Interagency Cooperation on Cyber Security: The Estonian Model

Piret Pernik and Emmet Tuohy
International Centre for Defence Studies
Toom-Rüütli 12-6, Tallinn 10130,
ESTONIA

Piret.Pernik@icds.ee

ABSTRACT

As Estonia saw in 2007 cyber attacks on a nationwide scale can affect the whole of society, both public and private sectors alike. Accordingly, addressing the consequences of such attacks and to preventing future incidents- requires a comprehensive approach involving coordination both within different government institutions and among commercial organisations such as telecommunications companies, internet service providers, etc. This paper is intended to illustrate the practice of interagency cooperation in Estonia in the field of cyber security. It identifies solution approaches toward enhancing interagency cooperation, thereby demonstrating how effective collaborative arrangements can be built and maintained in a domestic setting. The main part of the paper examines how nationwide and international cyber exercises have improved interagency cooperation. Finally, the conclusion identifies lessons learned from the Estonian case and offers recommendations applicable not just to Estonia, but to a wider context as well.

1.0 INTRODUCTION

The cross-border nature of cyberspace renders cyber security a relevant issue for international and national security & defence actors. Cyber risks endanger everyone – individuals, businesses, national and international organisations, governments, and militaries. The prevention and mitigation of cyber threats requires collaboration of all actors; in other words, a truly comprehensive approach across the individual, team, organizational, national, and international levels is needed. When the integrity of networks, critical infrastructures and industrial control systems is at risk, acting alone pays no dividends (ENISA 2013: 13). That greater cooperation at all levels is needed to ensure cyber security has been acknowledged by the EU, which from 2014 has started pan-European cyber exercises that will test technical, operational, and political level cooperation procedures and responses in preventing and mitigating cyber incidences (Ibid.: 14).

Many entities (governments, militaries, and international organisations) have launched policies and strategies to prevent and to respond to cyber incidents. These call for broad engagement from the public and private sectors as well as from civil society. Cyber exercises and training constitute an essential ingredient for successful interagency cooperation in addition to planning, information sharing and personal relationships. Cyber exercises make a good test ground for the implementation of the comprehensive approach to crisis management, a concept explained in more detail below.

This paper identifies conditions for successful interactions in conducting cross-sector cyber exercises. It reviews the literature on comprehensive approach in emergency and crisis management and identifies key requirements relevant to the conduct of exercises. It then considers the experience of Estonia in coordination of national cyber security efforts and investigates lessons learned from its experience organizing and participating in national and international cyber security exercises. Finally, it concludes with recommendations to policymakers on the use of cyber exercises as a tool for strengthening the collaboration that is essential for ensuring cyber security.

This research applies qualitative methods (analysis of legal acts, institutional set-up, and after action reports; as well as semi-structured interviews with subject matter experts). While there are limitations to qualitative data, the results of this study could be validated with further research by applying methods such as observation (in roles such as Exercise Monitor or Evaluator), questionnaires, and comparisons among different countries.

1.1 CA and interagency collaboration: concept and definitions

The comprehensive approach (hereinafter CA) is rooted in the belief that most conflicts reflect a complexity that cannot be solved by military means alone. It brings together a variety of government departments, non-governmental organizations, first responders, members of the private sector, and members of local communities working together to meet an overarching mission goal (Essens et al. 2013: 1). It has been described as 'interaction between various actors and organisations with the aim of generating coherent policy and action during periods of crises or disaster or in a post-conflict environment' (Hull 2011: 5).

While NATO has not yet adopted a definition of CA[1], it understands the concept as 'an orchestration of communication of all activities in a country, coming to a well-defined and well-understood end state' (Dijk 2010). NATO circles understand the idea as 'about how to facilitate coordination with non-military actors so as to make the NATO response more effective' (Tardy 2013: 115). The implementation of CA has been the responsibility of NATO member states rather than the Alliance itself; accordingly, national conceptions have prevailed over the theoretical NATO approach. This thus makes it difficult to talk about a genuine CA approach of NATO as such (Tardy 2013: 108).

Within the European Union, CA is used interchangeably with the term 'whole-of-government' (Smith 2013). CA is regarded a common and shared responsibility of all EU actors, including member states. A Joint Communication to the European Parliament and Council titled 'The EU's comprehensive approach to external conflicts and crises' describes CA as a tool to make optimal use of all relevant policy instruments (European Commission 2013). In spite of this rhetoric, CA is still an idea under development rather than a reality in EU security affairs (Smith 2013). What is more, there is a discrepancy between rhetoric on CA and actual practice; the EU has thus far been unsuccessful in developing the concept in crisis response planning (Mattelaer 2013).

In regards to NATO member states, President Obama's administration calls the integration of tools a 'whole-of government' approach that requires 'a deliberate and inclusive interagency process, so that we achieve integration of our efforts to implement and monitor operations, policies and strategies' (White House 2010: 14).[2] Some other NATO member states (UK, Canada, Norway and Denmark) have developed CA on a national scale, while France, Germany and most Southern and Easter European members states have made little progress in implementing it (Tardy 2013: 108).

[1] 2010 NATO's Strategic Concept stresses that 'a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximise coherence and effectiveness of the overall international effort.' (NATO 2010). Chicago Summit Declaration 2012 reaffirms Lisbon Summit decisions on a comprehensive approach stating that 'our operational experiences have shown that military means, although essential, are not enough on their own to meet the many complex challenges to our security.' (NATO 2012).

[2] According to the US military's joint doctrine a whole-of-government approach 'integrates the collaborative efforts of the departments and agencies of the US Government to achieve unity of effort'. It identifies combinations of the full range of available government capabilities and resources that reinforce progress and create synergies (Armed Forces of the United States 2011).

CA has been mainly used in crisis response, stabilisation, peacebuilding, and other out-of-area-operations, while at domestic level interagency cooperation and 'total defence' have been utilized more frequently. The common denominator of out-of-area & domestic operations is that they involve multiple actors and combine many dimensions (political, military, technological, informational, human, environmental, economic, etc.) and deal with a great number of dynamic factors and uncertainties. It is therefore assumed that the conditions for interagency cooperation and collaboration are relevant in both settings (Jermalavičius 2014: 10).

In the future, highly complex, smaller-scale, and collaborative operations are likely to become an international norm; meanwhile, at the domestic level, crises and national emergencies will necessitate effective collaboration among the joint, interagency, and public spheres (Essens et al. 2013: 1). Since the nature of cyber risks requires a multilevel and multi-stakeholder structure to detect the risks and meet cyber challenges, CA is relevant in this domain as well. Cyber attacks may originate anywhere in the world, with their source often difficult or impossible to identify. Cross-border cyber risks erode or eliminate traditional distinctions between homeland security and military defence, and between public authorities and private enterprise (Bendiek and Porter 2013: 166). They transgress national legal jurisdictions and render separation between domestic and foreign policy futile. Hence a response to cyber attacks requires cross-sector and cross-border cooperation among all actors.

Cyber security that encompasses many social domains (diplomatic, political, military, economic, internal security and so on) requires a truly comprehensive approach to crisis management. In order to keep ahead of impending threats, private sector collaboration and public-private information sharing are urgent requirements (Rendon Group 2011: iii). There is a broad consensus among experts that cyber exercises help to enhance the preparedness, responsiveness and knowledge of stakeholders in responding to cyber incidents (ENISA 2012). Thus, cyber exercises work simultaneously to strengthen cyber security and enhance implementation of CA.

1.2 Key CA requirements

Pivotal factors determining the effectiveness of CA are tradition and culture. A common culture underpinning effective CA includes shared terminology and multiagency institutions. It can be generated through three elements: education and training, the secondment of personnel, and the creation of joint units and partnerships among organizations (Menhinick and Gregory 2011: 166). 'Cultural' interoperability among organisations stems from interagency understanding, trust, and confidence that require close and ongoing training, liaisons, and exchanges, which are delivered by shared learning and education (Floyd 2009: 11). Exercises and training work as bricks in building a common interoperable culture, the basic foundation of CA.

Most people agree that other fundamental conditions for successful interagency cooperation are personal relationships, information sharing, planning, and exercises. Information sharing - which can range from episodic to more structured and formalised - is essential for successful CA as well as for coordinated interagency planning (Stickler 2010: 6). While people practice cooperation when taking part in exercises, they also form and nurture relationships, share information, and (in the role of planners) engage in collective planning, all of which are elements that are rehearsed during exercises.

The major role of interagency education and training - and the resulting real-world experience with partner departments - cannot be underestimated, because immersion in interagency partner environments leads to acculturation of all partners (Doughty and Erwin 2013: 249). It has been recommended that key interagency personnel must be educated in an interagency environment so that they become acculturated to the point where they fully appreciate the culture of their partners and clearly understand how they operate and why they do things as they do. They should also have real opportunities to actually work together in exercises that are intended to immerse them in an environment similar to that which they would face together in operations' (Ibid : 260).

1.2 Solution approaches in implementing CA: training and exercises

Many challenges that hinder collaboration in comprehensive environments have been identified by previous studies. They include disparate mandates, goals, opinions, ideas, organisational cultures, operational styles, and oversight mechanisms. These differences are not only between the military and the civilian sides, but also among civilian parties. Furthermore, an effort to coordinate different actors requires financial and human resources and capacity, and these are often underestimated or overlooked (Essens et al. 2013: 2).

Training and exercises for CA operations is also a challenge. First, collective training is complex, time consuming and expensive (Essens et al. 2013: 2). Second, military training has been increasingly streamlined due to reduced defence budgets. In the civilian side, large-scale collective training is even more difficult because civil organisations have less need and fewer human and financial resources for CA-specific training. It has been assumed that CA training may be an increasingly 'hard sell' in many NATO countries (Essens et al. 2013: 2).

It is difficult to transfer the practice of large- scale military training to the CA context because civilian agencies have fewer staff (and are unable to leave their desks unattended to participate in joint exercises) and because they do not attribute the same value to large-scale standardised and repetitive exercising within their organisations (Baumann 2012: 7). Civilian agencies tend to have smaller budgets, and are not used to devoting significant financial and human resources for training and exercises on an annual basis. Thus it is logical that the extent and nature of interagency exercises to practice complex operations involving multiple agencies are often very limited (Stickler 2010: 8). Given that CA-specific exercises will be increasingly difficult to organise in the future, other types of interagency exercises will have to fulfil the role of practising CA.

Against this backdrop, cyber exercises - whether multilateral, bilateral, or domestic - provide a testing ground for practising CA because the main part of society's critical services depend on security of ICT. Since many ICT networks are interdependent - they depend on other national and international services and networks - an effective response to a cyber incident is not possible without full scale national and international cooperation.[3]

Exercises work as tools for leveraging personal relationships that will be useful for responding to a real-world crisis. When military and civilian officials are immersed in an interagency environment in which solutions are developed by teams, it results in the establishment of relationships among individuals from all partner agencies that will prove extremely beneficial in future real-word situations. By becoming educated and trained in an interagency environment , an individual organisation's cultures, policies and philosophies become integrated with the missions of partner elements (Doughty and Erwin 2013 : 257).

Thus, we conclude that practising interagency cooperation during cyber exercises helps to build CA conditions that enable and facilitate cooperation at the team, organisational, national, and international levels. For CA multi-organisational teams should have a shared understanding of the problems they are tasked to address as well as use unified terminology. Common training, shared physical space, trust-building and appropriate team leadership styles are also extremely important elements (Jermalavičius et al. 2014: 15). Cyber exercises that reinforce many of these elements will immerse individuals into a CA mindset. Participation in international exercises supports national competence and practices, reinforces the creation of

[3] In Estonia 99.6% of banking transactions are done electronically. Public and commercial e-services depend on the functioning of ICT systems and the availability of electricity, including from cross-border critical infrastructures. Pursuant to the Emergency Act there are 42 vital services in Estonia and most of them are based on the use of ICT systems. Vital service means a service that is essential for the maintenance of the society, and the health, safety, security, economic or social well-being of people.

an international network of experts, and provides a reference point to test national preparedness, strengths, and weaknesses.

2.0 INSTITUTIONAL SETUP OF CYBER SECURITY IN ESTONIA

According to the Estonian Cyber Security Strategy 2008-2013, an advisory body of the government - the Cyber Security Council of the National Security Committee of the Government, founded in 2009 - assesses progress in implementing the strategy, while the Government endorses the strategy and implementation plans. The Cyber Security Council is headed by the Permanent Secretary of the Ministry of Economic Affairs and Communications, and its members are representatives from seven ministries, government agencies within their areas of responsibility, the Government Office, and the Estonian Defence Forces.[4] Based on need, the meetings can be extended to include private sector, academic, and research institutions. The Council is served by an expert-level interagency coordination group that meets regularly.

The key government agencies responsible for implementing the national strategy are the Ministry of Economic Affairs and Communications, the Ministry of Defence, the Ministry of the Interior, the Ministry of Foreign Affairs, the Ministry of Justice, the Ministry of Finance, and the Ministry of Education and Science.

- The Ministry of Economic Affairs and Communications ensures the continuous operation of vital services, and coordinates ICT and state IT-policy actions and development plans in the field of state administrative information systems. It coordinates the implementation of the Cyber Security Strategy 2008-2013 and 2014-2017 (including the drafting of the strategy for the period 2014-2017) and the Development Plan of Information Society 2020. A subdivision of the ministry, the Estonian Information System's Authority (RIA5) coordinates the development and administration of the state's information system, organises activities related to information security, and handles security incidents that occur in national computer networks. RIA advises and monitors the providers of public services. It also organises the protection of Estonia's critical infrastructure. The Estonian Technical Surveillance Authority, operating in the administrative area of the Ministry of Economic Affairs and Communications, is responsible for monitoring electronic communication services.
- The Ministry of Defence and its subordinate entities, the Estonian Defence Forces, the Defence League, and the Information Board (external intelligence service) are responsible for military aspects of cyber defence.
- The Ministry of the Interior is responsible for crisis management and coordinates the operation of vital services. It serves the Crisis Committee of the Government. Its subordinate agencies - the Police and Border Guard Board and the Internal Security Service – handle cyber security in the fields of law enforcement (cyber crime and terrorism).
- The Ministry of Justice and its subordinate Prosecutor's Office enforce the laws concerning cyber crimes.
- The Ministry of Foreign Affairs is responsible for Estonian cyber security activities in international organisations (the United Nations, International Telecommunication Union, etc.).
- The Government Office organises the operation of the National Security Committee of the Government, advises the Prime Minister on matters relating to national defence, and coordinates the leadership of national security and national defence.

[4] The council is served by the Ministry of Economic Affairs and Communications.

[5] In Estonian 'Riigi Infosüsteemi Amet' (RIA). CERT is a subdivision of RIA.

The National Security Committee of the Government assesses national security situation and advises the government regarding the organisation of issues concerning national defence. It assesses progress in implementing the Cyber Security Strategy and implementation plans before the Government endorses them. The Committee has six members: the Prime Minister, and the Ministers of Defence, Foreign Affairs, Interior, Justice and Finance; the Minister of Economic Affairs and Communications (MEAC) will also become a member in the near future. The advisory body of the Committee, the Cyber Security Council, provides inter-agency cooperation. It is headed by the Secretary General of MEAC and its members come from seven principal ministries and government agencies within their administrative areas, from the Government Office and the Estonian Defence Forces. The extended format of the Council includes also private sector stakeholders. The Council is served by an expert-level inter-agency coordination group.

A subdivision of MEAC, the Estonian Information Systems Authority, coordinates the development and administration of the state's information system. It advises and monitors the providers of public and vital services and organises the protection of critical infrastructure. The Authority encompasses a Computer Emergency Response Team (CERT), which handles security incidents that occur in Estonian computer networks.

2.1 How cooperation is consolidated in Estonia

In Estonia cyber security is considered part of an integrated national defence that calls for a comprehensive effort involving all sectors of national society (Ministry of Defence 2010). The underlying principle of the strategy is that cyber security shall be ensured through effective co-operation between the public and private sectors and through the co-ordinated efforts of all concerned stakeholders, including civil society. In this respect, as a small country Estonia has an edge over bigger countries – the small size of its cyber security community and the limited number of state authorities responsible for ensuring cyber security produce favourable conditions for easier public-private cooperation. In smaller countries organisations tend to be less hierarchical and rigid. As people know each other personally, they tend to trust others more than in impersonal interactions, and greater flexibility enables them to share information swiftly as cyber incidents evolve very fast.

In Estonia, public-private cyber security cooperation among commercial, governmental and academic bodies is well-established, spanning over nearly two decades (Kaska, Osula, Stinissen 2013: 7; 37).[6] The response to cyber attacks against Estonia in 2007 was coordinated by CERT, a structural entity of RIA that is responsible for the management of security incidents in national computer networks, with assistance from experts from private and public sectors within and outside of the country.

A key factor to the success of responding to the attacks was effective horizontal public-private cooperation (Tikk, Kaska, Vihul 2010: 34; Kaska, Osula, Stinissen 2013: 7). A year before the attacks, a working group was formed whose aim was to prepare the establishment of NATO CCD COE (Äripäev 2007). Public and private sector members of the working group formed an informal network of the cyber security community. In the opinion of Hillar Aarelaid, then the head of CERT, Estonia's weapon to combat cyber attacks against national networks was the size of the country and the enthusiasm of Estonian IT-specialists. In a small community people from public and private sector are able to call each other instantly when something happens to ask for advice – something that is impossible in bigger countries (Ibid.).

[6] A public-private cooperation intended to enhance the security of e-services and promote public awareness about protecting information systems was established in 2006 involving the Ministry of Economic Affairs and Communications, largest telecoms, commercial banks and later joined by the largest energy supplier, largest governmental e-service providers and others (Kaska, Osula, Stinissen 2013: 7). Memorandum of Understanding for 'Computer Security 2009.'

In 2007 the Estonian cyber security community as well as the Minister of Defence welcomed a proposal to establish a Cyber Defence League along the lines of the existing Estonian Defence League, and shortly after the proposal an informal cooperation network was initiated by the Estonian Defence League. Cooperation was in the beginning based at informal cooperation network (called by one interviewed expert a ‘gentlemen’s club’). A few years later, in 2009, the first territorial units were formed and in 2011 a Cyber Defence Unit (CDU) was established by a legal act.[7] In the early years the aim of the network was to share technical competence and information, thereby increasing the knowledge and skills of its members. The network provided for its members the opportunity to consult each other. It was expected that the aggregation of expert know-how would result in ‘collective brain that works better than adversary’s’ (Padar 2014).

In addition to the CDU’s unique cooperation model that brings together public and private sectors as well as the civilian and military spheres, RIA has played a major role in maintaining close relationships with private sector, including critical infrastructure owners. Since the establishment of RIA in 2011 comprehensive approach in domestic cyber security cooperation has significantly improved. RIA has initiated a number of informal, subject-matter-specific cooperation networks to facilitate smooth cooperation between public and private actors. These partially overlapping informal networks enable actors to share information on their area of expertise. Some examples are regular meetings and e-mail list exchanges for information security chiefs from government agencies, a CERT-network with members from public and private sectors, a Committee for the Protection of Critical Information Infrastructure, and a network for ISKE[8] experts. Close public-private cooperation has contributed to raising awareness among these actors. According to one expert interviewed for the present analysis, even as late as 2010 some government agencies believed that cyber incident would not concern them, but today all actors realise that their involvement is necessary to ensure cyber security.

Close personal relationships among cyber security community enable and facilitate cooperation, and it is believed that this constitutes an advantage. One expert illustrated this: ‘if a proposal is addressed to the organisation’s general email address, expect no response; but when it is emailed to a person you know, you’ll get immediate reaction’.

Other good examples are numerous public-private cooperation projects to educate, train and raise awareness. To bring some examples: in 1996 the Tiger’s Leap Program was established with the aim of supporting ICT education and infrastructure in high schools. In 2002 a similar project, the Tiger University Program, was created for universities.[9] In 2009 a public-private awareness raising program known as Computer Security 2009 was launched, and a Memorandum of Understanding for the establishment of an IT Academy was signed in 2009; it began operation in 2012. More recent years examples include the Smart Labs in 2012 and Raising Awareness of the Safe Use of Mobile Phones in 2013 campaigns.

2.2 Cyber Defence Unit of the Estonian Defence League

The CDU has refined earlier looser consultation and cooperation models into an advanced collaboration system that could be applied in other countries to strengthen cooperation among volunteers. The model enables to create a cooperative network to combine expertise from public and private sectors to facilitate the response to a cyber crisis.

The CDU is a national collaboration model integrated into the voluntary paramilitary national defence organisation, the Estonian Defence League. The unit seeks ‘to protect Estonia’s high-tech way of life by

[7] For overview see Kaska, Osula, Stinissen 2013: 7-8.

[8] State agencies ensure information security through the three-level baseline security system, ISKE.

[9] For more information see http://www. http://www.itcollege.ee/en/it-college/foundation-management/the-tiger-university/the-tiger-university-program/.

protecting information infrastructure and supporting the broader objectives of national defence' (Defence League 2014). The objectives of the unit are to develop a cooperation network of cyber experts, strengthen the security of critical information infrastructure, and promote cyber security awareness. The CDU works to ensure the secure functioning of national information infrastructure, enhance national cyber security cooperation, and strengthen cyber defence support capabilities that can be provided in time of crisis. The unit participates in training and education with the aim of improving the knowledge and skills of its members as well as of increasing cyber awareness and cyber security among the population as a whole. Membership in the unit is strictly voluntary, as is participating in any of its activities (Kaska, Osula, Stinissen 2013: 37-38).

Today the CDU aims to work as a reserve resource pool of well-trained IT specialists who can be deployed to manage domestic crises to assist in the protection of critical infrastructure both in the public and private sectors. To enhance cooperation with critical infrastructure owners the unit plans to establish special arrangements with them (e.g. identify which skills are required and designate accordingly individuals with specific IT-profile to enterprises). While the CDU seeks to provide a training platform for its members, in promoting cyber security awareness its approach is targeted more broadly (Padar 2014). It offers regular training and exercise opportunities for its members, organises and participates in national and international exercises, and holds seminars for government institutions (Kaska, Osula, Stinissen 2013: 22). Formal cooperation agreement is place with NATO CCD COE; and a joint Protocol for Intention with RIA and other cyber security actors has been signed. At international level the unit cooperates with the US Maryland National Guard by, *inter alia,* mutual participation in cyber exercises (Estonian Defence League 2013). In the Baltic Ghost regional cooperation format, which brings together the US European Command and the voluntary national defence organisations of the Baltic states, the CDU has invited its partners to observe its exercises (Cavanaugh 2013).

It is worth noting that key public and private cyber security community actors (including the top management of enterprises and of government agencies) belong to the CDU; this overlap facilitates the swift flow of new creative ideas between the subject- matter expert and management levels of public and private sector bodies.

According to a draft legal act (Ministry of Defence 2013), the CDU can be charged by a competent agency (RIA, the Ministry of Defence and agencies under its authority) with ensuring cyber security and providing assistance to specific government institutions, critical infrastructure owners, and in some cases also to other organisations. The tasks of the unit in such cases could include penetration testing, response to cyber incidents, and monitoring & analysis of digital data, as well as analysis of malware, spyware and viruses (Ibid.). Apart from a rapid response and reserve role of the CCDU in case of cyber incidents, the unit also works closely with RIA in its everyday operation.

As discussed above, the CDU has grown out of informal coordination and cooperation network in which most members knew each other personally, thereby functioning as a building block for trust. Evidently, private sector cyber security community relies on trust mechanisms to ensure their data and ideas are guarded (Rendon Group 2011: 36). By participating in training and exercises and providing assistance to governmental bodies and critical infrastructure owners the CDU creates the informal communication channels and relationships of trust that are central to effective cooperation in the case of a major cyber incident (Kaska, Osula, Stinissen 2013: 27). Similarly, the Estonian cyber security experts interviewed for this paper believe that good cooperation is primarily based on close personal relationships, a shared feeling of community, enthusiasm, and willingness of individual members to cooperate. That being said, to maintain this momentum, the government should proactively promote voluntary contribution by various incentives that will be discussed later in this paper.

2.3 National and international exercises in 2010-2013

Since 2010 Estonia has conducted and participated in 15 national and international interagency cyber exercises. The planning of future exercises is based on the principle of integrating national and international level cyber crisis regulation exercises to use financial and human resources more efficiently. At the national level, the cyber component is integrated into existing military and civil crisis management exercises. The principal national level coordinator of cyber exercises is RIA.

Since 2010 three national exercises have been conducted with whole-of-government participation: first, the CDU organised Cyber Hedgehog to test and train for the use of the e-voting system; also in 2010, a table-top crisis management exercise for the protection of critical infrastructure called Tallinn CIIP was organised the Ministry of Economic Affairs and Communications. Third, in 2012 a table-top strategic level decision making exercise of responding to a cyber incident known as Cyber Fever, was organised by the CDU. The private sector was engaged in the planning of Cyber Fever, and participated in Tallinn CIIP. In addition, the CDU took part of the planning process of the international exercise Baltic Cyber Shield in 2010. As early as 2009 the CDU was an observer at NATO's technical level exercise, Cyber Coalition, where it has participated annually since 2010. In 2012 a cyber component organised by the CDU, was introduced to the annual military exercise of the Estonian Defence Forces, Spring Storm. This was repeated in 2013, and is planned for 2014.

At the international level, government institutions have participated at the EU/ENISA cyber exercise Cyber Europe (2010 and 2012), and in a joint EU-US exercise Cyber Atlantic (2011). In 2012 CERT participated at the EU cyber exercise Eurospe. RIA has since 2011 participated in the NATO's annual technical exercise Cyber Coalition, and starting from 2013 has also served as an Exercise Controller in the planning process.

The private sector (in this case, the largest telecommunications companies and commercial banks) has participated in international level exercises (Cyber Europe 2012), even if only in activities at the national level. The private sector was also consulted concerning the scenario development of Cyber Europe. In addition, commercial enterprises contributed to the planning process of Cyber Coalition in 2012 and in 2013. An Estonian team comprised largely of private sector representatives participated at Locked Shields 2013, a technical exercise organised by the NATO CCD COE, (commercial banks, telecoms), while the CDU and RIA were involved in the planning process (both helped to organise Locked Shields the in the previous year as well).[10]

In 2013, for the first time Estonia hosted Cyber Coalition - the largest exercise of its kind in terms of participating countries. While the private sector was not directly involved in the planning, since many members from the CDU's organising team have daily jobs in commercial enterprises, their experience thus spread to the private sector. For the first time in a NATO exercise, an Exercise Controller came from the civilian side (RIA), a fact that was regarded by experts as useful practice, as civilian involvement in the planning and execution of military exercises helps transmit knowledge to the civilian side. It was also regarded as a useful reference point, since the same official participated in the planning of EU exercises - something that allows for the comparison and evaluation of best practices of both organisations.

Government experts interviewed for this paper believed that the conduct of the exercises has matured over the past years. As one put it, he would give an assessment of 'a solid three plus on a scale of one to five' of the Estonian contribution to NATO crisis management exercises. Overall, those we consulted were satisfied with Estonian performance, stressing that considering the more limited financial and human resources relative to larger member states, Estonia has done quite well.

[10] Private sector will be engaged also in Cyber Europe 2014 exercise. Annual exercise Locked Shield will also take place in 2014 and in 2015 Estonia will participate at Cyber Coalition.

3.0 EVALUATION OF CYBER SECURITY EXERCISES[11]

3.1 Lessons identified relevant to enhancing interagency cooperation

3.1.1 Planning process

At the beginning of the planning process, it is important to establish points of contact in all national agencies responsible for the planning of an exercise. A National Exercise Controller must attain a thorough understanding of the diverse mandates, responsibilities, and internal work procedures of the participating government agencies. For example, at the beginning of planning for the EU exercise Cyber Europe 2014, the principal national coordinator RIA engaged experts from the largest national electricity network operator. The controller must make sure that - appropriate officials (from technical, operational, and strategic levels) for a given scenario will be engaged, in order to eliminate the risks that the scenario would not match local circumstances (legal framework, institutional setup, etc.). Another important issue to be considered is that national planning teams should include a range of necessary experts (e.g. public relations and legal advisers).

As Exercise Controller for international exercises, RIA shares information with other government agencies as well as private and civil sector organisations, plans national-level activities originating from EU or NATO scenarios, and coordinates the tailoring of these scenarios to local specifics. Its role is to engage and establish links with all relevant national agencies, and build up knowledge on each agency's role, responsibilities and tasks in a particular scenario in order to select the right agencies for the needs of each exercise.

3.1.1.1 Scenarios

It is critical that scenarios be realistic and adjusted to local conditions. It is difficult to attract interest from the political and strategic levels; if decision-makers are not convinced that events enacted in the scenarios can happen in the real-world, it is even more challenging. To ensure maximum realism for the scenarios, the CDU involves technical and other experts from public and private sector in the design process. These experts then assess and evaluate aspects of the scenarios (for example in case of cyber events pertaining to critical infrastructure, industrial control system experts).[12] The planning process also identifies the lessons that to be tested in the exercise.

If scenarios contain information about vulnerabilities, they should be classified. It should also be ensured that people involved in the planning process refrain from disclosing details about scenarios to their peers, as their supervisors may pressure them to reveal such information in advance in order to improve their organisation's performance during the exercise.

Involving more actors from governmental and nongovernmental organisations in the planning phase, including any test runs, allows participants to harmonise divergent expectations and create a common culture (including shared terminology). Participants will gain understanding of the objectives of the endeavour as well as the mandates, roles, and responsibilities of other actors.

[11] This part of the paper is based on after action reports and interviews with government officials from the Ministry of Defence, RIA, and the CDU.

[12] Industrial Control Systems are command and control networks and systems designed to support industrial processes in such industries as gas and electricity distribution, water treatment, oil refining and railways. Industrial control systems constitute a strategic asset, with a rising potential for catastrophic terrorist attacks affecting these critical infrastructures. These systems have often been the target of malicious actors in cyber-attacks (ENISA 2013: 17).

3.1.2 Execution

Interactions and teamwork during the exercise engender the establishment and maintenance of strong personal relationships. Face to face contacts and opportunity to discuss issues off the record was regarded by the experts to be very important for the success of the exercise. In addition to benefits for the exercise itself, such personal interaction improves inter-agency cooperation in the long run. Teamwork offers a chance to discuss issues to actors who otherwise have little daily contact with each other. For example, during the exercises IT experts from commercial banks and the central bank, Bank of Estonia can discuss also broader issues related to their cooperation. Even though the establishment and the advancement of personal relationships are fundamental for success in the planning and execution phases, they are not sufficient to maintain experiences and institutional knowledge in the longer term. Thus informal relationships should in time be solidified into formal interagency agreements (e.g. Memorandums of Understanding that describe interagency information sharing, roles, responsibilities and tasks of actors, points of contact, etc.).

3.1.3 Evaluation

After action reports are completed for all domestic and international cyber exercises. Each institution contributes to a national report that is completed by RIA. In case of domestic exercises, an after action report is normally distributed to all involved parties, while for international exercises a comprehensive national report is assembled by RIA and submitted to the EU and NATO. A final consolidated EU or NATO report that includes contributions from other member states is normally distributed only to main domestic actors. A further national distribution list will be composed according to a need-to-know basis - reports are sent to actors whose duties require their knowledge of EU and NATO.

Concerning lessons identified issues that require immediate action or urgent improvement (e.g. if the leadership or decision making structures of agencies or the government, internal working procedures or legal framework need to be altered) will normally be adopted. Some legal acts have been amended in the past years and further steps have been planned (updating a national response plan for a major cyber incident, augmenting a list of vital services). Still, some lessons have been repeatedly identified in consecutive exercises. This can happen if an issue seems to have little relevance to the real world, and thus the altering the status quo is considered not to be worth the effort. While the slogan ‘don’t fix what isn’t broken’ may in some cases be justified given limited financial and human resources to do the necessary spadework, in other cases this unwillingness to implement improvements may be problematic, especially if the changes could have prevented damage from happening.

For improved crisis preparation, it is crucial to develop feedback mechanisms to ensure that lessons will be learned and implemented (ENISA 2012). A remedy would be to design, in addition to generic after action reports, more detailed implementation plans that will identify takeaway tasks and deadlines, as well as organisations and individuals responsible for implementation in agencies. Such implementation plans should set out a monitoring process for future progress. This has been done in the CDU, which has created a standardised format for after action reports that includes distinct domains (e.g. amendments of legal acts and work procedures, in public communication scheme, etc.), different versions with appropriate levels of detail (for Exercise Controllers, domestic players, international partners, etc.), and with different security levels (for public use, classified). The format includes also a requirement to conduct a hot wash-up (discussion by participants conducted immediately after the exercise).

It is assumed that each agency will take the initiative to implement the takeaway tasks that concern them, and thus a centralised monitoring system does not exist. There is a need for greater formalisation, as the implementation of lessons identified currently depends too much on the will of an individual. Here a greater push from the senior leadership to establish clear procedures would be welcome.

A related challenge is a need to feed lessons learned into national strategy and policy making processes. It is unfortunately common that individuals who participate in cyber exercises at the national, EU, and NATO levels are often not the same officials responsible for formulating and implementing cyber security strategy, and regular information sharing between these two groups is not systematic. It is recommended that these processes be synchronised - that way, exercises and training will match the ends, means, and available financial and human resources of the strategy; and takeaways from the exercises will be taken into account in the review and implementation of the strategy.

Even though post-exercise analysis of lessons learned is customary, such analysis has not had much concrete impact. Lessons are not learned until behaviour is changed and new thinking is institutionalised. Without this, lessons will continue to be observed and re-observed (Wells II L, Pudas T. J., McNitt B 2011: 217).

Cyber exercises have prompted tests of other crisis response capabilities. In 2010 the government-level table-top exercise Cyber Fever, which tested the decision making process in response to cyber event, provided the impetus for a regional-level crisis management exercise that involved the consequences of a cyber incident.

Yet, a number of important lessons that require political or legislative action have yet to be implemented. In any case, these issues (e.g. if the present composition of the Crisis Committee is optimal for cyber crisis management; how information is shared among strategic level bodies that handle security and crisis management - the Government and its advisory bodies, the Crisis Committee and the National Security Committee) should be discussed at the strategic and political levels.[13]

While there might be well-justified reasons for this lack of progress it may also be related to inertia and desire to maintain the status quo that is intrinsic to bureaucracies in general. Additionally, senior officials or cabinet members may be reluctant to bring issues to the cabinet level out of fear that this will result in new responsibilities for them. Obstacles that prevent a leader from accepting the need for change are time, resources, skills, community values, policies, and lack of desire (Cambron-McCabe 2008).

3.2 Cross-cutting lessons learned

3.2.1 Interagency information sharing and joint crisis communication

International exercises have demonstrated that teams are willing to share information if they do not need to consider the potential negative aspects of sharing, such as legal and political implications. Collaborative initiatives during the exercises have been seen even in the absence of a specific incentive in the exercise (e.g. blacklisting services, malware analysis, and sharing of tips and tricks to protect other teams) (NATO CCD COE 2013: 122). Since people attending the exercise get to know each other and develop trust, it is expected that they will be more confident about sharing share information with their peers from the exercise teams in the real world as well.

In regards to international cooperation, civilian agencies tend to favour civilian counterparts as their first choice of partners, in the same way that militaries prefer to cooperate within military structures (i.e. NATO bodies and NATO member states' militaries). If a joint national response is required, this diverse choice of

[13] The Crisis Committee is headed by the Minister of the Interior. It was suggested by one expert that in case of a cyber event that involves the area of responsibility of other ministries, respective ministers should lead the meeting of the Committee; currently other ministers are not members. With regards to the National Security Committee, the Minister of Economic Affairs and Communication is not a member of the committee, though this is expected to change in the near future. The National Security Committee endorses the Cyber Security Strategy, while the Crisis Committee monitors and analyses the organisation of national crisis management, including the assurance of the continuous operation of vital services.

partners may cause discrepancies in a coordinated national crisis response. Therefore, Standard Operational Procedures should determine crisis regulation procedures across the civilian side and in relation to civil-military interaction at the national level, including a crisis communication plan. The plan with domestic actors and with bilateral and multilateral partners outside the country should describe information-sharing procedures to ensure that national players know and follow them.[14] Timely information flow between technical and strategic levels is a must. It is crucial for the success of the exercise that both levels have identical and timely information.

The transition from a civilian emergency to a military crisis is not clear-cut. Therefore a crisis communication plan for national cyber exercises should include the military side even if the scenario does not foresee a role for the military in response to the crisis. A public communication scheme must be drafted for each exercise, and a direct communication link between technical level and public relations officers set up to ensure coherent public messages.

Concerning international exercises, there has to be a predetermined procedure about the sharing of national information with international players, including a single national point of contact to whom all national players are obliged to submit their feedback. Conversely, this single national point of contact should distribute information from EU/NATO bodies to other domestic players.

It was noted by the Estonian experts consulted for this paper that international coordination during the exercise functions well between agencies that are used to working together daily in the real world, e.g., national CERTs. This implies that cooperation routines should remain the same during daily business, exercises and the real-world cyber incidents. The underlying principle of inter-agency cooperation (that applies also to information sharing) is that competences and working procedures should overlap as much as possible during normal conditions and emergency situations alike; in other words, authorities' *modus operandi* should be the same during emergencies as it is in normal conditions).

Another challenge in international exercises is intelligence sharing. Key national players should have lawful access to classified information during the exercise. Intelligence agencies generally resist sharing exercise-related intelligence gained from international partners with domestic players even if exercise procedures require it (in general, intelligence services tend to gather as much information as possible and share as little as possible). While there is no panacea, the situation could be improved - in addition to the efforts to create trust - the loosening of normally rigid agency protocols that require information to flow first to the senior levels of agencies from which it will then be distributed to the lower levels (Stickler 2010: 7). Coordination and information-sharing meetings may also be helpful, although during the execution of the exercise it may be difficult to organise them due to limited time and resources.

Intelligence sharing with private sector poses also a challenge. Some classified information can be redacted and made unclassified. Commercial enterprises could be motivated to obtain security clearances if they have the incentive of gaining classified government information that will help them to reduce business costs. Some NATO member states have established public-private fusion centres and platforms to facilitate greater information and intelligence sharing, and have launched incentives for industries to encourage them to join. However, business enterprises calculate their risks first and foremost from the standpoint of continuity and profit; accordingly, cyber risks that are deemed significant from governments' viewpoint tend to have much smaller value according to the risk assessment scale of commercial organisations.

[14] ENISA has developed a good practice guide to improve information sharing among CERT teams that could be used as guidance to develop national procedures for national and international levels information sharing. See more in Cybersecurity Cooperation. Defending the Digital Frontline (ENISA: 2013).

Coordination committees that enable timely information exchange should be established at all levels (technical, operational/tactical, strategic). Real-time communication at a technical level is crucial for the success of the exercise (e.g. an organized mailing list, data sharing hierarchy, real-time chat room, a wiki[15], a voice communication system), however these forums shall not be flooded with too much information.[16] It is recommended utilize an infrastructure with a central set of resources that enables clear and effective communication (Rendon Group 2011: iv).

All players should have at least an elementary knowledge about the roles and responsibilities of decision making structures at the strategic level. To be able to develop and execute realistic scenarios, planners in particular must have a clear understanding of the crisis management structures and decision- making procedures across all agencies and at all decision-making levels.

3.2.2 The engagement of participants

Public-private partnerships during cyber exercises are essential due to private-sector ownership of most critical information infrastructure. In pan-European cyber exercises public-private cooperation should be intensified (ENISA 2012). By involving diverse organisations at different levels (technical, operational/tactical, strategic) necessary cooperation models can be developed.

The interviewed Estonian experts believed that voluntary contribution to cyber security in the country is primarily based on the goodwill and enthusiasm of individuals. To maintain momentum the government should motivate and offer new incentives to the CDU volunteers. Presently, incentives offered to CDU members are attractive training opportunities, possibility to gain new information and share experiences, and being part of a ‘community feeling’.[17]

The experts stressed that voluntary participation should not be ‘over-exploited’ in government’s attempt to reduce costs by utilizing an unpaid workforce. With reference to exercises private sector should not be overloaded by various events (as one expert put it, they should not become a ‘nuisance’), but private sector representatives should only be invited to training sessions at which they can learn something new and useful. The time of players should be used effectively during the exercise.

Private enterprises can be motivated to participate in exercises by providing attendees further training opportunities. Another incentive is the possibility of testing the resilience of their critical infrastructure, funded by the EU structural funds of the government. Further incentives include various informal social networking events, support to families of the volunteers, access to classified information, and others.

As pointed out by Stickler (2010: 8) key civilian players in exercises are frequently surrogate stand-ins for principal officials. This is understandable especially with regards to the senior level, since cabinet members, high-ranking government officials, and senior corporate officers are reluctant to spend more than a few hours

[15] A wiki is a web application that allows people to add, modify, or delete content in collaboration with others, e.g. Wikipedia.

[16] In the context of collaborative defence, high-volume detailed information is harder to share and utilize. It would be better to aggregate observations to fewer separate incidents, in order to build-up an incident history and share clever tips and tricks (NATO CCD COE 2013: 121).

[17] However, the use of CDU members in the exercises and crisis response may be inhibited due to their day-to-day professional jobs in other organisations; it is thus important that their employers support their work.

at exercise, especially if the real-world relevance of the scenario is not clearly apparent. [18] When cabinet members or senior officials are replaced by junior officials or technical level experts, there is a risk that the exercise will not accurately practice real-world procedures. It is also essential that information from technical level be 'translated' into comprehensible conceptions and terminology for political-level officials (so as not, as put by the interviewed Estonian expert, to use the 'language of butterflies'). The interviewed experts believed that in order to attract attention from political and strategic level, a long-term, high-level lobbying effort is necessary.

With regards to international exercises, senior national players should not be replaced by substitutes. This may cause misunderstandings in bilateral member state cooperation and hinder decision making during the exercise, especially in asymmetrical cases in which a key decision making role is played by a junior government official in one country, and in the other by the incumbent head of agency. Since civilian and military agencies in charge of cyber security are different in each country, some mismatch is inevitable (a four-star general may be talking to a less-senior civilian official), but the establishment of national points of contact would help to reduce surprises.

Finally, the EU and NATO should invite each other to observe cyber exercises. Cyber crisis management is likely to encompass both civilian and military aspects (partly because in some member states militaries have a greater role in cyber security than civilian agencies). As noted previously civilian crises may have military consequences as military networks depend on privately-owned critical infrastructure, and since a civilian emergency can easily escalate into a military crisis.

3.2.3 Ad-hoc operation vs formalised networks

Ad hoc and informal cooperation bestows many benefits. Informal organisations can adapt more easily as the nature of threats changes (Rendon Group 2011: 30). Informal social networks allow stakeholders to connect with each other efficiently with trust and validation, even though it may also result in the unintended omission of other potential stakeholders from which the network can benefit (Ibid.: 36).

The drawbacks of ad-hoc arrangements are the lack of transparency and accountability regarding decision-making procedures. Personal relations are prone to discontinuity resulting from the choices of individuals. In informal networks personality conflicts tend to be more pronounced, especially in an ad-hoc organization with a minimally defined leadership (Ibid.: 33). Personal relations are difficult to sustain and maintain over time, thereby undermining the creation and sustainment of trust (Stickler 2010: 7-8). Accordingly, some degree of institutionalisation and formalisation will be necessary in the longer term.

In addition to interference from individual personal inclinations (interests, priorities, sympathies and antipathies), ad-hoc cooperation formations tend to be temporary. When individuals who initiated or are responsible for coordination of meetings are seconded or leave their current positions, meetings tend to become less frequent as the group gradually fades from existence. Thus, ad hoc formations should in time be formalised into more enduring and less malleable forms.

Some Estonian experts stressed that while informal community is fundamental for cooperation (and other people allege that it is the best cooperation form for cyber space), from a national security viewpoint it should be structured into legislation and institutions so that the government has the right to require private and nonprofit entities to fulfil their duties in case of crisis. If capabilities are voluntary and cooperation formations largely informal, it is difficult to formulate a meaningful role for them in national security and defence policies and strategies.

[18] Since understanding the implications of cyber risks assumes some technical- level knowledge that is scarce at political level, they may reduce the possible consequences of a cyber incident.

3.2.4 Decision-making in response to cyber incidents

Even though internal decision making structures and processes to respond to cyber incidents are in place in many agencies, since cyber events evolve fast and decisions are required immediately, action is often taken outside of these structures. Formal procedures are still used, but primarily for the purposes of crisis communication and information sharing. Again, to ensure flexible decision making and agile responses to an incident, this practice may be better than following predetermined formal procedures.

Whether through formal or informal procedures, it is advisable that crisis decisions, be taken by those with a good understanding of the nature of an incident, including its possible technical, legal, political, and other implications. Therefore, in some cases it may be feasible to delegate interagency decision making from a top senior or management level to the next level below, while keeping the upper level well informed.

4.0 CONCLUSION AND RECOMMENDATIONS

This paper has explored the challenges of inter-agency cooperation in the field of cyber security. First, on the basis of a literature review, it has identified requirements for successful interaction relevant to cyber security communities. The empirical part of the paper investigated the practice of organising and participating in national and international cyber exercises in Estonia.

In comparison with other activity areas of integrated (previously called ‘total defence’) security and defence in Estonia, cyber security cooperation is among the most advanced fields.[19] Interactions and coordination among cyber security community have developed from cooperation on the elementary level (personal relationships, limited information access, and unstructured interagency process) to coordination at the intermediate level (organisational interagency relationships, actors willing to share information about future plans, and organised interagency process) (Stickler 2010: 7). Within the CDU, public-private and civil-military engagements have reached the most advanced cooperation form - collaboration. Personal relationships have been institutionalised in terms of membership, information access is extensive, ends and goals of the CDU reinforce objectives of national cyber security policy and of individual agencies, and interactions with other actors are systematic.

On the basis of the paper’s findings, it is recommended that interagency cooperation in cyber security be regularly practiced in national, EU, and NATO exercises. In addition, the following should be considered:

- Through educational programmes and training, continue to raise awareness among cyber security stakeholders (especially at the political and strategic levels) of the arrangements, mechanisms, and measures needed to ensure effective cyber security collaboration.
- Evaluate management structure to ensure it allows for optimal decision-making and management models during a cyber incident, while designing and reviewing agency and inter-agency contingency plans to ensure adequate response to a cyber incident.
- Clarify legal mandates, duties, responsibilities, and decision making procedures throughout the whole spectrum of cyber incidences and crisis management (from normal conditions up to a cyber attack equivalent to an armed conflict).

[19] The activity areas of integrated national defence in Estonia are: military defence, civil support to military defence, international efforts, ensuring internal security and sustainability of vital services and psychological defence (National Defence Strategy 2010: 4). Other areas where inter-agency cooperation is more advanced are the process of the risk analysis of emergency situations and host nation support for the reception of allied military force. See Jermalavičius et. al 2014: 54.

- Develop exercise scenarios that include transition from civilian crisis to military in order to practice civil-military cooperation, including decision making procedures.

- Ensure that cyber exercises are followed by substantial after-action reports and implementation plans, and monitor progress towards implementation. Develop feedback mechanisms for ensuring that lessons learned are distributed to all actors and implemented, and monitor progress. Feedback mechanisms include after action reports as well as empowerment of the actors to allow them to implement the changes. Verify that behaviour is ultimately changed and that changes are institutionalised.

- Engage all relevant stakeholders, especially from the private sector, early on into the planning process, thereby helping to build a sense of common purpose, disseminate knowledge, homogenize actors' expectations, and eliminate possible mistakes in the scenario.

- Develop and update Standard Operating Procedures for cooperation governing stakeholder interactions and coordination in cyber crisis management. Clarify the roles, responsibilities, authorities of actors, as well as the leadership arrangements for cyber security emergencies.

- Prepare and execute cyber exercises in accordance with ends and means of the Cyber Security Strategy, and subsequently take, lessons learned into account when reviewing strategy and contingency plans. National contingency plans should be developed and tested on a regular basis through exercises.

- Use exercise management (tools to support preparation, execution and evaluation), monitoring (real-time, periodic status reports), and evaluation tools (debriefing workshops, after action reports, hot wash-up sessions). The planning, execution and evaluation processes can be more efficient if they use well defined methodologies and tools to support them.

- Consider drafting political guidance for the arrangement of joint civilian-military crisis management exercises and hold frequent and regular exercises.

  Consider the establishment of a joint authority that plans and organises joint crisis management exercises to respond to the whole spectrum of civilian and military emergencies, including cyber security.[20] Such an authority could assemble lessons learned from exercises and real-world incidents, preparing an annual report with recommendations to the government.

[20] In Finland the Security and Defence Committee directs joint exercises of the government. The committee is responsible for monitoring and development of Finland's Security Strategy for Society that is based on comprehensive security concept and provides basis for crisis management (Resolution of the Finnish Government 16.12.2010).

REFERENCES

[1] Armed Forces of the United States, Joint Publication 3-16. Multinational Operations. 13 July 2013. https://www.fas.org/irp/doddir/dod/jp3-16.pdf

[2] Äripäev, Eestist saab NATO kübersüda (Estonia will become NATO's cyber heart). 18.05.2007. http://leht.aripaev.ee/publicationimages/pdf/lehed/3589.pdf

[3] Cambron-McCabe N., Preparation and development of school leaders: Implications for social justice policies. In Marshall C., and Oliva M., Leadership for social justice: Making revolutions in education (2nd ed.), 2008. Boston: Allyn & Bacon, 35–54, Cited in: Lape E., Comprehensive Approach on UNSCR 1325: Why the U.S. and Others Should Follow. In: Neal D. J, and Wells II L. (eds.), Capability Development in Support of Comprehensive Approaches Transforming International Civil-Military Interactions. Center for Technology and National Security Policy, INSS, December 2011. http://www.ndu.edu/CTNSP/docUploaded/ITX2_Capability%20Development%20for%20CA.pdf

[4] Cavanaugh S., Baltic Ghost: Regional Cyber Defense Cooperation between the Baltic States, EUCOM and the SPP, EUCOM. June 11, 2013. http://www.eucom.mil/blog-post/25209/baltic-ghost-regional-cyber-defense-cooperation-between-the-baltic-states-eucom-and-the-spp

[5] Baumann A. B., Silver Bullet or Time Suck? Revisting the Role of Interagnecy Coordination in Complex Operations. Prism vol. 3, no.3, INSS, 2012. http:// www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=143972

[6] Bendiek A., Porter L. A., European Cyber Security Policy within a Global Multistakeholder Structure, European Foreign Affairs Review 18, no.2 (2013): 155-180.

[7] Dijk G., *Comprehensive Approach: why it is a big NATO issue*. Interallied Confederation of Reserve Officers (CIOR) Symposium on NATO's Comprehensive Approach and the Role of Reservists, held on 11 August in Stavanger, Norway. http://www.cior.net/News/2010/COMPREHENSIVE-APPROACH-%E2%80%A6--and-why-it-is-a-big-NATO.aspx

[8] Doughty R.O, Erwin R.M., B*uilding National Security through Interagency Cooperation: Opportunities and Challenges.* In Wells II L., Hailes T. C., and Davies M.C. (eds.). Changing Mindsets to Transform Security: Leader Development for an Unpredictable and Complex World. Center for Technology and National Security Policy. INSS, 2013.

[9] Essens, P.J.M.D., Febbraro, A. R., Thompson M. M, and Baranski J.V., *Collaboration in a Comprehensive Approach to Operations: Introduction*, in Collaboration in a Comprehensive Approach to Operations: Effective Collaboration in Joint, Multinational, Multiagency Teams and Staffs, STO-MP-HFM-204, NATO Science and Technology Organization, October, 2013.

[10] Essens, P.J.M.D., Febbraro, A. R., Thompson M. M, and Baranski J.V., *Epilogue: Collaboration in a Comprehensive Approach to Operations*, in Collaboration in a Comprehensive Approach to Operations: Effective Collaboration in Joint, Multinational, Multiagency Teams and Staffs, STO-MP-HFM-204, NATO Science and Technology Organization, October, 2013.

[11] Estonian Defence League, *Küberkaitse on valdkond, kus Ameerika Ühendriigid õpivad Eesti kogemusest* (Cyber Security is the field where the US learns from Estonian experience). 01.03.2013, http://www.kaitseliit.ee/et/kindral-kiili-kuberkaitse-on-valdkond-kus-ameerika-uhendriigid-opivad-eesti-kogemusest

[12] European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to European Parliament and the Council – The EU's comprehensive approach external conflict and crises*. JOIN/2013/030 final. 11.12.2013. - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013JC0030:EN:NOT

[13] European Union Agency for Network and Information Security (ENISA), *On National and International Cyber exercises, Survey, Analysis and Recommendations.* October 2012. http http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012

[14] European Union Agency for Network and Information Security (ENISA), *Cybersecurity Cooperation. Defending the Digital Frontline.* ENISA, October 2013. http://www.enisa.europa.eu/media/key-documents/cybersecurity-cooperation-defending-the-digital-frontline

[15] Finnish Government, *Strategy for Security in Society.* Resolution of the Finnish Government 16.12.2010.
http://www.defmin.fi/en/publications/strategy_documents/the_security_strategy_for_society

[16] Floyd N, *How Defence can contribute to Australia's national security strategy*. Lowry Institute for International Policy, Sydney, August, 2009. Cited in: Menhinick R. T., and Gregory N. R., Educating and Training for a Comprehensive Approach: An Australian Perspective. In Neal D. J, and Wells II L. (eds.), Capability Development in Support of Comprehensive Approaches Transforming International Civil-Military Interactions. Center for Technology and National Security Policy, INSS, December 2011.

[17] Hull, C, *Focus and Convergence through a Comprehensive Approach: but which among the many*? Swedish Defence Research Agency, 2011.

[18] Jermalavičius, T., *Stakeholder Interactions in Comprehensive Security – Conditions for Success*, in Jermalavičius, T, Pernik, P, Hurt M with Breitenbauch H and Järvenpää P. Comprehensive Security and Integrated Defence: Challenges of implementing whole-of-government and whole-of-society approaches. ICDS report, December 2013, published February 2014.

[19] Kaska, K., Osula, A.-M., Stinissen, J. *The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis.* NATO CCD COE Publications, 2013.

[20] Mattelaer, A., *The Empty Promise of Comprehensive Planning in EU Crisis Management*. European Foreign Affairs Review 18, Special Issue (2013): 125-146.

[21] Menhinick R. T., and Gregory N. R., *Educating and Training for a Comprehensive Approach: An Australian Perspective.* In Neal D. J, and Wells II L. (eds.), Capability Development in Support of Comprehensive Approaches Transforming International Civil-Military Interactions. Center for Technology and National Security Policy, INSS, December 2011.

[22] Ministry of Defence, *Explanatory Memorandum to a draft regulation on the Estonian Defence League engagement in cyber security*. MOD, 02.04.2013. http:// http://eelnoud.valitsus.ee/main#KBab1QqK

[23] Ministry of Defence (MOD), *National Defence Strategy.* MOD, 2010. http:// www. www.kaitseministeerium.ee/files/kmin/img/files/KM_riigikaitse_strateegia_eng(2).pdf

[24] NATO, *Strategic Concept: For the Defence and Security of the Members of the North Atlantic Treaty Organisation,* 2010.

[25] NATO, *Chicago Summit Declaration*, 20.05.2012.

[26] NATO CCD COE. *Cyber Defence Exercise Locked Shields 2013 After Action Report.* Tallinn 2013. http://www.ccdcoe.org/publications/LockedShields13_AAR.pdf

[27] Padar, A. *Interview with the author*. February, 2014.

[28] Rendon Group, *Conficker Working Group: Lessons Learned,* June 2010, published January 2011. http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

[29] Riigikogu, *Emergency Act* (RT I 2009, 39, 262), 2009 http://www.riigiteataja.ee/en/eli/530102013054/consolide

[30] Smith M. E., *Institutionalizing the 'Comprehensive Approach' to EU Security.* European Foreign Affairs Review 18, Special Issue (2013): 25-44.

[31] Strickler, T *Interagency cooperation: Quo vadis?* Interagency Journal, Vol. 1, Issue 1, 2010, pp. 3-9.

[32] Tardy T., *NATO and the Comprehensice Approach. Weak conceptualisation, political divergences, and implementation challenges.* In Herd G.B. and Krindler J (eds.). Understanding NATO in the 21 Century. Allience Strategy, Security and Global Governence. Routledge, 2013.

[33] Tikk, E., Kaska K., Vihul L., *International Cyber Incidents: Legal Considerations*. CCD COE, 2010.

[34] Wells II L, Pudas T. J., McNitt B., Linking NATO Capacity to Local Stakeholders. In: Neal D. J, and Wells II L., *Capability Development in Support of Comprehensive Approaches Transforming International Civil-Military Interactions*. Center for Technology and National Security Policy, INSS, December 2011

[35] White House, *National Security Strategy,* May 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf