Modelling Total Defence Systems to Inform National Resilience Objectives – A Norwegian Case Study

Stig Rune Sellevåg
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, 2027 Kjeller
NORWAY

stig-rune.sellevag@ffi.no

ABSTRACT

The defence of Norway is built upon national defence, NATO's collective security, and bilateral support and reinforcements from close allies. These three lines of efforts are underpinned by the total defence concept that builds national resilience. The deteriorated security situation following the Russian invasion of Ukraine, the impact of the Covid-19 pandemic and the impact of climate change, call for strengthening national resilience and defence. To inform processes to establish and assess resilience objectives at the national level, a system-scale and cross-sector functional approach for modelling of total defence systems has been proposed. The functional approach is established on the basis of an abstraction-decomposition space for critical infrastructure systems, taking into account NATO's seven baseline requirements. Through this approach, cascading effects following disruptive events can be investigated by using dynamic inoperability input-output modelling. The modelling results can be used to aid resilience assessments of the total defence system for current and future defence scenarios.

Keywords: Layered resilience; Civil-military cooperation; Civil preparedness; Interdependencies; Simulation

1.0 INTRODUCTION

The Russian invasion of Ukraine on 24th February 2022 and the 2020–2022 Covid-19 pandemic have affected all sectors in society and identified weaknesses in our preparedness. The war in Ukraine, in particular, has created lasting changes in the security situation in Europe. In addition, the security situation is exacerbated by revisionist authoritarian states who seek to disrupt the current rule-based international order, non-state actors who seek to inflict terror or gain profits through criminal acts, and the impacts of climate change. This calls for strengthening national resilience and our defence capabilities [1].

The defence of Norway is built upon national defence, NATO's collective security, and bilateral support and reinforcements from close allies. These three lines of efforts are underpinned by the so-called total defence concept [2], where armed forces and civil preparedness efforts constitute a comprehensive whole-of-society approach to national security and defence. Given the direct involvement of the civil society, critical infrastructure and societal resilience become a vital part of the total defence.

The armed forces' reliance on civil resources and critical infrastructures operated by the private sector, has been acknowledged by NATO with the establishment of its seven baseline requirements [3]. Critical infrastructures are complex adaptive systems that undergo constant interaction with their economic, social and natural environments [4], [5], [6]. Despite the progress that has been made, understanding the fragility induced by the emergent properties of complex adaptive systems is still a major challenge [5], [7]. Strategies where risks are analysed, evaluated and treated individually, are therefore insufficient [7]. Thus, there is a need for active resilience strategies at the national level that exploit complexity theory-based system-of-systems approaches.

To this end, a system-scale and cross-sector functional approach for modelling total defence systems is proposed. The aim of the approach is to inform processes to establish and assess resilience objectives at the national level. This paper presents the approach and how it can be linked to a scenario- and capability-based approach for analysing the Norwegian defence force structure.

2.0 ANALYTICAL METHODS

The functional approach is established on the basis of an abstraction-decomposition space for critical infrastructure systems [8], taking into account NATO's seven baseline requirements. By combining this approach with so-called dynamic inoperability input-output modelling [9], [10], [11], [12], cascading consequences following disruptive events can be investigated for current and future defence-related scenarios. The latter requires a method for mapping the interdependencies between the different functions that constitute the total defence system. These three methods will be described in the following.

2.1 Framework for Describing Total Defence Systems

Sellevåg has proposed a system-of-systems-based framework for infrastructure planning and resilience policies that is grounded in theory for complex systems [8]. The framework consists of an abstraction hierarchy analysis and a part-whole decomposition of the system (work domain) under investigation. By imposing constraints on the system, the framework promotes design for adaptation, which is important since it would be impossible to prescribe, describe and risk assess all possible actions within a complex system.

The abstraction hierarchy of the framework consists of the following five conceptual levels [8]:

1) *Functional purposes* – The overall purposes of the system;
2) *Values and priority measures* – The values that are assessed and used to measure the system's progress towards the functional purposes;
3) *Purpose-related functions* – The generalised functions of the system that are necessary to achieve the functional purposes;
4) *Infrastructure-related processes* – The functional capabilities of the system's assets that enable the purpose-related functions;
5) *Assets* – The system's assets that undertake the infrastructure-related processes.

The part-whole decomposition consists of four levels: (1) whole system; (2) sectors; (3) sub-sectors; (4) types of entities [8]. Together, the abstraction hierarchy and the part-whole decomposition form an abstraction-decomposition space that can be used to describe the total defence system under study for modelling purposes. It is referred to ref. [8] for further details on the framework.

2.2 Dynamic Inoperability Input-Output Model

Describing the potential cascading consequences that follow disruptive events in a complex system is difficult without the support of modelling and simulation. For this purpose, several approaches have been proposed [13]. One of the most successful approaches is the so-called dynamic inoperability input-output model (DIIM) [9], [10], [11], [12]. With little computational cost, this approach is able to model how service degradation within one infrastructure influence other infrastructures' ability to operate.

DIIM is an economic-theory based model where infrastructure disruptions are modelled as a forced demand-reduction and where the cascading effects on other sectors are described by backward linkages [9], [10], [11], [12], [14], [15]. The service degradation following a disruptive event at a given time t is described as the system's inoperability, $\boldsymbol{q}(t) \in [0,1]^n$. The inoperability specify the normalised service loss for each of the n infrastructures that can be realised after a prolonged demand-side perturbation, $\boldsymbol{c}^*(t) \in [0,1]^n$ [9], [12]. Given the initial condition $\boldsymbol{q}(0)$ and if the final demand is stationary ($\boldsymbol{c}^*(t) = \boldsymbol{c}^*$), it can be shown that [9], [11]:

$$\boldsymbol{q}(t) = (\boldsymbol{I} - \boldsymbol{A}^*)^{-1}\boldsymbol{c}^* + e^{-\boldsymbol{K}(\boldsymbol{I}-\boldsymbol{A}^*)t}[\boldsymbol{q}(0) - (\boldsymbol{I} - \boldsymbol{A}^*)^{-1}\boldsymbol{c}^*] \tag{1}$$

Here, $\boldsymbol{A}^*$ is a $n \times n$ matrix that describes the interdependencies between the different infrastructures that constitute the system. Since $(\boldsymbol{I} - \boldsymbol{A}^*)^{-1} = \boldsymbol{I} + \boldsymbol{A}^* + \boldsymbol{A}^{*2} + \boldsymbol{A}^{*3} + \cdots$, where $\boldsymbol{I}$ is the identity matrix, cascading effects (*i.e.* second- and higher-order effects) are captured by the model. The matrix $\boldsymbol{K} = \mathrm{diag}(k_i)$ is the so-called infrastructure resilience coefficient matrix, where $k_i \propto 1/\tau_i$ and τ_i is the recovery time [9]. Thus, each k_i is influenced by the nature of each infrastructure i as well as the efforts to control it through risk management policies and preparedness efforts. Data on recovery times can come from requirements, be estimated by expert assessments or varied as part of a parametric analysis to investigate the effects of different recovery times.

2.3 Estimation of Interdependency Parameters

Three approaches have been proposed in the literature for estimating the $\boldsymbol{A}^*$ interdependency parameters: (*i*) use of physical connectivity [10], (*ii*) national account data [9], and (*iii*) expert assessments [16]. Of these approaches, the expert assessment method is considered as the most useful approach for the purpose of this work since mapping of physical connectivities would be too time-consuming and the use of national account data have limitations when describing temporal aspects of disruptive events. The expert assessment method takes advantage of the infrastructure operators' knowledge of the impacts of outages on their own infrastructure. By assessing the direct consequence (first order dependency) of an outage in infrastructure j on infrastructure i, the a_{ij}^* values of $\boldsymbol{A}^*$ can be estimated.

Using Zimmerman's [18] interpretation of interdependencies, the interdependency mapping was done by asking relevant domain experts the question: "On a scale from 0–5, how would you rate the direct impact on TDF_i occurring as a result of lack of services provided by TDF_j for the geographical region under study?" The experts were asked to consider the following service outage scenarios: (*i*) ≤ 1 day; (*ii*) 1–3 days; (*iii*) ≥ 7 days. The 5-point impact scale was established from data provided by Setola *et al.* [16] (see Table 1 in [16]), and fitted to a power law equation: $a_{ij}^* = 0.008X^{2.569}$, where X is the impact scale value (Figure 1).

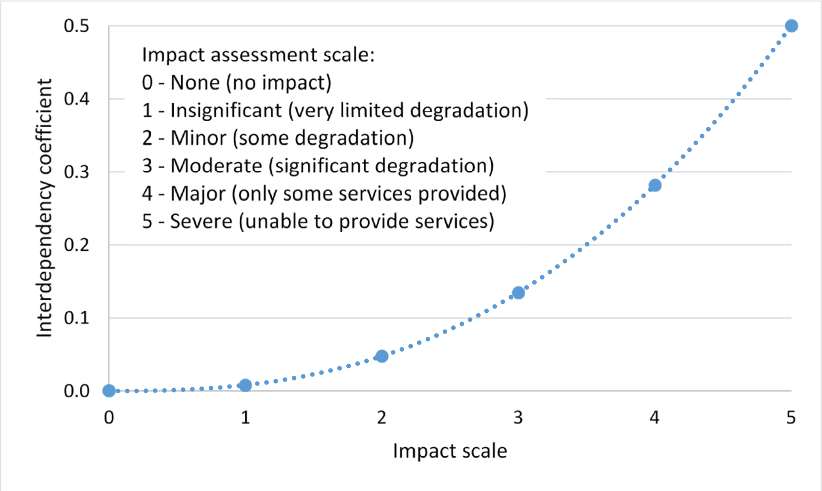

Figure 1: Impact assessment values.

3.0 RESULTS

To illustrate the use of the modelling approach, the Total Defence Concept of Norway is used as a case.

3.1 Civilian Total Defence Functions

Given that Norway is a small state, the Norwegian Armed Forces do not possess all resources that are needed to defend Norway in an armed conflict. Extensive civilian support to national and allied armed forces in crises and armed conflicts therefore constitutes the core of the Norwegian Total Defence Concept [2].

Sellevåg [17] has proposed a minimum set of civilian total defence functions (TDFs) for modelling the Norwegian total defence on the basis of the framework published in ref. [8]. The abstraction hierarchy for the system is displayed in Figure 2, where the lower abstraction levels are shown for the energy sector. The purpose of the system is to defend Norway through continuous operations in normal situations, crises and armed conflicts. To achieve the functional purpose, the civilian TDFs must ensure provision of essential services to national and allied armed forces. The values and priority measures are established on the basis of Norwegian preparedness legislation and NATO's baseline requirements and are as such relatively stable properties of the system. This will provide guidance if the system is experiencing stressful, unanticipated events. Financial services and services for positioning, navigation and time (PNT) were also included given the importance of such services for modern societies.

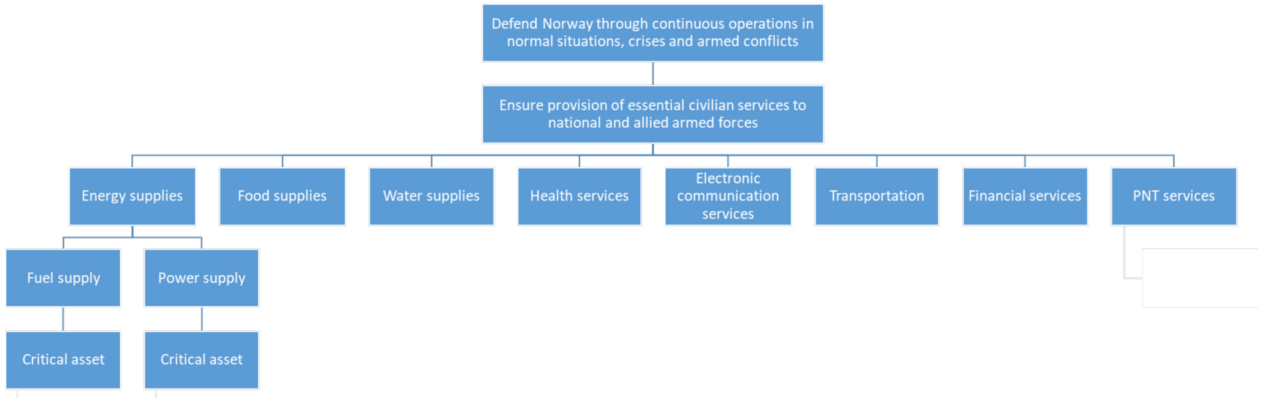

Figure 2: Abstraction hierarchy for the system of civil total defence functions [17].

3.2 Mapping of Interdependencies

For the Norwegian case study that is undertaken, it was decided to map interdependencies between the TDFs at the fourth level of abstraction (*cf.* Figure 2). Selected results from the interdependency mapping for the Norwegian case study are shown in Figure 3 (sensitive information exempt from public disclosure has been removed). As can be seen, the impact score for a given TDF_k varies considerably with outage duration and with which TDF that is suffering an outage. This reflects the current preparedness efforts that are in place. If TDF_4 is suffering an outage, the impact on TDF_k is assessed to be severe already after 24 hours outage duration. For other TDFs, it will take 3 days or more before TDF_k suffers major to severe impact.

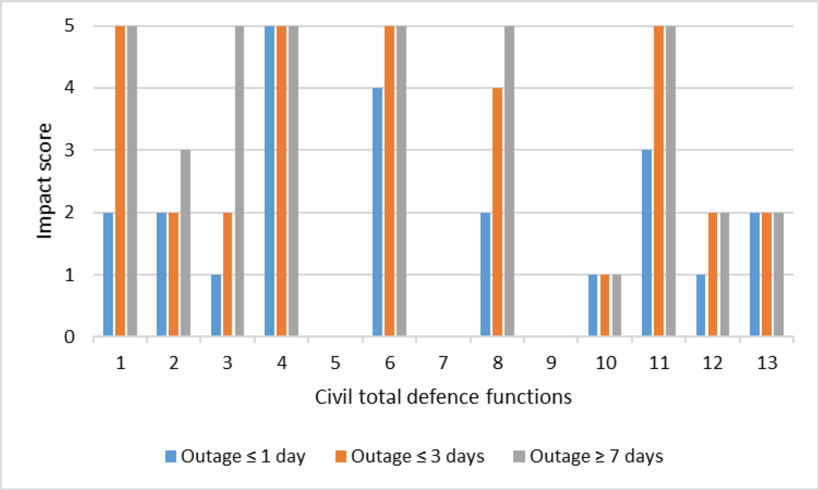

Figure 3: Interdependency mapping for Norwegian case study.

3.3 Resilience Assessment

After the interdependency mapping has been completed, the cascading effects following disruptive events can be investigated by using DIIM (eq. 1). The modelling results can then be used to assess the resilience of the total defence system for different scenarios. For the purpose of this work, resilience can be considered as "*the ability of the system to sustain or restore its basic functionality following a risk source or an event (even unknown)*" [19]. Following refs. [19], [20], the resilience loss (Q_i) for each TDF_i can be evaluated as (eq. 2):

$$Q_i = \int_{t_0}^{t_1} q_i(t)\,\mathrm{d}t \tag{2}$$

where t_0 is the start time for the disruptive event and t_1 is the time it takes to restore the functionality of TDF_i.

The resilience loss for the total defence system as a whole can then be calculated as given in eq. (3):

$$Q_i = \int_{t_0}^{t_1} q_i(t)\,\mathrm{d}t \tag{3}$$

The DIIM modelling results can also be used for assessing the probability that the system will restore its functionality to its pre-disaster level within a specified recovery time. This information can then be linked to results stemming from scenario- and capability analyses that are used for defence planning and force structure assessments [21]. The scenarios that are used for defence planning will provide readiness requirements for the different military force structure elements under study. If the system of civilian total defence functions is not able to recover from a disruptive event within a specified recovery time, it may negatively affect the readiness of the force structure elements, thus resulting in a military readiness gap [21].

4.0 CONCLUSION

This work has proposed a practical-in-use system-scale and cross-sector functional approach for modelling total defence systems that is grounded in theory for complex systems. The total defence system is described by using an abstraction-decomposition space for critical infrastructure systems, taking into account NATO's seven baseline requirements. By mapping the interdependencies between the system's functions, cascading effects following disruptive events can be investigated by using DIIM. The modelling results can be used to aid resilience assessments of the total defence system for current and future defence scenarios.

The limitations of the approach pertain primarily to the use of DIIM for modelling cascading effects. Firstly, only parts of the interdependency dimensions proposed by Rinaldi *et al.* [4] are covered by the model. Secondly, nonlinear effects are captured only to a certain extent. Thirdly, the a_{ij}^* coefficients are treated as constant in time, which is not a good approximation for large-scale and long-term disruptive events. Lastly, the system is modelled at a high level of abstraction where each TDF is modelled as a single entity whose operability depends on the availability of the services provided by the other TDFs.

Despite these limitations, the proposed approach can provide insight to national resilience aspects not easily gained otherwise. This is particularly the case for severe threats to national security that target vulnerabilities across different sectors of the society. It is therefore recommended to build a database of interdependency matrices for the civilian TDFs and the military force structure elements that constitute the total defence system. This database should be applicable for a broad range of scenarios that are used for security and defence planning. In order to achieve this, interdependency mapping should be undertaken for different geographical regions in the country. Further, it is recommended to take into account different outage periods for the TDFs, e.g. less than one day, one to three days, or seven days or more. Lastly, the database needs to take into account that the interdependencies likely will change for armed conflict scenarios compared to the peacetime situation.

5.0 ACKNOWLEDGEMENTS

This work was funded by the Norwegian Ministry of Defence through project grant 1619.

6.0 REFERENCES

[1] NATO, "Strategic Concept," 2022. [Online]. Available: http://www.nato.int/strategic-concept/.

[2] Norwegian Ministry of Defence and Norwegian Ministry of Justice and Public Security, "Support and Cooperation. A description of the total defence in Norway," 2018. [Online]. Available: https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf.

[3] NATO, "Resilience and Article 3," 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_132722.htm.

[4] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control System Magazine, vol. 21, pp. 11-25, 2001.

[5] E. J. Oughton, W. Usher, P. Tyler, and J. W. Hall, "Infrastructure as a Complex Adaptive System," Complexity, vol. 2018, p. 3427826, 2018.

[6] S. E. Chang, "Infrastructure resilience to disasters," The Bridge, vol. 39, pp. 36-41, 2009.

[7] D. Helbing, "Globally networked risks and how to respond," Nature, vol. 497, no. 7447, pp. 51-59, 2013.

[8] S. R. Sellevåg, "Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies," Security and Defence Quarterly, 2022, doi: 10.35467/sdq/146789.

[9] Y. Y. Haimes, B. M. Horowitz, J. H. Lambert, J. R. Santos, C. Lian, and K. G. Crowther, “Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology,” Journal of Infrastructure Systems, vol. 11, pp. 67-79, 2005.

[10] Y. Y. Haimes and P. Jiang, “Leontief-based model of risk in complex interconnected infrastructures,” Journal of Infrastructure Systems, vol. 7, pp. 1-12, 2001.

[11] C. Lian and Y. Y. Haimes, “Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input–output model,” Systems Engineering, vol. 9, no. 3, pp. 241-258, 2006.

[12] J. R. Santos and Y. Y. Haimes, “Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures,” Risk Analysis, vol. 24, pp. 1437-1451, 2004.

[13] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” Reliability Engineering and System Safety, vol. 121, pp. 43-60, 2014.

[14] S. Kelly, “Estimating economic loss from cascading infrastructure failure: a perspective on modelling interdependency,” Infrastructure Complexity, vol. 2, no. 1, p. 7, 2015.

[15] J. Oosterhaven, “On the limited usability of the inoperability IO model,” Economic Systems Research, vol. 29, no. 3, pp. 452-461, 2017.

[16] R. Setola, S. De Porcellinis, and M. Sforna, “Critical infrastructure dependency assessment using the input-output inoperability model,” International Journal of Critical Infrastructure Protection, vol. 2, pp. 170-178, 2009.

[17] S. R. Sellevåg, “Civil Support to Armed Forces – A Functional Approach for Modelling Total Defence Systems [in Norwegian],” Forsvarets forskningsinstitutt. FFI-report 22/01207, 2022.

[18] R. Zimmerman, “Social Implications of Infrastructure Network Interactions,” Journal of Urban Technology, vol. 8, no. 3, pp. 97-119, 2001.

[19] T. Aven et al., “Society for Risk Analysis Glossary,” Society for Risk Analysis, 2018. [Online]. Available: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf.

[20] M. Bruneau et al., “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities,” Earthquake Spectra, vol. 19, no. 4, pp. 733-752, 2003.

[21] D. F. Vatne, P. K. Køber, M. S. Guttelvik, B. Arnfinnsson, and Ø. R. Rise, “Norwegian long-term defence analysis - a scenario- and capability-based approach,” Forsvarets forskningsinstitutt. FFI-report 20/02367, 2020.