The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis

Nick Robinson
Royal Holloway, University of London
Egham Hill, Egham, TW20 0EX
United Kingdom
Nicholas.Robinson.2014@live.rhul.ac.uk

Laura Kask
University of Tartu
Ülikooli 18, 50090 Tartu
Estonia
kasklaura1@gmail.com

Robert Krimmer
TalTech – Tallinn University of Technology, Ragnar Nurkse Department of Innovation and Governance, DigiGovLab
Ehitajate tee 5, 12616 Tallinn
Estonia
robert.krimmer@taltech.ee

ABSTRACT

The Vienna Convention has been long enshrined as the cornerstone of modern diplomacy. However, recent technological advances may have shifted this landscape, with international law requiring to adapt in the face of novel and unique challenges. Taking the case of the Estonian Data Embassy in Luxembourg, we assess the applicability of the Vienna Convention outside of the traditional diplomatic mission and within a government-operated data centre. Evaluating the legal challenges and reinterpretations made by the Estonian government so far, this early analysis hopes to invigorate and advance discussions around the wider applicability of the Vienna Convention. Can similar diplomatic protections and inviolability be afforded to State data and information systems, or should such an international legal framework be updated to fit within a digital era?

CCS CONCEPTS

• **Applied computing** → **Computers in other domains** → Computing in government → *E-government*

KEYWORDS

Data Embassy, Vienna Convention, Diplomacy

ACM Reference format:

N. Robinson, L. Kask, R. Krimmer. 2019. The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019), Melbourne, VIC, Australia, April 3-5, 2019*, 6 pages. https://doi.org/10.1145/3326365.3326417

ICEGOV2019, April 3–5, 2019, Melbourne, VIC, Australia

ACM 978-1-4503-6644-1/19/04…$15.00
https://doi.org/10.1145/3326365.3326417

1. INTRODUCTION

The main aim of this paper is to open up a wider discussion and dialogue on the applicability and relevance of the Vienna Convention in a digital era. To do so, we take the case of the Estonian Data Embassy in Luxembourg, and its reinterpretation of the Vienna Convention, to assess whether State data and information systems within a government-operated data centre can be afforded similar diplomatic immunities and protections to that of a traditional diplomatic mission. This early exploratory analysis will question the pertinence of such international legal frameworks (that, ultimately, predate the digital age), before assessing the criterion around the potential revision of the Vienna Convention in the future.

Recent technological advances have contributed to major shifts within conventional diplomacy, meaning that international law has had to adapt to novel and unique challenges. Embassies are now also taking on anomalous forms with the advent of virtual embassies and now, in the context of Estonia, data embassies.

First, the paper will provide a short background on the Data Embassy Initiative and its relevant research to date (Section 2), before a discussion on the Vienna Convention and its current function and role within contemporary diplomacy and practice (Section 3). Next, we introduce the case study of the Estonian Data Embassy in Luxembourg (Section 4), detailing the Estonian government's decision to utilise government-operated data centres over physical Estonian embassy locations (Section 4.1), before a more detailed analysis on the Data Embassy and its applicability of the Vienna Convention (Section 4.2). This research draws largely upon early desk research, document analysis and

preliminary interviews with a number of Estonian officials and legal experts. The paper concludes with early findings from this analysis, before outlining next steps with regards to future research in this area.

2. BACKGROUND

The Estonian Data Embassy Initiative (DEI), and its primary goal of ensuring digital continuity, might offer a glimpse into how governments might wish to begin proactively safeguarding their digital ecosystem in the future [1]. The promise of extraterritorially storing backups of critical information systems and databases, in so-called 'data embassies' - and operating them from a secure data centre outside the State's own territorial borders - will continue to elicit interest from governments that are today faced with increasing, multifaceted uncertainties and disruptions: from cyberattacks and natural hazards, to legitimate threats to State sovereignty and territorial integrity [2].

A recent audit from the independent National Audit Office of Estonia found that the safety and preservation of numerous critical databases in Estonia were largely unsatisfactory and in need of greater attention [3]. A lack of a legal framework and 'significant deficiencies' with regards to information security point to serious frailties at the heart of the Estonian e-government ecosystem.

For a government or state that relies so heavily on its digital infrastructure, the core elements of a digital continuity policy would include a mixture of physical and virtual data storage means. Therefore, the DEI serves as only part of a more thorough and comprehensive policy where information and data storage principles should be set for the data and information systems that are critical to the functioning of the state. Today, progressive governments are looking towards cloud computing [4] and other innovative practices to ensure data security using the latest technology available, necessary across an increasingly volatile international security landscape.

To date, academic research around the DEI has remained scant, with a large proportion of analysis centred around the legal and policy environment with regards to hosting Estonian government data and services in the Public Cloud (e.g. the Estonian government has collaborated with Microsoft on two feasibility studies to assess the utility of a Virtual Data Embassy) [5, 6, 7, 8]. There has, however, featured little analysis or discussion with regards to the 'Physical Data Embassy' component of the DEI and overall Estonian government cloud concept [9]. With the first Data Embassy now being operational in Luxembourg, it would be timely to reflect upon the legal ramifications of this particular component of the project, of which the rest of this paper will now focus.

3. THE VIENNA CONVENTION ON DIPLOMATIC AND CONSULAR RELATIONS

The Vienna Convention on Diplomatic Relations (VCDR) has been described as the 'cornerstone' of modern diplomacy and international relations [10, 11]. From its conception in 1961, it has achieved near-universal participation and compliance by States, bringing clarity and uniformity to modern diplomatic practice. At its core, the VCDR provides a 'complete framework for the establishment, maintenance and termination of diplomatic relations on a basis of consent between independent sovereign States' [12].

Its counterpart, the Vienna Convention on Consular Relations (VCCR - 1963), soon followed, codifying the certain rights and obligations with regards to the conduct of consular relations. Although both have fallen victim to violations and controversy over the years [13], their high degree of observance and influence upon international relations, diplomacy and law cannot be undervalued.

For the purpose of this research we wish to focus on a number of integral components of the VCDR and VCCR that may be applicable within the context of the Estonian Data Embassy in Luxembourg. First, Article 24 of the VCDR states that "[t]he archives and documents of the mission shall be inviolable at any time and wherever they may be" [14]. Article 1(1)(k) of the VCCR, in turn, interprets these archives to include "all the papers, documents, correspondence, books, films, tapes and registers of the consular post, together with the ciphers and codes, the card indexes and article or furniture intended for the protection or safekeeping" [15]. Taken together, the Vienna Conventions therefore codify and explicate that any relevant information, including modern forms of information storage, is to be protected.

Since the adoption of the Vienna Convention in 1961, communications have changed substantially, and with it the terms 'diplomatic correspondence' and 'consular archives' have had to adapt. The Conventions have so far been flexible enough to accommodate new modes of communication and data storage, ranging from letters to CDs, briefcases with papers to external storage devices. Indeed, according to Denza, "It is probably better to simply rely on the clear intention of Article 24 to cover all physical items storing information" [11]. The driving force behind these Convention articles is clear: no matter how the information is transmitted or stored, it has to be protected under the Vienna Convention.

Article 27 of the VCDR and Article 33 of the VCCR concern the protection and inviolability of communications between diplomatic missions and sending State. Traditionally, this has come to represent analogue forms of communication, with the diplomatic bag and afforded diplomatic immunities becoming integral components. However, with more sophisticated and ubiquitous forms of communication, violations have been found to be commonplace, with little enthusiasm from States to modify underlying principles nor to desist from embassy surveillance or intercepting one another's communications [11].

Currently, the VCDR and VCCR are deemed to only apply within the context of a traditional diplomatic mission. It sets out special rules (e.g. privileges and immunities) with regards to the diplomatic mission itself, as well as the majority of diplomatic staff and the communications of the 'sending State'. Its general reciprocity and acceptance across the international community have, according to Bruns, 'made it difficult for alternative practices to evolve and for revolutionary powers to alter

recognised rules' [10]. Yet, with alternative methods and forms of diplomacy ever-evolving within a digital era - such as the formulation of 'virtual embassies' that function as digital representations of a diplomatic mission [11, 16] - the very nature of diplomacy, and even the embassy itself, maybe being called into question.

Furthermore, with the advent of the Estonian Data Embassy in Luxembourg, more prescient legal complexities are now emerging and being thrust into the international legal conversation: can the Vienna Convention be applied outside the context of a traditional diplomatic mission, such as a data centre? Moreover, can such similar protections - such as diplomatic immunity - be applied to data and information systems? The following section aims to examine these emerging inquiries within the context of the Estonian Data Embassy in Luxembourg.

4. THE ESTONIAN DATA EMBASSY IN LUXEMBOURG

On June 20th 2017, the Prime Ministers of both the Republic of Estonia and the Grand Duchy of Luxembourg signed an agreement concerning the hosting of Estonian data and information systems, thus establishing the world's first Data Embassy in Luxembourg [17].

In effect, the bilateral agreement laid the foundational structure from which the Estonian government could begin to systematically backup its information systems, databases and registries that are deemed critical to the continuity of the Republic of Estonia. In meeting with one the DEI's core principles, the Data Embassy located in Luxembourg should ensure that Estonia can operate and continue to function as a government, 'even in the direst of scenarios', which could include the loss of territory [6].

Located within a dedicated government-operated data centre in Betzdorf, Luxembourg, the Data Embassy will protect Estonian information systems and data in a similar capacity to a traditional diplomatic mission. Via the bilateral agreement, Luxembourg will agree to protect the inviolability of the Estonian premises (and thus its information systems and data) 'in the spirit' of the Vienna Convention [17]. Despite not being located within a traditional diplomatic mission, both governments have agreed to reinterpret some of the key principles of the VCDR, and, once fully established and operational, the Data Embassy will stand as the first example of two government's agreeing to provide this kind of inviolability.

After setting such an influential precedent, Estonia may look to establish additional Data Embassies in other territories, but could also serve as an inspiration for other governments to follow suit.

4.1. From embassy to data centre: an overview

In their initial exploratory research and analysis, Kotka and Liiv proposed two distinct solutions that would enable Estonian state information systems, data, and even e-services, to be housed and operated from outside of Estonian territory [1]. In keeping with the initiative's moniker, the first solution planned to utilise existing Estonian embassy locations across the world in an attempt to improve the regularity and scale of existing backup methods.

Interestingly, the Estonian government have been performing manual equivalent backups of this process for over a decade, with databases, backed up onto magnetic tapes, being transported via diplomatic bags to Estonian embassy locations on a regular quarterly basis. The proposed solution would, therefore, be deemed a pragmatic upgrade on previous inefficient and cumbersome methods, with the digital equivalent allowing for near-instantaneous backups or 'mirroring' of critical State information systems and databases.

In the event of an emergency - be it a large-scale cyberattack, natural disaster or any deemed threat to Estonia's sovereignty and territorial integrity - the Estonian government would be able to effectively 'switchover' and operate from the extraterritorial embassy. By utilising existing embassy buildings and infrastructure, it was felt that the Estonian government could pursue several possibilities with regards to securing and protecting its data. For example, Article 24 and 27 of the Vienna Convention were deemed most pertinent, ensuring the inviolability and immunity of mission archives and communications.

Ultimately, however, the proposed solution had numerous organisational, legal and technical challenges [1]. First, embassy locations do not meet the required security specifications for the housing of critical databases and hosting of data, comparative to that of a high-tiered data centre. From being able to operate to a greater level of redundancy, to limitations and vulnerabilities over existing telecommunications infrastructure, or even the level of technical competency found within an embassy, they were deemed unsuitable and even susceptible in the event of a crisis (either within Estonian territory or within the 'receiving State' itself). Furthermore, Estonia currently only maintains 37 diplomatic missions abroad. In fitting with the Estonian government's intention to operate within 'friendly' states, the scope of Data Embassy locations globally would be somewhat limited.

The second solution, of which the rest of this paper will now focus, then emerged as the most viable alternative. Under this proposal, the Estonian government would acquire server space within an existing data centre that fulfilled the necessary security and technical specifications that the first solution lacked. Then, as highlighted at the beginning of Section 4, a bilateral agreement signed between the Estonian government and the host State would ensure that the latter would fulfil specific obligations regarding the hosting of Estonian data and information systems.

Initially, it was perceived that the Data Embassy would function in similar pretences to a physical diplomatic mission. A small, demarcated area of an existing data centre - conceivably a separate, enclosed room with restricted access - would effectively be deemed under Estonian jurisdiction, whilst similar provisions such as inviolability of the mission premises and diplomatic immunity would be deemed applicable. As the following section will explore in greater detail, although core principles of the Vienna Conventions were indeed applicable, there were still

uncertainties regarding the overall applicability of the Conventions outside the context of a diplomatic mission. Officials from both Estonia and Luxembourg, however, worked on an agreement bilaterally that would perform in a similar capacity, thus serving as an interpretation of the Vienna Convention.

An explanatory memorandum between the two governments has also noted a number of reasons as to why Luxembourg has been prioritised as a partner for this project [18]. The number and efficacy of state-owned, high-security (Tier IV) data centres within Luxembourg was deemed most crucial, alongside a superior communications infrastructure that offers incredibly low latency and resiliency across its colocation network. Estonia currently has no such data centres within its territory. For Luxembourg, the partnership also signifies efforts to position itself as a 'hub' for other data embassies in the future, with other governments potentially following Estonia's lead. In late 2018, the Grand Duchy of Luxembourg and Principality of Monaco announced a partnership that would boost digital cooperation between the two administrations, with a similar data embassy solution to Estonia likely to be developed [19].

4.2. The Data Embassy and the applicability of the Vienna Convention

As highlighted in the previous section, the Vienna Convention was deemed insufficient for the hosting and protection of Estonian data and information systems. The remainder of this section will outline that, although both Conventions may be applicable, there remained a great deal of uncertainty regarding specific components of the Conventions and the legal precedent in this area.

By reinterpreting elements of the Vienna Convention, the Estonian government took the necessary steps to sign a bilateral agreement with Luxembourg regarding the hosting and protection of State information systems. The section will conclude with some early reflections on the DEI's potential impact upon the Vienna Convention and international customary law in the future.

4.2.1. Applicability of the Vienna Convention

Broadly speaking, the Vienna Convention concerns the comprehensive protection and inviolability of its staff, premises and communications. Given that its predominant function is to codify the rules for the exchange of embassies - but also the establishment, maintenance and termination of diplomatic relations - between sovereign States [11], there may be consensus that the Data Embassy goes against the overall purpose of the Vienna Convention.

This could first be interpreted by the Data Embassy not actually residing within a traditional diplomatic mission itself. Outlined in Section 4.1, the decision to utilise dedicated server space within existing government-operated data centres ultimately refutes the premise that the Estonian information systems could be protected under the 'broad church' of the Vienna Convention - specifically, Article 22 of the VCDR which ensures "[t]he premises of the mission shall be inviolable" [14]. Although specific text within the bilateral agreement refers to the Estonian server space as "premises", this is not in direct reference to a diplomatic mission itself as it is not directly recognised or registered as an embassy. Similarly, the Data Embassy also comprises of no staff or personnel (that work directly for the Republic of Estonia) that are involved with its day-to-day functioning, immediately conflicting with another one of the Vienna Conventions' core principles.

For the Estonian government, however, trust was also deemed an intrinsic factor. Within what is ostensibly a novel and challenging area, Estonia would risk applying the Vienna Convention without any form of legal precedent at present. As the Estonian government has been building trust in e-government for over 15 years, losing that societal trust would be detrimental. Hence why a bilateral agreement between two countries would give a more profound level of assurance that the data and information systems of the government are handled at the same level as in Estonia.

4.2.2. Bilateral Agreement

As the above section illustrates, it was deemed necessary for the Estonian government to take additional measures to ensure the data and information systems in Luxembourg were suitably protected under international law. Further to this, that additional powers could also be exercised with regards to Estonian jurisdiction outside of its own borders.

The basic principle of international law "according to which the exercise of jurisdiction to enforce on the territory of another State is permitted only if the latter provides consent for such behaviour (for example, based on a bi- or multilateral agreement), or such a right would be derived from international customary law" [20]. As the Data Embassy could not be afforded the exact same rights and privileges as a traditional diplomatic mission, it was necessary to enter into an agreement with the government of Luxembourg to set a clear legal framework to overcome the uncertainties surrounding the hosting of its data and information systems under the Vienna Convention.

The agreement, containing 10 articles, specifies the means for effective cooperation, support and operations regarding the premises in the dedicated government-operated data centre in Betzdorf, Luxembourg, whilst also governing the legal status of the premises, guaranteeing the necessary immunities and privileges on the basis of existing national and international law [21].

Crucially, the agreement is referred to be operating "in the spirit" of the Vienna Convention on Diplomatic Relations, and, although such wording is commonplace throughout international agreements today, the treaty preamble deliberately emulates aspects of the Vienna Convention through similar language, semantics and structure. Despite this, to avoid conflation with the Vienna Convention, the agreement refrains from using the term 'Data Embassy' in any capacity. Although there was clear intent to reflect the Convention, Estonian officials believed this proved problematic from a semantic and legal perspective to do so.

In short, the agreement serves as an interpretation of the Vienna Convention that, in effect, binds both 'sending State' and 'receiving State' to fulfil specific obligations and similar diplomatic protections to that of a traditional embassy.

4.2.3. *Setting an influential precedent*

With the agreement ratified by both respective Parliaments, it is, significantly, the first time two States have agreed to provide this kind of inviolability. For Luxembourg, they are providing certain privileges and immunities akin to that of an embassy, whilst for Estonia, they are extending the ability to exercise their powers of jurisdiction outside the traditional diplomatic mission.

Yet, as this preliminary discussion has elucidated, with no real precedent or experience to build on, uncertainties do still remain with regards to upholding particular privileges and immunities - particularly in regards to communications. How, for example, will Luxembourg respond to a relentless DDoS attack on its entire data centre facility? Or what happens when the cooling system of the data centre facility is not properly functioning and the watering systems flood the dedicated data centre space?

Despite a lack of precedent regarding States entering such novel forms of diplomatic relations regarding information systems, we may wish to look towards recent examples whereby international organisations have drafted and exercised similar bilateral agreements for hosting data outside of their original jurisdiction. For example, the eu-LISA agency for operational management of large-scale IT systems, based in Tallinn, Estonia, has a similar agreement in place enforcing that "The Protocol on the Privileges and Immunities of the European Union shall apply to the Agency" [22]. Similarly, both NATO and the EU Commission hold similar agreements with the Grand Duchy of Luxembourg to host data and information systems, enhancing their disaster recovery capabilities and resiliency in the process [23, 24].

Although neither of the three examples reflect the exact circumstances that we outline within this research regarding the Vienna Convention, they clearly demonstrate how new technological advances have had an influence on traditional Conventions and declarations, and may well root into international customary law. It may be some time before we see any additional data embassies in operation, despite the aforementioned future partnership between Luxembourg and Monaco, but any subsequent examples may offer credence to this ongoing debate.

5. CONCLUSIONS

This paper has identified that the Vienna Convention is not deemed presently suitable for the protection and inviolability of data and information systems outside of the traditional diplomatic mission. In this exploratory research, the case of the Estonian Data Embassy in Luxembourg has shown that although the Vienna Convention may be applicable in this context, a key challenge emerges in that it is yet to be tested in any given scenario and thus lacks a degree of legal precedent. In this case, an extra-legal layer in the form of a bilateral agreement was found to be sufficient, affording similar powers and immunities to both 'sending' and 'receiving' State.

As it seems at present, there is significant progress to suggest that the Vienna Convention could be extended in its current form to incorporate the protection of data and information systems outside the traditional diplomatic mission. Indeed, as other State's may follow Estonia's lead, the re-assessment of international law and the Vienna Convention may prove a beneficial solution.

6. FUTURE WORK

In acknowledging that this paper only serves as an early ongoing contribution to this novel area, any further analysis will ultimately require a more in-depth approach from an interdisciplinary perspective. In doing so, a more extensive analysis of relevant academic research, and the development, drafting and efficacy of similar bilateral agreements, in this context will be beneficial. Building on the preliminary interviews and document analysis conducted, future research will aim to develop a more thorough methodology, whilst building on any critical feedback and subsequent developments across the legal community moving forward.

ACKNOWLEDGMENTS

This research has received support from a number of funding bodies. Nick Robinson was supported as part of the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1), and partially from the Dora Plus program funded by the European Regional Development Fund. Laura Kask was supported by the European Union from the European Regional Development Fund. Robert Krimmer was supported by TalTech Digital Governance Competency Center (SS483), and the Estonian Research Council (PUT1361).

The authors would like to also express their gratitude to a number of colleagues, including Taavi Kotka and Innar Liiv, for early discussions on this paper.

REFERENCES

[1] Kotka, T. and Liiv, I. 2015. 'Concept of Estonian Government Cloud and Data Embassies', in Electronic Government and the Information Systems Perspective: Proceedings of the 4th International Conference EGOVIS 2015 in Valencia, Spain, September 1-3, 2015, Kö, A. and Francesconi, E. (Eds.), Springer International Publishing, 149-162.

[2] Robinson, N. and Martin, K. 2017. 'Distributed denial of government: the Estonian Data Embassy Initiative', Network Security, 9 (September 2017), 13-16.

[3] Riigikontroll. 2018. 'Guaranteeing the safety of critical databases requires considerably more care', (May 2018). Retrieved November 12 2018, https://www.riigikontroll.ee/Suhtedavalikkusega/Pressiteated/tabid/168/ItemId/995/amid/557/language/en-US/Default.aspx

[4] ENISA. 2015. 'Annex Good Practice Guide for securely deploying Governmental clouds'. Retrieved 13 November 2018, https://www.enisa.europa.eu/topics/cloud-and-big-data/good-practice-guide-for-securely-deploying-governmental-clouds-annex

[5] Kotka, T., Kask, L., Raudsepp, K., Storch, T., Radloff, R. and Liiv, I. 2016. 'Policy and Legal Environment Analysis for e-Government Services Migration to the Public Cloud', in Proceedings of the 9th International Conference on Theory and Practice of Electronic Governance – ICEGOV, Montevideo, Uruguay March 1-3 2016, 103-108.

[6] MEAC and Microsoft. 2015. 'Implementation of the Virtual Data Embassy Solution Summary Report of the Research Project on Public Cloud Usage for Government'. Retrieved 1 November 2018, https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf

[7] MEAC and Microsoft. 2016. 'Transforming digital continuity: Enhancing IT resilience through cloud computing'. May 2016. Retrieved 1 November 2018, https://www.mkm.ee/sites/default/files/transforming_digital_continuity_-_joint_research_report_finaly_may_20.pdf
[8] Kotka, T., Johnson, B., Cebul, T., Lovosevic, L. and Liiv, I. 2016. 'E-Government Services Migration to the Public Cloud: Experiments and Technical Findings' in Electronic Government and the Information Systems Perspective, A. Kő and E. Francesconi (Eds.), EGOVIS 2016, Springer International Publishing, 62-76.
[9] Kaljund, A, L. 2018. 'Restoration Doctrine Rebooted: Codifying Continuity in the Estonian Data Embassy Initiative', PoLAR: Political and Legal Anthropology Review, 41(1), 5-20.
[10] Bruns, K. 2014. 'The Vienna Convention on Diplomatic Relations: A Study of Success', Diplomatist, 2(5), 15-16.
[11] Denza, E. 2016. Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations (4th Edition). Oxford: Oxford University Press.
[12] Denza, E. 2018. 'Vienna Convention on Diplomatic Relations', Audiovisual Library of International Law. Retrieved 8 November 2018, http://legal.un.org/avl/ha/vcdr/vcdr.html
[13] Aceves, W. J. 1998. 'The Vienna Convention on Consular Relations: A Study of Rights, Wrongs, and Remedies', Vanderbilt Journal of Transnational Law, 31(2), 257-263.
[14] United Nations. 1961. 'Vienna Convention on Diplomatic Relations', 18 April 1961. Retrieved 3 November 2018, http://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf
[15] United Nations. 1963. 'Vienna Convention on Consular Relations', 24 April 1963. Retrieved 3 November 2018, http://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf
[16] Manor, I. 2014. 'On Virtual Embassies in the Age of Digital Diplomacy'. Retrieved 16 November 2018, https://digdipblog.com/2014/06/25/on-virtual-embassies-in-the-age-of-digital-diplomacy/
[17] Riigi Teataja. 2017. 'Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems', 20th June 2017. Retrieved 3 November, https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf
[18] Riigikogu. 2018. 'Ratification Act of the Republic of Estonia and the Grand Duchy of Luxembourg on the Agreement on the Accommodation of Data and Information Systems 563 SE' (21 March 2018). Retrieved 14 November 2018, https://www.riigikogu.ee/tegevus/eelnoud/eelnou/bd5c7fc4-b433-4075-ad44-37cd2eb488d8
[19] Lambert, Y. 2018. 'Luxembourg to enter digital partnership with Monaco'. Retrieved 19 January 2019, https://luxtimes.lu/luxembourg/35843-luxembourg-to-enter-digital-partnership-with-monaco
[20] Osula, A-M. 2015. 'Assessing Extraterritorially Located Data: Options for States', NATO Cooperative Cyber Defence Centre of Excellence, 1-27.
[21] Kask, L., Kittus, K. and Weekes, L. 'Data Embassy', SubTech Conference 12-14 July 2018. Retrieved 14 November 2018, https://oigus.ut.ee/en/studies/subtech-conference-2018
[22] European Commission. 2017. 'Regulation of the European Parliament and of the Council on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice', June 2017. Retrieved 15th November 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0352
[23] NSPA. 2016. 'Joint Luxemboug/NSPA Data Centre project launched'. Retrieved 15th November 2018, https://www.nspa.nato.int/en/news/news-20160509-1.htm
[24] MacGregor, A. 2016. 'European Commission opens new data centre in Luxembourg', Retrieved 15th November 2018, https://thestack.com/data-centre/2016/12/13/european-commission-opens-new-data-centre-in-luxembourg/