Regulation and Security Modelling of Essential Services in Network of Information Systems

Christophe Ponsard[1] and Robert Darimont[2]

[1] CETIC Research Center, Charleroi, Belgium christophe.ponsard@cetic.be
[2] Respect-IT, Louvain-la-Neuve, Belgium robert.darimont@respect-it.be

Abstract. In a globally connected world, cybersecurity has become a key issue for the citizen, companies but also operators of essential services such as energy, transportation, drinking water or health. The NIS European Directive requires countries to identify such operators to ensure that adequate cybesecurity measures are in place, that impacting problems are promptly notified and that an European cooperation is in place. Our work shows the benefit of a global modelling approach using i* to deploy the directive from understanding the cooperation and duties of all actors/roles through a regulation model, down to its implementation in a specific domain to support a cybersecurity risk analysis process. Our work is illustrated on the drinking water essential domain.

Keywords: Regulation modelling, cybersecurity, critical systems, case study

1 Introduction

Our world is increasingly dependent on information processing networks and systems. Their global interconnection makes them more vulnerable to cyber attack growing at a fast pace. In addition to protecting the citizens and companies, it is crucial to the secure critical infrastructures of our society and economy. The purpose of the Network of Information System directive (NIS) is precisely to provide a global framework at the European level to secure such infrastructures through a coordinated approach across member states (MS) [6].

The main Operator of Essential Services (OES) are energy production, various forms of transport (rail, sea, air, etc.), production and distribution of drinking water and hospitals. It is important to ensure that such operators have firm cybersecurity commitments in order to prevent and react to any attempt to attack their networks and systems. As OESs depend on Digital Service Providers (DSPs), e.g. for hosting data or services, those must also be adequately secured. In addition, the emergence of industry 4.0 is increasing risks due to the mix of information technologies (IT) and operation technologies (OT), e.g. through exposing industrial SCADA control systems with few intrinsic protection.

The NIS directive has defined a clear set of objectives:

1. monitoring of critical sectors by identifying OESs and making sure they have protective and notification measures against cybersecurity attacks.

2. creation of a regulatory framework strengthening the cybersecurity of DSPs.
3. development of national cybersecurity capacities, through one or more Computer Security Incident Response Team (CISRT, aka CERT).
4. cross-border cooperation between EU countries.

Unlike the General Data Protection Regulation (GDPR), the NIS is not a European regulation but a directive transposed at the national level in each of the MS. This process requires to set up a complex network of actors at different levels: EU level for cooperation between MS, setup of national contact points and CSIRT and, last but not least, the organisation of each OES domain.

The aim of this paper is to show the benefits of a modelling approach able to cope with organisational and prescriptive concepts in the NIS deployment. Different goal modelling approaches developed in the Requirements Engineering (RE) field can be considered, e.g. i* [17], KAOS [11] or more specialised regulation-oriented variants such as Nomos3 [9] or LegalGRL [7]. We focus here on i* [3] but also discuss other frameworks. Our modelling covers the organisation level and captures cybersecurity risks in the considered domain with a contribution to extending i* for that purpose. Our target audience is the people involved in NIS alignment: regulators, auditors, and implementors inside OESs/DSPs, in cooperation with cybersecurity experts who can validate/refine the models.

This paper is structured as follows. First, Section 2 provides a global NIS model through Strategic Dependencies across involved actors and their Strategic Rationales to understand their motivations to engage and collaborate. Then, Section 3 details a risk-oriented approach to address specific OES threats using the water domain as case. Section 4 discusses the resulting model in the light of related work before concluding and identifying future work in Section 5.

2 Global Modelling of the NIS Regulation

Modelling regulatory texts is the first step in a broader process to ensure compliance. Other logical steps are verification, analysis and enforcement. The resulting model has a number of benefits over legal texts: it enables a better understanding through graphical notations which are easier to navigate and decode than long and very formal legal documents in text format. In the NIS case, it is very important to make sure all actors understand their role, responsibilities and interactions with other actors, especially given the large scope covering many countries and domains.

In order to provide a global vision of the NIS, Figure 1 depicts the Strategic Dependency (SD) graph gathering all agents (EU, CSIRT Network, ENISA,...) and roles (MS, OES,...). It reflects the hierarchical structure from EU level to national level and then sector specific management for OESs/DSPs through the use of "participates in" links. Various types of OESs are modelled through "IsA" links. Complementary actors with specific roles are also associated through dependencies: the national cybersecurity agency is taking responsibility for the cybersecurity management at national level and OESs depend for being granted compliance. CSIRTs depend on OESs for notification and can provide support in return. They can themselves call for assistance from the ENISA and take part in the CSIRT EU network together with the CERT-EU. This diagram immediately reveals that the directive relies on a delegation of specific goals and tasks from the EU level to MS and finally to OESs/DSPs. This global interaction structure is far less easy to catch when reading of the 30 pages legal text.

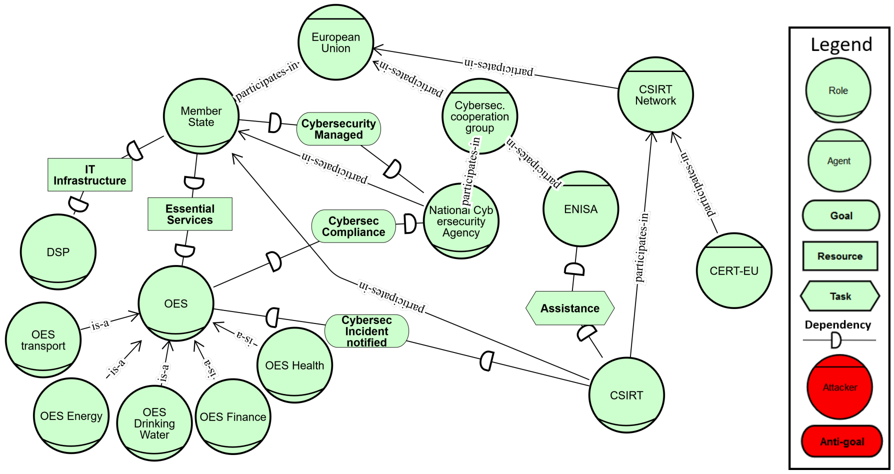

Fig. 1. Strategic Dependency diagram for the NIS directive

.

Figure 2 depicts the Strategic Rational (SR) view of the NIS. The goals of the European Union state the four core goals put forward in our introduction. The model highlights that the NIS relies on a progressive operationalization strategy: each MS must translate the directive in its national law. It can rely on its National Cybersecurity Agency to make sure that OESs and DSPs are respecting this transposition and on CSIRTs for specific tasks.

OESs follow a cybersecurity management process [10]. DSPs follow a similar approach but for more specific IT risks so we focus only on OESs here. The goal refinement inside an OES is structured according the steps proposed by the NIST reference framework: identify-protect-detect-respond-recover [13]. A deeper analysis is domain specific and detailed in the next section. Note that high-level goals and dependencies could be related to well-identified sections of the NIS text and could be traced in the model through dependency links. Those pointers to the text give the full "legal semantics" of what is expressed semi-formally in the SR diagram. The model is thus also a good navigable table of contents to find its way in the 30 page long NIS regulation document.

3 Domain-Level Analysis - Drinking Water Utility Case

To illustrate the instantiation in a concrete domain, we use a drinking water utility for its lesser complexity and maturity than other fields such as transport or energy. It requires a substantial infrastructure from water supply, treatment,

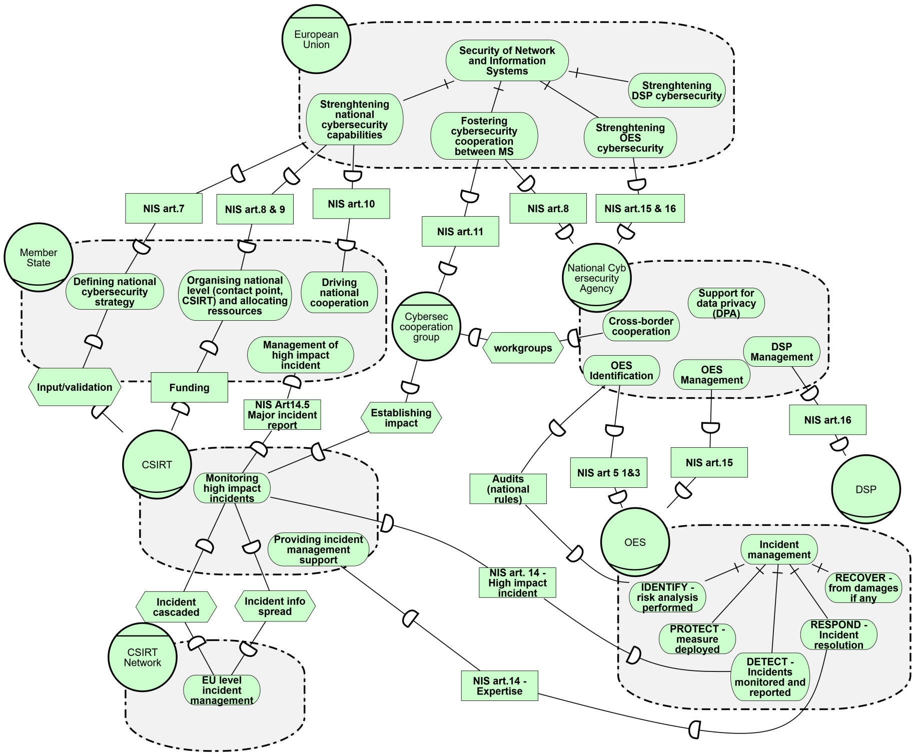
European Union
Security of Network and Information Systems
Strenghtening DSP cybersecurity
Strenghtening national cybersecurity capabilities
Fostering cybersecurity cooperation between MS
Strenghtening OES cybersecurity
NIS art.7
NIS art.8 & 9
NIS art.10
NIS art.11
NIS art.8
NIS art.15 & 16
Member State
Defining national cybersecurity strategy
Organising national level (contact point, CSIRT) and allocating ressources
Driving national cooperation
Management of high impact incident
Input/validation
Funding
NIS Art14.5 Major incident report
Cybersec cooperation group
workgroups
Establishing impact
National Cyb ersecurity Agency
Support for data privacy (DPA)
Cross-border cooperation
DSP Management
OES Identification
OES Management
NIS art.16
DSP
CSIRT
Monitoring high impact incidents
Providing incident management support
Audits (national rules)
NIS art 5 1&3
NIS art.15
OES
Incident management
RECOVER - from damages if any
IDENTIFY - risk analysis performed
PROTECT - measure deployed
DETECT - Incidents monitored and reported
RESPOND - Incident resolution
NIS art. 14 - High impact incident
Incident cascaded
Incident info spread
CSIRT Network
EU level incident management
NIS art.14 - Expertise

Fig. 2. Strategic Rationale diagram for the NIS directive

.

storage to finally reach consumers through a distribution network. The global chain is controlled by two OESs: the supplier and the distributor. The SR diagram in Figure 3 details how each actor is achieving its goals with milestones.

i* can be used in this part to perform the security risk assessment using some extensions depicted in Figure 3: an attacker agent is introduced with its motivations captured as (anti-)goals. An attack link is expressed using dependencies linking anti-goals to concrete actionable goals inside the attacked actor to break its goals. For reflecting the negative thinking, all attack concepts are coloured in red. This extension could be achieved through a minor relaxation of i* 2.0 rules inside the piStar tool used in this paper [14]. E.g. the attacker might deliberately want to hurt people through altering the treatment, which triggers a safety threat. It can be blocked by the QA process but the attacker might also take control over it to fake QA results either to mask its attack or to generate false alarms.

We cross-checked the risks inferred in our model with known attacks on water infrastructures [8] and referenced them in Figure 3. In 2000, a million litres of water was intentionally sent down a drain in the Maroochy attack. In 2006, an attack in Pennsylvania could have affected disinfectant concentration. In 2016, an insider attack caused metering alterations and incorrect billing.

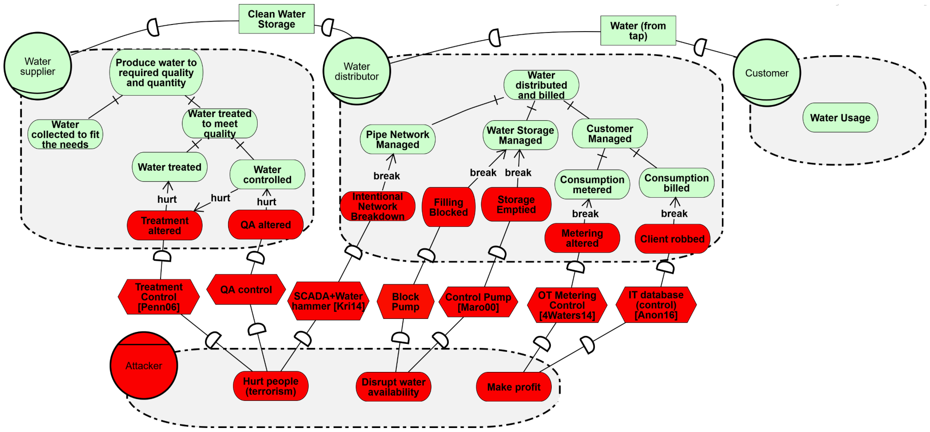

Fig. 3. Goal and attack modelling of the water domain

4 Discussion and Related Work

Regulation modelling is an active research field in RE. A systematic review highlights the importance of goal-oriented methods [1]. KAOS has also been used for regulation modelling [4]. A main difference is that KAOS focuses on the goal structure and identifies responsible agents at the leaf level. It has a weaker support to show all agent responsibilities and interactions across agents. In the scope of the NIS, i* SD and SR diagrams enable a better understanding. Actually, this work is close to the i* vulnerability-centric requirements engineering framework [5] which provides a richer security taxonomy making explicit the vulnerability concept and the exploit relationship. However, it tends to focus on operational tasks while our analysis is more concerned about (anti-)goals. A general i* framework for risk analysis also provides useful mechanisms for reasoning about risks and likelihood, although in the context of software development [2].

Considering the security risk analysis, others frameworks can be used, either generic RE (e.g. KAOS) or more specialised languages (e.g. attack trees [16]). KAOS has a more explicit notion of obstacles used as anti-goals in the security domain [12] and which partly inspired our modelling. However, i* is better at gathering and reasoning about the attackers' motivations and capabilities. Attack trees support a wider set of operators which can be used to further detail and quantify the model produced here [15].

On the practical side, our model is very complementary to the long legal text through the use of pointers from the model to specific NIS articles. The tagging process revealed quite easy and text coverage was used to check for completeness or missing aspects to be discussed with domain actors.

5 Conclusion and Perspectives

In this paper, we demonstrated how i* can be used for modelling the NIS directive and to support a domain specific risk analysis. The comparison with other frameworks such as KAOS revealed interesting benefits. As future work, we would like to validate various modelling approaches with OESs during the next NIS workshops planned in Belgium. We will also deepen our analysis of other essential domains and experiment with tooling to better support the integration of models and legal documents (e.g. through URL support). We also plan to align our approach with other security and risk-oriented i* extensions [2, 5] and to investigate the translation process of a legal text to an i* model.

Acknowledgement. This work was partly funded by the SAMOBI project of the Walloon Region (nr. 1910032).

References

1. Akhigbe, O., Amyot, D., Richards, G.: A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. REJ (04 2018)
2. Costal, D., et al.: Aligning business goals and risks in oss adoption. In: Conceptual Modeling. pp. 35–49 (2015)
3. Dalpiaz, F., Franch, X., Horkoff, J.: istar 2.0 language guide. CoRR **abs/1605.07767** (2016), http://arxiv.org/abs/1605.07767
4. Darimont, R., Lemoine, M.: Goal-oriented analysis of regulations. In: Workshop on Regulations Modelling and their V&V (ReMo2V), Luxemburg, June 5-9 (2006)
5. Elahi, G., Yu, E., Zannone, N.: A vulnerability-centric requirements engineering framework: Analyzing security attacks, countermeasures, and requirements based on vulnerabilities. Requir. Eng. **15**(1), 41–62 (Mar 2010)
6. EU: Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the union. http://data.europa.eu/eli/dir/2016/1148/oj (2016)
7. Ghanavati, S., Amyot, D., Rifaut, A.: Legal Goal-Oriented Requirement Language for Modeling Regulations. In: MiSE'14 (2014)
8. Hassanzadeh, A., et al.: A review of cybersecurity incidents in the water sector. Journal of Environmental Engineering **146**(5) (May 2020)
9. Ingolfo, S., Siena, A., Mylopoulos, J.: Nomos 3: Reasoning about regulatory compliance of requirements. In: IEEE 22nd Int. Req. Eng. Conference (2014)
10. ISO: ISO/IEC 27000 Family - Information Security Management Systems. https://www.iso.org/isoiec-27001-information-security.html (2013)
11. van Lamsweerde, A.: Requirements Engineering - From System Goals to UML Models to Software Specifications. Wiley (2009)
12. van Lamsweerde, A., et al.: From system goals to intruder anti-goals: Attack generation and resolution for security requirements engineering. In: RHAS (2003)
13. NIST: Cybersecurity Framework. https://www.nist.gov/cyberframework (2014)
14. Pimentel, J.: pistar tool for i* 2.0. https://www.cin.ufpe.br/ jhcp/pistar (2018)
15. Ponsard, C., Darimont, R.: Towards Quantitative Trade-Off Analysis in Goal Models with Multiple Obstacles Using Constraint Programming. In: 15th Int. Conf. on Software Technologies, ICSOFT, July 7-9 (2020)
16. Schneier, B.: Attack trees **24**(12) (1999)
17. Yu, E., Mylopoulos, J.: Enterprise modelling for business redesign: The i* framework. SIGGROUP Bull. **18**(1) (Apr 1997)