Small States and Cyber Security

The cases of Estonia, Lithuania, Georgia and Moldova

Name: A.N. Kil

Student number: s1328387

Professor: Dr. W.P. Veenendaal

Bachelor Project: Small States in World Politics

Date: 06-18-2018

Word count: 8388

Introduction

Cyber security is a global issue because of the increasing state's interdependency and the transnational nature of cyber security (Jang-Jaccard & Nepal, 2014, p.973; Pearson, 2011, p.5216). Cyber security is not only a threat for larger, but also for smaller states. The state's dependency on the internet for their critical information infrastructures is increasing, which makes the states more vulnerable for cyber attacks. Critical information infrastructures are the target of cyber attacks because of their vulnerability, and when attack, it can lead to devastating consequences as it could cripple the states economy and shut down government systems (Pearson, 2011, p.5115; EPSC Strategic Notes, 2017, p. 1-3; Do et al, 2017, p.1). This is especially dangerous for small states with vulnerable economies as they could collapse. Also it is more likely that small states will have less resources and knowledge to deal with cyber security than larger states. Another aspect that makes cyber security important is its cross-dimension. This means that it affects multiple dimensions, such as the political and legal (UNIDIR, 2013, p.92). Furthermore, small states are already victims of cyber attacks, for instance Estonia and Georgia endured cyber attacks by Russia in 2007 and 2008 respectively (Burton, 2013, p.216-222; Davis, Bradley & Dool, 2017; p.10). Therefore, it is important for small states that have predatory neighbours like Russia to be able to defend themselves against cyber attacks if it occurs in the future, as of they undertake no action they remain vulnerable for an attack. Also interesting is the possible influence of a membership of an international organisation, as they enable small states with the possibility to achieve certain goals. Therefore, it is interesting to see if a membership of an international organisation influences the way in which small states deal with cyber security. By researching this, small states will know if being a member of an international organisation is important to have regarding cyber security.

In this thesis, the way in which small states deal with cyber security will be researched. Furthermore, the influence of a membership of the European Union (EU) and North Atlantic Treaty Organisation (NATO) will be explored. Analysing if there is a difference between the states with a membership and non-member states will do this. Therefore the thesis will start with a literature in which all the important literature and theories will be discussed. After this the research question, its relevance and expectations will be broached. Followed by research design, methodology and data analysis. In this thesis a comparative qualitative research with multiple cases will be used in order to find out how small states deal with cyber security and if EU/NATO membership plays a role. These cases are Estonia, Lithuania, Georgia and Moldova.

Literature review

Cyber security as security issue

Security issues are a threat for states, regardless of their size, even more so for smaller states than for larger states (Sutton & Payne, 1993; p.580-581). This is because most small states are more vulnerable than larger states; small states have fewer resources than their larger counterparts to deal with security threats (Bartmann, 2002, p.370-372). A more recent security issue that states face is cyber security. According to critical security studies, cyber security is a security issue as it threatens the states though a military or non-military attack (Peoples & Vaughan-Williams, 2015b, p. 35-36). Furthermore, geographic location of the state is less of importance as cyber security is transnational (Burton, 2013, p.232). It also threatens the core value of a state as it targets the infrastructure, which is of importance for all states and involves every citizen that is dependent on it (Sutton & Payne, 1993, p.579; Gamreklidze, 2014, p.203-204; Carrapico & Barrinha, 2017, p.1259; EU2017, 2017). By attacking the states critical information infrastructures, it has the power to destabilize the state and can cause economic damage (EPSC Strategic Notes, 2017, p. 1-3). Therefore, cyber security is a new threat, as it goes further than territorial integrity and can be seen as a fifth domain after land, sea, space and air (Bartmann, 2002, p.360; EPCS, Strategic Notes, 2017, p.3). A few problems arise because cyber security is a new security issue. The divide between states that have the knowledge and capability to defend themselves and those that not is one of them (Gamreklidze, 2014, p.200-201). This is a problem for small states, as most of them do not have the knowledge or capabilities. According to Burton (2013, p.224) there is another implication for small states as most cyber attacks come from larger and more powerful states such as the US and China. Van der Meer (2016, p.1) explanation for this is that larger states have invested more in offensive cyber security and are more prepared to use them in comparison than small states. This is a problem for small states as according to realist theory small states rely on larger states for protection (Burton, 2013, p.218).

Small states and security theory

Because of their size, small states have limited means in order to secure their safety, as they do not have the resources for defence, intelligence-gathering facilities and surveillance. Therefore small states, unlike larger states, do not rely on conventional means or military power (Bartmann, 2002, p.364). According to the liberal perspective of international relations, small states will cooperate with other states and look for institutions and international rules in order to secure their safety (Burton, 2013, p.218; Bartmann, 2002, p.361-365). Further in the literature review the subject of small states and why they join international organisations will be broached. Bandwagoning and balancing are realist approaches to explain how small states deal with security issues. With bandwagoning small states join forces with a larger and stronger state and with balancing small, states join alliances to create balance against powerful actors (Burton, 2013, p.218; Vaicekauskaité, 2017, p.10-11).

According to neorealism, states are self-reliant when it comes to national security and invest in military means to protect themselves (Peoples & Vaughan-Williams, 2015, p.18). This could possible translate to states independently investing in cyber security defence capabilities in order to withstand cyber attacks.

Small states and international organisations

Small states join international organisations in order to secure their safety and because the divide between small and large states does not exist in most international organisations (Thorhallsson & Wivel, 2006, p.21). Furthermore, realism states that small states join international organisation because of converging interest or dominating power relations (Tillman, 2015, p.22). By joining an international organisation, small states are not only able to cooperate with other states, but also enables them to operate and exert influence under the right circumstances in order to advocate their interest (Thorhallsson & Wivel, 2006, p.22; Tillman, 2015, p.21-22; Luša, 2016, p.11). For instance, a small NATO member state gains access to the discussions on global security issues and play an innovative role in international relations, which would otherwise be hard to do (Luša, 2016, p.5). Small states can influence EU policy making through three different mechanism, these are: bargaining power, argumentive power or through power/reputation, although it is said that small states still have a disadvantage because of their limited bargaining power (Panka, 2010, p.799-802). Small states can also follow different strategies in international organisations; the glue strategy in which small states try to gain influence and promote their own security interest, or the dissolvent strategy, in which small states try to extract benefits from a consensus rule in which they refuse a common policy without concessions in other issues (Luša, 2016, p.5). In this case, small states could join international organisations in order to secure their safety against cyber attacks and advocate its importance.

How small states deal with cyber security

Because cyber security is important, it has to be prioritised in public policies and backed up by appropriate measures in order to have an adequate cyber defence. This can be done through a national cyber security strategy (EPSC Strategic Notes, 2017, p.1; Gamredklidze, 2014, p.208-209). Therefore, small and large states alike have to create strong regulatory frameworks and policies in order to secure their critical information infrastructures against cyber attacks (EU2017, 2017; Robinson, 2017). International organisations and allies are important for the sharing of information, cooperation and coordination, but also the training of Information Technology (IT) specialists and raising awareness are needed (Franke & Brynielsson, 2014, p.19-20; Robinson, 2017; UNIDIR, 2013, p.92). IT also plays a role in the defence against cyber attacks. Security analysts rely on Intrusion Detection Systems (IDS). This provides them with a way to be able to detect network intrusion and network misuse by matching patterns of known attacks against other network systems. When IDS finds a similar kind of 'attack' it gives out an alert (Ben-Asher & Gonzalez, 2015, p.51-52).

Moreover, small states, like larger states, deal with cyber security through investing money on cyber defence. How much states spend on cyber defence is not only based on their dependency on the internet and the technology that comes with it, but also on the threat and risk of enduring a cyber attack (Robinson, 2017). Budget, or money, comes with a complication for some small states. This is because larger states usually have more money at their disposal than most small states. For instance, France had a budget of one billion Euro and UK one of 1.9 billion ponds (Robinson, 2017). These are large amounts that small states are unlikely to meet.

According to Denning (2013, p.108-110) there are two kinds of cyber defence systems that can be distinguished, an active cyber defence and a passive cyber defence. An active cyber defence has as goal to directly destroy, nullify or to reduce the effectiveness of a cyber threat and a passive cyber defence uses a less direct approach than an active cyber defence in order to minimize the effectiveness of a cyber attack by focusing on reinforcing the system against cyber attacks. Furthermore, passive defence has as goals to make cyber assets more resilient to attack and active defence is taken against a specific threat (Denning, 2013, p.109-110).

Cyber security and international organisations

Because cyber security is a relatively new security issue, military alliances and international institutions like the EU and NATO are only starting to create and develop mechanism in order to tackle cyber security. The EU sees cyber security as too transnational for member states to handle on a national scale, and should be done on an international scale (Carrapico & Barrinha, 2017, p.1266). Therefore is does not come as a surprise that cyber security is a top issue on the EU policy agenda after attacks such as WannaCry and NotPetya (Barrinha & Farrand-Carapico, 2018). Furthermore, at EU level, member states work together in order to protect the EU against cyber attacks (EU2017, 2017). In order to deal with cyber security the EU has created diverse initiatives and mechanisms. For instance, is has the EU 2016 Global Strategy, the EU Cyber Security Strategy, (EU-CSS) invested in the Network and Information Security Directive, which focuses on cooperation between member states and has plans to create an EU Cyber Security Agency (Carrapico & Barrinha, 2017, p.1257-1260; Barrinha & Farrand-Carrapico, 2018; EPSC Strategic Notes, 2017, p.1). EU-CSS is based on three pillars; the protection of critical information infrastructure, cybercrime and cyber defence (Carrapico & Barrinha, 2017, p.1261-1262). Additionally the EU has the Agency for Network and Information Security (ENISA), which objectives are to enhance network and information infrastructures and raising awareness about cyber security (EPSC Strategic Notes, 2017, p.7). Furthermore, the EU has based its dealings with cyber security on four different constituencies; IT security, law enforcement, intelligence and diplomacy and defence related aspects (EPSC Strategic Notes, 2017, p.7). These include the Computer Emergency Response Teams (CERTs) and Computer

Security Incident Response Teams (CSIRTs), which are used both on European and National level (EPSC Strategic Notes, 2017, p.7). An important law that applies to cyber security is the General Data Protection Regulation (GDPR); which set the free flow of data as a principle (EPSC Strategic Notes, 2017, p.6).

Although the EU has these promising frameworks and institutions, these do not come without any problems for their small member states (Burton, 2013, p.219-220). According to Burton (2013, p.219-220) this causes a number of issues for small states; they have to create a number of facilities in order for this strategy to succeed, the problem hereby is that not every small state has the resources to achieve this, as requires funds and knowledge to establish these facilities. Another problem small states have to deal with is that although EU strives to deal with cyber security on an international scale, it places the responsibility for dealing with cyber security on its member states (Barrinha & Farrand-Carrapico, 2018). This leaves small states to mostly deal with cyber security independently, whilst they look towards the EU for assisting them.

NATO finds cyber security important and therefore sees cyber attacks as a threat that has negative implications for the national and transnational security (Pernil, 2014, p.1). Thus, NATO has approved the Policy on Cyber Defence and the Cyber Defence Management Authority to coordinate cyber defence and has included cyber defence in NATO exercises (Pernik, 2014, p.4-5). Because NATO sees cyber security as an important issue, it has included cyber security attacks in their collective self-defence, meaning NATO will help a member state when it asks for help after enduring a cyber attack (NATO, 2016, p.1; Pernik, 2014, p.5). This means that NATO will provide aid to a member state when it endures a cyber attack, which has to be approved by the council beforehand (Pernik, 2014, p.5). This gives small states with NATO membership an extra security aspect that small states without NATO membership do not have. Furthermore, NATO also provides its members assistance in securing and protecting their online networks and infrastructures (NATO, 2016, p.1-2).

Research question

Although research is done on cyber security, this is mostly about the medium large and large states rather than about small states (Van der Meer, 2016, p.1-2). It is important to know how small states are affected by cyber security, as they are not less important because of their smallness and make up over half of the member states of the United Nations (UN); (Hughes & Colarik, 2016, p.19). Also, it is important to know how small states with a reliance on information structure should act, because the more dependent they are on it, the more vulnerable they become for a cyber attack and the more damage an attack can inflict (Burton, 2013, p.223; Gamreklidze, 2014, p.204-205). According to liberal theory, alliances and memberships of international organisations are important for states in order to deal with security issues, such as cyber security. Because international organisations, such as EU and NATO, play important roles for small states, it is important to know if EU/NATO membership influences the way in which small states cope with cyber security. If EU/NATO membership has advantages for small states, other small states can join international organisations in order to decrease their vulnerability against cyber attacks rather than dealing with it independently. This leads to the following research question: how do small states deal with cyber security, and does EU/NATO membership influence the way how small states deal with cyber security? Therefore the scientific relevance of this research is to figure out if small states can benefit of a membership of an international organisation in regard to cyber security. In order to be able to answer this research question four cases will be examined. These are Georgia, Estonia, Moldova and Lithuania. Later on in this paper the reason for the selection of these four cases will be discussed.

Expectations

The expectation of this thesis, based on liberalism, is that small states will seek security against cyber security, in the form of a membership of an international organization or other forms of cooperation with states and organisations instead of following neorealism theory that states will be self-reliant and not join an international organisation. This is because small states lack the resources and knowledge that larger states have in order to deal with cyber security independently. Through international organizations small states will be able to create cyber defence capabilities, which they could not have done independently.

The second expectation is that small states, like larger states, will reinforce its cyber defence by the creation of a national cyber security strategy and the creation of other policies that enhance it. This includes a budget for cyber defence. Small states will also make use of the training of IT specialist in order to tackle cyber security.

The third expectation is that a small state that is a member of EU/NATO will be more capable to deal with cyber security, as it can use the guidelines that EU and NATO has provided and participate in its cyber security institutions. Therefore, small states know what to do and can rely on the EU/NATO policies and institutions. For instance, members of NATO can rely on the collective self-defence system when it endures a cyber attack.

Conceptualisation and operationalization

The concept of a small state will be conceptualized in two ways. The state as an entity that is a member of the UN and smallness by the number of inhabitants the state has. Therefore a small state is a state that is a member of the UN with a limited number of inhabitants. The conceptualization of smallness based on the number of inhabitants, is chosen because of the fact that most definitions of a small state are based on this instead of territorial size and because of its simplicity and convenience. (Commonwealth Secretariat, 2011; 2015; Hey, 2003, p.2-3). The threshold of the number of inhabitants will be five million. The Commonwealth Secretariat (2011; 2015) also uses this threshold for their classification on small states in their works. This is because when looked at Europe thirty-three states have less than five million inhabitants, which means more states are included and enough states remain to research how small states deal with cyber security and therefore more applicable to more states (European Union, 2018; Crossley & Sprague, 2012, p.27-30).

Cyber security is a difficult concept to conceptualize, as it is relatively new and therefore no single worldwide definition exists. For its conceptualization, two definitions will be used that complement each other. The first definition is from Thomas (2009, p.7-8), he described cyber security as having an implicit transnational nature in which the initiators and the victims are in different states in which web-based technologies are used in order to attack the targeted group. This highlights the transnational nature of cyber security and that cyber attacks use the internet. The UN specialized agency for information and communication; the International Telecommunication Union (ITU) offers the second definition that complements the definition of cyber security (ITU, 2018b). According to ITU (2018a) cyber security is a collection of many things, such as security safeguards and polices, which are used to protect the cyber environment. This shows that cyber security is also about the protection against cyber attacks. The combination of both definitions illuminates both sides of the concept of cyber security, the aggressive nature through the use of the internet and the protective nature by protecting the cyber environment against cyber attacks.

Research design and methodology

This research has as goal to find out if EU/NATO membership influences how small states deal with cyber security and if it has any advantages. Therefore, a qualitative design with a comparative multiple-case study will be used. The four cases that will be researched are: Georgia, Estonia, Lithuania and Moldova. The most similar system design (MSSD) will be used to compare these states. The MSSD is chosen as it focuses on the independent variable, how does X affects Y (Anckar, 2008, p.395; Seawright & Gerring, 2008, p.304). This applies to the research, namely; how does EU/NATO membership influence the way in which small states deal with cyber security. Furthermore, it improves theory building and can confirm the expectations of this thesis (Bryman, 2016, p.74). Although there are benefits, MSSD comes with a limitation; this is that most cases are never similar except for one variable (EU/NATO membership); (Seawright & Gerring, 2008, p.305).

Only six states former Soviet Union states remain with less than five million inhabitants; Georgia, Estonia, Lithuania, Moldova, Armenia and Latvia. From these six cases, Georgia, Estonia, Lithuania and Moldova are chosen. Besides earlier named similarities, Russia can be seen as a threatening neighbour state. Estonia and Georgia are specifically chosen because they endured a cyber attack from Russia in 2007 and 2008 respectively. Besides the common variables of these four states, there is also distinctive difference that separated the cases in two different groups and therefore makes them a good fit for MSSD. This distinguishing variable is EU/NATO membership and enables this research to find out what the influence is of membership for the small states that deal with cyber security. Estonia and Lithuania are EU and NATO member states since 2004, and Georgia and Moldova are not. Another reason why these four states, and Armenia and Latvia are not chosen is based on the ITU Global Cyber Security Index (GCI) of 2017. The GCI is an index that measures the level of cyber security commitment of the ITU member states with a scale from 0 to 1, with 1 being the highest score (Acayo, 2017; DigiAnalysys, 2017; Hankewitz, 2017; ITU, 2017, p.9). GCI composes the score through the answering of questionnaires by the members states, which are based the five pillars of the Global Cybersecurity Agenda (legal, technical, organisational, capacity building and cooperation), and with supporting evidence of their own research (Hankewitz, 2017; ITU, 2017, p.9). Estonia, Georgia, Moldova, Lithuania and Latvia are in the top hundred of the ranking. Armenia is not chosen, as scored below the top hundred, which makes them less similar to the other cases and its score too low in order to see how they deal with cyber security. Estonia and Georgia are in the top ten ranking, whilst Lithuania and Moldova have the lowest score of the group in the top hundred, Latvia scores in the middle (DigiAnalysys, 2017). The difference between the top two and bottom two, which both include an EU/NATO member and non EU/NATO member, is interesting to research to see why this difference exist, as it could be expected that EU/NATO members would rank the highest and non

EU/NATO member the lowest, but this is not the case. By researching these four states, the influences of EU/NATO membership on cyber security could be discovered.

In order to compare these four states and answer the research question a content analysis will be employed. In this content analysis multiple sources will be used, these include policy and strategy papers of the government of the four states and other government documents that are related to the cyber security domain. Not only government documents and websites will be used, as it is important to look further the given narrative of each state. Therefore EU and NATO documents will also be consulted, as the goal is to find out if EU/NATO membership can impact the way states deal with cyber security. Furthermore, other documents and websites will be used that are connected to cyber security, for instance those of the ITU and the UN. By looking at both documents of states and official organisations that are not part of the state, any biased information will be filtered out when the data does not correspond. News articles can also provide a different perspective to how states deal with cyber security. These sources will be selected through being informative about cyber security, so it has to include this concept or the concept of a cyber attack. The chosen sources will be researched in what information it provides about cyber security, how it corresponds to how small states deal with cyber security, in what way an international organisation as EU and NATO provide aid in regard to cyber security and if they make a difference in how small states deal with cyber security. Furthermore, triangulation will be used in order to validate the different sources (Ammenwerth, Iller & Mansmann, 2003, p.239-241). By researching the data of different sources it will become clear what kind of cyber security policy the four cases have, and what influence the EU/ NATO has and therefore if membership can make a difference.

Data-analysis

In the following section, the four cases and how they deal with cyber security will be analysed. First the EU/NATO member states and then the non-member states will be analysed. Therefore, Estonia, Lithuania, Georgia and Moldova will be analysed is this order. According to the GCI of ITU, they rank 0.871; 0.504; 0.819 and 0.418 respectively (DigiAnalysys, 2017).

Estonia

Estonia endured a cyber attack in 2007, during the attack, fifty-eight Estonian websites were offline; these included the websites of the government, banks and newspapers in a three-week period by Russia as the result of relocating a Soviet War Bronze Soldier Statue (Davis, Bradley & Dool, 2017; p.10; E-estonia, 2017; Sterling, 2018). Before these cyber attacks, cyber security was not seen as a main security threat, as there was no policy concerning cyber security (E-estonia, 2017). After the cyber attack of 2007, Estonia managed to rank fifth in cyber security commitment in the world according to GCI (Invest in Estonia, 2018; Perez, 2017). How Estonia managed to reach this position will be explained in the following paragraphs.

Conform to the expectations, Estonia created a national cyber security strategy and other policies in order deal with cyber security. According to the Ministry of Foreign Affairs of Estonia (2018), ITU (2015b, p.188-189) and NATO (Osula, 2015, p.6) Estonia adopted a national cyber security strategy, in which goals, such as the development and establishment of domestic procedures and institutions, the creation of regulatory and legal frameworks in order to deal with cyber security and created a Cyber Security Strategy Committee were set (Ministry of Foreign Affairs of Estonia, 2018; UNIDIR, 2013, p.18). Estonia also created, Digital Agenda 2020, a policy document which goal is create an environment that facilitates the use of ICT (Osula, 2015, p.6-7). The most important institution that was established in order to deal with cyber security is the officially recognized Incident Response Department (CERT-EE) that works together with the Information System Authority for the protection of critical information infrastructures (E-estonia, 2017; ITU, 2015b, p.188-189). CERT-EE is the national variant of the EU CERT, which established after the EU recognized the importance of cyber security. The Annual Report Cyber Security Branch measures all the cyber security developments (ITU, 2015b, p.27). This shows the influence of the EU in how Estonia deals with cyber security as it has copied it.

Besides the mandatory GDPR of the EU, Estonia adopted laws. For instance, a law was approved in 2018, which transposes the EU directive on security network and information systems (ERR, 2018). Furthermore, in 2015 Estonia’s Defence League’s Cyber Defence Unit had a budget of thirty-two million euro (Sterling, 2018). This budget is only a small amount from what UK and France spend on cyber security. What is impressive though, is that despite Estonia's limited budget, it ranks higher than UK or France according to GCI as Estonia has a higher level of commitment.

As liberal theory states, Estonia cooperates and develops trainings with other states and international organisations and has signed agreements in the field of cyber security in order to deal with cyber security and cyber attacks (E-estonia, 2017; e-Governance Academy, n.d.). The reasoning for this according to Ministry of Foreign Affairs of Estonia (2018) is that cyber security is important for domestic affairs and forms an integral aspect of broader security because of its transnational nature. According to ITU (2015c) and the Ministry of Foreign Affairs of Estonia (2018) this is achieved through information exchange and strengthening alliances and partnerships, examples are Luxemburg, NATO, UN and Organisation for Security and Co-operation in Europe (OSCE) (E-estonia, 2017; ITU, 2015b, p.188-189).

According to Invest in Estonia (2018), Estonia is a global leader in cyber security as it has a proactive role. This is supported by Estonia's GCI ranking, the housing of joint trainings and headquarters. As a member of EU and NATO, Estonia works closely together with these international organisations. Examples are NATO's Cyber Coalition in 2016 in Estonia and Locked Shields, which is organised with the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) among others (E-estonia, 2017; CCD COE, 2018; Mshvidobadze, 2015, p.32). Locked Shields trains security experts and is the world's largest international cyber defence exercise (E-estonia, 2017). Estonia also houses the headquarters of the CCD COE and of the EU Agency for the operational management of large-scale IT systems (EU-LISA) (Perez, 2017; Ministry of Foreign Affairs of Estonia, 2018). This shows Estonia's willingness to further encourage cyber defence and work together with NATO and EU to put cyber security on the agenda of other states.

To see if these measures work, the number of cyber attacks Estonia has managed to block is important. Up to three hundred cyber incidents are reported to have occurred, a small number in comparison of how many cyber attacks that were stopped by the mechanisms Estonia has created to deal with cyber security (E-estonia 2017). Also the WannaCry cyber attack did not affect Estonia, because of the cyber awareness for ransonware that was already established (Perez, 2017). This shows that Estonia's cyber defence capabilities are capable of defending its critical information infrastructures.

Estonia created national cyber security strategy, policies, institutions, budgets and the training of IT specialists to deal with cyber security. It also works closely with other states, like the EU and NATO. This falls in line with both liberal theory and the first and second expectation. Estonia's involvement with EU/NATO regarding to create more awareness for cyber security shows that Estonia might use these international organisations not specifically for their benefit. Therefore, it seems that although

Estonia is a small state, it uses EU/NATO membership to raise more awareness about cyber security. Furthermore, Estonia works more closely with NATO then with the EU. This could stem from the fact that the EU mostly leaves cyber security to the responsibility of its member states.

Lithuania

With a GCI of 0.504, Lithuania ranks 63 globally, despite Lithuania’s low score, the Military Strategy of the Republic of Lithuania sees cyber attacks as a main risk for its e-government dependency on critical information structures and communication technologies and therefore want to protect them (Global Cyber Security Capacity Centre, 2017, p.6). Although Lithuania does not have a national cyber security strategy, which does not fall in line with the expectations, is has created other policies and strategies. Like the EU, it has an incident response team; the National Lithuanian Computer Emergency Response Team (CERT-LT), which tasks include coordination and cooperation on national and international level with incident response organisations. Another institution that Lithuania created is the National Cybersecurity Centre, which deals with cyber incident management (Global Cyber Security Capacity Centre, 2017, p.4-7; ITU, 2015b, p.291-293).

Besides adopting law in order to deal with cyber security, Lithuania also ratified the GDRP and the Law on Cyber Security, which lays the foundation of the organisational structure of cyber security (ENISA, 2016; Global Cyber Security Capacity Centre, 2017, p.7-8). This shows that Lithuania makes utilises EU legislation in order to deal with cyber security. Furthermore, Lithuania has a budget for cyber defence, according to the National Audit Office (2015, p.6) over 20.9 million euro was spent on cyber security between 2011 and 2014 and that 15,6 million euro from the national budget and EU funds are allocated for 2015-2020 for dealing with cyber security. This shows a high level of commitment of cyber security, but also that it is less money than larger states spend and that Lithuania also relies on the EU for money in order to deal with cyber security.

Another expectation that Lithuania fulfil is that of the importance of trainings for public and private sectors and IT specialists. Other ways that Lithuania improves is cyber security is though exercises, seminars, courses but these rarely done by a certified teacher (Global Cyber Security Capacity Centre, 2017, p.37-37). Awareness is also of importance for Lithuania as it has incorporated it in government agencies and is discussed in the media by journalists (Global Cyber Security Capacity Centre, 2017, p.7).

Like liberal theory states, Lithuania relies on cooperation and alliances with other states and international organisations. Therefore it is not surprising that Lithuania has agreements with Europol, Interpol and non- EU neighbour states on exchanging information and is a member of EU, NATO among others (Global Cyber Security Capacity Centre, 2017, p.17; ITU, 2015b. p.298-293). Because Lithuania is a member of the EU, they work closely together, for instance the European Commission sponsors a programme for raising awareness amongst schools. Furthermore, another program that is supported by the EU (European Cybercrime Training and Education Group) is the Centres of Excellence for Cybercrime and Cybersecurity, which brings the national Cybercrime Centres of Excellence in EU states together and provides access to network resources (Global Cyber Security Capacity Centre, 2017, p.46-47). Lithuania also leads the project for the creation of rapid cyber respond teams and mutual assistance in case of a cyber attacks which falls under the Permanent Structures Cooperation of the EU framework (defense-aerospace, 2018). Lithuania also works closely with NATO, for instance its participation at NATO multi-national cyber security exercise Cyber Coalition 2013 and participation in the European Cyber Security Month (Global Cyber Security Capacity Centre, 2017, p.32-33).

Another way to observe how Lithuania deals with cyber attacks are the number of attacks that Lithuania deals with. In 2017, there were more than fifty thousand cyber attacks, which was more than the year before, from which around five-hundred were seen as a medium-and high incidents, all of them handled by the NSCS and was able to block a global attack like NotPetya (Schultz, 2018; Xuenguan, 2018). These incidents go from small hooliganism to criminal offenses. Furthermore, according to the Defence Minister, the state's cyber security defences were better, which led to being better in discovering and handling the incidents (Xuenguan, 2018).

Lithuania created different institutions and organisational structures in order to combat cyber security, such as CERT-LT. Lithuania does not have a national cyber security strategy, which does not fall in line with the formulated expectation. What does conform to liberal theory and the first expectation is that Lithuania relies on international cooperation. The second expectation also corresponds with Lithuania actions; it has a budget to deal with cyber security, focuses on the training of IT specialists and the creation of policies to deal with cyber security. Furthermore, it becomes clear that Lithuania relies on the EU, not only for money but also benefits from different projects in order to deal with cyber security.

Both Estonia and Lithuania are members of the EU and NATO, and have created different policies and instructions that deal with cyber security, such as CERTs, and work with international organisations and have international alliances. But there is one significant difference; Estonia and Lithuania both rank completely different from another on the GCI. This shows, that although a small state has a membership, this does not necessary imply that small states can deal with cyber security better. It shows that how much a state invests in cyber security defines how to deal with it.

Georgia

During the cyber attack in 2008 by Russia, both the websites of the Georgian president and of the Ministry of Foreign Affairs of Georgia were unavailable for the public for consultation and instead pictures were shown (Gamreklidze, 2014, p.201-203). Unable to deal with the cyber attack independently due to the lack of knowledge, policies and institutions, Georgia reached out to the international community for aid (Gamreklidze, 2014, p.202). After the cyber attack, Georgia has enhanced and improved its cyber security, as Georgia ranked number 8 globally with a GCI of 0.819 (DigiAnalysys, 2017; Perez, 2017). Which steps Georgia undertook to deal with cyber security will be discussed in the following paragraphs.

After the cyber attack in 2008, Georgia created a national cyber security strategy as theory predicted, namely the Cyber Security Strategy of Georgia, which included the creation of a system that could anticipate, avoid and terminate and deal with cyber attacks and included cyber security in its National Security Concept of Georgia (Ministry of Foreign Affairs of Georgia, 2014; National Security Concept of Georgia, 2012, p.2-3; Tielidze, 2016, p.1-2). This makes it clear that before the attack cyber security was not seen as a security issue, as it was not included in any policies. Since Georgia's creation of institutions that deal with cyber security, cyber attacks have been mitigated, for instance the attack on the Georgian Ministry and attacks on government computers regarding military data (Lomidze, 2011).

According to ITU (2014, p.1) and Cyber Security Strategy of Georgia, Georgia created a Computer Agency Response Team, the CERT-GOV-GE to deal with cyber security. These and the creation for instance of the Data Exchange Agency, which is responsible for the implementation of cyber security polies, the training of IT specialists and Cyber Lab shows how Georgia deals with cyber security and makes up for its lack of having a national cyber security strategy (Data Exchange Agency, 2012, p.6-7; Tielidze, 2016, p.7-9; ITU, 2014; Mshvidobadze; 2015, p.35-37). Furthermore, the training of IT specialists falls in line with the expectation as it enables Georgia to deal with cyber security. Georgia also adopted different laws, these included the creation of a legal basis for operations and agencies, defining its functions and implementation internationally recognized cyber security standards (Data Exchange Agency, 2012, p.5-6; ITU, 2014, p.1). Additionally, Georgia had a total defence budget of 310 million dollar in 2017, from which a section was allotted for cyber defence (Lorenz, 2018; Interfax-Ukraine, 2017).

According to three different sources (Data Exchange Agency, 2012, p.5-8; Ministry of Foreign Affairs of Georgia, 2014; Tielidze, 2016, p.5) Georgia relies on international alliances and cooperation for sharing knowledge and experiences and therefore wants to strengthen its relations with international organisations (EU, OSCE, NATO, UN and ITU) although there were no official partnerships with states in 2014. Georgia's reliance on international alliances does not come as a surprise after the cyber attack of 2008, in which international aid was needed and came from the US in the from of one million dollar in aid to strengthen Georgia's defence capabilities (National Security Concept of Georgia, 2012, p.19; Gamreklidze, 2014, p.202). This shows that without a EU/NATO membership Georgia was not capable to deal with a cyber attack, as EU and NATO's cyber security policies were unavailable. Therefore, it does not come as a surprise that CERT-GOV-GE wants to join ENISA, as Georgia pursues EU and NATO membership in order to improve its security environment (Mshvidobadze, 2015, p.40; National Security Concept of Georgia. 2012, p.15-16; Lorenz, 2018). This falls in line with liberalism and the expectation that small states seek security in a membership of an international organisation. Adding to the importance of alliances, Georgia pursues an active participation in international cyber security activities, supporting regional cyber security initiatives and initiating bilateral and multilateral cooperation with national CERTs, an example is their membership of the ITU-IMPACT initiative (Data Exchange Agency, 2012, p.5-8; Tielidze, 2016, p.5; ITU, 2014, p.1-2).

Georgia has created a national cyber security strategy and other supportive mechanisms, such as CERT-GOV-GE and policies like the Cyber Security Concept. This shows that Georgia does create policies and institutions in order to deal with cyber security. Furthermore, Georgia invests in the training of IT specialists, which also falls in line with the second expectation. Additionally Georgia follows liberalism, as it seeks membership of an international organisation and emphasizes on working with other states and organisations. Georgia's vulnerability for a cyber attack could stem from lacking cyber security measures, but also because of the possibility that it was not a member of EU or NATO.

Moldova

Moldova has a GCI score (0.418), ranking them 79th globally, the lowest of all the four states. Despite its low ranking, Moldova has invested in dealing with cyber security. For instance, the creation of policies like the National Strategy for Information Society Development –Digital Moldova 2020, which goal is to create conditions for the public and private use of IT and to develop Cybersecurity Strategy, in which training; risk awareness and international cooperation are focal points (Ministry of Information Technology and Communications, 2016; European Commission, 2018, p.8). This shows that although Moldova does not have a national cyber security strategy, which does not fall in line with the expectation, it did create other policies, which also fall in line with the expectation.

Furthermore, Moldova created departments, like the Division for Cybercrime Investigation and Research and the Intelligence and Security Service. These departments implement the laws on preventing cybercrime through the creation of a 24/7 national contact point (Spinu, 2015, p.9).

According to ITU (2015a, p.1) and has a national governmental CERT of Moldova (CERT-GOV-MD), which is an internationally officially recognized institution that implements the cyber security strategy policies. These different institutions show that Moldova puts the necessary time and energy in cyber security in order to deal with, as Moldova sees it as a security issue. And in line with the European Cyber Security Strategy, the project Enhancing Cybersecurity: Protecting Information and Communication Networks was started, with as goal to create local capacities that can prevent and respond to cyber attacks (Spinu, 2015, p.9). Moldova also adopted laws in regard to cyber security, these laws defined the notions and types of cyber crimes, the definition of competent bodies in combating cyber crime among others; one of these laws is the Law on Preventing and Combating cybercrime (Sibiu, 2015; ITU, 2015a, p.1; Spinu, 2015, p.6). Also Moldova had an estimates defence budget of 24.5 million dollar in 2017, in which a part was allotted for cyber security (Lins de Albuquerque & Hedenskog, 2016, p.26).

Following liberal theory and expectations, Moldova relies on international cooperation and treaties for dealing with cyber security (Sibiu, 2015). Therefore Moldova has partnerships and alliances with many organisations and states, these include the OSCE, Interpol, Europol, with different departments of other states such as Ukraine and Romania regarding cyber security, with CERTs of nations like Israel, the International Policy Cooperation Centre of the GIP, EU and NATO (Sibiu, 2015; ITU, 2015a, p.2-3; NATO, 2018). An example of its alliance with a state is the joint cyber security project by the e-Governance Academy of Estonia and the e-Governance Centre of the Republic of Moldova (ITU, 2015a, p.2-3; ITU, 2015b, p.322-324; Sibiu, 2015). Another example is Moldova’s partnership with NATO; it has a multi-year cyber defence project, with as goal such as establishing a Moldovan Armed Forces Cyber Incident Response Capability (NATO, 2018). This shows that although Moldova is not a NATO member state, it does have a partnership. Other examples are the different projects Moldova participates in, one of these international projects is the Cyber-Crime@EAP of 2011, a Council of Europe initiative, with as goal to strengthen the capacities of states to cooperate effectively against cyber crime, which included workshops and trainings (Spinu, 2015, p.7). Furthermore, the e-Governance Academy (n.d.) supports the development of cyber security through for instance the sharing knowledge, seminars. Moldova also organizes an awareness event, the European Cyber Security Month, which provides educational and professional training programs for the general public and promotes cyber security in higher education and certification of professionals (ITU, 2015a, p.2-3; Spinu, 2015, 9).

An approach to see how the Moldovan cyber security defence systems works is to look at the number of cyber attacks. In 2016 there were more then six million cyber attack attempts, this shows the importance of a national centre for cyber security (Media AZI, 2017). Furthermore, Moldova’s cyber security defence systems have successfully identified and blocked a computer virus in 2015 that targeted information systems of public institutions at an early stage (Security and Intelligence Service of the Republic of Moldova, 2016; TRM, 2015). This shows that Moldova's cyber security defence is able to block attacks.

Moldova follows liberal theory and the expectation that is seeks alliances with international organisations and states in order to deal with cyber security, it benefits from their alliances, through sharing knowledge and experience. Although Moldova does not have a national cyber security, it has created other policies to deal with cyber security, in which the CERT-GOV-MD is most important as it follows international guidelines. Furthermore, Moldova adopted different laws and trains IT specialists. This falls partly in line with the second expectation, but not fully because of the missing national cyber security strategy. Interesting though is that although Moldova created different policies and institutions, such as a CERT, and has international allies, it does not rank high on the GCI. This could be partly because of their lack of a national cyber security strategy, the implementation of their policies or even because they are not a member of EU/NATO.

Both Georgia and Moldova have created policies and institutions, like CERT and have alliances with EU and NATO in order to deal with, although not being a member of them. However there are differences between the states, the GCI ranking and the national cyber security strategy. Georgia has a national cyber security strategy and ranks high, whilst Moldova has the lowest score of the group and does not have a national cyber security strategy. This shows that not having a EU/NATO membership does not immediately mean that small states are less capable to deal with cyber security, although, is seems that Georgia was vulnerable for the cyber attack without any membership. But is also makes clear that Georgia's commitment in dealing with cyber security is higher than that of Moldova.

Conclusion

In the beginning of this thesis the goal was formulated to find out how small states deal with cyber security issues and if EU/NATO membership influences this. Before the research was conducted, three expectations were formulated. In the following paragraphs, every expectation will be discussed in order to see if they were met or if they are false.

The first expectation was that small states would follow liberal theory, meaning that they would seek security in the form of an international organisation. In all the four cases, this is accurate. Both Estonia and Lithuania are not only members of EU and NATO, but also work together with other organisations regarding cyber security. Furthermore, through being a member of these organisations or through alliances there is a sharing of knowledge, laws and regulations relating to cyber security. Although Georgia and Moldova are not members of EU/NATO, they do have partnerships with them. For all the four small states, this means that they rely on international alliances for their safety, and therefore helps them deal with cyber security, instead of dealing with cyber security as neorealism describes it. The small states did not became self-reliant and tried to deal with cyber security independently, despite cyber security being a national security issue. Furthermore, it can be said that Estonia follows the glue strategy as it uses international organisation in order to promote its security issues, for them and other states.

The second expectation is that small states will create national cyber security strategies and other policies that enhance this, including the training of IT specialists and having a cyber budget. Estonia and Georgia are only states that have a national cyber security strategy. Although Lithuania and Moldova do not have a national cyber security strategy, they have created other policies like Estonia that deal with cyber security; these policies include the creation of institutions like CERTs. All the four states also focus on the training of IT specialists. As the literature states, these are all important factors to deal with cyber security, as all states are dependent on critical information structures and try to decrease their vulnerability for cyber attacks. In the case of Estonia and Georgia, is became clear that they created the policies and institutions after the attacks to create cyber defences in order to prevent damaging cyber attacks. Furthermore, both Estonia and Lithuania have a cyber budget, although less then larger states like France.

The third expectation was that small states with EU/NATO membership are more capable to deal with cyber security. In the case of Estonia, this is true. After the cyber attack it did not need international aid, unlike Georgia. In the case of Lithuania, this is less true. Although it is capable of dealing with cyber security through EU regulation and other institutions provided, it ranks only 63 globally. This could be because the EU mostly leaves cyber security to the responsibility of the states themselves, but this also means that Estonia, with its fifth place globally, did it mostly independently aside from the international alliances, which Lithuania also has. More interesting, it seems like Estonia uses its membership to create more cyber security awareness for other states, than only using the providing help the EU provides. It is also interesting, that Georgia, which is not a member of the EU/ NATO scores high on the GCI, this means that although is does not have any membership, it is investing in cyber security defences by creating its own policies and institutions to deal with cyber security. Furthermore Lithuania, which is a member of EU and NATO scores low despite having EU and NATO regulations and laws.

Therefore, national cyber security policies are important for small states, but also other supportive policies and institutions, such as CERTs and training of IT specialists. International alliances are important to deal with cyber security, but it does not seem that having an EU/NATO membership influences how small states deal with cyber security, as both Estonia and Georgia rank high, despite Georgia not having EU/NATO membership. Furthermore, Estonia does not use the EU/NATO in order to increase their cyber security, but uses it a platform to advocate their interest to other states. This shows that how small states deal with cyber security depends what they do and their alliances, but not necessary that a membership of EU/NATO guarantees being better equipped to deal with cyber security, as also without EU/NATO membership there are alliances with them. Furthermore, it is on the small state itself to decide what to do about cyber security.

Appendix

CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Teams
CERT-EE	Incident Response Department of Estonia
CERT-GOV-GE	Computer Emergency Response Team of Georgia
CERT-GOV-MD	Computer Emergency Response Teams of Moldova
CERT-LT	National Lithuanian Computer Emergency Response Team
CSIRT	Computer Security Incident Response Teams
ENISA	European Union Agency for Network and Information Security
EU	European Union
EU-CSS	EU Cyber Security Strategy
EU-LISA	European Agency for the operational management of large scale IT systems in the area of freedom, security and justice
GDPR	General Data Protection Regulation
GCI	Global Cyber Security Index
IDS	Intrusion Detection System
IT	Information Technology
ITU	International Telecommunication Union
MSSD	Most similar system design
NATO	North Atlantic Treaty Organisation
OSCE	Organisation for Security and Co-operation in Europe
UN	United Nations

References

Acayo, A. (2017). Global Cybersecurity Index Overview: 2nd Annual Meeting of Community of Practice on Composite Indicators and Scoreboards. International Telecommunication Union. Retrieved from: https://composite-indicators.jrc.ec.europa.eu/sites/default/files/02%20-%20Global%20Cybersecurity%20Index%20-%20Grace%20Acayo.pdf

Ammenwerth, E., Iller, C., & Mansmann, U. (2003). Can evaluation studies benefit from triangulation? A case study. *International Journal of Medical Informatics, 2-3*(70), 237-248. doi: 10.1016/S1386-5056(03)00059-5

A National Structure Will Be Created in Moldova to Combat Cyber Security Incidents. (2017, November 22). *Media Azi.* Retrieved from: http://media-azi.md/en/stiri/national-structure-will-be-created-moldova-combat-cyber-security-incidents

Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology, 11*(5), 389-401. doi: 10.1080/13645570701401552

Barrinha, A., & Farrand-Carrapico, H. (2018, January 16). How coherent is EU cybersecurity policy?. Retrieved from: http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/

Bartmann, B. (2002). Meeting the Needs of Microstate Security. *The Round Table, 265*(91), 361-374. doi: 10.1080/0035853022000010335

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior,* (48), 51-61. doi: 10.1016/j.chb.2015.01.039

Bryman, A. (2012). Research designs. In A. Bryman (eds.), *Social Research Methods* (p. 44-78). Oxford: Oxford University Press.

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science, 2*(65), 216-238. doi: 10.1177/0032318713508491

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor?. *JCMS: Journal of Common Market Studies, 55*(6), 1254-1272. doi: 10.1111/jcms.12575

CCD COE. (2018). *NATO Won Cyber Defence Exercise Locked Shields 2018*. Retrieved from: https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html

Commonwealth Secretariat. (2011). Social and Economic Data on Small States. *Small States: Economic Review and Basic Statistics,* (15), Commonwealth Secretariat: London. Retrieved from: http://dx.doi.org/10.14217/smalst-2011-7-en.

Commonwealth Secretariat. (2015). What Are Small States?. *Small States: Economic Review and Basic Statistics,* (18), Commonwealth Secretariat: London. Retrieved from: http://dx.doi.org/10.14217/smalst-2015-2-en.

Crossley, M., & Sprague, T. (2012). Learning from Small States for Post-2015 Educational and International Development. *Current Issues in Comparative Education, 15*(1), 26-40. Retrieved from: https://files.eric.ed.gov/fulltext/EJ1000213.pdf

Cyber attack on five public institutions. (2015, February 4). *TRM.* Retrieved from: http://trm.md/en/social/atac-cibernetic-la-cinci-institutii-publice/

Data Exchange Agency. (2012.). Cyber Security Strategy of Georgia: 2012 - 2015. Retrieved from: https://www.unodc.org/cld/lessons-learned/geo/cyber_security_strategy_of_georgia_2012-2015.html?&tmpl=cyb

Davis, G., Bradley, J., & Dool, R. (2017). *The Digital Fog of Cyber: Case Study of the 2007 Cyber Attack on Estonia* (ProQuest Dissertations and Theses). Retrieved from https://search-proquest-com.ezproxy.leidenuniv.nl:2443/docview/1960840146/?pq-origsite=primo

Denning, D.E. (2013). Framework and principles for active cyber defense. *Computeres & Security,* (40), 108-113. doi: 10.1016/j.cose.2013.11.004

DigiAnalysys. (2017). *ITU Global Cyber Security Index*. Retrieved from: http://www.digianalysys.com/itu-global-cyber-security-index-2017/

Do, C., Tran, N., Hong, C., Kamhoua, C., Kwiat, K., Blasch, E., et al. (2017). Game Theory for Cyber Security and Privacy. *ACM Computing Surveys (CSUR), 50*(2), 1-37. doi: 10.1145/3057268

E-estonia. (2017). How Estonia became a global heavyweight in cyber security. Retrieved from: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

e-Governance Academy. (n.d.). *Cyber Security Capacity in Moldova*. e-Governance Academy. Retrieved from: http://www.ega.ee/project/cyber-security-capacity-in-moldova/

European Commission. (2018). *Joint Staff Working Document: Association Implementation Report on Moldova.* Retrieved from: https://eeas.europa.eu/sites/eeas/files/association_implementation_report_on_moldova.pdf

European Union. (2018). *About the EU: The 28 member countries of the EU*. Retrieved from: https://europa.eu/european-union/about-eu/countries_en

EU2017. (2017). *Cybersecurity and the Estonian Presidency.* Retrieved from: https://www.eu2017.ee/news/insights/cybersecurity-and-estonian-presidency

ENISA. (2015). *Lithuania –New Law on Cyber Security.* Retrieved from: https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/lithuania-2013-new-law-on-cyber-security

EPSC Strategic Notes. (2017). *Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level.* European Political Strategy Centre. Retrieved from: https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness: A systematic review of the literature. *Computers & Security,* (46), 18-31. doi: 10.1016/j.cose.2014.06.008

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue. *Journal of International Communication, 2*(20), 21-20. doi: 10.1080/13216597.2014.954593

Georgia's military budget should be over 2% of GDP, it will bring republic closer to NATO standards. (2017, May 27). *Interfax-Ukraine.* Retrieved from: https://en.interfax.com.ua/news/general/424500.html

Global Cyber Security Capacity Centre. (2017). *Cybersecurity Capacity Review: republic of Lithuania.* Retrieved from: https://www.nrdcs.lt/en/press-releases/lithuania-s-cyber-security-capacity-are-we-cyber-ready-to-embrace-digital-era-/80

Hankewitz, S. (2017, August 23). Estonia ranks highest in Europe in cyber security. *Estonian world.* Retrieved from: http://estonianworld.com/security/estonia-ranks-highest-in-europe-in-cyber-security/

Hey, J.A.K. (2003). Introducing Small State Foreign Policy. In J.A.K. Hey (eds.), *Small States in World Politics* (p. 1-12). Boulder: Lynne Rienner Publishers.

Hughes, D. & Colarik, A.M. (2016). Predicting the Proliferation of Cyber Weapons into Small States. *Joint Force Quarterly,* (80), 19-26. Retrieved from http://ndupress.ndu.edu/Media/News/Article/969646/predicting-the-proliferation-of-cyber-weapons-into-small-states/

Invest in Estonia. (2018). *Cyber security*. Retrieved from: https://investinestonia.com/business-opportunities/cyber-security/

ITU. (2014). *Cyberwellness Profile of Georgia*. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Georgia.pdf

ITU. (2017). *Global Cybersecurity Index.* Retrieved from: https://www.itu.int/pub/D-STR-GCI.01-2017

ITU. (2015a). *Cyberwellness Profile, Moldova*. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Moldova.pdf

ITU. (2015b). *Global Sybersecurity Index & Cyberwellness Profiles*. Retrieved from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ITU. (2015c). *Cyberwellness Profile of Estonia*. Retrieved from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Estonia.pdf

ITU. (2018a). *Definition of cybersecurity*. Retrieved from: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

ITU. (2018b). *About International Telecommunication Union (ITU).* Retrieved from: https://www.itu.int/en/about/Pages/default.aspx

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 5*(80), 973-993. doi: 10.1016/j.jcss.2014.02.005

Lins de Albuquerque, A., & Hedenskog, J. (2016). *Moldova: A defence sector reform report.* Retrieved from:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjWlMfnstXbAhXKZFAKHdeJD4gQFgg9MAM&url=https%3A%2F%2Ffoi.se%2Freport-search%2Fpdf%3FfileName%3DD%253A%255CReportSearch%255CFiles%255C0f389bc6-56ac-483d-baf6-44a1dbd0983e.pdf&usg=AOvVaw3VkW0tMXyH20gSfFtQz3L4

Lithuania's Initiative of Cyber Rapid Response Force Formation Greenlighted in Brussels. (2018, March 6). *defense-aerospace*. Retrieved from: http://www.defense-aerospace.com/articles-view/release/3/191324/eu-approves-lithuania's-cyber-rapid-response-force-initiative.html

Lomidze, I. (2011). *Cyber Attacks Against Georgia.* Data Exchange Agency. Retrieved from: http://dea.gov.ge/uploads/GITI%202011/GITI2011_3.pdf

Lorenz, W. (2018). Putting Georgia on the 2018 Summit Agenda. *PISM, 3*(163). Retrieved from: http://www.pism.pl/Publications/PISM-Policy-Paper-no-163

Luša, D. (2016). *Small States Influence in NATO: exercising an Active Foreign Policy*. Retrieved from: http://paperroom.ipsa.org/papers/paper_57110.pdf

Ministry of Foreign Affairs of Estonia. (2018). *Cyber Security.* Retrieved from: http://vm.ee/en/cyber-security

Ministry of Foreign Affairs of Georgia (2014.) *National Security Concept of Georgia.* Retrieved from: http://www.mfa.gov.ge/MainNav/ForeignPolicy/NationalSecurityConcept.aspx?lang=en-US

Ministry of Information Technology and Communications. (2016). *Cyber Security Programme.* Government of Moldova. Retrieved from: http://old.mtic.gov.md/en/projects/cyber-security-programme

Mshvidobadze, K. (2015). *Georgia Cyber Barometer Report*. Georgian Foundation for Strategic and International Studies. Retrieved from: https://gfsis.org/files/library/pdf/2423.pdf

National Audit Office. (2015). *Executive summary of the public audit report: The cyber security environment in Lithuania.* Retrieved from: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwibhaqsm5TbAhUOiKYKHcRZAWEQFggrMAA&url=http%3A%2F%2Fwww.vkontrole.lt%2Ffailas.aspx%3Fid%3D3504&usg=AOvVaw3gdLk7idTc2YHKfI2MoJr3

National Security Concept of Georgia. (2012.). *Cyber Security Strategy of Georgia*. Retrieved from: https://mod.gov.ge/uploads/2018/pdf/NSC-ENG.pdf

NATO. (2016). *NATO Cyber Defence.* Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

NATO. (2017). *Science for Peace and Security Programme*. Retrieved from: https://www.nato.int/cps/en/natohq/topics_85373.htm

NATO. (2018). *NATO launches second cyber defence project with Moldova*. Retrieved from: https://www.nato.int/cps/en/natohq/news_152364.htm

Osula, A. (2015). *National Cyber Security System: Estonia*. Talinn: NATO Cooperative Cyber Defense Centre of Excellence. Retrieved from: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ESTONIA_032015_1.pdf

Panke, D. (2010). Small states in the European Union: Structural disadvantages in EU policy-making and counter-strategies. *Journal of European Public Policy, 17*(6), 799-817. doi: 10.1080/13501763.2010.486980

Pearson, I. (2011). Smart grid cyber security for Europe. *Energy Policy, 39*(9), 5211-5218. doi: 10.1016/j.enpol.2011.05.043

Peoples, C. & Vaughan-Williams, N. (2015). *Critical Security Studies: An Introduction*. New York: Routlegde

Perez, R. (2017, June 20). Estonian cyber-security ranks best in Europe, fifth in the world. *SC Media.* Retrieved from: https://www.scmagazineuk.com/estonian-cyber-security-ranks-best-in-europe-fifth-in-the-world/article/669379/

Pernik, P. (2014). *Improving Cyber Security: NATO and the EU.* International Centre of Defence Studies. Retrieved from: https://www.icds.ee/fileadmin/media/icds.ee/reports__hidden_/Piret_Pernik__Improving_Cyber_Security.pdf

Robinson, N. (2017, April 6). Spending for success on cyber defence. *NATO review magazine.* Retrieved from: https://www.nato.int/docu/review/2017/also-in-2017/nato-priority-spending-success-cyber-defence/en/index.htm

Schultz, T. (2018, February 28). Stealthy sleuths: Lithuania calls for 'cyber Schengen' zone. *DW.* Retrieved from: http://www.dw.com/en/stealthy-sleuths-lithuania-calls-for-cyber-schengen-zone/a-42769925

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research. *Political Research Quarterly, 61*(2), 294-308. doi: 10.1177/1065912907313077

Security and Intelligence Service of the Republic of Moldova (2016). *12 state institutions – target of cyber attacks from abroad.* Retrieved from: http://www.sis.md/en/comunicare/noutati/12-state-institutions-target-cyber-attacks-abroad

Sterling, B. (2018, January 9). Estonian Cyber Security. *Wired.* Retrieved from: https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/

Sibiu. (2015). *Cyber-threats seen for Moldova*. Ministry of Internal Affairs of the Republic of Moldova; General Inspectorate of Police; National Inspectorate of Investigations: Centre for combating cyber crime. Retrieved from: https://www.first.org/resources/papers/istanbul2015/artur-degteariov.pdf

Spinu, N. (2015). Creating and strengthening cybersecurity in the Republic of Moldova. *Information & Security: An International Journal*, (32), 1-12. Retrieved from: http://dx.doi.org/10.11610/isij.3208

Sutton, P. & Payne, A. (1993). Lilliput under Threat: the Security Problems of Small Island and Enclave Developing States. *Political Studies*, *41*(4), 579-593. doi: 10.1111/j.1467-9248.1993.tb01657.x

Thomas, N. (2009) Cyber Security in East Asia: Governing Anarchy. *Asian Security*, *1*(5), 2-23. doi: 10.1080/14799850802611446

Tielidze, G. (2016). New Cybersecurity Strategy of Georgia: Tallin E-governance Conference. Retrieved from: http://2016.tallinnconference.ee/app/uploads/2016/06/Cyber_Georgia.pdf

Tillman, K. (2015). *Why States Seek Membership in Supranational Institutions . (*College of Saint Benedict/Saint John's University). Retrieved from: https://digitalcommons.csbsju.edu/cgi/viewcontent.cgi?referer=https://www.google.nl/&httpsredir=1&article=1075&context=honors_theses

UNIDIR. (2013). *The Cyber Index: International Security Trends and Realities*. Retrieved from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Vahtla, A. (2018, March 3). Estonian government approves new cybersecurity bill. *EER.* Retrieved from: https://news.err.ee/686763/estonian-government-approves-cybersecurity-bill

Vaicekauskaité, Z.M. (2017). Security Strategies of Small States in a Changing World. *Journal on Baltic Security, 3*(2), 1-15. doi: 10.1515/jobs-2017-0006

Van der Meer, S. (2016). *Medium-sized states in international cyber security policies.* Clingendael: Netherlands Institute of International Relations. Retrieved from: https://www.clingendael.org/sites/default/files/pdfs/PB_Medium_sized_states_international_cyber_security.pdf

WorldAtlas. (2017). *What countries made up the former Soviet Union (USSR*). Retrieved from: https://www.worldatlas.com/articles/what-countries-made-up-the-former-soviet-union-ussr.html

Xuenquan, M. (2018, March 23). Number of cyber incidents in Lithuania to grow: report. *Xinhua.* Retrieved from: http://www.xinhuanet.com/english/2018-03/23/c_137058158.htm