuba rejected Western proposals, advocated prominently by Estonia, affirming the applicability of self-defense rights and international humanitarian law to cyber operations (Korzak, 2017). Three months later, at the 2017 Internet Governance Forum, delegates from 92 countries referenced the Tallinn Manual 2.0,produced under Estonian institutional leadership, as authoritative guidance on international cyber law (Schmitt, 2017).

This juxtaposition presents a puzzle for international relations theory. Kenneth Waltz's neorealism holds that material capabilities determine power: small states lacking military and economic resources exercise minimal agency (Waltz, 1979). Estonia's GDP of $37 billion ranks 107th globally; its military expenditure of $700 million represents 0.001 percent of global defense spending (World Bank, 2024, for 2023 data). Estonia hosts NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), led the development of the Tallinn Manual, maintains the EU's first Cyber Diplomacy Department, and exercises institutional leadership in UN cyber governance forums.

This paper investigates the following research question: Under what scope conditions can small states exercise meaningful influence in international norm-setting, and what does Estonian cyberdiplomacy reveal about the domain-specific limitations of neorealist theory? The analysis contributes to IR scholarship by: (1) specifying domain characteristics that moderate neorealist predictions; (2) demonstrating norm entrepreneurship mechanisms through which small states exercise bounded agency; (3) identifying when small state influence succeeds versus fails; and (4) clarifying the relationship between material power and domain-specific influence.

The paper proceeds through six sections: literature review on great power theory, small state agency, and cyber power; materials and methods specifying research design and operationalization; results and discussion presenting theoretical framework, case evidence, analysis, and counterarguments; conclusion synthesizing findings and implications.

LITERATURE REVIEW

Neorealism and Material Power

Waltz's Theory of International Politics (1979) grounds state behavior in system structure: anarchy, functional similarity of units, and distribution of capabilities. Only the third variable changes, reshaping polarity and altering state behavior. Power correlates with material capabilities: military strength, economic capacity, technology, population, and geography (Waltz, 1979, p. 131). Mearsheimer's offensive realism modifies this, arguing great powers maximize power seeking regional hegemony rather than merely ensuring survival (Mearsheimer, 2001). This framework generates testable predictions: rising powers destabilize systems; balancing emerges against threats; small states align with great powers. Yet neorealism encounters difficulties in domains where material asymmetries do not translate into influence. Keohane and Nye's Power and Interdependence (1977)

[1] Logos University International, Paris, France
[*] Corresponding author's e-mail: guilherme.barcha@gmail.com

demonstrated that power varies across issue areas, but this insight remained marginalized in mainstream realism.

Small State agency and norm entrepreneurship

Handel (1981) defines small states as those unable to affect the international system through military or economic means alone, yet argues they retain conditional agency. Panke (2010) demonstrates that small EU states overcome disadvantages through coalition-building and argumentation. Ingebritsen (2002) shows Scandinavian states function as norm entrepreneurs through moral authority and policy innovation.

Understanding how small states exercise agency requires examining multiple dimensions of power beyond material capabilities. Barnett and Duvall (2005) distinguish four power dimensions: compulsory (direct control), institutional (shaping rules), structural (determining positions), and productive (constituting meanings). Small states may lack compulsory power but exercise institutional and productive power.

Finnemore and Sikkink (1998) specify norm entrepreneurship mechanisms. Norms emerge when entrepreneurs use organizational platforms to persuade critical mass of states. Success requires: (1) institutional platforms; (2) framing resonating with existing values; (3) credible principled motivation; and (4) coalition-building reaching tipping points. After cascading, norms become internalized and taken-for-granted.

Cyber power and distinctive domain characteristics

Nye (2010, 2011) defines cyber power as "ability to obtain preferred outcomes through use of electronically interconnected information resources" and notes cyberspace creates "power diffusion" because "low price of entry, anonymity, and asymmetries in vulnerability mean small actors have more capacity" than in traditional domains. Valeriano and Maness (2015) provide empirical analysis of 190 cyber incidents (2001-2014), finding cyber operations rarely achieve strategic effects through coercion, suggesting power operates through influence rather than domination.

Cyberdiplomacy refers to diplomatic efforts establishing international norms, legal frameworks, and governance institutions for state behavior in cyberspace (Barrinha & Renard, 2017). The field emerged following Estonia's 2007 cyber attacks, which catalyzed NATO engagement. The Tallinn Manual process (2009-2017) exemplifies institutional norm-setting: assembling experts to interpret existing international law's application to cyberspace (Schmitt, 2013, 2017).

This literature identifies theoretical gaps that this paper addresses: neorealism lacks domain-specific analysis; small state scholarship requires specification of scope conditions for agency; cyber governance literature needs systematic theory-testing. This paper fills these gaps by specifying when and how small states exercise influence in technical-legal domains.

MATERIALS AND METHODS

Research design

This study employs process tracing, comparative case analysis, and norm life cycle theory to assess whether Estonia exercises independent causal influence. Process tracing examines "the chain of events by which initial conditions are translated into outcomes" (George & Bennett, 2005, p. 206), identifying mechanisms linking Estonian actions to international outcomes. Three cases are analyzed: (1) Tallinn Manual development and diffusion, (2) UN GGE deliberations (2013-2021), and (3) bilateral cyber cooperation.

Comparative analysis examines Latvia and Lithuania as "most similar" cases: Baltic states with comparable populations, post-Soviet histories, NATO membership, and geographic proximity to Russia. Variation in outcomes despite structural similarity indicates causal factors beyond material position.

Operationalizing influence

Influence is operationalized at three levels with ascending evidential standards

Level 1 (Rhetorical): States cite Estonian-developed frameworks in official documents. Weak evidence; citation may reflect convenience.

Level 2 (Behavioral): States adopt policies previously rejected following Estonian advocacy. Requires demonstrating: (a) initial opposition; (b) Estonian engagement; (c) subsequent adoption; (d) acknowledgment of Estonian role.

Level 3 (Outcome): International norms reflect Estonian preferences differing from initial great power positions.

Evidence of Levels 2-3 supports independent agency. Evidence confined to Level 1 suggests permissive consensus. Failure cases identify scope condition boundaries.

Data sources

Primary sources: Estonian Ministry of Foreign Affairs Cybersecurity Strategy 2019-2022 (Republic of Estonia, 2019), Cyber Diplomacy Department reports; NATO CCDCOE Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013) and Tallinn Manual 2.0 (Schmitt, 2017); UN GGE reports (2013, 2015, 2021); bilateral agreements (Estonian-Singaporean, Estonian-Ukrainian); Netherlands Ministry of Foreign Affairs Letter to Parliament on the International Legal Order in Cyberspace (July 2019).

Secondary sources: Academic literature on norm entrepreneurship, small state theory, cyber conflict, and international cyber law.

Published statements: Publicly available interviews, speeches, and policy documents from Estonian officials including Ambassador Tiirmaa-Klaar.

RESULTS AND DISCUSSION

Theoretical framework: scope conditions for Small State agency

Norm entrepreneurship and contingent agency

Finnemore and Sikkink (1998, p. 898) define norm entrepreneurs as "agents having strong notions about appropriate behavior" who "convince a critical mass

of states to embrace new norms." Success requires organizational platforms, resonant framing, principled motivation, and coalition-building.

Small states function as entrepreneurs when possessing: (1) concentrated expertise in emerging technical domains; (2) institutional positions providing advocacy platforms; (3) credible commitment to principles; and (4) alliances with like-minded states. However, constraints include great power vetoes, resource limitations, institutional access dependence, and technical expertise insufficiency alone.

This paper conceptualizes small state agency as contingent agency: meaningful but bounded influence operating within structural parameters set by great power tolerance. Small states are not powerless (contra neorealism's determinism) but neither do they exercise unconstrained autonomy (contra liberal optimism). Agency exists but remains contingent on structural conditions.

Domain-specific power characteristics

Baldwin (1979, p. 164) argued power is domain-specific: "A may be powerful in some domain but not others." The cyber domain exhibits five characteristics reducing great power advantage:

1. Technical complexity: Specialized expertise not directly correlated with military spending or GDP
2. Mutual vulnerability: All states face cyber threats regardless of size, creating interdependence
3. Low barriers to entry: Cyber capabilities developed with modest resources compared to conventional military systems
4. Epistemic uncertainty: Novel technology creates demand for expert guidance to interpret legal and technical questions
5. Nascent institutionalization: Underdeveloped governance creates openings for early movers before great power consolidation

These characteristics suggest scope conditions where small state agency expands. Conversely, domains with established great power dominance, clear capability asymmetries, and consolidated institutions constrain small state agency.

Scope conditions: logical framework

This paper identifies six scope conditions moderating neorealist predictions about small state powerlessness. These conditions operate hierarchically:

Necessary Condition:

• SC4 (Great Power Alignment): Small state influence requires great power non-opposition as necessary condition. Without SC4, influence fails regardless of other conditions.

Enabling Conditions (increase probability of influence given SC4):

• SC1 (Domain Characteristics): Small states exercise greater relative influence in technical-legal domains with high complexity, mutual vulnerability, nascent institutions, and epistemic uncertainty than in traditional military or economic domains.

• SC2 (Institutional Positioning): Small states hosting international organizations or chairing working groups exercise greater influence than those lacking such positions.

• SC3 (Epistemic Authority): Small states facilitating authoritative knowledge production exercise influence through productive power when great powers face uncertainty.

• SC5 (Coalition Strength): Small state influence increases when building coalitions amplifying voice beyond individual capacity.

• SC6 (Norm Maturity): Entrepreneurs exercise greater influence when norms are emerging than when status quo hardens and antipreneurs consolidate resistance.

Framework Logic: Small state influence in norm-setting requires great power non-opposition (SC4) as necessary condition. Given SC4, influence probability increases with favorable domain characteristics (SC1), institutional platforms (SC2), epistemic authority (SC3), coalition strength (SC5), and favorable timing (SC6). The combination of enabling conditions determines influence magnitude within parameters set by great power tolerance. This framework specifies when neorealism's predictions prove insufficient rather than replacing structural theory. Neorealism correctly identifies ultimate constraints (great power veto) but inadequately explains mechanisms operating within those constraints. The theoretical contribution is identifying domain-level and strategic variables moderating structural predictions.

Case study: Estonia's transformation from victim to norm entrepreneur

From vulnerability to strategic opportunity (2007-2012)

In April 2007, Estonia experienced three weeks of DDoS attacks following dispute over relocating a Soviet war memorial (Herzog, 2011; Tikk *et al.*, 2010). The attacks, attributed to Russian state-sponsored actors, paralyzed government websites, financial systems, and media. At the time of the 2007 attacks, Estonia's digital dependency: 95 percent of banking online, 98 percent of tax declarations electronic, created asymmetric vulnerability (Kalvet, 2007).

Rather than retreating, Estonia strategically converted vulnerability into institutional opportunity. NATO established the CCDCOE in Tallinn (May 2008), with Estonia as the host nation providing infrastructure and approximately 30 percent of the budget (NATO CCDCOE, 2020). Estonia developed its first National Cybersecurity Strategy (2008), among the earliest comprehensive national strategies globally. By 2019, Estonia established the Cyber Diplomacy Department within the Ministry of Foreign Affairs, appointing Ambassador-at-Large Heli Tiirmaa-Klaar (Republic of Estonia MFA, 2019).

This strategic choice reflected deliberate positioning: Estonia framed its 2007 experience initially through victim identity (2007-2010), emphasizing vulnerability

and need for international protection. This victim framing built solidarity with other vulnerable states and moral authority. Subsequently (post-2013), Estonia transitioned to entrepreneur identity, positioning as cyber resilience model and norm leader. This identity evolution was strategic: victim framing when advocating defensive norms (protect critical infrastructure); entrepreneur framing when proposing legal innovations and institutional leadership.

The Tallinn manual and institutional leadership (2009-2017)

In 2009, the CCDCOE invited an International Group of Experts (IGE) to produce a manual on international law applicable to cyber warfare. Twenty international law experts from multiple countries met eight times (2010-2012) in Tallinn, producing Tallinn Manual 1.0 (2013) with 95 "black letter rules" (definitive legal principles) interpreting how existing international law applies to cyber operations (Schmitt, 2013).

The Manual's interpretive approach, which claims to "restate extant law" rather than create new law, enhanced its legitimacy (Schmitt, 2013, p. 4). However, "restatement" involved interpretive choices on contested questions: When does cyber operation constitute "use of force"? When do operations violate sovereignty? What due diligence obligations exist? The Manual's interpretations filled normative vacuums (Jensen, 2017).

Tallinn Manual 2.0 (2017), with 31 experts, broadened scope to peacetime operations, providing 154 rules with over 500 pages of commentary (Schmitt, 2017).

Evidence of influence

Level 1 (Rhetorical): Multiple states reference the Tallinn Manual in their national cyber strategies. The US Department of Defense Law of War Manual (2016) cites Tallinn Manual 15 times. The UK, France, Germany, Netherlands, Australia, Canada, and Japan published position papers engaging Tallinn frameworks (Jensen, 2017; Schmitt & Vihul, 2014).

Level 2 (Behavioral): The Netherlands provides the strongest evidence. In July 2019, the Dutch Minister of Foreign Affairs published a comprehensive position paper adopting Tallinn Manual interpretations on sovereignty violations, due diligence, and countermeasures (Netherlands Ministry of Foreign Affairs, 2019). The paper explicitly states: "In this regard, the Netherlands expressly adopts the approach taken by the IGE [International Group of Experts] according to which sovereignty may be violated either on the basis that effects of the operation manifest on territory or the operation interferes with inherently governmental functions" (Netherlands MFA, 2019, p. 3). This explicit adoption of the IGE/Tallinn Manual interpretive framework represents Level 2 behavioral influence, as the Netherlands moved from strategic ambiguity to a clear legal position following expert clarification.

Evidentiary Limitation: Direct evidence linking Dutch position change specifically to Estonian advocacy (rather than to NATO CCDCOE as the institutional sponsor or to the IGE, the international expert group) remains limited. The Dutch paper references the Manual and IGE collectively, not Estonia specifically. This reflects institutional attribution dynamics: epistemic authority accrues to the international expert community and NATO institution rather than Estonia as individual state. Estonia's contribution is providing the institutional platform and organizational infrastructure enabling expert consensus formation, rather than producing knowledge directly as a national actor.[1]

Counterevidence: Russia and China explicitly rejected Tallinn Manual interpretations. Chinese scholars criticized it as "manipulation by Western think tanks" exceeding international law (Ku, 2017, p. 12). Russian Ministry of Defense called it "potentially dangerous" (quoted in Tikk & Kerttunen, 2017). Neither participated in Tallinn Manual 2.0, promoting alternative cyber sovereignty frameworks (Ling, 2021). This reveals scope condition boundaries: Estonian-facilitated influence operates within NATO/Western sphere but fails to persuade states with conflicting governance models, confirming SC4 (Great Power Alignment) as necessary condition.

UN GGE: success and failure (2013-2021)

Estonia participated in three UN GGEs (2013, 2015, 2017) and the Open-Ended Working Group (OEWG, 2019-2021).

2013-2015 GGEs (Success): Both reached consensus affirming international law applies to cyberspace. The 2015 GGE identified 11 voluntary norms, including: states should not harm critical infrastructure; cooperate on cybercrime; exercise due diligence, preventing territory use for harmful activities (UN GGE, 2015). Estonian participation legitimized its norm advocate positioning.

2017 GGE (Failure): Estonia and Western states advocated explicit affirmation of self-defense rights under UN Charter Article 51, international humanitarian law applicability, and countermeasures rights. Russia, China, and Cuba rejected this language, arguing it would militarize cyberspace. After two years, GGE failed without consensus report (Korzak, 2017; Tikk & Kerttunen, 2017).

US representative Michele Markoff stated: "The reluctance of a few participants to seriously engage on international legal issues prevented consensus" (Markoff, 2017). Russian representative Andrei Krutskikh stated: "Use of force in cyber and real space alike is absolutely inadmissible" (quoted in Tikk & Kerttunen, 2017, p. 4).

Interpretation: The 2017 failure demonstrates SC4 (Great Power Alignment) as necessary condition. Despite Estonian institutional position, epistemic authority facilitation, and coalition-building with Western allies, advocacy failed when conflicting with Russian and Chinese core interests. This represents critical negative evidence: Estonian norm entrepreneurship reaches structural limits when great power interests diverge,

regardless of institutional platform or expert authority. Neorealism's predictions hold at this structural boundary. 2019-2021 OEWG (Partial Success): Open to all 193 UN members, the OEWG reaffirmed 2015 GGE norms but avoided explicit self-defense/IHL language causing 2017 failure (UN OEWG, 2021). Ambassador Tiirmaa-Klaar characterized this as "progress within constraints," accepting partial success over total failure (Tiirmaa-Klaar, 2021). This reflects contingent agency: small states adapt strategy to structural constraints rather than confronting great power vetoes.

Analysis: mechanisms and scope conditions

Four mechanisms of Estonian influence

Mechanism 1: Institutional platform for epistemic authority

Estonia exercises influence by providing an institutional platform enabling international expert consensus formation. The Tallinn Manual represents the most comprehensive cyber law interpretation, produced by 20-31 international experts (not Estonian nationals exclusively) convening under Estonian institutional auspices. Estonia's contribution is hosting NATO CCDCOE, organizing expert meetings, providing administrative infrastructure, and funding publication—creating organizational platform for epistemic community formation.

This mechanism operates through productive power (Barnett & Duvall, 2005): shaping how issues are understood through facilitating knowledge production rather than directly compelling state behavior. Epistemic authority accrues to the international expert group and institutional sponsor (NATO CCDCOE) rather than Estonia individually, but Estonia gains reflected authority and legitimacy through institutional association.

Evidence: Widespread state citations of Tallinn Manual; adoption of interpretations in national strategies; Netherlands' explicit reference to "IGE approach" demonstrating deference to expert consensus; use of Manual in legal training at military and diplomatic academies globally.

Mechanism 2: Institutional positioning and agenda-setting

Estonia's hosting of NATO CCDCOE provides platform for norm entrepreneurship beyond knowledge production. The CCDCOE organizes annual conferences (CyCon), training exercises (Locked Shields involving 2,000+ participants from 30 countries), research publications, and expert consultations. This creates regular interactions where Estonian priorities receive disproportionate attention.

Agenda-setting power derives from organizational position rather than material capabilities (Barnett & Finnemore, 2004). Estonia shapes NATO cyber doctrine, training curricula, and research agendas through CCDCOE director appointments, working group chairs, and administrative control. Evidence: NATO Cyber Defense Pledge (2016) incorporated Estonian-advocated principles on burden-sharing and collective defense applicability to cyberspace.

Mechanism 3: Coalition-building with like-minded States

Estonia amplifies voice through coalitions with small and medium states sharing cyber vulnerability. Estonian MFA coordinates with Latvia, Lithuania, Netherlands, Finland, Denmark, and Singapore on cyber norm advocacy (Republic of Estonia MFA, 2019). At 2021 OEWG, 34 states endorsed joint statement on cyber norm implementation coordinated through Estonian diplomatic channels (UN OEWG, 2021, Annex A).

Coalition-building reflects SC5: single small state voice carries limited weight, but coordinated small state coalition signals broader consensus and constrains great power arbitrary action through multilateral pressure.

Mechanism 4: Credible principled commitment

Estonia benefits from perceived principled commitment rather than strategic manipulation. As cyber attack victim (2007) rather than aggressor, Estonia claims moral authority in advocating protective norms. As digitally dependent state requiring stable cyberspace for economic functioning, advocacy for cyber stability norms appears self-consistent rather than hypocritical.

This addresses the "persuasion paradox": why should states accept norms proposed by self-interested actors? Finnemore and Sikkink argue that altruistic framing enhances persuasiveness (1998, p. 898). Estonia frames cyber norms as universal protection (all states benefit from stable, peaceful cyberspace) rather than particular Estonian advantage. Evidence: Developing country support for Estonian positions at UN forums; adoption of Estonian capacity-building assistance by Singapore, Ukraine, Georgia, Kenya, Moldova (Republic of Estonia MFA, 2019, pp. 12-14).

Scope conditions: when influence succeeds vs. fails

Domain and institutional conditions (SC1-SC3)

Estonian influence in cyber domain (technical-legal domain with characteristics identified above) substantially exceeds influence in traditional domains. Within-case evidence documenting cross-domain variation:

NATO Conventional Force Planning: Estonia contributes 0.3 percent of NATO defense spending (NATO, 2023). Estonia's military (6,600 active personnel) represents 0.2 percent of NATO total forces. Estonian representatives participate in NATO Military Committee but hold no chair positions in major planning committees (unlike cyber domain where Estonia hosts CCDCOE). NATO's Enhanced Forward Presence in Estonia (announced 2016, deployed 2017) was decided by US, UK, and Germany without Estonian veto power or significant input on force composition, command structures, or operational parameters. Estonia accepted battalion deployment locations and framework nations' decisions as fait accompli (NATO, 2017).

EU Economic Policy: Estonia holds 7 votes (0.2 percent) in EU Council weighted voting system. Estonian Members of European Parliament (7 of 705 total) participate in legislative process but hold no Economic Affairs Committee leadership positions. Estonia adopted the Euro (2011) on terms and timetables set by European Central Bank and Eurozone member consensus, with Estonia accepting convergence criteria requirements without negotiating leverage. Estonia's positions on Banking Union architecture, fiscal rules revision, and COVID-19 recovery fund had negligible impact on final frameworks, which reflected Franco-German compromises (Kölling, 2020).

UN Climate Negotiations: Estonia participates in UNFCCC Conference of Parties negotiations but is not member of leadership coalitions. Small island developing states (SIDS) exercise disproportionate influence as norm entrepreneurs on climate ambition through High Ambition Coalition; Estonia plays no comparable role. Estonia's Nationally Determined Contribution (NDC) is subsumed under EU collective target, with Estonia having no independent visibility in climate negotiations. Review of UNFCCC negotiation literature and COP decision documents shows zero citations of Estonian diplomatic initiatives as shaping negotiation outcomes (Bäckstrand & Kuyper, 2017; Obergassel *et al.*, 2016).

Conclusion from cross-domain comparison: Estonian influence varies dramatically across domains, confirming domain-specificity (SC1) rather than general Estonian diplomatic capacity or NATO favoritism operating uniformly. Cyber domain characteristics (technical complexity, nascent institutions, epistemic uncertainty) enable Estonian influence unavailable in conventional security, economic policy, or climate governance.

Great Power alignment proves decisive (SC4):

The 2017 GGE failure demonstrates SC4 as necessary condition. When Russian and Chinese interests conflicted with Estonian-advocated positions (explicit self-defense rights, IHL applicability), institutional platform (UN GGE membership), epistemic authority (Tallinn Manual reference), and coalition strength (Western allied support) proved insufficient. Conversely, 2013-2015 GGE success occurred because proposed norms (protect critical infrastructure, cooperate on cybercrime, exercise due diligence) aligned with all major powers' interests in cyber stability. SC4 operates as gatekeeper: without great power non-opposition, other enabling conditions cannot generate influence.

Coalition strength amplifies but doesn't override (SC5)

Coalition-building amplifies voice (34-state OEWG joint statement coordinated by Estonia) but failed to overcome great power resistance in 2017. The 2017 failure partly reflected insufficient coalition-building beyond NATO allies: Western states held common position but lacked broader developing country support. Russia and China successfully framed self-defense language as militarization, appealing to developing countries' interests in avoiding cyberspace arms races. Estonian advocacy failed to counter-frame effectively, revealing coalition-building limitations when great powers mobilize opposing coalitions.

Norm maturity affects entrepreneur vs. antipreneur advantage (SC6):

Estonian entrepreneurship succeeded during cyber governance emergence (2008-2015) when institutional architecture remained fluid and great powers lacked consolidated positions. As norms matured post-2017, Russia and China as norm antipreneurs (Bloomfield & Scott, 2016) consolidated resistance, deploying alternative cyber sovereignty frameworks and building

Table 1: Comparative Cyber Capabilities and Diplomatic Positioning

Indicator	Estonia	Lithuania	Latvia
National Cybersecurity Index (2024)*	90.91	93.51	72.3
ITU Global Cyber Index Ranking (2021)	3rd	9th	15th
NATO CCDCOE Status	Host nation	Sponsoring nation	Sponsoring nation
First National Cyber Strategy	2008	2011	2014
Dedicated Cyber Ambassador	2018	2023	None
UN GGE Participation	2013, 2015, 2017	2021	None
Tallinn Manual Expert Contribution	6 experts (2 IGE members)	1 expert	None
Cyber Diplomacy Publications (2015-2024)	54% of Baltic total	26% of Baltic total	20% of Baltic total

Sources: National Cybersecurity Index (NCSI, 2024); ITU Global Cybersecurity Index (ITU, 2021); NATO (2024); respective government documents; Schmitt (2017); Vasilevska et al. (2025).

Note: The National Cybersecurity Index measures domestic cybersecurity measures (legislation, technical capacity, organization) rather than international diplomatic influence. Lithuania's higher score reflects robust domestic cyber defenses but not international norm leadership, confirming the distinction between domestic capacity and international agency.

counter-coalitions. SC6 suggests timing matters critically: early positioning creates path dependence favoring entrepreneurs; later entry faces organized antipreneur resistance with established alternatives.

Comparative analysis: why Estonia leads in the Baltic Region

Latvia and Lithuania share Estonia's structural characteristics: small population (Latvia 1.9M, Lithuania 2.8M), post-Soviet history, NATO/EU membership since 2004, and geographic proximity to Russia. Yet Estonia leads significantly in cyberdiplomacy.

Key Finding

Despite Lithuania's higher National Cybersecurity Index (domestic measures), Estonia leads dramatically in international cyberdiplomacy indicators: institutional hosting, expert contribution to norm-setting, diplomatic positioning, and research output.

Explaining variation

Factor 1: First-mover advantage and crisis-driven investment

Estonia's 2007 cyberattacks provided focusing event (Kingdon, 1984) catalyzing investment in cybersecurity governance and international positioning. Latvia and Lithuania observed Estonian experience but lacked equivalent crisis justifying comparable resource allocation. Estonia's crisis response deliberately converted vulnerability into institutional opportunity: inviting NATO cyber center to Tallinn, developing comprehensive national strategy, positioning officials as experts internationally.

Lithuania's first national cyber strategy came 3 years after Estonia's (2011 vs. 2008); Latvia's came 6 years later (2014). This timing gap allowed Estonia to shape emerging international frameworks before competitors established positions. Path dependence ensued: NATO selected Tallinn (not Vilnius or Riga) for CCDCOE location, creating institutional advantage; Tallinn Manual project emerged from Estonian institutional base; Estonian diplomats gained expertise head-start enabling subsequent leadership positions.

Factor 2: Concentrated investment in cyber expertise

Estonian government made strategic choice to concentrate resources in cyber domain rather than dispersing across multiple priorities. Estonia's Tallinn University of Technology established specialized Cyber Security curriculum (2009), producing trained workforce for government, CCDCOE, and private sector. Estonia's Information System Authority (RIA) expanded from 50 employees (2007) to 220 (2024), developing specialized technical capacity. Estonia's E-Governance Academy provided training and capacity-building programs for 40+ countries, positioning Estonia as knowledge exporter and building international networks (E-Governance Academy, 2020).

Budget comparison: Lithuania's cyber budget increased from €2.5M (2012) to €8.5M (2020); Latvia's from €1.8M (2014) to €5.2M (2022). Estonia's cyber budget grew from €5M (2008) to €25M (2022), representing proportionally larger investment relative to GDP and demonstrating concentrated commitment (World Bank, 2024; respective national budget documents).

Factor 3: Strategic identity construction

Estonia explicitly constructed strategic identity as "cyber defense leader" and "digital society model," using cyberdiplomacy for status-seeking and regional differentiation. Estonian officials consistently frame Estonia as exemplar of cyber resilience, leveraging successful e-governance systems (digital signatures, e-residency, blockchain applications) for international credibility. This identity construction appears in official documents, diplomatic communications, and international fora presentations, creating coherent narrative positioning Estonia as cyber expert (Republic of Estonia MFA, 2019).

Lithuania pursued broader strategic identity as "regional leader" and "bridge to East" without cyber-specific focus. Latvia lacked coherent cyber-domain strategic identity, treating cybersecurity as defensive requirement rather than diplomatic opportunity. This identity divergence shaped resource allocation decisions and diplomatic prioritization: Estonia concentrated efforts building cyber reputation; Lithuania and Latvia dispersed efforts across multiple foreign policy priorities.

Addressing counterarguments

The Neorealist response

Counterargument: Estonian "influence" is epiphenomenal. NATO great powers allowed Estonia institutional space because Estonian positions served NATO interests. When positions diverge, Estonia is overruled (2017 GGE). Estonia has no independent effect; observed influence reflects delegation by great powers seeking convenient mouthpiece for positions they find politically costly to advocate directly.

Response: Three types of evidence suggest agency beyond simple delegation:

First, Estonian positions sometimes diverged from initial great power positions, with convergence occurring toward Estonian advocacy rather than vice versa. Tallinn Manual Rule 13 (sovereignty violations by cyber operations below use-of-force threshold) initially faced skepticism from US and UK governments preferring strategic ambiguity on sovereignty questions. Estonian-led IGE expert deliberation produced consensus interpretation eventually adopted by US and UK in subsequent position papers (Jensen, 2017; Schmitt, 2019). This temporal sequence suggests Estonian institutional platform shaped great power convergence rather than implementing predetermined positions.

Second, when US and European allies disagreed on

cyber operations' legal status (2013-2015 period), Estonia maintained consistent positions advocating clarification and legal certainty. Western great powers gradually converged toward Estonian-advocated positions over multi-year period. If Estonia merely implemented delegation, Estonian positions should track great power splits rather than showing independent coherence preceding convergence.

Third, non-NATO states (Singapore, Japan, South Korea, Ukraine, Georgia, Moldova, Kenya) requested Estonian cyber capacity-building assistance and adopted Estonian-modeled cyber strategies (Republic of Estonia MFA, 2019, pp. 12-14). If Estonia simply reflected NATO power, non-NATO states would lack incentive to defer to Estonian expertise rather than engaging directly with US or UK. Estonian technical assistance is valued because of perceived expertise, not NATO affiliation.

However, the counterargument correctly identifies structural constraints. Estonian influence is permissive rather than autonomous: great powers tolerate Estonian leadership when convenient and override when conflicting with core interests. The theoretical position is contingent agency: meaningful but bounded influence operating within parameters set by great power tolerance. This does not refute neorealism but specifies its scope conditions: neorealism explains ultimate constraints (great power veto) but inadequately explains mechanisms operating within those constraints (norm entrepreneurship, institutional positioning, epistemic authority).

Norm antipreneurs and resistance

Bloomfield and Scott (2016) introduce "norm antipreneurs", actors resisting normative change who enjoy strategic advantages when status quo is entrenched or when offering alternative normative frameworks. Russia and China function as antipreneurs in cyber norm contests, deploying resistance strategies including:

Framing contestation: Depicting Western-advocated self-defense language as "militarization of cyberspace" rather than legal clarification, appealing to developing countries' concerns about arms races.

Coalition-building: Mobilizing developing countries skeptical of Western legal dominance, emphasizing sovereignty and non-interference principles resonating with post-colonial sensitivities.

Alternative proposals: Promoting cyber sovereignty frameworks emphasizing state control over domestic cyberspace, information flows, and internet governance as alternative to Western "internet freedom" models (Ling, 2021; Mueller, 2017).

Estonian norm entrepreneurship confronts structural antipreneur advantages. Great powers resisting normative change possess greater resources, institutional access, and veto capacity than small state entrepreneurs. The 2017 GGE failure exemplifies this dynamic: antipreneurs (Russia, China) defeated entrepreneurs (Estonia, Western allies) through successful counter-framing and coalition mobilization with developing countries.

This analysis suggests SC6 (Norm Maturity) as additional scope condition: Entrepreneurs exercise greater influence during norm emergence (2008-2015 cyber governance nascence) than after status quo hardens and antipreneurs consolidate organized resistance (post-2017). Timing matters critically: early positioning creates path dependence favoring entrepreneurs before antipreneurs organize counter-coalitions and alternative frameworks. As norms mature, antipreneur advantages increase while entrepreneur opportunities contract.

Liberal institutionalism and domain-specificity

Counterargument : Liberal institutionalism already explains small state influence through institutions (Keohane, 1984). What does this paper add beyond confirming existing liberal theory?

Response: Three contributions beyond liberal institutionalism:

First, domain-specific scope conditions: Liberal institutionalism treats institutions as generally empowering for small states but doesn't systematically specify variation across domains. This paper demonstrates institutional empowerment varies predictably based on domain characteristics (technical complexity, epistemic uncertainty, nascent institutionalization). Some domains create substantially more opportunities than others; institutional theory requires domain-specific specification to explain this variation.

Second, precise mechanisms: While liberal institutionalism identifies that institutions matter, it provides less granular specification of mechanisms through which small states exercise influence. This paper combines institutionalism with constructivist norm entrepreneurship theory (Finnemore & Sikkink, 1998) and Barnett and Duvall's (2005) relational power framework to identify four specific mechanisms: institutional platform for epistemic authority, institutional positioning for agenda-setting, coalition-building for voice amplification, and credible principled commitment for persuasion. This provides more detailed causal understanding than general institutional empowerment claims.

Third, scope conditions and limitations: Liberal institutionalism sometimes overstates institutional autonomy from power politics. This paper demonstrates clear limits through negative evidence: when great power interests diverge (2017 GGE), institutions fail to constrain power politics regardless of small state institutional positions. The contribution is specifying conditions where institutional mechanisms operate effectively versus where neorealist power politics reasserts dominance. This represents theoretical synthesis acknowledging conditional applicability rather than treating theories as mutually exclusive paradigms.

CONCLUSION

The theoretical contribution is identifying domain-level and strategic variables moderating neorealist predictions. This represents scope condition specification rather than

theoretical replacement: neorealism explains behavior in traditional security domains; constructivist/liberal mechanisms explain behavior in nascent technical-legal domains. Theoretical synthesis recognizing conditional applicability advances scholarship beyond paradigm debates.

Theoretical and practical implications

For IR Theory: This research contributes by identifying scope conditions for neorealist propositions. Neorealist predictions about small state powerlessness apply in: traditional military domains with clear capability hierarchies; zero-sum security competition; consolidated institutional environments where great powers control agendas; contexts with observable, quantifiable material power asymmetries. Neorealist predictions require supplementation in: technical-legal domains with high complexity and epistemic uncertainty; nascent institutionalization windows before great power consolidation; domains with mutual vulnerability creating cooperative incentives; contexts where expert consensus shapes state preferences.

Rather than debating whether realism or liberalism/constructivism better explains international politics universally, IR scholarship should specify scope conditions where each framework applies. Neorealism explains high-politics security domains; constructivism/liberalism explains technical-legal domains with institutional density and epistemic communities. This represents theoretical synthesis recognizing conditional applicability.

For Small State Strategy: Estonian cyberdiplomacy offers strategic lessons for policymakers: (1) invest early in emerging domains where governance institutions remain underdeveloped; (2) concentrate resources in specific domains generating comparative advantage; (3) convert vulnerabilities into opportunities by leveraging crisis experience; (4) seek institutional hosting opportunities providing agenda-setting platforms; (5) build coalitions systematically with like-minded states; (6) strategically align with but don't depend exclusively on great powers.

Success requires specific enabling conditions: early timing before great power consolidation; institutional access (NATO, EU, or comparable organizations); great power non-opposition to advocacy positions; and strategic alignment with alliance interests. The Estonian model is relevant for small states seeking technical-institutional leadership in emerging domains but not universally transferable to contexts lacking these conditions.

Limitations and future research

This research faces five limitations suggesting future directions:

First, causal identification challenges persist given institutional overlap between Estonian agency and NATO consensus-building. Attribution to Estonia versus NATO CCDCOE versus international expert community (IGE) remains partially ambiguous. Future research employing natural experiments (comparing cyber norm evolution in regions with versus without Estonian engagement) or counterfactual analysis could strengthen causal claims.

Second, limited temporal scope (2007-2024) captures emergence but not long-term trajectory. As cyber governance matures and great powers consolidate positions, will Estonian influence persist, contract, or evolve? Longitudinal research tracking influence over 20-30 years would reveal sustainability.

Third, single case focus limits generalizability despite comparative analysis. Cross-domain comparison (Estonian cyber vs. Singaporean AI governance vs. Norwegian climate diplomacy vs. Swiss humanitarian norm leadership) could identify generalizable mechanisms versus domain-specific factors.

Fourth, behavioral impact assessment demonstrates rhetorical influence more convincingly than behavioral change. Do states actually change cyber operations patterns following norm adoption, or merely adopt rhetorical positions without behavioral compliance? Future research employing quantitative event data analysis would assess behavioral effects.

Fifth, great power perspective is under-examined. Do US, UK, German policymakers perceive Estonian advocacy as influential, or view Estonia as convenient institutional host? Interviews with great power officials could clarify delegation dynamics.

REFERENCES

Bäckstrand, K., & Kuyper, J. W. (2017). The democratic legitimacy of orchestration: The UNFCCC, non-state actors, and transnational climate governance. *Environmental Politics, 26*(4), 764–788. https://pureadmin.qub.ac.uk/ws/portalfiles/portal/157820476/Kuyper_and_Backstrand_Orchestration_EP_post_print.pdf

Baldwin, D. A. (1979). Power analysis and world politics: New trends versus old tendencies. *World Politics, 31*(2), 161–194.

Barnett, M., & Duvall, R. (2005). Power in international politics. *International Organization, 59*(1), 39–75.

Barnett, M., & Finnemore, M. (2004). Rules for the world: International organizations in global politics. Cornell University Press.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs, 3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bloomfield, A., & Scott, S. V. (2016). Norm antipreneurs and theorising resistance to normative change. *Review of International Studies, 42*(2), 310–333.

E-Governance Academy. (2020). Annual report 2019–2020. E-Governance Academy Foundation.

Egloff, F. J. (2022). Semi-state actors in cybersecurity. Oxford University Press.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887–917.

George, A. L., & Bennett, A. (2005). Case studies and

theory development in the social sciences. MIT Press.
Handel, M. I. (1981). Weak states in the international system. Frank Cass.
Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3
Ingebritsen, C. (2002). Norm entrepreneurs: Scandinavia's role in world politics. *Cooperation and Conflict, 37*(1), 11–23.
International Telecommunication Union. (2021). Global Cybersecurity Index 2020: Measuring commitment to cybersecurity. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and insights. *Georgetown Journal of International Law, 48*(3), 735–778.
Kalvet, T. (2007). E-governance in Estonia: Implementation and best practices. *Journal of Baltic Studies, 38*(1), 17–34.
Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton University Press.
Keohane, R. O., & Nye, J. S. (1977). Power and interdependence: World politics in transition. Little, Brown.
Kingdon, J. W. (1984). Agendas, alternatives, and public policies. Little, Brown.
Kölling, M. (2020). Estonia in the Eurozone: Overcoming the triple vulnerability. *Journal of European Integration, 42*(8), 1143–1158.
Korzak, E. (2017, July 31). UN GGE on cybersecurity: The end of an era? The Diplomat.
Ku, J. (2017). How China's views on the law of jus ad bellum will shape its legal approach to cyberwarfare (Aegis Series Paper No. 1707). Hoover Institution, Stanford University. https://www.hoover.org/research/how-chinas-views-law-jus-ad-bellum-will-shape-its-legal-approach-cyberwarfare
Ling, J. (2021). China's cyber sovereignty concept and its impact on international law. *Chinese Journal of International Law, 20*(3), 483–512.
Markoff, M. G. (2017, June 23). Explanation of position on the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. U.S. Department of State. https://2017-2021.state.gov/remarks-and-releases-bureau-of-arms-control-verification-and-compliance/explanation-of-position-on-the-2016-2017-un-gge/
Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton & Company.
Mueller, M. (2017). Will the Internet fragment? Sovereignty, globalization and cyberspace. Polity Press.
National Cybersecurity Index. (2024). NCSI 2024 rankings. https://ncsi.ega.ee/
North Atlantic Treaty Organization. (2017). Boosting NATO's presence in the east and southeast. NATO Public Diplomacy Division.
North Atlantic Treaty Organization. (2023). Defence expenditure of NATO countries (2014–2023). NATO Public Diplomacy Division.
North Atlantic Treaty Organization. (2024). NATO Centres of Excellence. https://www.nato.int/cps/en/natolive/topics_68372.htm
NATO Cooperative Cyber Defence Centre of Excellence. (2020). Annual report 2020. NATO CCDCOE. https://ccdcoe.org/
Netherlands Ministry of Foreign Affairs. (2019, July 5). Letter to parliament on the international legal order in cyberspace. Government of the Netherlands.
Nye, J. S. (2010). Cyber power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
Nye, J. S. (2011). The future of power. PublicAffairs.
Obergassel, W., Arens, C., Hermwille, L., Kreibich, N., Mersmann, F., Ott, H. E., & Wang-Helmreich, H. (2016). Phoenix from the ashes: An analysis of the Paris Agreement to the United Nations Framework Convention on Climate Change. Wuppertal Institute for Climate, Environment and Energy.
Panke, D. (2010). Small states in the European Union: Structural disadvantages in EU policy-making and counter-strategies. *Journal of European Public Policy, 17*(6), 799–817.
Republic of Estonia. (2019). Cybersecurity strategy 2019–2022. Ministry of Economic Affairs and Communications. https://www.mkm.ee/en/objectives-activities/digital-society/cybersecurity-strategy
Republic of Estonia Ministry of Foreign Affairs. (2019). Cyber diplomacy. Estonian MFA. https://vm.ee/en/cyber-diplomacy
Schmitt, M. N. (Ed.). (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge University Press.
Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
Schmitt, M. N. (2019, October 14). The Netherlands releases a tour de force on international law in cyberspace: Analysis. Just Security. https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/
Schmitt, M. N., & Vihul, L. (2014). The nature of international law cyber norms (Tallinn Paper No. 5). NATO CCDCOE.
Tikk, E., Kaska, K., & Vihul, L. (2010). International cyber incidents: Legal considerations. NATO CCDCOE.
Tikk, E., & Kerttunen, M. (2017). The alleged demise of the UN GGE: An autopsy and eulogy. Cyber Policy Institute.
Tiirmaa-Klaar, H. (2021, September 30). Lessons from Estonia's cyber ambassador (Y. X. Poon, Interviewer).

GovInsider Asia. https://govinsider.asia/intl-en/article/heli-tiirmaa-klaar-lessons-from-estonias-cyber-ambassador

United Nations Group of Governmental Experts. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN Doc. A/70/174). https://undocs.org/A/70/174

United Nations Open-Ended Working Group. (2021). Final substantive report (UN Doc. A/AC.290/2021/CRP.2). https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.

Vasilevska, S., Vasilevskis, E., & Vitolina, Z. (2025). Cybersecurity policy analysis and research cooperation in the Baltic States. *Research for Rural Development, 40*, 326–332.

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley.

World Bank. (2024). World development indicators. World Bank Group. https://databank.worldbank.org/