Development of Cybersecurity Governance in the EU Region

Vivit Widi Haryati[1], Sekar Indira Sihwiyati[2], Arum Meira Talitasyadiah[3]
[123]Universitas Pembangunan Nasional Veteran Jakarta

Abstract

Today, the presence of technology in the era of globalization provides a new threat, especially in cybersecurity. Therefore a strategy needs to be formed as an action by international relations actors in solving complex problems in cybersecurity. Therefore, this article is here to discuss global issues in the field of cybersecurity, especially how the European Union, which is a regional organization, forms a regime to regulate the cybersecurity landscape for its member countries. This research uses a qualitative-descriptive research method through secondary data collection in the form of official EU documents, reports of related institutions, and website articles. As an analytical tool in this research, the authors use the theory of neoliberal institutionalism and the concept of regionalism. Through This research the authors found that global governance has an important role in dealing with complex issues in cyberspace, especially in the region through a landscape of institutional cooperation, such as the European Union's Cybersecurity Act released by ENISA.

Keywords: *Uni Eropa, Cybersecurity, Global Governance, Regime, ENISA*

1. INTRODUCTION

Entering the era of globalization, various global problems began to emerge and were difficult to deal with independently by the governments of countries in the world. In an increasingly complex world, the presence of a concept of connectivity between global actors is indispensable to become a bridge to solve global problems, the most popular concept in this era is "global governance" or global governance. In Jentleson's (2021) writing, it is explained that global governance is concerned with a mechanism or way of making, directing, managing, and regulating policies and actions of society or global.

The meaning of global governance is closely related to several developments both empirically and normatively that facilitate the development of international relations actors and global network systems to create a 'generalized behavioral principle' (Bainus & Rachman, 2022). Global governance consists of very varied pieces or elements. These elements consist of international organizations both state-based and non-state-based, international law, international norms, and other elements. Where an element in global governance may not only focus on one issue or problem but can intersect with other elements (Nursita, 2019).

The presence of global governance is inseparable from the development of digital technology. The presence of information technology itself was brought about by the industrial revolution 4.0 which then revolutionized the way of life with a number of advances that made meeting human needs simpler and more enjoyable (Simorangkir et al., 2023). However, on the other hand, technological developments not only create new conveniences but also create new dangers that not only cover the business and industrial fields but also go beyond security issues.

The presence of information technology that has been inherent in human life can provide a new threat in various aspects of global society. Especially for developing countries, they often fail to improve governance and sustainable results in their information technology affairs. According to Simorangkir, Legionosuko, and Waluyo (2023), one of the threats that is quite watched out for is in the field of strategy, where the presence of technological and information advances can result in the rise of cyberspace. This then creates a new dilemma for the government, namely the issue of cybersecurity. Digitalization has now become a new space for countries in the world to maintain their national security because all aspects of life have been integrated through technology and information.

Currently, countries in the world in maintaining their national security tend to carry out regional cooperation, especially in responding to cybersecurity challenges. Regional activities carried out by countries in a region are usually in the form of negotiations or cooperation construction. According to Nurwahidin, Octavian, and Utomo (2018), regionalism can be used as a way to improve welfare, respond to external challenges, and solve problems together. This can be proven by the formation of several regional organizations such as ASEAN, the European Union, NATO, and so on.

In the issue of global governance in the cybersecurity arena, the organization in the European region, namely the "European Union", is one of the regional organizations that is interesting to research. The European Union has gone through various incidents and cyber crises in the European region which makes this organization one of the regions that has a good cybersecurity system compared to other regions because the European Union is able to create a cybersecurity certification scheme under the European Union Cybersecurity Law (Ananda et al., 2022). Global governance research on cybersecurity in the European Union is an important thing to do. With the presence of this research, it is easy to understand how global governance can provide great benefits in solving complex problems in the midst of the era of globalization, especially in regional cybersecurity flows.

Discussing cybersecurity in global governance, especially in the European Union region, has been presented in several literatures. First, a discussion of this issue was written by Ananda, Putranti, and Dir with the title "Analysis of The EU Cybersecurity Act Under The Theory of Neoliberal Institutionalism" where in this paper discusses one of the Wannacry Ransomware viruses as a cybersecurity crisis that disrupts the running of companies in the European Union. This study discusses how the role of cybersecurity regulation from the Cybersecurity Act as a regime and ENISA as a business law through neoliberal institutional theory in writing its research. They also emphasized that the regulations carried out by the regime can be handled appropriately by releasing an ICT (Information and Communications Technology) service product so that it can improve cybersecurity and build a positive contribution to the European Union's Digital Single Market

Furthermore, in the paper Markopoulou, Papakonstantinou, and de Hert with the research title "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law and Security Review" discusses the relationship between the NIS directive and the European Union's GDPR Law, both of which have their own purposes and mechanisms. From the mechanism of the two entities, the researcher found that the two intersect. Where one of them has to leave the other unaffected by its regulations whether any security measures, personal data breaches, or even each incident must be assessed separately based on their respective situations.

In addition, there is also another research that is a source in the discussion in this paper, namely an article compiled by Saleh, Yuliana, and Pramudian with the title "Digital Security in Estonia" which was published in 2022. Their article discusses digital security in Estonia which has a long history in building the country's cybersecurity and its participation in the European Union and NATO so that the Estonian state is considered to have a good level of cybersecurity in the European Union's cybersecurity regime.

In analyzing global governance, the theory of neoliberal institutionalism is a theory that is relevant and comprehensive enough to understand the issues that occur. The theory pioneered by Robert Keohane supports the importance of establishing institutions or institutions in building international cooperation with the assumption that the state is not the only main actor in international relations. Institutionalist neoliberalism is a fragment of the understanding of liberalism based on the view of freedom and equal rights in political values (Ananda, et al. 2022).

In this theory, international institutions and organizations become an embodiment of cooperation in an anarchic international structure. Complex international problems and differences in the interests of each country allow conflicts to arise, so this theory exists to understand and see that institutions equipped with binding rules are important to guarantee international cooperation. Keohane explained that in building international cooperation, the actors involved must have the same interests so as to give rise to cooperation in the form of agreements and organizations in global politics. Cooperation in different interests gave rise to institutional variations that led to the formation of international regimes in handling various kinds of international issues. (Keohane, 1989)

In addition, the concept of regionalism can also be used to analyze the actors involved in handling an international issue. Regionalism in general can be interpreted as an understanding of elements such as social, economic, historical, and cultural elements in the unification of individuals or communities in a region. Regionalism comes from the word "region" which, according to Hopkins and Mansbach (1973), is a territorial grouping based on geographical aspects, economic and cultural interdependence, and interdependence and communication involvement in international organizations. Through this, regionalization can be a concept to understand the formation of organizations in a region and see how regional organizations or groups respond to international issues that develop as globalization progresses, one of which is the issue of cybersecurity.

2. RESEARCH METHOD

A simple research method to examine how the European Union (EU) global governance in the cyber domain can maintain cyber security from cybercrime (Cyber Crime) can be started by using a descriptive qualitative method with the technique of writing a literature study, where in this study uses various sources from books, journal articles, and other references sourced from the internet as a reference for the author in explaining how the European Union and regime in it to handle cybersecurity regionally. Descriptive qualitative research also provides an overview in describing a phenomenon or social condition to be studied (Waruwu, 2023).

In this stage, the researcher will collect data and information related to EU global governance in the cyber domain, including the policies, regulations and institutions involved. The data sources used by the authors are secondary data derived from official documents such as EU decisions, reports from relevant institutions, journal articles,

website articles, and case studies from EU member states that have successfully overcome cybersecurity challenges.

3. RESULT AND DISCUSSION

The development of globalization and technological advances have made the use of the digitalization system more comprehensive in various fields. Ease of access to information and communication for the public supports the efficiency and effectiveness of work, as well as international cooperation whose escalation is supported by technological and scientific developments. Even so, these developments are accompanied by real cybersecurity threats and can affect global dynamics. Cybersecurity issues, although not included in traditional security issues, can threaten the security of the state, institutions, and international organizations. In dealing with cyber threats, organizations and individuals must determine the right steps because the increase in cybersecurity problems can affect world politics and can give rise to tensions and conflicts (Hamonangan & Assegaff, 2020).

Security issues in cyberspace are growing over time. The increased use of the internet since the 1990s has made cyber threats more impactful globally. Davies' (2021) article in Cyber Magazine explains that the ease of internet access makes organized crime entities use it as a source of income by stealing public and government data through the web. This caused network security threats to increase in the mid-1990s, resulting in an urgency in the mass production of antivirus programs to protect government and public data. Cyber threats then became more diverse and increased with the emergence of criminal organizations that funded large-scale cyberattacks in the 2000s and the development of ransomware (malicious malware) outbreaks that threatened the security of organizational data. (Davies, 2021).

Threats in cyberspace are also inseparable from the increased dependence on cyber infrastructure so that countries compete to improve cyber technology to achieve national interests. Modern technology that has progressed, especially in cyberspace, has a significant impact on all aspects of life, making people and governments dependent on digitalization in their daily activities. At the same time, the potential threat is increasingly widespread from the consequences of cyber developments, such as an increase in virus or malware attacks and theft of data or information that can affect financial losses, loss of property, to threats to the life of a person or group (Heffer & Goel, 2018).

Cyber developments also have the potential for cyber wars between countries or regions. In an article written by Heffer and Goel (2018), it is explained that countries have recognized the potential for cyber attacks in the military field so that they are actively developing digital weapons which can lead to a cyber arms race. Therefore, an approach from diplomacy and international cooperation is needed to prevent and mitigate the cyber arms race before it leads to a global catastrophe (Heffer & Goel, 2018).

In the midst of an anarchic international system, neoliberal institutionalism strongly promotes international cooperation that is considered to be appropriately carried out through the formation of institutions and strong rules of the game. In Keohane's (1984) thought, the rules of the game are in the form of "a set of principles, rules, norms, and decision-making procedures on which the expectations of actors are based". Keohane's thinking can be proven to be in harmony with the case of a cyber attack carried out by Russia against Estonia in 2007 in the form of a DDoS (Distributed Denial of Service) attack on Estonian government websites and lasted for approximately two weeks (Firman, 2018). In response to these problems, the Estonian government created the Estonia Cyber Security Strategy for 2008-2013 policy document which was inaugurated in 2007.

The implementation of the policy is carried out by forming the Cyber Defence League. The Estonian government has also improved Estonia's national defense in cyberspace by establishing several institutions and implementing inter-agency cooperation such as the Cyber Security Council at the State Security Committee, the Estonian Informatics Centre, and CIIP (Critical Information Infrastructure Protection). (Saleh et al., 2022).

If we focus on a region, Europe becomes a fairly interesting region, where if we identify in the concept of regionalism according to Couloumbis and Wolfe (1986) the European Union is a region that has strong geographical and political and military criteria where the grouping of countries in this region consists of countries located on the European continent with the majority having the same alliance and ideological orientation. When it comes to maintaining security in the region, stakeholders in the EU are vulnerable to security threats in the ever-evolving cyberspace. This then challenges the European Union to think of new ways of addressing the damage that arises from the poor use of cyberspace (Bechara & Schurch, 2020).

Actors in Cybersecurity Governance in the European Union: A Neoliberal Study of Institutionalism

International security issues are increasingly growing and diverse after the end of the cold war. Changes that continue to shift over time along with the flow of globalization, especially in the field of technology, make all countries in the world pay special attention especially to cyber security which can potentially be a disaster if not handled seriously. In examining the digital industry 4.0, the increasing use of ICT (Information and Communications Technology) can increase the potential for substantial challenges because it is undeniable that the impact of the digital industry in various sectors is one of the strong evidence for the development of ICT.

In cyber securitization, which has unlimited space, both physical and visual, that separates traditional and non-traditional boundaries, is a factor of threats that can affect national security (Jose HS, 2021). The implication factor of national security threats that can provide encouragement is that a country must prioritize domestic policies in achieving its national interests and in cyberspace a rule of law needs to be established (Dunn & Wenger, 2019). In addition to the need for domestic policies or international policies formed by each country as a form of cyberspace security, it also needs to be carried out by international organizations, institutions, or regimes. Every organization across the country is competing to adopt a digital transformation strategy in improving their capabilities. Through one of the focuses of neoliberal theory, namely institutionalist neoliberalism, in which this theory generally views countries in forming an international organization that aims to make it easier for each country to contribute or cooperate with other countries in it (Imannulloh & Rijal, 2022).

Neoliberal institutionalists exist through a debate between neorealists who view that cooperation will be very difficult if it occurs in anarchic conditions. This is not disputed by the institutionalists, under circumstances where anarchy can affect the international structure. Both statements can be concluded that both do not deny that cooperation will be very difficult if the international world is placed in a position of mutual suspicion and anarchy. Institutionalist neoliberalism is present as a view, especially for institutionalists who provide solutions for cooperation that can be done through international regimes (Rosyidin, 2023). The international regime becomes a principle, norm, rule and procedure that becomes an explicit and implicit decision-making, where international relations actors can unite in making these decisions (Keohane, 2005). The European Union as a regional organization is present as a form of cooperation between countries

in Europe in maintaining the existence of sustainability of technology which will bring many benefits to economic development as well as in the security of digital technology in the European Union. So, in this principle, it can be concluded that, it will be very important to cooperate between countries to prevent the risk of cyber security itself in overcoming a cyber threat.

Actors in global governance in the field of non-traditional security in European Union countries build complex cooperation in forming a Cybersecurity Act policy. This is in accordance with international institutions or organizations forming a state of dependence between countries and other international actors that can have considerable effects (Keohane & Nye, 1973). Thus, the European Union is taking a harmonized approach to dealing with cyber threats that harm society. The European Union also implements a standardization that can improve cybersecurity and build cyber resilience that can make a positive contribution to the maximum Digital Single Market (Ananda et al., 2022).

Cybersecurity Act hadir menjadi sebuah regulasi yang dibentuk oleh Uni Eropa. Cybersecurity Act sendiri merupakan sebuah regulasi yang dibentuk oleh ENISA (The European Parliament and The Council of The European Union) 2019/881. Di mana Cybersecurity Act tersebut, mengatur mengenai pasar internal dalam menanggapi sebuah tantangan terkait keamanan dari berbagai produk ICT, layanan ICT, dan proses ICT itu sendiri di dalam Digital Single Market.

This is also supported by looking back at Krasner's (1983) opinion where "Governance without Government" became a real elaboration of the global system, where the organization became a meeting arena for international actors to discuss issues other than cyber security in the European Union, of course, ENISA as an international regime. ENISA as an international regime that does not directly contribute by providing a report on the ENISA Threat Landscape. The report contains to identify key threats and trends, as well as relevant measures on cyber attacks, DDoS attacks, zero-day exploits, and other cases both past and present. ENISA provides an insight into the cybersecurity landscape for its member countries.

International Law in the Governance of Cybersecurity of the European Union

The presence of global governance is not spared from the presence of pillars or elements of global governance itself. One of the pillars that is closely related in regulating the global society in the era of technological advancement is international law. International Law itself can be defined as a set of rules and principles that govern all cross-border relations, both state and state, or it can also be a country with other legal subjects, both non-state and non-state law subjects (Kusumaatmadja, 2003). According to Article 38 Paragraph (1) of the Statute of the International Court, the sources of international law itself consist of international customs, international agreements, as well as additional legal sources such as court decisions and the opinions of legal experts (Risnain, 2020).

Problems arising from cyberspace give rise to cyber threats which, if left unchecked, can pose a real threat to sovereignty so that all countries in the world need to pay attention to their cybersecurity. Among the countries in the world, one of the countries that reportedly received the most cyber threats was the United States with 4,000 cyberattacks during 2020. Further in the Allianz Global Corporate & Speciality report (2020), Singapore has also experienced cyberattacks with the emergence of a data leak case from Singapore's Ministry of Defence through a malware virus sent via email to accounts belonging to 2400 Singaporean personnel. If we shift to the European Union

region, cases of cyber threats often occur and had caused a cyber crisis in the European Union in 2017 through the "WannaCry" Ransomware Epidemic attack which targeted various large companies that provide vital services in the European Union (Ananda et al., 2022).

Internationally, to deal with increasingly complex cyber threats, global governance must strive for the presence of international law to regulate and maintain cybersecurity in all countries in the world. Various international conventions and agreements to address cybersecurity issues have been made, one of which is the "Budapest Convention" on cybercrime, which was initiated by the Council of Europe for the rest of the world. This convention is here to harmonize the law while improving investigative techniques that are expected to combat crime in cyberspace (Ramayanti & Lubis, 2023). Not only that, there is another guide that can be used by the global community, namely the "Tallinn Manual 2.0" which is a guide for policyholders and legal experts to explain that Cyber Espionage acts are part of cyber crimes that are carried out secretly to gather information (Mustameer, 2022).

According to Keohane (1989) in the Theory of Institutional Neoliberalism, the institution that is formed can determine the behavior of all actors involved so that cooperation can run more clearly and smoothly, where the form of the institution can be in the form of an organization, a set of rules, and conventions. In an effort to deal with various cyber threats, the European Union applies Keohane's thinking by issuing the Cybersecurity Law where this Law is a set of rules established through Regulation (EU) 2019/881 to improve cybersecurity in the territory of the European Union through a permanent mandate which is then given to the European Union Agency for Network and Information Security (ENISA) (Ananda et al., 2022). The Cybersecurity Law according to Article 288 of the Treaty on the Functioning of The European Union (TFEU) not only gives a permanent mandate to ENISA but is binding in its entirety and applies directly to all members of the European Union.

In addition to the Cybersecurity Law, the European Union also issued another legal instrument, namely the General Data Protection Regulation (GDPR) in July 2016 in April. According to Markopoulou, Papakonstantinou, and Hert (2019), the principle of personal data security is one of the basic principles of the GDPR. Referring to article 3 of the GDPR, the applicability of the GDPR is not only limited to the territory of the European Union.

The presence of a set of laws that have been established in the territory of the European Union helps governments in the European Union have a harmonized approach in dealing with various forms of cyber threats that are starting to develop over time. The existence of a law regulating cybersecurity in the European Union also has the potential to improve cybersecurity while building cyber resilience. It does not stop there according to Article 52 of Regulation (EU) 2019/881, the law that regulates cybersecurity can help evaluate and provide information on risks to cybersecurity in the European Union (Ananda et al., 2022).

4. CONCLUSION

Global governance plays an important role as a bridge for international relations actors in dealing with global problems, both empirical and normative. The presence of technology in the era of globalization presents new challenges, especially in the field of cybersecurity, which requires a mature strategy from international relations actors. This article highlights the importance of global governance in addressing complex problems in cyberspace, especially in regional areas through a landscape of institutional

cooperation, as the European Union has done with the Cybersecurity Act released by ENISA.

This article illustrates the relevance of neoliberal theories of institutionalism and the concept of regionalism in the context of international relations, which emphasizes the importance of cooperation between institutions or organizations in a regional region in solving global challenges. The dynamics of cybersecurity, which includes history, international relations actors, and international law, are the main focus in understanding the complexity and importance of cross-border cooperation in addressing security threats in today's digital world. The rapid development of information technology also complicates the dynamics of cybersecurity. The increasing global dependence on digital infrastructure also reinforces the urgency to increase international cooperation in securing the digital space that is vital to various economic and social sectors.

5. REFERENCE

Couloumbis, T. A.. & Wolfe, J. H. (1986). Introduction to International Relations. Englewood Cliffs, N.J. : Prentice-Hall

Hopkins, R. F. & Mansbach, R. W. (1973). Structure and Process in International Politics. Harper and Row.

Keohane, R. O. (1989). Neoliberal Institutionalism. A Perspective on World Politics, in International Institutions and State Power. Westview Press.

Keohane, R. O. (2005). After Hegemony Cooperation and Discord in the World Political Economy. Princeton Univeristy Press.

Keohane, R. O., & Nye, J. S. (1973). Power and interdependence. Longman.

Kusumaatmadja, M., & Agoes, E. R. (2003). Pengantar Hukum Internasional. Alumni.

Risnain, M. (2020). Hukum Internasional dan Kepentingan Nasional Indonesia. Sanabil.

Rosyidin, M. (2023). Teori hubungan internasional: dari perspektif klasik sampai non-Barat. PT. RajaGrafindo Persada-Rajawali Pers.

Laporan :

Allianz Global Corporate & Speciality (2020). Allianz Risk Barometer Identifying The Major Business Risks For 2020. https://www.allianz.com/en/economic_research/insights/publications/specials_fmo/2024_01_16-Allianz-Risk-Barometer.html

Artikel Jurnal :

Ananda, S., Putranti, I., & Dir, A. (2022). Analysis of the Eu Cybersecurity Act Under the Theory of Neoliberal Institutionalism. Arena Hukum, 15(1), 176–199. https://doi.org/10.21776/ub.arenahukum.2022.01501.9

Bainus, A., & Rachman, J. B. (2022). EDITORIAL: Tata Kelola Global dalam Hubungan Internasional. Intermestic: Journal of International Studies, 7(1), 1-10. https://doi.org/10.24198/intermestic.v7n1.1

Bechara, F. R. & Schurch, S. B. (2020). Cybersecurity and Global Regulatory Challenges. Journal of Financial Crime, 8(2), 359-374. https://doi.org/10.1108/JFC-07-2020-0149

Dunn, C. M. & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Hamonangan, I. & Assegaf, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional Yang Damai Di Era Digital. Padjadjaran Journal of International Relations (PADJIR), 1(3), 311-333. https://doi.org/10.24198/padjir.v1i4.26246

Imannulloh, E. R., & Rijal, N. K. (2022). Upaya indonesia dalam mendorong prioritisasi perekonomian negara berkembang melalui G20: perspektif hyper-globalist. Indonesian Perspective, 7(1), 79-101.

Jentleson, B. W. (2021). Global Governance, the United Nations, and the challenge of trumping Trump. JSTOR, 23(2), 143–149. https://doi.org/10.1163/19426720-02302001

Jose, H. S. (2021). Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral, POPULIKA, 9(2), 70-85. https://doi.org/10.37631/populika.v9i2.390

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law and Security Review, 35(6), 1-11. https://doi.org/10.1016/j.clsr.2019.06.007

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. Jurnal yustika, 25(1), 40-53. https://doi.org/10.24123/yustika.v25i01.5090

Nursita, R. D. (2019). Cyberspace: Perdebatan, Problematika, Serta Pendekatan Baru Dalam Tata Kelola Global. Journal of Islamic and International Affairs, 4(1), 80–99. https://doi.org/10.21111/dauliyah.v4i1.2934

Nurwahidin, Octavian, A., & Utomo, A. W. (2020). Kepentingan Negara-Negara Pantai Menghadapi Ancaman Transnational Non State Actor Di Selat Malaka. Jurnal Maritim Indonesia, 8(2), 189–217. https://doi.org/10.52307/IJM.V8I2.42?sid=semanticscholar

Ramayanti, H., & Lubis, A. F. (2023). Peran Hukum dalam Mengatasi Serangan Cyber yang Mengancam Keamanan Nasional. Jurnal Hukum Dan HAM Wara Sains, 2(09), 904–912. https://doi.org/10.58812/jhhws.v2i09.672

Simorangkir, T. B., Legionosuko, S. D., & Waluyo, S. D. (2023). Cyber Security Dalam Studi Keamanan Nasional: Politik, Hukum Dan Strategi, 17(10), 2409–2414. https://doi.org/10.33578/mbi.v17i10

Proceedings :

Heffer, A. & Goel, S. (2018). Mitigating Cyber Warfare through Deterrence and Diplomacy. WISP 2018 Proceedings. 21. https://aisel.aisnet.org/wisp2018/21

Artikel Website :

Davies, V. (2021, October 4). The History of Cybersecurity. Cyber Magazine. https://cybermagazine.com/cyber-security/history-cybersecurity.

Firman, F. A. (2018, November 11). Kebijakan Pertahanan Cyber Estonia Dalam Merespon Tindakan Cyber Sabotage Oleh Rusia Kepada Estonia. UNIKOM Repository. https://repository.unikom.ac.id/59424/

Saleh, A, K., Yuliana, A. D., & Pramudian, G. W. (2022). Digital Security in Estonia. ResearchGate. https://www.researchgate.net/publication/362017438