Interdependence of Internal and External Security

Ilkka Tikanmäki[1,1] and Harri Ruoslahti[12]
[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland
Ilkka.tikanmaki@laurea.fi
harri.ruoslahti@laurea.fi
DOI: 10.34190/EWS.21.112

Abstract: Changes in the security environment, affecting both internal and external security, have been rapid in recent times. Security challenges related to hybrid phenomena, cybersecurity and organized cross-border crime significantly influence the development of the security environment. Global interdependence contributes to the nature of security, e.g., within the EU the free movement of goods and people have increased interdependence. The importance of situational awareness created and shared jointly by security actors is based on up-to-date information and assessments. Seamless cross-administrative collaboration promotes situational awareness (SA) and real-time situation picture. Thus, situational awareness is important for decision-making at different levels in various operating environments. Preparing for threats in accordance with the principle of total security is to safeguard the vital functions of society through cooperation between authorities, business, organizations, and citizens. Preparedness is a matter of comprehensive security and the vital functions in society involve cooperation between authorities, organizations, and citizens. As the operational environment is constantly changing, it has become increasingly difficult to distinguish between internal and external security and responding to changing threats may require revisions in policies and practices, and improved cooperation between actors. Significant changes in security situations may require addressing jurisdiction for security authorities and other actors, as jurisdiction is always based on the law. Effective cooperation between authorities requires responsible management, confidentiality, and appropriate allocation of resources. On an individual level, commitment, cooperative spirit, and personal contacts become critical to the success of collaborative work. The Common Operational Picture (COP) is a tool for achieving a good level of situational awareness, which in turn requires improved decision-making abilities and precise responses to situations that may arise. Positive developments are taking place in the field of information systems and information exchange between authorities. As threats change, so should the policies of states' internal and external security authorities be considered, also requiring reviewing the competences of these authorities, and how national legislation enables the security authorities to act in the face of possible threats.

Keywords: comprehensive security, internal security, external security, cooperation, situation picture, situation awareness, hybrid, common information systems

1. Introduction

Changes in the security environment have been rapid in recent times, affecting both internal and external security (European Commission, 2020). Security challenges related to organized cross-border crime, hybrid phenomena and cybersecurity will significantly influence the development of the security environment. The importance of situational awareness created and shared jointly by security actors is based on up-to-date information and assessments (Endsley, 2015). Threats and disturbances must be anticipated, prepared, and responded to.

Traditional security thinking has seen security as a separate entity that is only considered when a threat has already occurred. Changes in security situations are more likely in the future and it is difficult to prepare for them. (Ministry of Interior, 2017). In Finland, preparedness is looked as comprehensive security, the vital functions of society involves cooperation between authorities, organizations, and citizens. The relationship between external and internal security are closely interlinked (Prime Minister's Office, 2009; Hyvönen and Juntunen, 2021).

Terrorism and radicalization, cybercrime and illegal immigration pose challenges to the maintenance of internal security, while external security is affected by issues such as social and economic crises that do not respect national borders (Ministry of Interior, 2016). The Police Board has identified as a priority in internal security strategy the fight against organized crime, cybercrime and terrorism, and the fight against illegal immigration; as a means, the Police Board presented e.g. better exchange of information and cooperation with third countries (Police University College, 2020). "Preparedness and response for security threats require a strong national and

[1] https://orcid.org/0000- 0001-8950-5221
[2] https://orcid.org/ 0000-0001-9726-7956

international co-operation, pre-agreed arrangements for cooperation between the authorities, business and NGOs." (Tuohimaa, Tikanmäki and Rajamäki, 2011, p. 611).

The research problem of this paper is to examine interdependencies between internal and external security, by looking at some the main phenomena, threats, risks related to security, how are they influencing the security and preparedness and how has Finland considered them?

2. Hybrid threats and hybrid influence

The Finnish Security Strategy for Society (YTS2017) defines hybrid engagement as an activity that "pursues its own goals through a variety of complementary means and by exploiting the weaknesses of the target". Means of hybrid influence can be economic, political, or military, and can be used simultaneously or sequentially with technology and social media. (The Security Committee, 2017.)

Hybrid influence can be divided into geo-economics, information, and electoral impact. Energy policy can be used as a tool for foreign influence (geo-economics), with cross-border energy transmission and imports. Trolls and cyber weapons can be used for information and electoral impact, based on a supranational IT infrastructure. (The Finnish Institute of International Affairs, 2018.)

Hybrid threats are not a new phenomenon for public authorities in Finland, the first Strategy for securing the vital functions of society discussed which authorities, business and organizations designed, prepared, and practised long-term responses to a wide range of security threats. (Finnish Government, 2003). Securing vital functions of society and managing overall security include preparing for threats, managing, and recovering from the disruptions and emergencies. Critical functions in society include leadership, international and EU action, defence capabilities, internal security, economy, infrastructure and security of supply, population capabilities and services, and mental resilience (Finnish Terminology Centre, 2017).

Hybrid threats can target vital functions and critical targets in society and may involve pressure, information operations and cyber operations (Järvenpää 2017). Due to varied and changing threats, authority policies in internal and external security need to be adapted to the new situation. Combating hybrid threats requires "an understanding of government, authorities, and industry to protect functions critical to decision-making and overall security in society. The best way to achieve this is through a coherent situation picture, the development of policies and practices, and training." (Lalu and Puistola, 2015, p. 4.) Resource sharing and resources common use are emphasized in preparing for hybrid threats (Uusipaavalniemi and Puistola, 2016).

General safety analysis plays a key role in identifying early forms of hybrid influence. As a result, the skills required by operators to detect and identify hybrid effects will increase. Actors should develop the necessary "capabilities and cyber security in cooperation with national and international actors". (Ministry of Interior, 2016, p. 13.)

A key objective of hybrid influence is to narrow the national sovereignty of another state. Mäkelä (2018, p. 13) describes hybrid influence as "a systematic activity in which a state or non-state actor can simultaneously use various military means or, for example, economic or technological pressure, as well as information operations and social media". The goal is to keep the hybrid effect at a level where it does not escalate into open conflict (Mäkelä, 2018.) Combating hybrid influencing requires the identification of one's own weaknesses, proactive preparation, situation awareness and situation understanding, clear procedures and leadership (Puistola, 2018). One defining characteristic is the continuous utilization of identifiable asymmetries, whether in the actual war or non-violent phase. Asymmetries are utilized as a combination of surprise, abuse, and deception. (Cederberg and Eronen, 2015.)

3. Interdependence of Internal and external security

The boundary between external and internal, national, and international threats has become less clear, which affects the activities of security authorities (Prime Minister's Office, 2009). Threats can be divided into civilian and military in nature (McNeese et al., 2006), while civilian crisis management and military operations have come closer to one another, requiring civilian and military actors in both (Bendiek, 2017). The Ministry of Interior of Finland has identified that the main national threats and risks are large-scale uncontrolled influx of refugees, influencing energy networks and production, organised crime, and social exclusion, where the extreme

consequence of social exclusion can be radicalization and intensification of extremism (Ministry of Interior, 2017).

Global interdependence contributes to a further tightening of security, EU membership with its consequent free movement of goods and people, for example, have positively increased interdependence. The global sustainability crisis affects security, as it affects economy and well-being. There is a focus on climate change and the sufficiency of natural resources. The use of information networks is restricted by security and political considerations. Automation, artificial intelligence and robotization blur the interface between technology and humans (Ministry of Interior, 2017).

Disruptions to normal conditions can be dealt with existing jurisdictions of authorities, while significant changes in the security situation may require additional jurisdiction for security authorities and other actors. Jurisdiction is based on law, and while some jurisdictions are always valid, others can only be used under law crisis and during specifically defined situations. E.g. the jurisdiction of the Armed Forces is based on the Armed Forces Act, the police on the Police Act, and the Border Guard has special crime prevention functions, which are provided for in the Law on Crime Prevention at the Border Guard. (Finlex, 2020a, 2020b, 2020c.)

In Finland, cooperation between the police and judicial system has been natural and effective, and except for some coercive measures, the police have decision-making powers during operations. There is also "need to develop national legislation to match the current operational environment (Ministry of Interior, 2016, p. 73). Similar cooperation between the police and judiciary system is not possible everywhere, as national legislation in some countries limits some cooperation (Tikanmäki and Rathod, 2019, p. 211). Critical infrastructure, e.g. electricity and telecommunications, are an important and vulnerable part of vital societal functions. (The Security Committee, 2017; Järvenpää, 2017.).

The Finnish security cooperation model covers all levels and actors of society, as the Domestic Security Program sets intergovernmental targets for different sectors of government. The comprehensive security concept requires resource sharing, coordination, and joint planning by and between authorities (Valtonen and Branders, 2021; Tuohimaa, Tikanmäki and Rajamäki, 2011). According to the Security Committee "Preparedness measures include contingency planning, continuity management, advance preparations, training and preparedness exercises" (The Security Committee, 2017, p. 9). Global threat scenarios and disruptions that effect to the internal and external security of the society.

The description of the threat scenario in this context refers to potential disruption in the security environment that is a threat or event that jeopardizes the vital functions or strategic missions of the society. Extensive and close co-operation between authorities and other actors is needed to manage disruptions (Ministry of the Interior, 2019). National action plans for security in Finland include measures and elements that promote internal and external security. Security actors include authorities and relevant companies, legal frameworks for jurisdiction, and collaboration and information sharing for situation understanding.

On a European level, new concepts of security have shifted perceptions of internal and external threats, blurring the division between foreign and domestic policy. Internal security has an important role in operational cooperation. On an operational level, there are networks of task-based law enforcement authorities, and network management is carried out by law enforcement authorities on both macro (e.g. judges) and the micro levels (individual police and judicial authorities work together), and across borders. (Lavenex and Wichmann, 2009.)

European cooperation in space and on air, land, and maritime domains, joint capabilities, common training, and multiple collaboration projects increase safety and security. Command and Control (C2), interoperability and common strategic culture pave way to more resilient European Union (EU). The EU Global Strategy (EUGS) states: "The EU has invested significantly in the resilience of the Eastern partners, beginning with Ukraine, in areas such as rule of law, energy, critical infrastructure, cyber, strategic communications, and the reform and strengthening of the security and defence sectors". (European Union, 2019.)

The EU has invested heavily in protecting maritime threats, such as, piracy and human trafficking. The efforts of the EU have reduced maritime accidents and helped prevent environmental disasters (European Union, 2019). The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) improves capacity to combat and

prevent hybrid threats and enhance resilience within the EU. Hybrid CoE cooperates with NATO on hybrid and cyber issues (Hybrid CoE, 2020).

4. Cooperation between authorities

Developments in telecommunications and information systems have made our society complex and vulnerable. This development combined with threats, such as climate change, general unrest, increased violent civic activism and growing economic insecurity, as has been noted during the Covid19 epidemic. Responsibility for preparedness against crises in the Finnish society lies in the hands of e.g. the military, security authorities, the National Emergency Supply Agency, as well as security companies (Parmes, 2020.). A small country like Finland can only be effective in its crisis management when authorities and communities cooperate (Tikanmäki and Ruoslahti, 2017).

Valtonen (2010) proposes a theoretical model for cooperation between security actors, with criteria for cooperation and descriptions of cooperation processes. The author calls for effective cooperation between authorities, and this requires responsible management, confidentiality, and appropriate allocation of resources. On an individual level, a spirit and commitment to cooperate, and personal contacts become critical for successful collaborative work. Developing co-operation skills become a most important area when developing inter-authority co-operation (Valtonen, 2010.)

Krogars (2005) presents the overall process for crisis management, which lays a foundation for networking. Lanne (2007) defines a central vocabulary of security collaboration from the perspective of corporate security. The aim of her study is to develop a business security management model that could also be used in public sector security activities.

International cooperation between emergency services are hampered by differences in country-specific organizations and management systems, legislation, and security concepts. These differences make it difficult to receive international aid or to provide aid abroad. (Ministry of Interior, 2016, p. 54). Confidential relations between security authorities are essential. Extensive cooperation is needed to achieve the common goal, a safety and security community. Thus, cross-border and cross-sector cooperation is essential (McNeese et al., 2006).

The cornerstones of cooperation between public authorities and industry are situational awareness, training, and the confidential exchange of information between actors (Uusipaavalniemi and Puistola, 2016). Cyber security aims at systems and infrastructures being resilient, and situation awareness is a main prerequisite for cyber security (Pöyhönen et al., 2020).

4.1 Situation picture and situation awareness

The situation picture is a description of the common security situation and includes an analysis of the current situation and an assessment of the future. A common situation picture is an essential part of the information shared by one or more users. Common situational awareness enables collaboration task planning and assists all echelons to achieve situational awareness. (Kuusisto, 2005; Alberts et al., 2001.) The key issue in creating a situation picture is to organize the acquisition of information from different actors in society and to tailor it to the needs of each user. Creating a situation picture involves understanding the situation and assessing the evolution of the situation. "Collecting and sharing a situation picture is a prerequisite for situation management" (Tikanmäki and Ruoslahti, 2019, p. 419.)

In the User-defined Common Situation picture, the approach is network-centric and allows for multiple sources of information (Loomis et al., 2008). The Global Situation and Command and Control System (GCCS) situation picture presented by Butler et al. was intended to use existing commercial products and reduce the complexity of existing systems (Butler et al., 1996).

Smooth, seamless cross-administrative collaboration promotes situational awareness and real-time situation picture, as situational awareness (SA) is important for decision-making at different levels in various operating environments (Lehto and Limnéll, 2021). The Common Operational Picture (COP) is a tool for achieving a good level of situational awareness. A good level of situational awareness requires improved decision-making abilities and precise responses as situations arise. Automation and data fusion are becoming increasingly important in

new computing platforms where humans must be able to operate. Technical systems/devices play a major role as sources of information, especially in Situation Centres' environment. (Timonen, 2018.)

In some cases, situational awareness has been considered to be a large amount of diverse information produced from multiple sources. Critical Infrastructure (CI) situational awareness has the same elements and prerequisites as traditional situational awareness, but there is a difference in the mechanisms by which the situational awareness is achieved. Command & Control (C2) systems are typically focused on geospatial thinking, while a critical infrastructure operator focuses on geographic, logical, and physical systems. (Timonen, 2018.)

Interaction and exchange of information between authorities are important for building awareness of cooperation and promoting cooperation to enhance maritime safety. Ruoslahti and Tikanmäki (2019) state that "European maritime cooperation aims at increasing situational awareness, sharing best practices, improving interoperability, removing overlapping activities, and promoting cross-border and cross-sector cooperation (p. 160).

4.2 Common information systems

There are European wide and regional initiatives and developments in the field of information systems and information exchange between authorities. EU projects such as EUCISE2020, MARISA, RANGER and ANDROMEDA are producing or have made significant progress in data models and collaborative information systems (ANDROMEDA 2019; EUCISE2020 2020; MARISA 2020; RANGER 2016.). The basis for this cooperation was the European CISE Road Map in 2010, which defined the outcome of maritime information exchange and cooperation between authorities (European Commission, 2010a, b).

The European Commission (2013) identifies seven user communities operating on the European maritime domain: 1) Maritime Safety including Search and Rescue (SAR) and prevention of pollution caused by ships; 2) Fisheries control; 3) Marine pollution preparedness and response in Marine environment: 4) Customs; 5) Border control; 6) General law enforcement; and 7) Defence. (European Commission, 2013.) These user communities have several common IT systems in use on the land border and maritime domains.

The Finnish Police, Border Guard and Rescue Services also use the same field Command System to facilitate the coordination of accidents and other situations. A common situation picture (including available units, resources, etc.) for all authorities involved in the event promote co-operation between the rescue and police authorities, and information becomes also shared between police, rescue services, social and health services, the Border Guard, Defence Forces and Customs, and other possible authorities. (National Police Board, 2020.)

5. Conclusions

In a globalized world, internal and external security cannot be separated. The distinction between internal and external security is becoming increasingly difficult as their operational environments are constantly changing and converging, as seen in Figure 1, below. In some situations, it is necessary to influence external security through internal security and vice versa. Mainly the same authorities are responsible for responding to threats, be they external or internal. The use of national, regional, and EU-wide common information sharing systems and databases to enhance cooperation between authorities are important elements in strengthening security. Rapid and up-to-date exchange of information between security authorities is needed to maintain situational awareness and understanding. Though, needed to build situation awareness, real-time information sharing may involve risks, as any collaborating entity may become subject to a cyber-breach, and the integrity of the shared data may become questionable (Pöyhönen et al., 2020).

Because cross-sectoral barriers may slow down the exchange of information between administrative sectors, staff exchanges are recommended to improve situational awareness and to develop common operating models. Increasing the knowledge levels of authorities and strengthening their exchange of information with one another across organizational boundaries, and with practitioners in need of the information promote preparedness and situational understanding (e.g. Parmes, 2020; Tikanmäki and Ruoslahti, 2017; Ministry of Interior, 2016)

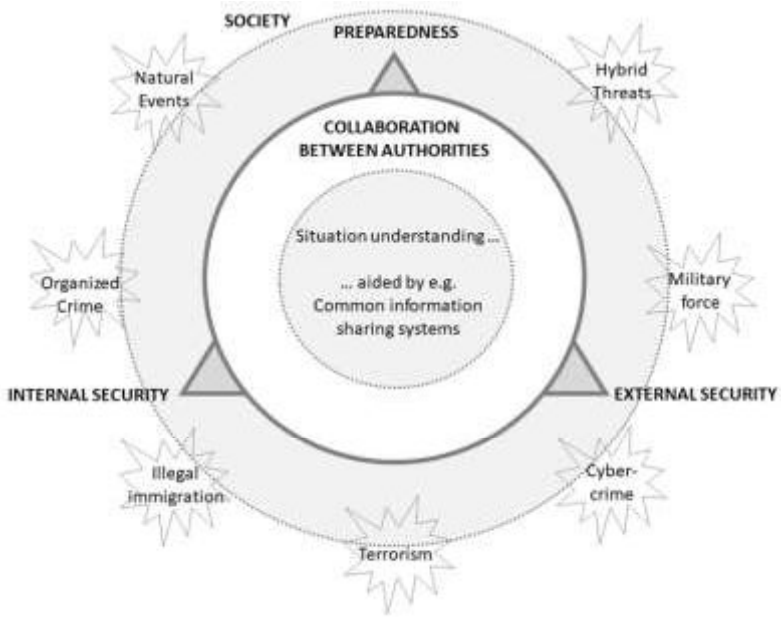

Figure 1: Interdependence of preparedness, and internal and external security in society

State actors organized to detect and respond to hybrid threats, practice policy and operative revisions with improved cooperation between relevant actors. From the point of view of e.g. the Border Guard, hybrid threats include illegal immigration, cross-border crime, foreign fighters, and terrorism. During times of peace, cooperation with internal security actors becomes emphasized in maintaining border security (Järvenpää, 2017; The Security Committee, 2017; Ministry of Interior, 2016).

As threats change, the policies of state authorities responsible for internal and external security should be actively considered. This requires reviewing competences of these authorities and revising national legislation to enable security authorities to act when faced by threats (e.g. Tikanmäki and Rathod, 2019; Järvenpää, 2017). Since hybrid threats are both internal and external in nature, European Member States and third nations should be more willing to share information about their domestic developments. Security authorities need to 'be prepared' for anything and everything.

References

Alberts, D., Garstka, J., Hayes, R. and Signori, D. 2001. *Understanding Information Age Warfare*. Washington D.C.: Assistant Secretary of Defence C3I/Command Control Research Program. CCRP Publication Series.

ANDROMEDA. 2019." An Enhanced Common Information Sharing Environment for Border Command, Control and Coordination Systems". The European Union's H2020 research and innovation programme under grant agreement no 833881.

Bendiek, A. 2017. A paradigm shift in the EU's Common Foreign and Security Policy: from transformation to resilience. (SWP Research Paper, 11/2017). Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. Available at <https://nbn-resolving.org/urn:nbn:de:0168-ssoar-54521-8> [Accessed 25 September 2020]

Butler, S., Diskin, D., Howes, N. and Jordan, K. 1996. Architectural design of a common operating environment. IEEE Software, vol. 13, pp. 57-65. Available at <https://ieeexplore.ieee.org/document/542295> [Accessed 21 March 2020]

Cederberg, A. and Eronen, P. 2015. How can Societies be Defended against Hybrid Threats? Strategic Security Analysis. September 2015 No.9. Geneva Centre for Security Policy (GCSP).

Endsley, M. 2015. Final Reflections: Situation Awareness Models and Measures. *Journal of Cognitive Engineering and Decision Making* 2015, Volume 9, Number 1, March 2015, pp. 101–111.

EUCISE2020. 2020. "EUropean test bed for the maritime Common Information Sharing Environment in the 2020 perspective." Available at < http://www.eucise2020.eu/> [Accessed 11 March 2020]

European Commission. 2020. COM(2020) 605 final. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy.

European Commission, 2013. CISE Architecture Visions Document (Study supporting the Impact Assessment). Brussels: European Commission.

European Commission. 2010a. COM (2010) 584 Final. Communication from the Commission to the Council and the European Parliament: on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain.

European Commission. 2010b. Integrating Maritime Surveillance. Common Information Sharing Environment (CISE). Available at < https://op.europa.eu/en/publication-detail/-/publication/2d412889-77fd-4db5-b6fd-51b237410cf6 [Accessed 11 March 2020]

European Union. 2019. The European Union's global strategy. Three years on, looking forward. Available at <https://eeas.europa.eu/topics/eu-global-strategy_en> [Accessed 15 March 2020]

European Union. 2018. A Europe that Protects: Countering Hybrid Threats. Available at <https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en> [Accessed 21 March 2020]

Finlex. 2020a. Laki puolustusvoimista 11.5.2007/551. Available at <https://www.finlex.fi/fi/laki/ajantasa/2007/20070551> [Accessed 15 March 2020]

Finlex. 2020b. Poliisilaki 22.7.2011/872. Available at <https://www.finlex.fi/fi/laki/ajantasa/2011/20110872> [Accessed 15 March 2020]

Finlex. 2020c. Laki rikostorjunnasta Rajavartiolaitoksessa 30.1.2018/108. Available at <https://www.finlex.fi/fi/laki/ajantasa/2018/20180108> [Accessed 15 March 2020]

Finnish Government. 2003. Strategy for securing the vital functions of society. In Finnish: Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia. Valtioneuvoston periaatepäätös 27.11.2003.

The Finnish Institute of International Affairs. 2018. Hybridivaikuttaminen ja demokratian resilienssi - ulkoisen häirinnän mahdollisuudet ja torjuntakyky liberaaleissa demokratioissa. FIIA Report 55/2018.

Finnish Terminology Centre. 2017. Vocabulary of Comprehensive Security. ISBN 978-952-9794-36-2 (PDF). Available at <http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf> [Accessed 14 March 2020]

Hybrid CoE. 2020. What is Hybrid CoE? Available at <https://www.hybridcoe.fi/> [Accessed 15 March 2020]

Hyvönen, A. E., and Juntunen, T. 2021. From "spiritual defence" to robust resilience in the Finnish comprehensive security model. *Nordic Societal Security: Convergence and Divergence*. London: Routledge, 154-178.

Järvenpää, M. 2017. Viranomaisten toimivaltuudet kohteiden suojaamisessa hybridiuhkia vastaan. Tiede Ja Ase, 74.

Krogars, M. 1995. *Verkostoilla kriisinhallintaan*. Dissertation. Vaasa: Ankkurikustannus Oy.

Kuusisto, R. 2005. From Common Operational Picture to Precision Management. Managemental Information Flows in Crisis Management Network. Available at <http://julkaisut.valtioneuvosto.fi/handle/10024/78700> [Accessed 21 March 2020]

Lalu, P. and Puistola, J. 2015. Hybridisodankäynnin käsitteestä, Puolustusvoimien Tutkimuslaitoksen katsaus 01-2015. Helsinki: Puolustusvoimien tutkimuslaitos.

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. Dissertation. Helsinki: Edita Prima Oy.

Lavenex, S. and Wichmann, N. 2009. The External Governance of EU Internal Security', Journal of European Integration,31:1,83 — 102.

Lehto, M., and Limnéll, J. 2021. Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139-148.

Loomis, J., Porter, R., Hittle, A., Desai, C. and White, R. 2008. "Net-centric collaboration and situational awareness with an advanced User-Defined Operational Picture (UDOP)," in International Symposium on Collaborative Technologies and Systems (CTS), pp. 275-284.

MARISA. 2020. "Improving maritime surveillance knowledge and capabilities through the MARISA toolkit." Available at <https://www.marisaproject.eu/> [Accessed 11 March 2020]

McNeese, M.D.,Pfaff, M.S.,Connors, E.S.,Obieta, J.F.,Terrell, I.S.,and Friedenberg, M.A. 2006. Multiple vantage points of the common operational picture: Supporting international teamwork. In Proceedings *50th Annual Meeting Human Factors and Ergonomics Society* (pp.467–471). Doi: 10.1177/154193120605000354

Ministry of Interior. 2019. National risk assessment 2018. Internal Security. Publications of the Ministry of Interior 2019:9.

Ministry of Interior. 2017. Hyvä elämä - turvallinen arki. Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta. Ministry of Interior publications 15/2017. Helsinki: Lönnberg Print & Promo.

Ministry of Interior. 2016. Interdependence of Internal and External Security. Will the operational culture change with the operational environment? Available at <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79230/37_2017_Interdependence%20of_nettiin.pdf> [Accessed 4 March 2020]

Mäkelä, J. 2018. Merelliset hybridiuhat. [lecture]. Held on 23 May 2018. Finnish National Defence University.

National Police Board. 2020. Turvallisuusviranomaisille yhteinen kenttäjärjestelmä. Available at <https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/turvallisuusviranomaisille_yhteinen_kenttajarjestelma_32185> [Accessed 12 March 2020]

Parmes R. 2020. "Varautumisen historia ja nykyhetki" in Viestimies I/2020 pp.16-19. Newprint Oy: Raisio. ISSN 0357-2153.

Police University College. 2020. Varautuminen eilen – varautuminen huomenna. Poliisiammattikorkeakoulun raportteja 136. Heino, O., Huotari, V. and Laitinen, K. (eds.). Tampere: PunaMusta Media Oyj, 2020.

Prime Minister's Office. 2009. Finnish Security and Defence Policy 2009. Government Report. Prime Minister's Office Publications 13/2009. Helsinki: Helsinki University Print Bookstore.

Puistola, J-A. 2018. Kokonaisturvallisuus ja hybridivaikuttaminen. [lecture]. Held on 23 May 2018. Finnish National Defence University.

Pöyhönen, J., Rajamäki, J., Lehto, M. and Ruoslahti, H. 2020. Cyber Situational Awareness in Critical Infrastructure Protection. Annals of Disaster Risk Sciences, Vol 3, No 1 (2020): Special issue on cyber-security of critical infrastructure. Available at <https://ojs.vvg.hr/index.php/adrs> [Accessed 2 April 2021]

RANGER. 2016. "Radars for long distance maritime surveillance and SAR operations." The European Union's H2020 research and innovation programme under grant agreement no 700478.

Ruoslahti, H. and Tikanmäki, I. 2019. Complex Authority Network Interactions in the Common Information Sharing Environment. In Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019), Volume 3: KMIS, pages 159-166. September 17-19, 2019, Wien, Austria.

The Security Committee. 2017. The Security Strategy for Society. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 2.11.2017. ISBN: 978-951-25-2959-9.

Tikanmäki I. and Rathod P. 2019. Enhancing the Development of Interaction between Authorities in Maritime Surveillance. In: Ntalianis K., Croitoru A. (eds) Applied Physics, System Science and Computers II. APSAC 2017. Lecture Notes in Electrical Engineering, vol 489. Springer, Netherlands, ISSN: 1876-1100, pp. 207-214.

Tikanmäki, I. and Ruoslahti H. 2019. How are situation picture, situation awareness, and situation understanding discussed in recent scholarly literature? *In Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management* (IC3K 2019), Volume 3: KMIS, pages 419-426. September 17-19, 2019, Wien, Austria.

Tikanmäki, I. and Ruoslahti H. 2017. Increasing Cooperation between the European Maritime Domain Authorities. *International Journal of Environmental Science*, Volume 2, pp. 392-399. ISSN: 2367-8941. IARAS, Nicosia, Cyprus.

Timonen, J. 2018. A Common Operating Picture for Dismounted Operations and Situation Room Environments. National Defence University. Series 1: Research publications No. 19. Academic Dissertation. Tampere: Juvenes Print.

Tuohimaa, T. and Tikanmäki, I. 2011. The Strategic Management Challenges of Developing Unmanned Aerial Vehicles in Public Safety Organizations, *10th WSEAS international conference on communications, electrical & computer engineering*, Playa Meloneras, Spain, Mar 2011, ISBN: 978-960-474-286-8, pp. 34-39.

Tuohimaa, T., Tikanmäki, I. and Rajamäki, J. 2011. Cooperation challenges to public safety organizations on the use of unmanned aircraft systems (UAS), *International Journal of Systems Applications, Engineering and Development*, Issue 5, Volume 5, 2011 pp. 610-617.

Valtonen, V. 2010. Turvallisuustoimijoiden yhteistyö operatiivis- taktisesta näkökulmasta. Maanpuolustuskorkeakoulu. Taktiikan laitos. Julkaisusarja 1, n:o 3. Edita Prima Oy: Helsinki.

Valtonen, V., and Branders, M. 2021. Tracing the Finnish Comprehensive Security Model. *Nordic Societal Security: Convergence and Divergence*. London: Routledge, 91-108.