THE TALLINN PAPERS

A NATO CCD COE Publication on Strategic Cyber Security

LIINA ARENG

LILLIPUTIAN STATES IN DIGITAL AFFAIRS AND CYBER SECURITY

Tallinn Paper No. 4.
2014

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

No. 3 Hannes Krause "NATO on Its Way Towards a Comfort Zone in Cyber Defence" (2014)

Roles and Responsibilities in Cyberspace

The theme of the 2014 Tallinn Papers is 'Roles and Responsibilities in Cyberspace'. Strategic developments in cyber security have often been frustrated by role assignment, whether in a domestic or international setting. The difficulty extends well beyond the formal distribution of roles and responsibilities between organisations and agencies. Ascertaining appropriate roles and responsibilities is also a matter of creating an architecture that is responsive to the peculiar challenges of cyberspace and that best effectuates strategies that have been devised to address them.

The 2014 Tallinn Papers address the issue from a variety of perspectives. Some of the articles tackle broad strategic questions like deliberating on the stance NATO should adopt in cyberspace matters, or exploring the role small states can play in this domain. Others touch upon narrower topics, such as the right to privacy in the growingly intrusive national security context and whether software manufacturers should be compelled to bear their burden of cyber security by making them liable for faulty software. The thread running through all the papers, however, is their future-looking approach, one designed to inspire discussion and undergird strategic development.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

Lilliputian States in Digital Affairs and Cyber Security[1]

Liina Areng[2]

The size of a state has generally been seen as directly connected to its capabilities and influence in international politics. There is no definitive or universal definition of a "small state" and metrics range from less than 16 million people (the Netherlands is most commonly used as a benchmark for "smallness") or less than 1.5 million (according to the World Bank standard), but there is agreement that small states exist, are numerous, and share several common challenges.[3] However, being "small" or "large" is not always clear-cut: the power that Switzerland has in the banking sector or Kuwait in the oil business, or the success of Norway in international peace-making efforts, demonstrates that "smallness" should not be confused with "weakness".

This paper analyses how innovation and technological change help small states attain influence in international relations and, through this new asymmetric toolbox of "digital power", gain leverage in international cyber security. The transition from the traditional understanding of power, defined by nominal values such as population size or territory, to digital power of decentralised information flows and services is a relatively recent phenomenon. Digital power yields to the asymmetric notion of efficiency, permitting small states to boost their positions vis-à-vis larger states through innovative and adept practices, such as specialisation in science and technology. "The barriers to entry in the cyber domain"[4] are low, allowing smaller entities to exercise significant power against larger opponents through a variety of widely available and inexpensive

1 The title was inspired by Robert O. Keohane's essay 'Lilliputians' Dilemmas: Small States in International Politics' 23(2) *International Organization* 291-310 (1969).

2 Head of International Relations, Estonian Information System Authority; NATO CCD COE Ambassador.

3 Wilhelm Christmas-Møller, 'Some Thoughts on the Scientific Applicability of the Small State Concept: A Research History and a Discussion' in Otman Höll (ed.), *Small States in Europe and Dependence* (1983) 35-53; Olav F. Knudsen, 'Small States: Latent and Extant: Towards a General Perspective' 5(2) *Journal of International Relations and Development* 182-198 (2002).

4 Joseph S. Nye, 'Cyber Power,' Belfer Center for Science and International Affairs, Harvard Kennedy School (2010), p. 4, available at: http://belfercenter.ksg.harvard.edu/publication/20162/cyber_power.html.

cyber tools. This new avenue enabling growth in state capacity will be illustrated by drawing on the example of Estonia.

Small But Smart:[5] Balancing the Costs and Benefits of Smallness

With some exceptions, small states generally have less economic and military resources than large states. According to Rothstein, "a small power is a state which recognizes that it cannot obtain security primarily by the use of its own capabilities, and that it must rely fundamentally on the aid of other states, institutions, processes, or developments to do so."[6] Small states are not only numerous, but also diverse. They differ in wealth, productivity, ambition, attainment and security concerns. Some states rest in stable regional settings, others in volatile, confrontational surroundings. Small states, both "old" and "new", also have varied historical experiences and cultural identities; they experience different political emotions, from worries of being politically marginalised to enduring existential fears. It seems fair to presume that the less favourable the geopolitical settings, the more their survival and prosperity depend on their administrative and political elite, whose leadership and administrative acumen may serve to compensate for the lack of domestic resources and the deficiency of traditional sources of "hard" power.

Success in external affairs, particularly for a small state, begins with strong and stable statehood. Internal strength and stability rest on a state's ability to provide adequate public services to its citizens. A small state seeks to provide the same amount and quality of public services as a large one, but with fewer resources. It is evident that small states have higher per capita costs to provide public services. However, when budgets are limited, creative thinking and agility are usually encouraged. Unsurprisingly then, smaller administrations are easier to reform. Therefore, smaller states are more adaptable to technological change and innovation.

An information society brings significant savings for public administration and the delivery of public goods. For small states, automation not only reduces costs, but also enhances the efficiency of public services, which can be made equally

5 Pertti Joenniemi, 'From Small to Smart: Reflections on the Concept of Small States' 9 *Irish Studies in International Affairs* 61-62 (1998). Joenniemi associates small state with "smart".

6 Robert L. Rothstein, *Alliances and Small Powers* (New York: Columbia University Press, 1968), 29.

accessible to citizens both in central as well as remote, scarcely populated locations of the country. Automation increases productivity and raises the economic well-being of societies. The size of a population is no longer a precondition for mass production and for services of scale. Quantity in the workforce is replaced by quality, and there is an increasing demand for highly skilled and creative people. This might be a challenge for small states, but when small is coupled with smart and innovative, a good economic climate, low levels of bureaucracy, easily accessible public services, quality education, good healthcare, and a fair and inclusive society, it should be possible to attract and retain a skilled workforce, capital and ideas.

When it comes to governance and bureaucracy, another benefit of small states is that they are inherently better organised, with short communication links within and between public agencies. Less political distance between local and national governance leads to significant autonomy in decision-making. Thus, reaction times, for example in a crisis when quick decisions are needed, are short. Similarly, defence, crisis management, and other capabilities are available at short notice and are more dynamic. This becomes a particular advantage in cyber crisis situations developing at a speed measured in milliseconds, requiring quick and agile reactions.

Compared to larger states, small states tend to be more rational when it comes to external affairs. The lack of strategic bargaining power vis-à-vis larger states usually makes them avoid open confrontation and encourages compromise. That should make small states better partners in diplomacy, particularly in conflict resolution, where they are generally perceived as selfless, altruistic mediators. Indeed, as they are generally less visible in international disputes, they are perceived to have fewer "hidden agendas". Advocacy for internet freedom and cyber security, for example, is an ideal, politically un-loaded topic that allows small countries to attract supporters and followers and to build digital power.

It is clear that a small state cannot radically transform international affairs, or destroy or build any international institutional structures, on its own. To mitigate their limitations, small states need to create and participate in networks. Cross-border cooperation creates synergies and economies of scale, and contributes to national security. This is valid especially for regions that have sufficiently similar political aspirations to forge a common position in the international system such as the Baltic or Nordic states. Cooperation is more successful in regions where economic, cultural or historical ties already exist between states, enabling them to build upon the existing history of trust with new avenues of cooperation, including cyber security.

To influence larger partners' decisions, small states need to earn their respect and trust, creating an environment which benefits smart tactics, charismatic leaders and good networking skills. Politicians and diplomats from small states have been remarkably successful as international mediators and in shaping the processes in international institutions, primarily by mastering the skill of searching for compromise. "Size in terms of political influence and power – of having the necessary human resources able to negotiate supra-regional policies – is becoming key to the economic success of small states."[7]

Generally, small states must use their structural advantages, the efficiency and adaptability of their domestic specialisation that has international leverage. The European Union is generally considered an organisation where small states have proportionally more say in common policy decisions than their territorial size or GDP would suggest. Although the EU provides smaller states with the ability to "disproportionately" influence common policy and legislation, the small state still needs an adequate number of bureaucrats to represent its interests, and a critical mass of other states (preferably including larger states) to push ideas into common policy. Automation does not offer an alternative to people-to-people interaction in policy-making and diplomacy.

Of course, small states are also competitors over resources, markets and attention, and over positions and ranking in the forums of the "large and mighty" (OECD, WTO etc.). In this battle, a small state's success depends on its self-perceptions and its ability to portray itself to others. As several analysts suggest – the key to small states' success is their ability to master the tools of "soft power".

An important projection of soft power is a state's good reputation. Reputation is something that develops over time through the active branding of a state. Creating a name, story or symbol of a state is delivered by systematic and persistent public diplomacy. By imposing positive symbols, it is possible to mitigate some negative connotations or historic legacy. For example, in Estonian public and political discourse, becoming a "boring Nordic country" is often used as a desirable image for Estonia together with e-Estonia.

Small states need to be smart in order to maximize their influence, and "smartness" can be achieved through innovation.[8] Several historically low-tech small states, such as Sweden, Denmark, Finland, Austria and Ireland,

7 Rainer Kattel, Tarmo Kalvet and Tiina Randma-Liiv, 'Small States and Innovation' in Robert Steinmetz and Anders Wivel (eds.), *Small States in Europe* (2010) 71.

8 David Arter, 'Small State Influence within the EU: The Case of Finland's 'Northern Dimension Initiative" 38(5) *Journal of Common Market Studies* 677–97 (2000).

have managed to gain leading positions in new industries like nanotechnology, biotechnology, telecommunications and cyber security. This has not been mere coincidence, but a systemic and comprehensive national innovation strategy encompassing important elements such as investment in human capital, research and development, and well-functioning institutions.

These examples suggest that a country's digital power base depends on whether the government has prioritised the development of a focused and comprehensive ICT strategy, an organisational structure and a national competence base, including investment in education and research and development. The limitations stemming from being small can even be advantageous. Resource limitations, for instance, narrow the number of issues which small states are able to prioritise, and promote quick consolidation of gains in the short-term, while the attention of bigger states is scattered across different topics and between shorter and longer term goals.[9] Although small states might have fewer resources to invest in cutting-edge research and development, they can still achieve remarkable success through clever and consistent prioritisation of resources in ICT and technological innovation.

The digital age brings several new opportunities for small states to increase their international "weight". The ICT revolution has also been called the "death of distance",[10] making every actor in cyberspace – small or large – theoretically possess a global reach, broadening the scope of friends and foes[11] and offering new avenues of influence. ICT makes it possible for small and peripheral states to improve connectivity with the rest of the world and widen the channels to disperse and absorb information. This affects commerce, people-to-people communication, and distance learning, but also broadens small states' means of projecting political, social and economic activity and power.

Can technological power outweigh traditional military power? In the military domain, as in other domains, the "actual" size is outweighed by "functional" size. Modern militaries depend extensively on information technology for command and control, surveillance, logistics, navigation and targeting. This raises their efficiency and combat power, but such dependencies potentially introduce increasingly complex vulnerabilities. The ability to gather, analyse

9 Anette Baker Fox, 'The Power of Small States: Diplomacy in World War II' in Christine Ingebritsen, Iver Neumann and Sieglinde Gstohl (eds.), *Small States in International Relations* (2012) 39-54.

10 Rainer Kattel, Tarmo Kalvet and Tiina Randma-Liiv, *supra* note 7, p. 79.

11 Johan Eriksson, 'Power Disparity in the Digital Age' in Olav F. Knudsen (ed.) *Security Strategies, Power Disparity and Identity: The Baltic Sea Region* (2007) 135.

and exploit information has always been crucial to national security, and digital development has made it profoundly easier.

Cyber operations have become an indispensable element of modern conflict. Cyber means are planned and used as an effective force multiplier, an enhancement for traditional means or as a stand-alone capability that can give substantial asymmetric advantage to states that are considered weaker in terms of traditional combat power. In modern warfare, small states can distract, disrupt and demoralise a larger opponent by skilful use of cyber tools, exploiting timing, surprise, and an adversary's specific vulnerabilities. These vulnerabilities are not restricted to military targets; the ability to attack civilian targets such as the financial sector, public utilities or traffic control can be far more dangerous, and, subsequently, more effective, at discouraging and deterring potential adversaries because of its immediate social and political effects. The possibility of using different and unpredictable strategic combinations of cyber tools affecting military, political, economic and social targets makes the opponents in asymmetric warfare more equal. The asymmetry is also created by the imbalance of attack space – larger, technologically dependent nations possess a larger network space with a greater number of weak spots vulnerable to attacks, while the smaller nation has a smaller network surface to protect. "Mass" is no longer a decisive factor in the military strategic and operational equations. Even a lone cyber warrior can wreak havoc in an opponent's networks, making information technology a powerful tool for a small but sophisticated actor that possesses sufficient skill and cunning.

Estonian Case Study: Digital Innovation

Estonia is a small state by all of the three core criteria defined by Geser:[12] substantial "objective" figures (territory, population), relational characteristics (comparison to other countries) and perceived "subjective" smallness (self-perception and external perception). While territory and population are not very dynamic features (although as explained later, Estonia has an innovative plan to rapidly grow in citizens), the "perceived smallness" is something in the capacity of a given state to change. To increase its "functional size" Estonia has put an emphasis on the transformative power of ICT and innovation.

The defining foreign policy concern for Estonia has traditionally been its large

12 Hans Geser, 'Was ist eigentlich ein Kleinstaat?' in Romain Kirt and Arno Waschkuhn (eds.) *Kleinstaaten-Kontinent Europa: probleme und Perspektiven* (2001) 90.

and unpredictable Eastern neighbour; Russia. Estonian national strategies (including the Cyber Security Strategy 2014-2017[13] and the Digital Agenda 2020[14]) and foreign policy is focused on reducing this vulnerability, which is now, at the peak of the Russia-Ukraine crisis, more vividly felt as a threat to national security and survival than at any other time since the dissolution of the Soviet Union more than two decades ago.

Naturally, Estonia joined NATO and the EU (including the Eurozone), and embraces a strong transatlantic relationship. Although sometimes perceived as shy and quiet (national characteristics), Estonia has been a picture-perfect kid on the block; "the only country in Europe that meets the rules of every club to which it belongs [...] the eurozone's targets on debt, inflation and government deficit, as well as NATO's standard: 2 per cent of GDP on defence."[15] Having fulfilled its organisational commitments, Estonia holds a positional advantage for effective engagement in international affairs. Perhaps it is the national introversion or other historical and cultural reasons that explain why Estonia is not fully using its solid standing in international organisations to build up a powerful foreign policy, but there is one niche where Estonia's activities are truly visible and are followed with keen interest, where being a small state has not hindered it in confidently pursuing an opinion-leader's role: cyber security and digital development. Estonia has captured attention as a country which has quickly responded to such challenges in the modern information society as the use of technological innovation and shift to e-services. Estonia has been effective in developing and promoting digital services both locally and abroad, making digital development a successful case of "soft power" projection.

In public administrative affairs, Estonia is a typical example of an "everybody-knows-everybody" society that nurtures trust and flexibility, and so the transformation from physical to digital government and e-services has been relatively easy. In 1995 the Estonian government started an ambitious Tiger-Leap program, computerising all the schools in Estonia, which was followed by the Look@World program, teaching the elderly population how to use computers and the internet. In 2005, Estonia was the first country in the world to hold

13 Ministry of Economic Affairs and Communications, 'Estonian Cyber Security Strategy 2014-2017' (2014), available at: https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf.

14 Ministry of Economic Affairs and Communications, 'Digital Agenda 2020 for Estonia' (2014), available at: http://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf.

15 Edward Lucas, 'Against Putin, It's time to Channel JFK,' *PoliticoMagazine* (22 August 2014).

nationwide elections over the internet. I-voting has gained increasing popularity in the 7 elections since then. In 2014, at the European parliament elections, 33 per cent of voters chose to cast their ballots online. Estonian i-voting success has received a lot of attention and amazement from larger nations, as Estonia still remains the only country in the world with a functioning nationwide i-voting system.[16] For a small country like Estonia, i-voting has also been an effective way to encourage Estonians abroad to remain engaged in Estonian society and politics, with the ultimate aim of inducing them to return. Maintaining a closely connected diaspora is also an effective safety net for a small country to voice its national security concerns abroad, particularly, if for some reason such as a successful information operation, or cyber attack, the voice from home has been blocked or distorted.

Estonia is also trying to increase its "objective" size by an ambitious e-residents project. To promote Estonian e-services and to increase the "safety net" of people abroad who are psychologically or economically attached to Estonia, the government has approved a concept to start issuing digital IDs to non-residents, starting from the end of 2014.[17] Estonia expects to have 10 million e-residents by the year 2025. Future high-flying e-projects have clear national security implications; Estonia is now exploring options to duplicate vital national databases in highly secure datacentres in friendly states abroad. The project is known as "Data Embassy" and is designed to ensure the digital continuity of the Estonian state, even in the event that it loses sovereignty over its territory.[18]

Attracting and retaining skilful IT security experts has been identified as one of the biggest problems in developing effective cyber security in all nations, big and small. However, for small states, attracting the best and brightest and the means to afford them is inherently more difficult. To deal with this problem, Estonia has established a unique concept of public-private cooperation in cyber security; the Estonian Cyber Defence League.

In the aftermath of the 2007 attacks against Estonian public and private information systems, Estonia began to develop a voluntary unit of cyber experts under the Defence League, a militarily-organised voluntary national defence organisation dating back to 1918. The main aim is to attract patriotically motivated

16 Anto Veldre, 'E-voting is (too) secure' (2014), available at: https://www.ria.ee/e-voting-is-too-secure/.

17 Kalev Aasmäe, "This is so freaking huge man, it's insane': The plan to let anyone become European – digitally,' *ZDNet* (19 May 2014).

18 *Supra* note 14.

IT security talent, mostly experts employed by banks, software companies, ISPs and the public sector, to prepare for and help the government to respond in large-scale cyber crises. The unit offers a "trust circle" to exchange information and best practices, to train, and to experiment. Another important element of the Cyber Defence League's activity is exercises and awareness raising.[19]

Coupled with the effective mitigation of the cyber attacks in 2007, the existence of the Estonian Cyber Defence League has been one of the most important elements of Estonian cyber deterrence. The location of NATO's Cooperative Cyber Defence Centre of Excellence in Tallinn since 2008 adds yet another large building block to Estonia's "functional" size in cyber security. Myths and hype remain around the notoriety of the "Estonian cyber shield", but it is without question a brilliant example of how a post-Soviet grey, dull, and poor country can leap to the forefront of international attention and do so with a positive image.

What about regional cooperation? Estonia invests much attention into cooperation with the Nordic-Baltic countries, both as a group and bilaterally. That encompasses cyber defence technical information sharing and assistance, pooling of resources, and inter-agency cooperation. All states in the Nordic-Baltic region are small and are therefore compelled to work more closely together. Besides, cooperation in cyber defence comes down to trust more than anything else, and trust is easier to build among like-minded nations that have a long and well-developed history of cooperation, such as the Nordic countries. The image of the Nordic region as innovative and high-tech, but also welfare-oriented and just, is a highly attractive "soft power" case with great potential to export its model to other regions. Estonia's goal is to contribute to the vision of making the region a centre of excellence for ICT security and e-government infrastructure development. Given the tight network of economic relationships and cross-border dependencies of ICT infrastructure, it would be logical to construct a strong Nordic-Baltic cyber defence alliance that would allow close-to-real-time information sharing and effective pooling of capabilities. A jointly built and maintained Nordic-Baltic "cyber shield" would be paramount in mitigating existing human resource constraints in the cyber defence sector.

Driven by interdependencies and mutual vulnerabilities between states, it can be tempting for small and less resourceful states to become free riders in

19 More on the Estonian Cyber Defence League in Kadri Kaska, Anna-Maria Osula and Jan Stinissen, 'The Cyber Defence Unit of the Estonian Defence League – Legal, Policy and Organisational Analysis,' NATO CCD COE Publications (2013).

cyber security, expecting to receive international assistance during large-scale cyber attacks affecting other nations. However, the ability to count on large states' support in times of crisis is based on a good amount of "homework" in first securing networks and building effective institutional frameworks that encourage reliability and trust. A good example is the Estonian Cyber Defence League's cooperation with the Maryland National Guard, where over years of joint training and sharing best practice a strong link has been created between the Estonian and US cyber communities, establishing solid ties for mutual assistance during a crisis or emergency.

Estonia has also been an active contributor to raising awareness in international organisations by pushing cyber security to the forefront of international attention, particularly in NATO and the EU. Estonia assumed the leading role in the process of developing NATO's first cyber defence policy in 2008 and has contributed to a number of EU initiatives to foster ICT security. Estonia's latest victory on the international digital "scene" was the announcement that former Prime Minister Andrus Ansip had been chosen to assume the position of the EU Commissioner for the Digital Single Market. Ansip will be steering the digital development of the world's largest economy, adding him to the list of small states' politicians shaping the policy processes in powerful international organisations.

Estonia is an example of how small states can effectively combine the elements of "soft" and "hard power", the latter being more successful when the shared resources of an alliance of states are available. Being part of NATO and the EU is an effective national security guarantee for Estonia. As both organisations are dedicating serious attention to cyber security cooperation and assistance, Estonia has an important ground of support to project effective "cyber power".

Conclusion

A state's "smallness" is contextual and relational; it is rather a perception of a state, and therefore not a static feature in space and time. With smart choices, a small state can out-compete nations which are geographically, demographically, economically or militarily much larger.

There are several ways in which the "Lilliputians can tie up Gulliver."[20] It starts with focusing on issues in which they have a comparative advantage, some specific niche. Estonia has found that niche in developing innovative

20 Keohane, *supra* note 1, p. 310.

e-government and cyber security solutions, building experience that it gladly shares with others. Estonia is striving to become an ICT and cyber policy innovator and entrepreneur by generating new ideas and testing them in practice. Small states in general have a lot to gain from information society advances, which have become a powerful transformational tool for government, for business, and for society as a whole. Small states have a great advantage in that they have more freedom of action to put forward bold plans and to test and experiment, because of a number of qualitative characteristics that separates them from large states. Automation is a vital enabler, helping to overcome the important human resource constraints.

Finding that niche should also help to pursue a vigorous, oversized foreign and security policy. International organisations enable visibility, while sharing information and knowledge. For European "Lilliputians", the EU seems well suited to empowering small states, as it moderates the traditional big-small power asymmetry in inter-state affairs. International organisations also enable the pooling of security, including cyber security.

Digital power gives a clear asymmetric advantage in national security to small states. Although traditional major powers invest heavily in the development of ICT and cyber warfare capability, small states still have more opportunity to compete in this domain than in traditional warfare because, in modern warfare, "mass" is no longer a decisive factor. Even though cyberspace cannot entirely replace physical space in inter-state conflict, the diverse and unpredictable combinations of ICT methods in asymmetric warfare dilute the traditional power and dominance logic. Efficient, autonomous and well-trained cyber defence forces within a limited, well-protected cyber attack space can secure victory by using innovative techniques to breach the less defensible network breadth of large state cyber defence or cyber warfare organisation. The "large and powerful" cannot take for granted that they will always come out as winners from cyber conflicts with a small state, particularly if small states have jointly (or in combination with larger states) developed a seamlessly functioning cooperation network that builds upon a pool of individual states' expertise and capabilities routinely tested in regional exercises. Given the level of economic integration and cross-border dependencies of critical infrastructures, a Nordic-Baltic "cyber shield" might emerge in the not-so-distant future.

A small state's ability to project a combination of "soft power", to win friends and increase its visibility and influence, and "hard power", to enforce deterrence, needs intellect, courage, creativity and forward-mindedness. The digital revolution creates a number of new opportunities for small states, and

small states are likely to play an ever more decisive role in international security.